Methods to assess and manage security in interconnected electrical power systems

Author(s):
Mäkelä, Olli

Publication Date:
2013

Permanent Link:
https://doi.org/10.3929/ethz-a-010087017

Rights / License:
In Copyright - Non-Commercial Use Permitted
Methods to Assess and Manage Security in Interconnected Electrical Power Systems

A dissertation submitted to

ETH ZURICH

for the degree of

Doctor of Sciences

presented by

OLLI MÄKELÄ
M. Sc. Helsinki University of Technology, Finland
born on the 18th of June 1983
citizen of Finland

accepted on the recommendation of
Prof. Dr. Göran Andersson, examiner
Prof. Dr. Liisa Haarla, co-examiner

2013
Preface

This dissertation has been written during my PhD studies at the power systems laboratory of the ETH Zurich during the years 2009-2013. This thesis has been done as a part of the project ”Security of Multi-Area Power Systems” financed by swisselectric research.

I would like to thank Professor Göran Andersson for supervision of this work and Professor Liisa Haarla for acting as a co-examiner. I would also like to thank Dr. Marek Zima for giving helpful comments during the course of the project.

I would also like to acknowledge the Foundation of the Association of Electrical Engineers in Finland, Emil Aaltonen Foundation, Walter Ahlström Foundation and KAUTE Foundation for financial support I have received during the project.

Finally, I would like to thank my colleagues, friends and family for support.
Contents

List of Acronyms ............................................. xiii

1 Introduction .............................................. 1
  1.1 Background and Motivation .......................... 1
  1.2 Interconnected Power Systems ................. 4
  1.3 Recent Blackouts ................................. 4
    1.3.1 USA and Canada 2003 .................. 5
    1.3.2 Sweden and Denmark in 2003 ....... 6
    1.3.3 Italy in 2003 ........................... 6
    1.3.4 European System Disturbance in 2006 .... 6
    1.3.5 India 2012 ................................ 7
  1.4 Security, Reliability and Risk ............... 7
  1.5 Simulation Methods ............................. 7
    1.5.1 DC Power Flow Approximation .......... 7
    1.5.2 Probabilistic Power Flow ............ 8
    1.5.3 Distributed Slack Bus .................. 8
  1.6 Contributions .................................. 9
  1.7 Outline of Dissertation ...................... 10
  1.8 List of Publications .......................... 11

2 Data Exchange and Coordination ...................... 13
  2.1 Introduction .................................. 13
    2.1.1 On European Practices .................. 13
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.2 Literature Review</td>
<td>15</td>
</tr>
<tr>
<td>2.1.3 Contribution of Author</td>
<td>15</td>
</tr>
<tr>
<td>2.2 Response of Neighboring Control Areas</td>
<td>16</td>
</tr>
<tr>
<td>2.3 Fluctuating In-Feed in Interconnected Power Systems</td>
<td>17</td>
</tr>
<tr>
<td>2.3.1 Uni-, Bi- and Multilateral Compensation</td>
<td>18</td>
</tr>
<tr>
<td>2.4 Results</td>
<td>18</td>
</tr>
<tr>
<td>2.4.1 Results on Response of Neighboring Control Areas</td>
<td>18</td>
</tr>
<tr>
<td>2.4.2 Results on Compensation</td>
<td>21</td>
</tr>
<tr>
<td>2.5 Conclusions</td>
<td>26</td>
</tr>
<tr>
<td>3 Security Assessment</td>
<td>31</td>
</tr>
<tr>
<td>3.1 Introduction</td>
<td>31</td>
</tr>
<tr>
<td>3.1.1 Background</td>
<td>31</td>
</tr>
<tr>
<td>3.1.2 Literature Review</td>
<td>32</td>
</tr>
<tr>
<td>3.1.3 Contribution of Author</td>
<td>33</td>
</tr>
<tr>
<td>3.2 Execution of Security Assessment</td>
<td>34</td>
</tr>
<tr>
<td>3.2.1 Contingency List</td>
<td>34</td>
</tr>
<tr>
<td>3.2.2 Coordination in Interconnected Power Systems</td>
<td>35</td>
</tr>
<tr>
<td>3.2.3 Computational Complexity of Security Assessment</td>
<td>36</td>
</tr>
<tr>
<td>3.2.4 System Security State Classification</td>
<td>40</td>
</tr>
<tr>
<td>3.3 Risk-Based Security Assessment</td>
<td>41</td>
</tr>
<tr>
<td>3.3.1 Introduction</td>
<td>41</td>
</tr>
<tr>
<td>3.3.2 Risk</td>
<td>42</td>
</tr>
<tr>
<td>3.3.3 Probability of Contingency</td>
<td>42</td>
</tr>
<tr>
<td>3.3.4 Severity of Contingency</td>
<td>45</td>
</tr>
<tr>
<td>3.4 Model of Cascading Failure</td>
<td>47</td>
</tr>
<tr>
<td>3.4.1 Introduction</td>
<td>47</td>
</tr>
<tr>
<td>3.4.2 Data and Parameters</td>
<td>47</td>
</tr>
<tr>
<td>3.4.3 Wind Power Modeling</td>
<td>49</td>
</tr>
<tr>
<td>3.4.4 Power Flow and Tripping of Lines</td>
<td>50</td>
</tr>
<tr>
<td>3.4.5 Generation Adjustment and Load Shedding</td>
<td>50</td>
</tr>
</tbody>
</table>
5.3 Robust Re-Dispatch of Generators
5.3.1 Introduction
5.3.2 Problem
5.3.3 Linear Program Formulation
5.3.4 Security Margins
5.3.5 Prices
5.4 Security and Reliability
5.5 Optimal Reliability Level
5.6 Results
5.6.1 Robust Re-Dispatch of Generators
5.6.2 Optimal Reliability Level
5.7 Conclusions
6 Conclusions
7 Future Research
A Test Systems
A.1 6-Bus Test System
A.2 IEEE RTS-96 Test System
A.2.1 Three Area System without Wind
A.2.2 Three Area System with Wind
A.2.3 Single Area System
A.2.4 Two Area System
Bibliography
Curriculum Vitae
Abstract

The operating environment of power systems has changed in a fast pace during the last years and this change can be expected to continue in the future. Mainly this change can be explained by two major trends. First, the liberalization of the power market in Europe has led to a situation where the power flow pattern in the system changes from one hour to another. Second, an increasing share of electricity is produced using sources of electrical power that have a fluctuating nature. Examples of such production types are wind power and photovoltaic (PV).

The transmission system operators (TSOs) are responsible for secure and reliable operation of their own network that is a part of an interconnected power system. The two above mentioned trends set new challenges for TSOs from the security and reliability point of view. In this dissertation, methods are presented that help the TSOs to face the challenges better in interconnected systems.

This dissertation contributes to the assessment and management of security in interconnected power systems by proposing additional data exchange among TSOs to account for fluctuations of in-feed in the assessment. Moreover, this dissertation contributes to the classification of power system security states by proposing a method that is particularly useful in systems with fluctuating in-feed. The dissertation contributes to analysis and handling of contingencies by considering the probability and severity of events in the systems. Also, this dissertation presents results on execution of the security assessment in interconnected power systems and this issue has been studied from the computational complexity point of view. Additionally, the dissertation proposes a method to handle uncertain power flows of lines in the system by robust re-dispatching of generators. Also, a method to estimate the optimal level of security and reliability needed in the robust re-dispatch method has been presented.
The methods have been illustrated with simulations using the IEEE RTS-96 test system.
Kurzfassung

## List of Acronyms

**ACER**  Agency for the Cooperation of Energy Regulators  
**CA**  control area  
**CGM**  common grid model  
**DACF**  day-ahead congestion forecast  
**EC**  European Commission  
**EENS**  expected energy not supplied  
**ENTSO-E**  European Network of Transmission System Operators for Electricity  
**HVDC**  high voltage direct current  
**LP**  linear program  
**m.u.**  monetary unit  
**OPF**  optimal power flow  
**PTDF**  power transmission distribution factor  
**PV**  photovoltaic  
**RSCI**  regional security coordination initiative  
**SSC**  Security Service Centre  
**TSC**  Transmission System Operator Security Cooperation  
**TSO**  transmission system operator  
**VOLL**  value of lost load
Chapter 1

Introduction

In this chapter, a description of the operating environment of power systems is given that motivates the topic of this dissertation. Moreover, relevant terms are defined and methods are reviewed. Finally, the contributions and structure of the dissertation are presented.

1.1 Background and Motivation

A power system is an essential piece of infrastructure in the current world. People and companies utilize electricity for many purposes and it would be difficult to imagine life without electricity. Therefore, a high level of security and reliability of system operation are important.

TSOs are responsible for security and reliability of their operated control area (CA) in the system. For many decades, power systems have operated successfully and with a high level of reliability. However, recently TSOs have faced new challenges: First, fluctuating in-feed from renewable energy sources has increased substantially in the European power system [1]. Second, the market liberalization introduced in Europe has led to an increase of cross-border exchanges between countries [1].

Germany may be a good example of the progress in terms of increase of fluctuating in-feed from renewable energy sources. The total installed
Chapter 1. Introduction

Hydro: 15%
Wind: 45%
Solar: 36%
Other: 5%

Figure 1.1: Renewable energy capacity by sources in Germany in 2011. Source of data: [2].

capacity of wind and solar power is about 1/3 of the total net generation capacity [1]. The capacity of wind and solar generation is very high compared with other renewable energy sources, Fig. 1.1. In terms of energy, the share of wind and solar generation of the whole renewable energy generation is smaller than the capacity Fig. 1.2. These numbers mean that if the weather is favorable for wind or solar production, the produced amount may be substantial. However, if the sun does not shine and wind does not blow, the production of renewable energy sources is low. This dependency on the weather conditions creates a source of uncertainty that should be taken into account in planning and operation of power systems. Due to the market liberalization, the historical values of power flows may not indicate the future power flows in the system. For example, in Fig. 1.3 export of electricity from German to Switzerland is presented for the years 2010, 2011 and 2012. The values of export have been measured every month on the 3rd Wednesday of the month at 11.00 a.m. As we may see, the amount of export varies con-
1.1. Background and Motivation

Hydro: 19%
Wind: 42%
Solar: 17%
Other: 22%

Figure 1.2: Renewable energy production by sources in Germany in 2011. Source of data: [2].

Figure 1.3: Trading of electricity from Germany to Switzerland on the 3rd Wednesday of the month at 11.00 a.m. Source of data: [3]

siderably from one year to another. To overcome the challenges related to fluctuating in-feed and market liberalization, TSOs need new tools, methods and practices that are applicable in interconnected power systems. Today, TSOs operate and control power systems independently
with no or limited coordination and data exchange among other TSOs. Coordination among TSOs may be a solution for the issue of interconnected power systems.

1.2 Interconnected Power Systems

An interconnected power system is operated by many TSOs independently. A single TSO operates one CA. The operation of independent TSOs may be coordinated by exchanging data and communicating between parties. Recently, coordination initiatives of Coreso [4], Transmission System Operator Security Cooperation (TSC) [5] and Security Service Centre (SSC) [6] try to enhance coordination and communication among TSOs in order to overcome coordination challenges in interconnected power systems. Examples of interconnected power systems are European Network of Transmission System Operators for Electricity (ENTSO-E) Regional Groups Nordic and Continental Europe. In the USA, Western and Eastern Interconnections are examples of an interconnected power system.

In Fig. 1.4, the synchronous areas in Europe are presented. Totally, there are seven synchronous areas. In Continental Europe, one synchronous area covers many countries. For most of the countries, there is a single TSO that is responsible for operation of the grid within the country. Exceptions exist, for example, in Germany four TSOs operate the German grid. The countries are connected with each other using interconnections and electricity is traded between these countries. Therefore, the systems operated by many TSOs are called interconnected power systems. In the past, the interconnections were built to provide mutual support between control areas. Today, the interconnections are used also for trading of electricity.

1.3 Recent Blackouts

Most of the time, security of a power system is maintained and customers do not experience a shortage of electricity. However, during the past ten years, a few major blackouts have occurred in Europe, the USA, Canada and India, for example.
1.3. Recent Blackouts

1.3.1 USA and Canada 2003

The blackout in Eastern Interconnection happened on the 14th of August, 2003. In [8], it has been mentioned that this blackout left over 50 million people without electricity and 63 GW of load was shed. 63 GW represents 11 % of the total load of the Eastern Interconnection. The blackout affected eight U.S. states and two Canadian provinces. A final report on the blackout has been published by a U.S.-Canada power System Outage Task Force [9]. The final report makes 46 recommendations to prevent or minimize the scope of future blackouts. The recommendations cover a wide range of different issues ranging, for example, from institutional issues to clear definitions of system security states and responsibilities.

Figure 1.4: Synchronous areas in Europe. Source of figure: [7].
1.3.2 Sweden and Denmark in 2003

In addition to the blackout in the USA, a blackout took place in Sweden and Denmark as well in 2003. The blackout in Sweden and Denmark in 2003 has been reviewed in [10]. The authors in [10] point out that the reason was a combination of a loss of a 1200 MW unit and a double busbar fault. The situation was beyond the security criterion used. According to the authors of [10], the disturbance led to a loss of supply of 4500 MW in Sweden and 1850 MW in Denmark.

1.3.3 Italy in 2003

In 2003, a major blackout took place in Italy and in some regions of Switzerland [11], [12], [13]. In [13], one main reason identified for the blackout was the unplanned and deviating power flows of lines between France and Italy as well as between Switzerland and Italy. According to the authors, the disturbance started when the Lukmanier transmission line had a fault. This caused a redistribution of power flows in the system and resulted in an overloading of the San Bernardino line. The loading of the line was 110 %. The authors of [13] report also that at this time Italy imported electricity and could not decrease consumption until the San Bernardino line had a ground fault 24 minutes after the fault of the Lukmanier transmission line. The report [13] describes how a series of failures happened after the fault of the San Bernardino transmission line and resulted in a blackout in Italy.

1.3.4 European System Disturbance in 2006

Few years later, a system disturbance occurred in Europe [14], [15]. The disturbance started from the Northern Germany and split the power system in Continental Europe into three islands and 15 million households faced an interruption of electricity supply [14]. The report [14] presents two main reasons that led to this incident: First, the N-1 criterion was not filled in the control area of E.ON Netz. Second, the coordination among TSOs of E.ON Netz and RWE was not sufficient after taking the double-circuit line Conneforde-Diele out of operation in the control area of E.ON Netz.
1.4. Security, Reliability and Risk

1.3.5 India 2012

India faced a blackout in 2012 and left 700 million people without power [16]. In [16] experts cited say the cause to be in the weak infrastructure. According to the experts cited, India must invest more in its power system infrastructure.

1.4 Security, Reliability and Risk

In the following, the definitions of reliability, security and risk are presented:

- **Reliability**: “Reliability of a power system refers to the probability of its satisfactory operation over the long run. It denotes the ability to supply adequate electric service on a nearly continuous basis, with few interruptions over an extended time period.” [17]

- **Security**: “Security of a power system refers to the degree of risk in its ability to survive imminent disturbances (contingencies) without interruption of customer service. It relates to robustness of the system to imminent disturbances and, hence, depends on the system operating condition as well as the contingent probability of disturbances.” [17]

- **Risk**: Risk is the expected value of undesired or harmful consequences of an event. That is, a measure of risk is a product of the probability and (negative) consequences of the event [18].

1.5 Simulation Methods

1.5.1 DC Power Flow Approximation

In the simulations, the DC approximation of power flows [19] has been used because the thermal limits of lines are the limiting factors in Continental Europe, see Section 1.6. The approximation assumes that voltage magnitudes are 1 p.u. at nodes, resistances are small and may be neglected and differences between angles of voltages are small [19]. By
using these assumptions, the power flows of lines $F$ may be solved from the net nodal injections for a given topology of the system:

$$F = \hat{X}T\tilde{B}^{-1}(G - L),$$

where $X$ is the reactance matrix with reactances of lines at the diagonal, $T$ is the adjacency matrix, $\tilde{B}$ is the nodal admittance matrix, $G$ and $L$ are vectors of generation and load at nodes.

### 1.5.2 Probabilistic Power Flow

In literature, the probabilistic power flow methods are used to model uncertainties of power flows due to fluctuations of loads and generation. Besides the probabilistic power flow, similar methods are known also as a stochastic power flow. Within this dissertation, the probabilistic power flow has been used as a tool to solve security related problems.

The method of [20] has been used to model the probability distributions of power flows of lines in this dissertation. The benefits of the method are that it is computationally efficient, applicable for linear models and allows to consider correlations of forecast errors. The expected power flows of lines are obtained from the DC power flow solution. By exploiting this probabilistic power flow method, the variances of probability distributions of power flows of lines may be computed using the following equation:

$$\Sigma = A\sigma A^T,$$

where $A$ is a matrix mapping the net nodal injections to power flows of lines, $\sigma$ is a covariance matrix of forecast errors where variances of forecast errors are at the diagonal and correlation may be considered in the non-diagonal elements and $\Sigma$ is a covariance matrix of power flows distributions of lines with variances of power flows of lines at the diagonal and covariances of power flows of lines in the non-diagonal elements.

### 1.5.3 Distributed Slack Bus

Due to fluctuations of loads or generation, the power balance is not necessary met anymore and the surplus or deficit has to be compensated in the rest of the system. The normal DC power flow model presented
in Section 1.5.1 assumes that the fluctuations are compensated at the slack bus. This does not present the real operation very well, because in reality the fluctuations are compensated at many nodes. In order to model this property, the distributed slack bus is used in the simulations. The distributed slack bus may be modeled using the power transmission distribution factors (PTDFs) [21]:

\[ P_{DF_{ln}} = \frac{\Delta F_l}{\Delta P_n}, \]  

where \( \Delta F_l \) is the change of the power flow of the line \( l \) due to an exchange of \( \Delta P_n \) between the node \( n \) and the reference bus or buses. For linear system models, the PTDF matrix is constant for all generation and load patterns. Thus, to compute the probabilistic load flow with the distributed slack bus, the matrix \( A \) in Eq. 1.2 is replaced with the PTDF matrix.

1.6 Contributions

This dissertation contributes to the secure operation of interconnected power systems. Especially, contributions to the following topics should be mentioned:

- **Data exchange.** It is shown that to consider the fluctuations of power flows in interconnected power systems, data exchange between TSOs should be organized. In order to properly consider fluctuating in-feed sources in the neighboring CAs, the variance and the mean of the power in-feed uncertainty should be exchanged. Also, if two or more sources correlate with each other, the correlation should be considered. If the fluctuating in-feed points with correlation are located in different CAs, the TSOs have to agree on the procedure to estimate the correlation. These issues have been discussed in Chapter 2.

- **System security states.** Due to fluctuating in-feed, it may not be possible to classify the system into a system security state uniquely. Therefore, an index to express the probability of different system security states is proposed in Chapter 4.
• **Contingency analysis and handling.** In Chapter 4, a contingency analysis and handling method to consider both the probability and severity of the contingency in power systems with fluctuating in-feed is proposed. Moreover, the computational complexity of the security assessment in an interconnected power system has been analyzed.

• **Power flows management.** Chapter 5 proposes a robust re-dispatch method that takes fluctuations of power flows into account and gives adjustments of generators to meet a given probability level without security limit violations. In addition, a method to decide an optimal security limit violation probability for the robust re-dispatch method is presented. The method to decide the optimal probability is based on a cost-benefit analysis and considers the monetary costs of re-dispatching and penalties paid due to customer interruptions.

In the dissertation, the DC approximation of power flows has been used. The methods developed are applicable for the synchronous area in Continental Europe because lines are relatively short and thermal security limits are the constraining factors [22]. Other systems, like the Nordic synchronous area, may need additional studies to complement the results of the methods proposed in this dissertation. This is because the lines are long and dynamic stability limits may put additional constraints on the operation of the system [22].

### 1.7 Outline of Dissertation

The dissertation has the following structure:

In Chapter 2, methods for data exchange and coordination in interconnected power systems are proposed. These topics are important to ensure security of interconnected power systems.

In Chapter 3, a security assessment method that considers the possible cascade triggered is presented. Moreover, an analysis on computational complexity of the security assessment in interconnected power systems is presented.
1.8. List of Publications

In Chapter 4, a security assessment method for systems with fluctuating in-feed is proposed. This is of growing important due to increasing fluctuating generation in power systems.

In Chapter 5, a robust re-dispatch method is presented. The method considers uncertainties of power flows due to fluctuating in-feed or loads and provides a re-dispatch of generators so that security limit violations can be avoided with a given probability. A method to estimate an optimal value for this probability using the cost/benefit analysis is proposed.

Conclusions are drawn in Chapter 6 and in Chapter 7 suggestions for future research are proposed.

1.8 List of Publications

During the course of this dissertation work, some pieces of results have already been presented in the following publications:


Chapter 2

Data Exchange and Coordination

Data exchange is an important means to coordinate operation of TSOs in interconnected power systems. In this chapter, existing literature has been reviewed. Also, a need to exchange data on network topology including information on fluctuating in-feed among TSOs is demonstrated.

2.1 Introduction

2.1.1 On European Practices

In interconnected power systems, data exchange and coordination among TSOs are needed in order to maintain the security of the whole interconnected power system. The main guidelines for data exchange and coordination in Europe are presented in the Operation Handbook of ENTSO-E [23], Network Code on Operational Security [24] and the supporting document of the network code on operational security [22].

Network codes are documents that regulate the operation of a TSO. The development process of a network code has been presented in [22] and in the following it has been reviewed. Briefly, the process starts in the European Commission (EC) that makes a request to the Agency for the Cooperation of Energy Regulators (ACER) for a draft of a framework
guideline. Then, ACER submits the framework to the EC. After this the EC asks ENTSO-E to make a network code with technical details. This process takes about 12 months. After ENTSO-E has finished with technical details, ACER assess the network code and makes a proposition to the EC whether the network code should be accepted or rejected. If the EC accepts the network code, the network code will be legally binding in the member countries.

ENTSO-E has published information regarding the data exchange and coordination in Supporting Paper for the Operational Security Network Code dated 14.12.2012 [22]. In this paper, ENTSO-E presents the common grid model (CGM) and gives guidelines for TSOs to perform coordinated security assessments. The CGM is done for different time frames and geographical regions [22]. This CGM allows a coordinated security analysis. The problems related to the confidentiality of data has been solved in the 3rd Energy Package by unbundling transmission from production and consumption [22]. Therefore, the confidentiality issues should not limit data exchange among TSOs [22].

On the implementation side, European industry has launched regional security coordination initiatives (RSCI) to improve coordination among TSOs. The initiatives Coreso [4], SSC [6] and TSC [5] have so far been launched.

These security initiatives have two components; security assessment and remedial actions. The security assessment does not cause direct costs to the TSOs. However, the remedial actions may cause costs and this raises an issue on cost sharing among participants. In Europe, some countries have made an agreement [25]. Cost sharing is not a topic of this thesis and later in the thesis it has been assumed that there is a scheme for cost sharing among participants.

Coreso and TSC have a centralized security assessment. Coreso is based on a centralized approach where the remedial actions are proposed by Coreso. Each TSO is responsible for implementation of these proposals. In the TSC initiative, a decentralized approach is used for remedial actions and remedial actions are planned multilaterally among member TSOs. A TSO may be a member of several RSCI and guidelines for this have been presented in [22].
2.1. Introduction

2.1.2 Literature Review

In research literature, few publications are available on data exchange and security assessment in interconnected power systems. They mainly consider de-centralized policies and concentrate on necessary data exchange.

In [26], the authors present a security assessment method for interconnected power systems that needs exchange of tie-line power flow information and equivalent models of CAs among TSOs. The method has two steps: In the first step, a TSO performs a security assessment for the own control area by modeling the neighboring CAs using equivalent models. The change in the tie-line flow is observed after every contingency and this tie-line information is communicated to other TSOs in order to give them an opportunity to assess the effect of these tie-line power flow deviations on their own CA. The needed information to be published by a TSO are the equivalent model of their own CA and change of tie-line flows after contingencies.

Another approach widely documented in literature uses decomposition methods [27] and the coordination of CAs is achieved by exchanging information associated with the decomposition method used. Applications to power system and optimal power flow (OPF) have been presented in [28], [29] and [30]. The methods formulate the OPF problem so that each CA is an own subproblem and coordination between subproblems ensures that the problem converges to the solution that would be obtained by solving the original OPF as one problem. In these formulations, the needed data exchange between TSOs is the data needed for coordination of the optimization problem. The decomposition methods may be used to solve the power flows in interconnected power systems [31] and, therefore, these methods may be used to do a security assessment also.

2.1.3 Contribution of Author

In this chapter, the author has done two main contributions. First, it is shown that TSOs should exchange data regarding their own area in order to make the right decisions in operational planning and real-time. Without knowing the situation around the own CA it is difficult to make appropriate decisions. Decisions based on information not taking into account the rest of the interconnected system may lead to a
situation where the system security is at stake or unnecessary remedial actions are executed and money is lost. Second, improvements to data exchange regarding forecast errors or fluctuations of wind or PV in-feed are proposed. This additional data exchange is important in order to account for the uncertainty of power flows of lines.

2.2 Response of Neighboring Control Areas

An important issue in security assessment is the modeling of the system beyond the own responsibility area. The reason is the response given by the system outside of own borders of a TSO and the effect on own power flows and actions. This problem may arise both in operational planning and real-time.

Generation schedules are changing every hour due to the market clearing. If the data is not exchanged for every hour, the response of the neighboring area may not be known or it may be estimated misleadingly by using historical values. Moreover, the intra-day data set contains updated information. However, if changes are done after the exchange of the intra-day data set, the security assessment done by TSOs may again give misleading information.

To model the neighboring CA, one possibility is to use the so called X-node method [23]. In this method, the tie-lines are cut from the middle of the tie-line and virtual busses are added to the ends of the tie-lines cut in order to model the exporting or importing power flows. The exporting tie-line is modeled using a load at the virtual bus and the importing tie-line is modeled using a generation unit at the virtual bus. The values of units are obtained from the power flows in the N situation. The method has been illustrated in Fig. 2.1.

In the operational planning, the power flows of tie-lines have to be estimated based on trades of electricity, for example. In real time, if measurements are available from the tie-lines, the values are obtained from these measurements. The values of the X-node model assume that the tie-line power flows are constant after disturbances within CAs.
2.3 Fluctuating In-Feed in Interconnected Power Systems

Fluctuating in-feed, for example from wind or PV, is substantial in many countries today. In interconnected power systems, fluctuations within one CA may cause changes in power flows of lines in another CAs. In order to study the needed information exchange, the propagation of fluctuations in the interconnected power systems has to be studied.

The forecast errors have an additive nature: If an additional source of uncertainty is added to the system, the distributions of power flows of lines become wider, or the variance increases. This has two main consequences: First, misleading results regarding the probability of a line overloading may be obtained if all sources of uncertainty are not considered properly. Second, if a certain confidence level of re-dispatch of generators with uncertain power flows of lines is required, the higher costs occur as will be explained in Chapter 5.

The fluctuations of wind or PV in-feed have to be compensated in the rest of the system in order to keep the power balance in the system. By using the DC power flow model, the fluctuations are inherently compensated at the slack bus. By using the PTDFs, a distributed slack bus

![Diagram of the X-node method](image)
can be modeled and the compensation of fluctuations is done at many locations by using a pre-defined rule.

2.3.1 Uni-, Bi- and Multilateral Compensation

Unilateral compensation refers to a case where fluctuations of fluctuating in-feed are compensated within the own CA. The bilateral compensation means that the fluctuations of in-feed are compensated jointly with another TSOs. If three or more parties are participated in compensation, it is called the multilateral compensation. In bi- and multilateral cases, the compensation is done over borders of CAs. In these cases, the allocation of cross-border capacity is important. Bi- or multilateral compensation cannot be done when no capacity is available, i.e. it is already used by the markets. Therefore, the capacity between CAs has to be either reserved for compensation, or we may use the leftover capacity that is not used by the market.

2.4 Results

2.4.1 Results on Response of Neighboring Control Areas

A 6-bus test system has been used to illustrate the response of the surrounding system and its importance to security assessment and remedial action planning. The system is illustrated in Fig. 2.2 where lines are indicated by a number without frames and the busses are numbered using numbers with frames. The system has two CAs. After splitting the tie-lines, the values for the equivalent units at virtual busses are obtained from the steady-state power flow solution. In the simulations, all line faults have been considered as credible contingencies. However the lines to the virtual busses are not considered as credible contingencies as they would split the system into two islands. A per-unit corresponds to 100 MW. The detailed parameters of the test system are given in Appendix A. In the analysis of the system, the DC approximation of power flows has been used.

The simulation results are presented in Fig. 2.3 and Fig. 2.4 for the CAs A and B, respectively. The red bar depicts the thermal limit of the
2.4. Results

Figure 2.2: 6-bus test system used in simulations. The system has two CAs.

line, the green bar is the estimate of the respective TSO of the power flow of the line and the blue bar is the power flow of the respective line if all available information is considered by the TSO. In these figures, the highest power flow of a line over all possible N-1 situations is shown. Monitoring of this value is meaningful because it is used in the standard N-1 security assessment to make a verdict whether the system is secure or insecure. The results are twofold: First, misleading results regarding the security of the system may be achieved. Second, the TSO A obtains also misleading information regarding power flows within his own area that exceed the thermal limit of the line.

The first issue may be seen from the results of the CA B. Based on the estimate of the power flow of the line 6 in the second CA, the power flow of this line is smaller than the line limit. However, the real power flow that considers the real response of the surrounding system is higher than the line limit, Fig. 2.4. Therefore, the TSO of the second area does not see this overloading. Both TSOs obtain a result that their systems are N-1 secure, but the whole system is not N-1 secure.

The second issue is visible because the estimated power flow of the line 1 of the CA 1 is much higher than the line limit. However, when the response of the surrounding system is considered, the power flow of the line is much lower and no line limit violation is observed. These results show that the TSO may execute remedial actions that would not be
necessary and, therefore, unnecessary costs may be due.

The results obtained show that the TSO may have two-folded drawbacks if the response of the surrounding power system is not modeled properly. First, TSOs may obtain misleading information regarding the security of the whole system. Second, unnecessary remedial actions may be executed and, thus, costs occur if the remedial actions executed have an associated cost. To avoid these situations, data exchange should be performed among TSOs. At day-ahead, the model for the surrounding system is available from the day-ahead congestion forecast (DACF) data set in Europe [23]. If the schedules are changing every hour, the data set should be available for every hour. In intra-day, the changes made in the settings of controllable devices or in network topology and generation should be communicated to other TSOs in order to update the model of the surrounding system.

Figure 2.3: Maximum power flows of lines compared with the line limit in the N-1 situation in the CA A. Values for the full model and for a model with limited information are presented.
2.4. Results

Figure 2.4: Maximum power flows of lines compared with the line limit in the N-1 situation in the CA B. Values for the full model and for a model with limited information are presented.

2.4.2 Results on Compensation

The situation with unilateral compensation has been illustrated using simulations with two areas of the IEEE RTS96 test system, see Appendix A.

The results are obtained using the nominal loading level, i.e. the given values in the test system. The nominal loading level corresponds also to the loading level of 100 %. If the loads and generation of the system are increased by 20 %, the loading level of the system is 120 %.

The variance of the forecast error of the wind has been assumed to be 20 % of the forecasted value. The wind generation locates at nodes 101, 102, 107, 201, 202 and 207. The forecast errors at nodes 101, 102 and 107 correlate with each other and forecast errors at nodes 201, 202 and 207 correlate with each other. The correlation is 80 %. The fluctuations
Table 2.1: Simulated situations and the amount of wind in-feed resources within CAs. The total generation of the system is 5700 MW.

<table>
<thead>
<tr>
<th>Wind In-Feed</th>
<th>CA A</th>
<th>CA B</th>
<th>Total wind in-feed</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 % wind</td>
<td>225 MW</td>
<td>225 MW</td>
<td>450 MW</td>
</tr>
<tr>
<td>24 % wind</td>
<td>684 MW</td>
<td>684 MW</td>
<td>1368 MW</td>
</tr>
<tr>
<td>24 % wind and export</td>
<td>1254 MW</td>
<td>114 MW</td>
<td>1368 MW</td>
</tr>
</tbody>
</table>

have been compensated using other generators within the own CA.

Three different scenarios have been studied. In the first case, the wind in-feed corresponds to about 8 % of the whole generation and the wind generation is located equally in the CAs A and B. In the second case, the share of in-feed has been increased to correspond 24 % of total generation. In the third case studied, wind generation corresponds again to 24 % of total generation of the system. However, about 9 %, or 114 MW, is located in the CA B and about 91 %, or 1254 MW, of wind generation in the CA A. The total generation of the system is 5700 MW including wind in-feed in all three cases. The details are summarized in Table 2.1.

### Wind In-Feed 8 % of Generation

The first case considers that 8 % of generation is originated from fluctuating sources. In this case, the total forecasted wind in-feed is 450 MW totally by considering generation of both CAs. The total generation of the system is 5700 MW including wind generation. The fluctuations of in-feed are compensated equally with all generators within own CA. Therefore, the net export/import does not change due to fluctuations and settings of frequency control do not have to be modified. The three tie-lines between the CAs are included in the results and the corresponding line numbers are 12, 24 and 41.

The results for a scenario with 8 % of generation from wind in-feed are presented in Fig. 2.5 and in Fig. 2.6 for CAs A and B, respectively. The results show that the uncertainty of lines is mainly due to generation within the own CA. A small effect of fluctuations of wind in-feed of the CA B on the lines of the CA A may be seen for the lines 11 and 12 that are connected between the nodes 107-108 and 107-203. This shows
2.4. Results

Figure 2.5: Variance of power flow distributions of lines within the CA A with 8% of generation from wind in-feed. Blue line: Uncertainty from own generation; Green line: Total uncertainty; Red line: Uncertainty originating from the neighboring CA.

that wind generation within the CA B generates uncertainty regarding power flows of these two lines that are located within the CA A.

Wind In-Feed 24% of Generation

The second case considers that 24% of generation is from wind in-feed. Thus, the total forecasted wind in-feed is 1368 MW while the total generation of the system is 5700 MW like in the previous case.

The results obtained have similarities with the first case, see Fig. 2.7 and Fig. 2.8, but have also differences compared with the first case. The results show that the uncertainty of the power flows of lines within CAs are mainly due to wind fluctuations within their own CAs. The difference compared with the first case is that the magnitude of the variance is much higher. For example, line 11 has a variance of 0.07 in the
first case but in the second case the variance is about 0.24. Reasons for this difference could be the increased wind in-feed and the assumption that the variance of the forecast error is 20% of the expected in-feed.

**Wind In-Feed 24 % of Generation and Export or Import**

The third case considers a situation where 24 % of total generation is from wind in-feed and the CA A has a surplus of 570 MW whereas the CA B has a deficit of this size. The results are shown in Fig. 2.9 and in Fig. 2.10.

Due to high wind generation within the CA A, the variances of power flow distributions of lines within the CA A are high and the respective values within the CA B are small. The results show also that uncertainty
Figure 2.7: Variance of power flow distributions of lines within the CA A with 24% of generation from wind in-feed. Blue line: Uncertainty from own generation; Green line: Total uncertainty; Red line: Uncertainty originating from the neighboring CA.

of the lines within the CA A is mainly due to wind production in the CA A. In the CA B, the uncertainty of power flows of lines is caused by wind in-feed of both CAs.

Comparison of Uni- and Bilateral Compensation

The results regarding the difference between uni- and bilateral compensation of fluctuations are presented in Fig. 2.11 and Fig. 2.12. The figures show that there are deviations in the value of the variance of the power flow distribution of the lines. Therefore, if two CAs do compensation of fluctuations bilaterally, the power flow distributions of lines change compared to the unilateral policy. Thus, not only the sources of uncertainty of surrounding CAs affect power flow distributions of lines, but also the policy used. One justification to have bi- or multilateral
Figure 2.8: Variance of power flow distributions of lines within the CA B with 24% of generation from wind in-feed. Blue line: Uncertainty from own generation; Green line: Total uncertainty; Red line: Uncertainty originating from the neighboring CA.

compensation of fluctuations would be economic benefits that may be obtained by increasing the size of the market.

2.5 Conclusions

The conclusions of this chapter are twofold: First, the results show that availability of data and network models for every hour is important in order to plan remedial actions and to perform the security assessment properly. Without available data, the security assessment may give misleading results regarding the security of the system and need for remedial actions. Therefore, an increasing data exchange would increase system security and it could be operated economically more efficiently than without coordination. Secondly, this chapter proposes that
Figure 2.9: Variance of power flow distributions of lines within the CA A with 24% of generation from wind in-feed and a surplus of 570 MW within the CA A. Blue line: Uncertainty from own generation; Green line: Total uncertainty; Red line: Uncertainty originating from the neighboring CA.

The TSOs should exchange data regarding the forecast error of in-feed among each other in order to identify the power flow distributions of lines. The results obtained show that without considering the forecast error of the neighboring CAs, the parameters of power flow distributions of lines may be misleading and, therefore, these results may complicate the decision making process of TSOs.
Figure 2.10: Variance of power flow distributions of lines within the CA B with 24 % of generation from wind in-feed and a surplus of 570 MW within the CA A. Blue line: Uncertainty from own generation; Green line: Total uncertainty; Red line: Uncertainty originating from the neighboring CA.
Figure 2.11: Variance of power flow distributions of lines within the CA
A. Comparison of uni- and bilateral compensation.

Figure 2.12: Variance of power flow distributions of lines within the CA
B. Comparison of uni- and bilateral compensation.
Chapter 3

Security Assessment

This chapter reviews literature on security assessment. Computational complexity of the security assessment is analyzed and a cascade model used to estimate the severity of the contingency is presented.

3.1 Introduction

3.1.1 Background

One of the main aims of TSOs is to ensure operational security of the power system. This leads to a high level of reliability and customers do not face interruptions in electricity supply. To assess the state of the power system in terms of security, the TSOs perform a security assessment. During the assessment, the response of the system to disturbances is studied.

Often, the own CA of a TSO is called the responsibility area. The system beyond the own CA is called the observability area. This naming convention is used in Europe [23]. In an interconnected system, the security assessment is done by every TSO independently. Contingencies of the observability area outside the responsibility area are considered if the influence on the responsibility area is over a certain threshold [23].

The main purpose of the security assessment is to identify the state of the system and be a basis for decisions regarding remedial actions and whether these remedial actions should be planned and executed or not.
3.1.2 Literature Review

A good overview of the security assessment procedure in power systems has been presented by Morison et al. [32] wherein the authors go through components associated with security assessment. Often, in the security assessment the so called N-1 method is used. The N-1 method states that a system should be robust against single component contingencies that are considered credible. In literature, publications that propose improvements to this method are available. In the following, a few of these improvements are presented.

The N-1 method considers only single contingencies. Sometimes, it may be necessary to consider also many simultaneous failures of components. In these cases, the computational complexity increases fast. Therefore, in [33] the authors have identified high risk N-k contingencies for online security assessment that are added to the list of credible contingencies.

The thermal ratings are a function of many factors. In [34], the authors have presented a probabilistic method to estimate the thermal capacity of a line. The authors argue that the thermal ratings may be increased by considering the risk related to an overload. In [35], the authors have presented a set of risk-based indices that help decision making in the control room. In [36], probabilistic security assessment for operational decision making has been presented.

The hidden failures are failures that a TSO has not identified. Often, these failures are due to malfunction of protection system. In [37], the importance of consideration of hidden failures in security analysis has been presented. The authors refer to a study reported to the North American Reliability Council (NERC). The study says that the protection system was playing a role in 73.5% of all major disturbances.

There are also publications that consider the cascade initiated by initial fault or faults. These approaches may have benefits because in [38] IEEE PES CAMS Task Force on Understanding, Prediction, Mitigation and Restoration of Cascading Failures found out that blackouts do not occur during peak hours as commonly has been thought. According to the task force, many blackouts take place in spring and fall. The members of the task force point out that the dynamics of the system is important. During spring and fall components of power systems are in maintenance and, therefore, the dynamics of the system is different compared with trained situations.
3.1. Introduction

In [39], the authors have presented a method to estimate the level of security based on cost/benefit analysis. They argue that costs related to an increased security margin are justified by reduction of lost load. The authors have estimated the expected outage cost by using Monte Carlo simulations. In [40], the authors have considered time-dependent phenomena and weather conditions in the estimation of the value of security.

In [41], Kirschen et al. have compared the deterministic N-1 security boundaries with a risk-based measure. The authors have used the expected outage costs to measure risk. They also emphasize the importance of modeling weather conditions because it changes the risk level considerably. The weather conditions they have modeled by adjusting the failure rate of overhead lines.

A probabilistic indicator of system stress has been published in [42]. The authors have used the expected energy not supplied (EENS) to measure the stress in the system. The authors have used Monte Carlo simulations to estimate the EENS.

The cascading process may also be modeled using high-level probabilistic models without modeling power system physics. Such models are presented in [43], [44] and [45]. A summary and review of different models have been done in [46].

3.1.3 Contribution of Author

In this chapter, the contribution of the author is the development of the cascade code. The author shows with the cascade code that by using the results computed of the post-contingency states of the power system, the extent of load shed may be difficult to estimate. With the studied system, no causal reason-consequence relation was found between any post-contingency values studied and load shed. The results of the author support ideas that the severity of a contingency should be measured using load shed or other customer related measure. The author has also presented results on computational complexity of the security assessment in an interconnected power system.
3.2 Execution of Security Assessment

3.2.1 Contingency List

One important element of the security assessment is the contingency list that contains a list of credible contingencies. This list is created by the TSO.

The list may be established by using the probability of the contingency [42]. All single contingencies that exceed a specific threshold are considered as credible contingencies. The contingency list, however, may include also some higher order contingencies in addition to single faults as stated by the authors in [42]. According to the authors, a loss of any double circuit line is considered as a credible contingency in the United Kingdom.

If the probability of a contingency is used as a criterion to create the list, the probabilities of contingencies should be estimated. The estimation of a probability of a contingency may be difficult because disturbances are rare in power systems and amount of data is not available for accurate estimation. Therefore, the estimates obtained using historical data may be biased. In the literature, there are different ways to define the probability of a contingency. They are discussed in Section 3.3.3.

In establishing the contingency list, the severity of contingencies should also be considered. This is a reason why sometimes a loss of a double line, single busbar or common mode failures are listed as credible contingencies [23].

The process to create a list of contingencies may be even more difficult at the present environment where power flow patterns of lines vary from one hour to another and fluctuating in-feed is connected to the grid. This leads to a situation where the severity of a contingency depends on the market situation in the system. Also weather conditions play a big role because the amount of subsidized in-feed of wind and PV depends on wind and solar radiation conditions.

From the computational point of view, the security assessment is possible to be done parallel by dividing the list of contingencies for available computing units and by combining the results after simulations. If the system is very large and a high order of security is tested, the computational burden may increase too much and the security assessment
cannot be done within the given time limits even though multiple computers are utilized. In Section 3.2.3, computational issues related to the execution of the security assessment are discussed in single and interconnected power systems.

### 3.2.2 Coordination in Interconnected Power Systems

Contingency analysis and handling needs special attention in interconnected power systems because many TSOs are involved in the security assessment. Only with proper coordination among TSOs, it may be ensured that the whole interconnected power system is secure against all credible contingencies of the whole system.

A goal of the contingency analysis and handling has been summarized in [23] with the sentence ”No cascading with impact outside my border”. Moreover, the TSOs should consider the relevant contingencies in the observability area and check whether these cause security limit violations in their responsibility areas [23].

However, in order to identify all possible disturbance propagation scenarios, three ways how disturbances may propagate from one CA to another must be considered. The following three execution rules ensure that all propagation scenarios due to credible contingencies, i.e. a fault of a single component or simultaneous fault of multiple components, are considered in the security assessment:

1. Run contingency analysis by considering all credible contingencies in the whole system. Monitor the response of the whole system to the contingency.

2. Run contingency analysis by considering only credible contingencies of the own responsibility area. Monitor the response of the whole system to the contingency.

3. Run contingency analysis by considering all credible contingencies of the whole system and monitor the response on the own responsibility area.

All these three rules listed above lead to a situation where the propagation of a disturbance from one CA to another can be identified and remedial actions, if needed, may be planned.
If the contingency analysis is run only considering contingencies of the responsibility area and only the responsibility area is monitored, security of the whole system may be not be guaranteed. Thus, in interconnected power systems collaboration among TSOs is needed in order to guarantee the security of the whole system.

### 3.2.3 Computational Complexity of Security Assessment

#### Introduction

The computational complexity of the security assessment may be computed using the Big O\(^1\) analysis. The Big O analysis is presented in [47], for example. The Big O analysis of the security assessment algorithm describes how the computation time increases with the size of the power system, or the input of the algorithm, increases.

In the following sections, three different security assessment algorithms are presented and they are analyzed from the computational complexity point of view. One algorithm has a centralized approach where one entity is responsible for the whole system. Two algorithms have a decentralized approach where multiple TSOs are responsible for security.

#### Assumptions

In the following analysis of computational complexity of the security assessment, it has been assumed that the matrix multiplication \( C = AB \) is performed as follows\(^2\):

\[
C(i, j) = \sum_{k=1}^{p} A(i, k)B(k, j), \tag{3.1}
\]

where the size of \( A \) is \( m \times p \) and the size of \( B \) is \( p \times n \). The size of \( C \) is \( m \times n \).

If the matrix multiplication is done this way, the computational complexity of the matrix multiplication does not depend on zero elements. This means that specific connections between nodes of the system do

---

\(^{1}\)Known also as "Big Oh" as used in [47].

\(^{2}\)Matlab version R2011a does the matrix multiplication using this method.
not affect the computational complexity of the matrix multiplication. In the security assessment, matrix multiplication is used to solve the power flows in the system.

In the analysis, only real power flows are considered in the system. Moreover, the DC power flow approximation has been used. As credible contingencies, we have considered line faults. It has been assumed that thermal limits of lines are the security limits restricting the operation of the system.

**Centralized Security Assessment**

The centralized security assessment considering single line faults may be done using Algorithm 3.2.3. In the algorithm, $l$ is the total number of lines of the system.

**Algorithm 1** Centralized security assessment algorithm.

```plaintext
1: for $i = 1$ to $l$ do
2:  modification of matrices to represent the new topology in the post-contingency state
3:  inversion of the admittance and reactance matrices
4:  compute power flows of lines in the post-contingency state
5:  compare security limits of lines and computed power flows of lines
6:  end for
```

The computational complexity of the tasks inside the for-loop may be calculated individually and then the results may be summed up. In the following computations, it has been assumed that the ratio between lines and buses stays the same as the size of the power system increases, or $l = kn$ where $k$ is a constant.

The modification of matrices to represent the new topology in the post-fault state can be done in a constant time and, thus, the complexity is $O(1)$. This means that the modification of the matrices does not depend on the size of the matrices, or the power system.

The complexity of a matrix inversion is $O(n^3)$ using the Gaussian elimination, if the size of the matrix is $n \times n$. Thus, the complexity of the inversion of the admittance matrix $B_{[n \times n]}$ is $O(n^3)$. Here, the size of the matrix is presented in brackets. The same complexity $O(n^3)$ is valid also for the inversion of the reactance matrix $X_{[l \times l]}$. 
The complexity of the computation of power flows is a result of matrix multiplications. The complexity of a matrix multiplication is $O(nmp)$ if the size of the first matrix is $n \times m$ and the size of the second matrix is $m \times p$ [47]. The power flows of lines may be computed using the following equation assuming the DC power flow approximation:

$$F_{[l \times 1]} = X_{[l \times l]}^{-1} T_{[l \times n]} B_{[n \times n]}^{-1} P_{[n \times 1]},$$

(3.2)

The complexity of the comparison of power flows of lines with the thermal limits of lines is $O(n)$. The total computational complexity of the tasks inside the for-loop is thus $O(1) + O(n^3) + O(n^3) + O(n) = O(n^3)$. The for-loop increases the complexity by $n$. Therefore, the total complexity of the security assessment using this algorithm is $O(n^4)$.

**Decentralized Security Assessment**

The security assessment may be done also decentralized when there is no single entity that performs the security assessment for the whole power system, but many entities perform the analysis.

In the decentralized security assessment, there are two possibilities to run the security assessment to ensure the security of the whole system: First, the TSO may consider faults within own responsibility area and monitor consequences in the observability area. This is called Algorithm 1. Second, the TSO may study consequences of faults in the observability area to the responsibility area and this is called Algorithm 2.

**Decentralized Algorithm 1**

The first case tests possible contingencies within the responsibility area and monitors the observability area. The procedure is presented in Algorithm 3.2.3. In the algorithm, $l_0$ is the number of lines within the responsibility area.

Using the complexities computed in the previous section, the total complexity of this algorithm is $O(1) + O(n^3) + O(n^3) + O(n) = O(n^3)$. The for-loop does not increase the computational complexity as the size of the power system increases because the number of lines within the responsibility area $l_0$ does not increase.
3.2. Execution of Security Assessment

Algorithm 2: Decentralized security assessment: Algorithm 1.

1: for \( i = 1 \) to \( l_0 \) do
2: modification of matrices to represent the new topology
3: inversion of the admittance and reactance matrices
4: compute power flows of lines in the post-contingency state
5: compare security limits of lines and computed power flows of lines
6: end for

Decentralized Algorithm 2

The second case tests faults within the responsibility and observability area. The procedure is presented in Algorithm 3.2.3.


1: for \( i = 1 \) to \( l \) do
2: modification of matrices to represent the new topology
3: inversion of the admittance and reactance matrices
4: compute power flows of lines in the post-contingency state
5: compare security limits of lines and computed power flows of lines
6: end for

For this algorithm, the computational complexities of the tasks within the for-loop are \( O(1) + O(n^3) + O(n^3) + O(n) = O(n^3) \). Because the for-loop increases the total complexity by \( l \), the total computational complexity is \( O(n^4) \).

Comparison of Algorithms

The analysis done states that the centralized approach has a computational complexity of \( O(n^4) \). The decentralized algorithm 2 has also the same computational complexity \( O(n^4) \). The decentralized algorithm 1 has a computational complexity of \( O(n^3) \). The difference is mainly due to the fact that the number of for-loop runs increases as the system increases. It is also possible to do the adjustment to matrices without inversion of the matrices in \( O(n) \). Because the matrices in network problems are often sparse, sparse methods may be used to make the multiplication of matrices faster. However, in these both cases the decentralized algorithm 1 has still the lowest computational complexity.
3.2.4 System Security State Classification

The TSOs make the decisions on remedial actions based on the results obtained from the security assessment. To illustrate the system security state of the power system and to help decision making, the power system is classified to one of the system security states. The states are normal, alert, emergency and automatic actions. They are defined as follows [23]:

- **Normal state:** No security limit violations are present in the N³ or N-1 situation.
- **Alert state:** No security limit violations are present in the N situation, but security limit violations are present at least in one of N-1 situations.
- **Emergency state:** Security limit violations are present in the N and N-1 situations, but remedial actions are possible.
- **Automatic actions state:** Security limit violations are present in the N and N-1 situations and no manual remedial actions are possible.

The system security states are illustrated in Fig. 3.1. The states form different sets where the normal state has the tightest constraints. Alert and emergency states have looser constraints than the normal state. If the constraints of these three states are exceeded, the system is said to be in the automatic actions state. Mathematically, the system states may be depicted using sets:

\[ S_{\text{normal}} \subseteq S_{\text{alert}} \subseteq S_{\text{emergency}} \subseteq S_{\text{automatic actions}} \]  

where \( S_{\text{normal}} \), \( S_{\text{alert}} \), \( S_{\text{emergency}} \) and \( S_{\text{automatic actions}} \) are the sets corresponding to the system security states.

The decision making is based on the classification of the system state. Often, the TSOs plan and execute remedial actions if the system is not in the normal state.

In [48], a probabilistic technique has been developed for a generation system. With the method proposed by the authors, the generation

\[ \text{The N situation is a situation in a system where all components planned are in operation and no unplanned outages are present.} \]
3.3. Risk-Based Security Assessment

3.3.1 Introduction

In the past, the contingency list has worked well and system security has been able to maintain. However, two drawbacks may be identified: First, the probabilities of contingencies of the contingency list are not specified. All credible contingencies are considered to be equally probable if they exceed a certain given threshold. Second, the severity of the event is not considered. Some contingencies may have just a small effect on the system but certain contingencies may lead to cascades. In the worst case, load has to be shed or a blackout takes place. The aim of the risk-based security assessment is to consider both the probability and severity of the contingency.

Figure 3.1: Graphical representation of system security states.

The system may be classified into the healthy, marginal and at risk states. Moreover, the authors propose a risk index that is the probability of residing in an undesirable operating state.
3.3.2 Risk

The risk is an expected value of negative consequences. In this dissertation, the amount of load shed has been used as a measure to consider negative consequences. This is in line with the definition of security presented in Section 1.4 and highlights the aim to avoid interruptions of customer service. The risk is thus defined as a product of the probability and load shed of the contingency:

\[ R = \mathbb{E}(LS) = \sum_c p_c LS_c, \]  

(3.4)

where \( R \) is the total risk of the system, \( \mathbb{E}(LS) \) is the expected load shed, \( p_c \) is the probability and \( LS_c \) is the load shed after the contingency \( c \).

The definition of risk, Eq. 3.4, may get values from 0 to the value of the total load of the system. The definition shows also that probability and severity of contingencies may compensate each other partly. If the probability of a contingency is high but it is not severe, the risk associated with the contingency may be moderate or small depending on values of probabilities and severities. On the other hand, severe and unlikely contingencies may have the same risk as some other contingencies. Therefore, the contingencies form iso-curves where the risk of contingencies is the same, but severity or probability may be different.

The definition of risk, Eq. 3.4, means also that the risk may be zero if no load is shed even though the system is not N-1 secure and overloading of lines is present in the post-contingency state. But, the risk-based security assessment takes into account, for example, situations where an overloading of a line with low capacity is present but a trip of this line does not lead to further thermal limit violations.

In the following sections, methods to decide the probability and severity of a contingency are presented.

3.3.3 Probability of Contingency

In the following, five different methods to estimate the probability of a contingency are presented. Two of the methods require data. The estimation of the probabilities based on the frequency or Bayesian definitions needs historical data to get the estimates. Three other methods
have been presented that do not need data to estimate the probabilities. These three methods help to overcome the problem related to small amount of disturbance data in power systems due to small fault rates.

Often, fault statistics for power systems are given by stating the number of faults per kilometer and year. Thus, there is an underlying assumption that the longer lines are more exposed to faults than short lines. This idea has been used in the fourth method where it has been assumed that the probability of a fault on a specific line is proportional to its length.

**Frequency Definition**

If data are available, the probability of a contingency \( c \), \( p_c \), may be estimated by using the frequency definition \([49]\):

\[
p_c = \lim_{N \to \infty} \frac{N_c}{N},
\]

where \( N \) is the total number of disturbances and \( N_c \) is the number of disturbances associated with the contingency \( c \). The estimate approaches the probability \( p_c \) as \( N \) approaches infinity.

The drawback of this method is that it needs a large number of samples in order to give an estimate that is close to the probability of the contingency \( p_c \). With a small sample size, the probability estimates may be significantly biased.

**Bayesian Probability**

Another possibility to estimate the probability is to use the Bayesian probability \([50]\):

\[
p(C_c|E) = \frac{p(E|C_c)p(C_c)}{p(E)},
\]

where \( p(C_c|E) \) is the probability of a contingency when evidence \( E \) has been considered. In the context of power systems, evidence is fault data collected. \( p(C_c) \) is the initial estimate for the probability of the contingency and \( p(E|C_c) \) is the probability of evidence that the contingency
$C_c$ has happened. The probability of evidence $p(E)$ has been defined as follows:

$$p(E) = \sum_c p(E|C_c)p(C_c). \quad (3.7)$$

The advantage of the Bayesian approach compared with the frequency definition is that it may give better estimates for the probability $p(C|E)$ if the initial guess $p(C)$ is near the right probability. Therefore, a large amount of data may not be necessary needed.

**Equally Distributed Probabilities**

In power systems, the fault rates are normally small and, therefore, no large amount of data is available. In [49], a solution for this problem has been presented by assuming all contingencies equally likely. Then the probability of every contingency is $p_c = 1/N_{\text{lines}}$, where $N_{\text{lines}}$ is the total number of lines.

This comes from the fact that the sum of probabilities of all credible contingencies is one. Therefore, if all contingencies have the same probability and the number of contingencies increases, the probability of a single contingency decreases.

**Probability Based on Length of Lines**

In [51], a method to decide the frequency of faults is estimated using the length of lines:

$$\lambda_l = \frac{L_l}{L_{\text{tot}}} \lambda_{\text{tot}}, \quad (3.8)$$

where the fault rate of the line $l$ is $\lambda_l$, $\lambda_{\text{tot}}$ is the total number of faults during the time interval under study, $L_{\text{tot}}$ is the length of the system during the time interval under study and $L_l$ is the length of the line $l$.

If we substitute $\lambda_l = p_l N_f$ and $\lambda_{\text{tot}} = N_f$ in Eq. 3.8, the probability of the fault of the line $l$ is

$$p_l = \frac{L_l}{L_{\text{s}}}, \quad (3.9)$$

where $p_l$ is the probability of a fault of the line $l$, $L_{\text{s}}$ is the total length of the system and $N_f$ is the total number of faults.
3.3. Risk-Based Security Assessment

Educated Guess and Human Expertise

Often in power systems, disturbances occur rarely and no large amount of data are available. One possibility is to use human expertise and make an educated guess on the probabilities of disturbances. The accuracy of estimates depends on the experts.

Time-Variance of Probabilities

The weather conditions do have an impact on the fault rate and bad weather conditions increase the fault rate of the power system [40]. However, the weather conditions may also have an effect on the probability distribution of faults and cause that the probabilities of faults are time-variant. This means that the probability of a contingency changes due to bad weather. This is the case if the bad weather does not affect the whole system but only certain geographical areas of the system. If the weather conditions are modeled so that the probability distribution over contingencies changes, the probabilities are time-variant.

If bad weather conditions are modeled by increasing the fault rate of the system, the probabilities are time-invariant. Therefore, the bad weather does not affect the security assessment. However, an increasing fault rate will decrease the reliability of the system if the faults leads to customer interruptions, see Section 5.4.

3.3.4 Severity of Contingency

The severity of a contingency may be measured in many different ways. Based on the existing literature, two main methods have been identified; Seversities based on the N and N-1 situations and consumer side measures.

Severity Measures Based on N and N-1 Situations

Traditionally, the state of the power system is classified in a system security state to help decision making. For this classification the values are monitored in the N and N-1 situations and the state of the system is determined based on these values.
The values are measured in the N situation and in the N-1 situations after the disturbance. The possible values may be measured using either relative or absolute values. The metric may be, for example, the highest overloading of the line, average loading of lines or mean loading of lines. Also, more complicated measures may be used, for example, an average loading of the 20 most loaded lines.

We have found that there exist difficulties to measure the severity in N and N-1 situations using relative and absolute values. If the severity is measured using absolute values, small overloading of lines with high capacity may have even a smaller severity than an overloading of a line with small capacity, if the lines are designed to withstand a certain percentage of fluctuations in the power that goes through the line. However, if the protection system is set to switch-off a line after an overloading, a line with a high capacity is more severe than a line with a small capacity because parallel lines to the switched line are loaded more.

The same problem arises if relative loading of lines is used. Lines with small capacities and high relative overloading might not have so severe consequences as a small overloading of a high capacity line because the parallel lines may stand the fault of a small capacity line better than a fault of a high capacity line. Moreover, the severity should consider how the power flows of lines change after the protection system has switched off the overloaded line(s). Results illustrating these issues will be presented in Section 3.5.4.

**Consumer Side Severity Measures**

One purpose of the power system is to connect electricity producers with consumers and TSOs aim to operate the grid so that this can be achieved with a high level of reliability. Therefore, the customer side measures are important to consider. The customer side severity could be measured using the load shed or EENS. Other possible customer side measures are energy unserved, amount of power lost and number of customers affected [52].

In the literature, publications are available that consider consumer side severity measures. In [53], Ciapessoni et al. present a method to assess risk related to N-1 contingencies. They measure the risk by the expected load lost. They also present a method to measure the risk using the
post-contingency values. Finally, they present a method to find control action that minimize the shift of generators and risk together after the first step of the cascade.

In [41], Kirschen and co-workers have compared risk-based and deterministic security assessments. They point out that the deterministic security assessment gives a result that says whether there is an unacceptable risk or no risk at all. They found out that the deterministic criterion gives results that represent multiple risk levels. They also emphasize the importance of considering weather conditions. With a bad weather, for example during thunderstorms or high winds, the fault rates of overhead lines are higher than with a nice weather. The effect of weather on the fault rates they have considered by adjusting the average failure rate for transmission lines.

### 3.4 Model of Cascading Failure

#### 3.4.1 Introduction

To measure the severity of contingencies using consumer side measures, the progress of a cascade and the forthcoming load shed should be studied. The load shed measured in MW may be used as a consumer side measure for severity. A flowchart of the cascade algorithm is presented in Fig. 3.2. The cascade has been modeled using the DC power flow approximation. In the following, the steps of the cascade algorithm are explained.

#### 3.4.2 Data and Parameters

In order to perform the cascade simulation, the following data is needed: Generation at nodes, available capacity of generators, loads at nodes, thermal limits of lines, line admittances and topology of the network. To model the forecast errors of fluctuating in-feed sources, the variance of the forecast error has to be known and this issue is discussed more in Chapter 4.
Chapter 3. Security Assessment

Figure 3.2: Flow chart of the cascade algorithm.
3.4. Model of Cascading Failure

3.4.3 Wind Power Modeling

If wind power, or other fluctuating in-feed, scenarios are simulated, a random number is generated from the standard normal distribution using the \texttt{randn}-command of Matlab and then multiplied by the standard deviation of the distribution of the forecast error or fluctuations ($\sigma$). By considering the forecasted wind in-feed, $\mathbb{E}(G^w_g)$, the total generation at the in-feed node is

$$G^w_g = \mathbb{E}(G^w_g) + \sigma \delta,$$

where $\delta$ is a random number from a standard normal distribution $N(0,1)$.

This dissertation does not concentrate on the capacity allocation for reserves and, therefore, it has been assumed that there is enough capacity to compensate the fluctuations in the system. Thus, at the start of the model of cascading failure the power balance is present.

In the wind power simulations, the fluctuations are compensated at chosen nodes and the cascade is simulated many times. The average value of load shed is the characteristic value used as an estimate to describe the load shed, $\hat{LS}$:

$$\hat{LS} = \frac{\sum_s LS^w_s}{N_s},$$

where $LS^w_s$ is a load shed of the scenario $s$ and $N_s$ is the number of scenarios.

First, the possible existing islands of the system are identified. The list of the islands is obtained from the reactance matrix of the system by using the Depth-First-Search algorithm [54]. The nodes connected with each other are obtained by starting from one node and stacking all neighboring nodes in a stack. Then, a node is taken from the stack and all unvisited neighboring nodes are stacked. This is repeated until the stack is empty. By comparing the list of connected and visited nodes with the nodes of the system, it is possible to check whether all nodes of the system have been visited. If this is not the case, an unvisited node is selected as a new starting node and the Depth-First-Search algorithm is repeated. This way the islands of the system and the nodes of a specific island can be identified. After this task, the necessary matrices to model the power flows in the island are formed.
3.4.4 Power Flow and Tripping of Lines

The contingencies are simulated by tripping all lines sequentially one after another. The power flow is run in the system and the overloaded lines are tripped. After tripping of lines, the power flow is performed again. This is done until no overloaded lines exist in the system and the system has not split into two or more subsystems. If the system under study has split into island, the new islands will be added to the list of islands.

3.4.5 Generation Adjustment and Load Shedding

After the line tripping, the power balance of the system or islands is checked. The total sum of generation at nodes is calculated and compared with the total sum of loads at nodes. The power mismatch, $\Delta P$, is

$$\Delta P = \sum_n (G_n - L_n), \quad (3.12)$$

where $G_n$ and $L_n$ are generation and load of the node $n$.

If generation and load do not match in the system, the output of generators is adjusted in order to meet the mismatch in the power balance. The adjustment is done using the following formula, if capacity is available:

$$G_g = G_g^0 - \frac{G_g^{\text{max}} - G_g^0}{C_a} \Delta P, \quad (3.13)$$

where $G_g$ is the new output of the generator $g$, $G_g^0$ is the current output of the generator $g$, $G_g^{\text{max}}$ is the sum of current output and available capacity of the generator $g$, $C_a$ is the total available capacity of generators of the island and $\Delta P$ is the mismatch between generation and load in the system.

By using this formula, the generators that have a smaller available capacity than others, adjust the output less. The available capacity, $C_a$, is calculated using the following formula:

$$C_a = \sum_g (G_g^{\text{max}} - G_g^0). \quad (3.14)$$
3.4. Model of Cascading Failure

If no capacity is available, the following equation has been used to adjust generation:

\[ G_g = G_g^0 - \frac{G_{max}}{C_{tot}} \Delta P, \quad (3.15) \]

where \( C_{tot} \) is the total generation capacity of the island and it is calculated as follows:

\[ C_{tot} = \sum_g G_{max}^g. \quad (3.16) \]

If the output of a generator is negative after these adjustments, or \( G_g < 0 \) for any \( g \), the island has a blackout and all the load is lost because the frequency would increase too much. If the output of a generator is higher than the technical upper limit, load shedding is performed.

3.4.6 Load Shedding

A TSO triggers load shedding randomly. In this way, the TSO may obey the non-discriminatory policies. In our simulations, the expected load shed for every load unit is assumed to be equal in terms of MW. In this way, consumers with a high load do not obtain an advantage. All loads are decreased by the expected load shed. The load cannot be negative and, therefore, the value of the load is set to zero, if the value of the load is smaller than zero after decreasing the value by the expected load shed.

It has been assumed that all loads at nodes have the same expected value for load shed, or \( EV_1 = EV_2 = \ldots = EV_N \), where \( N \) is the number of nodes. The expected value \( EV_j = p_j L_j \), where \( p_j \) is the probability that we shed load at the load bus \( j \) and \( L_j \) is the load at this node. The probabilities needed to calculate the expected load shed are obtained from the following matrix equation:

\[
\begin{pmatrix}
  L_1 & -L_2 \\
  L_2 & -L_3 \\
    & \ddots & \ddots \\
  1 & \ldots & L_{N-1} & -L_N \\
\end{pmatrix}
\begin{pmatrix}
  p_1 \\
  p_2 \\
    \vdots \\
  p_N \\
\end{pmatrix}
= \begin{pmatrix}
  0 \\
  \vdots \\
  0 \\
  1 \\
\end{pmatrix}. \quad (3.17)
\]
After load shedding has been performed, the power imbalance is tried
to be set to zero by adjusting generation. If the power imbalance is zero
after the generation adjustment, the model of cascading failure is run
further. Otherwise, another round of load shedding is performed. The
total amount of the load shed is obtained by comparing the initial and
end situations of the system.

3.5 Results

3.5.1 Results on Computational Complexity

In this section, we present results on computational complexity of the
security assessment, security assessment and risk-based security assess-
ment. For the computational complexity study, we have created an
artificial large power system and studied how scalable the security as-
sessment algorithms are. Also, the computation time needed as the
system increases has been studied. The artificial system has been cre-
ated by considering matrices that have the same dimensions as a real
power system of that size. The simulations follow the algorithms given
in Section 3.2.3.

Centralized Security Assessment

The results for the large scale system are presented in Fig. 3.3. From the
figure it is visible that the computation time needed for the centralized
security assessment increases fast with respect to the size of the system.

Decentralized Security Assessment

We used the same artificial large power system to test the scalability
of the de-centralized security assessment algorithm. The results for de-
centralized security assessment algorithms are presented in Fig. 3.3.
These results match with the results of analysis of computational com-
plexity. The derived computational complexities of the centralized and
decentralized algorithm 2 are the same. They are also higher than
the computational complexity of the decentralized algorithm 1. This is
clearly visible in the figure and the advantage of the first decentralized
algorithm comes bigger when the size of the power system increases
compared to the the decentralized algorithm 2 and centralized algorithm.

![Graph showing computational time as a function of the size of the system](image)

**Figure 3.3:** Computation time needed as a function of the size of the system. As the system increases, the de-centralized algorithm 1 performs computationally better than the de-centralized algorithm 2 and the centralized algorithm. Also the computational complexities of algorithms are marked in the figure.

**Discussion**

In the analysis it has been assumed that the number of lines increases linearly as the number of busses increases. Based on the European model from [55] this is a good approximation, Fig. 3.4. The graph has been done using cumulative sum of lines and buses. Data used is presented in Table 3.1. The average value for $\frac{N_l}{N_b}$ is 1.29.

**3.5.2 Security Assessment**

A security assessment and a risk-based security assessment have been performed using the IEEE RTS-96 test system. In the security assess-
### Table 3.1: Number of busses and lines in Europe. Data from [55] and extracted by Troupakis [56].

<table>
<thead>
<tr>
<th>Country</th>
<th>Busses ($N_b$)</th>
<th>Lines ($N_l$)</th>
<th>Ratio ($\frac{N_l}{N_b}$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>317</td>
<td>518</td>
<td>1.63</td>
</tr>
<tr>
<td>Germany</td>
<td>228</td>
<td>312</td>
<td>1.37</td>
</tr>
<tr>
<td>Switzerland</td>
<td>47</td>
<td>76</td>
<td>1.62</td>
</tr>
<tr>
<td>Italy</td>
<td>138</td>
<td>203</td>
<td>1.47</td>
</tr>
<tr>
<td>Portugal</td>
<td>24</td>
<td>44</td>
<td>1.83</td>
</tr>
<tr>
<td>Spain</td>
<td>192</td>
<td>315</td>
<td>1.64</td>
</tr>
<tr>
<td>Austria</td>
<td>36</td>
<td>42</td>
<td>1.17</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>34</td>
<td>52</td>
<td>1.53</td>
</tr>
<tr>
<td>Denmark</td>
<td>8</td>
<td>8</td>
<td>1.00</td>
</tr>
<tr>
<td>Poland</td>
<td>96</td>
<td>137</td>
<td>1.43</td>
</tr>
<tr>
<td>Hungary</td>
<td>25</td>
<td>34</td>
<td>1.36</td>
</tr>
<tr>
<td>Slovakia</td>
<td>24</td>
<td>29</td>
<td>1.21</td>
</tr>
<tr>
<td>Croatia</td>
<td>16</td>
<td>18</td>
<td>1.13</td>
</tr>
<tr>
<td>Slovenia</td>
<td>8</td>
<td>8</td>
<td>1.00</td>
</tr>
<tr>
<td>Belgium</td>
<td>23</td>
<td>21</td>
<td>0.91</td>
</tr>
<tr>
<td>Netherlands</td>
<td>23</td>
<td>24</td>
<td>1.04</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>3</td>
<td>2</td>
<td>0.67</td>
</tr>
</tbody>
</table>
3.5. Results

Figure 3.4: Cumulative graph of the number of lines and busses in Europe based on the data in Table 3.1 starting from France and by considering countries in order of the table by ending to Luxembourg.

ment, line faults were considered as credible contingencies. The lines between the nodes 207-208 and 307-308 were not included because the nodes 207 and 307 are connected to the rest of the system only with a single line. The DC power flow approximation has been used and overloading of lines was considered. Three different loading levels were considered and results have been compared. Moreover, a comparison between relative and absolute overloaded lines has been done.

The results for the security assessment with the loading level of 100 % have been presented in Fig. 3.5. The results show that the system is N-1 secure at the nominal loading level and no line is overloaded in any N-1 situation. The results for the loading level 130 % are presented in Fig. 3.6. There are overloaded lines in some N-1 situations. Thus, the system is not N-1 secure. The results for the loading level of 150 % are presented in Fig. 3.7. Also in this case, overloaded lines are present in N-1 situations, as expected based on the result for the loading level of 130 %.
Figure 3.5: Maximum loadings of lines in the N-1 situation when all credible contingencies are considered and when the loading of the system is 100% of the nominal loading.

Figure 3.6: Maximum loadings of lines in the N-1 situation when all credible contingencies are considered and when the loading of the system is 130% of the nominal loading.

**Comparison of Relative and Absolute Values**

The challenge of evaluating the severity of an overloading of a line relates to relative and absolute values. The overloading of lines with the loading
3.5. Results

Figure 3.7: Maximum loadings of lines in the N-1 situation when all credible contingencies are considered and when the loading of the system is 150% of the nominal loading.

level of 150% has been presented in relative values in Fig. 3.8 and with absolute values in Fig. 3.9.

The results indicate that either using the relative or absolute values to measure the severity of the overloading, different results may be obtained. This may be seen by considering the lines 5 and 10, for example.

The relative severity results show that in the worst N-1 situation they both are overloaded about 16%. The N-1 situations do not have to be caused by the same contingency for both lines. The severity is close to the value obtained for the line number 102 where this line is overloaded about 20% in the worst N-1 situation.

The absolute valued results results show other results. If the severity of the overloading of lines 5 and 10 are measured in MW, the overloading of both lines is about 29 MW in the worst N-1 situation. However, the line 102 is overloaded 99 MW in the worst N-1 situation. This shows that if post-contingency values are used to measure the severity, it may be difficult to find a measure that captures the severity of the overloading.
Figure 3.8: Overloading of lines as relative to the capacity of the line. The loading of the system is 150%.

Another problem to use the post-contingency values in the security assessment is that they do not state anything how the cascade progresses in the system. The cascade may decay in the system after few line trips or it may lead to severe customer interruptions. This issue has been studied within this dissertation in Section 3.5.4. This issue is relevant because in Section 1.4 we defined that security refers to the ability of the system to survive imminent disturbances (contingencies) without interruption of customer service. In order to better understand the triggered cascade and its severity, a security assessment method using consumer side measures is presented in the following section.

### 3.5.3 Risk-Based Security Assessment

The simulations are performed with the IEEE RTS-96 test system illustrated in Fig. A.2 and in the following sections the results are presented.

**Probabilities of Contingencies**

The probabilities of contingencies have been obtained using the methods presented in the previous sections. Two sets of probabilities of contingencies have been estimated by assuming all contingencies equally likely
3.5. Results

Figure 3.9: Absolute overloading of lines. The loading of the system is 150%.

and by assuming that the probabilities are proportional to the length of lines. In Fig. 3.10 probabilities of contingencies have been presented based on these two assumptions. The red line corresponds to equally distributed probabilities of contingencies. The probabilities of contingencies 52 and 90 have been considered to be zero because the lines connecting the busses 207 and 307 are connected with only one line to the rest of the system. The bars are the probabilities obtained based on the length of lines. The total number of credible contingencies is 118.

Severity of Contingencies

A way to consider the security of the system is to consider consumer side variables and the effect of interruptions to customers. An example of such a variable is load shed. Compared with the results obtained using values of N and N-1 situations, the use of consumer side variables takes into account that all security limit violations may not be severe and they may not lead to severe problems on the customer side.

The load shed due to a contingency is simulated using the cascade model presented earlier in 3. Results for two different loading levels are presented in Fig. 3.11 and Fig. 3.12. When the loading level is 130% of the nominal level, two contingencies lead to customer interruptions.
The contingencies are the trips of the lines between the nodes 303 and 324 as well as 324 and 316. The load shed in both cases is the same because the both contingencies trigger exactly the same cascade.

If the loading level is 150% from the nominal, many contingencies trigger cascades that lead to customer interruptions. The two contingencies shown in Fig. 3.11 do not lead to the highest amount of lost load. Therefore, the contingencies that are the most severe at the loading 130% are not the most severe contingencies at the loading 150%. Thus, the severity of a contingency depends on the load level of the system. The values of load shed for the loading level 150% are slightly greater than for the loading level of 130% because the load is higher in the first case. Therefore, the numbers are not directly comparable with each other.

**Expected Load Shed**

The expected load shed is the risk of the system. The expected load shed is obtained by combining the results of the two previous sections.
3.5. Results

![Contingency Load shed (MW)](image)

Figure 3.11: Load shed at the loading level of 130 %. Two contingencies lead to customer interruptions. Actually, these two contingencies trigger exactly the same cascade and therefore the amount of load shed is exactly the same in both cases.

Results have been presented in Table 3.2. In the table, $p_e$ refers to equal contingency probabilities and $p_l$ refers to probabilities obtained based on the length of the lines. The expected load shed increases as the loading of the system increases. However, this is, at least partly, due to a higher load of the system.

The probabilities of contingencies have an effect on the expected load shed. If the loading of the system is 130 % of the nominal value, the expected load shed using the probabilities based on the length of lines gives a smaller value than the expected value using equal probabilities for all contingencies. For the case with the loading level 150 %, the situation is exactly the other way around. The magnitude of the difference is -30 % at the loading level of 130 % and 6 % at the loading level of 150 %. This result may be explained by the results obtained earlier: The severity of contingencies is dependent on the loading level.
3.5.4 Post-Contingency Indicators

**Background**

The security assessment done gives a clear rule to help the decision making: If there is an overloaded line in any N-1 situation, necessary remedial actions have to be planned and executed. The drawback of this method is that it may be too conservative: One line may be overloaded in one of the N-1 situations and, therefore, remedial actions have to be planned and executed.

Table 3.2: Expected load shed as a function of the loading level and with equal and line based probabilities.

<table>
<thead>
<tr>
<th></th>
<th>loading 1.0</th>
<th>loading 1.3</th>
<th>loading 1.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected load shed, ( p = p_e )</td>
<td>0</td>
<td>30 MW</td>
<td>331 MW</td>
</tr>
<tr>
<td>Expected load shed, ( p = p_l )</td>
<td>0</td>
<td>23 MW</td>
<td>404 MW</td>
</tr>
</tbody>
</table>

Figure 3.12: Load shed at the loading level of 150 %. Totally, 14 contingencies trigger a cascade that leads to customer interruptions.
However, it may be that an overloaded line in the N-1 situation does not start a cascade and cause customer interruptions. If no customer interruptions take place, the remedial actions would actually be unnecessary.

Moreover, fluctuating in-feed changes the power flows in the grid continuously. Theoretically, it would be possible to plan remedial actions to ensure that the system is N-1 secure for all possible in-feed scenario by considering the technical limits of in-feed units. However, in practice this would most likely lead to very high operation costs due to high re-dispatching. Thus, in practice there may be no guarantee that the system is N-1 secure because the system is not N-1 secure for all scenarios of in-feed.

Here, we have studied how we could use post-contingency indicators to predict the size of expected load shed. The result gives an answer to the question: Is a simulation of a cascade the only way to predict the magnitude of expected load shed or can we predict the expected load shed with good accuracy using the values of N and N-1 situations?

Results

In order to study, whether post-contingency values and security limits violations in the N-1 situation can be used to estimate the size of expected load shed, 1000 random dispatches were generated that all are N secure but not necessary N-1 secure. The test system used is the IEEE RTS-96 test system. The technical limits of generation at nodes were set to 1000 MW to create as versatile generation patterns as possible. Moreover, 1000 MW may be considered as a representative of the largest units in the system\(^4\). For every dispatch run, random cost coefficients were generated. This ensures that these 1000 dispatches are not same with each other. Otherwise, no changes were made to the original test system.

Mean and median loadings of lines and the highest overloading of the line in the N-1 situation in relative and absolute values have been studied as explaining factors for the expected load shed. The power flows of lines for all N-1 situations were collected into a three-dimensional array \(A(f, c, d)\). In the array, \(f\), \(c\) and \(d\) refer to the flow of a line, number

\(^4\)However, even larger units are possible. The forthcoming unit in Olkiluoto, Finland has a power of 1600 MW.
Chapter 3. Security Assessment

Figure 3.13: The expected load shed against the median loading of lines relative to the capacity of a line in the N-1 situation. Totally 1000 states were studied.

of a contingency and number of a dispatch. For the test system used, the size of the array is $119 \times 120 \times 1000$. The results of the expected load shed for every dispatch were plotted against the median, mean and highest loading of a line in the system. The metric from the N-1 situation is calculated from the data of the array. In our simulations, the equally distributed set of probabilities has been used, see Fig. 3.10 and Section 3.3.3.

In Fig. 3.13 and Fig. 3.14, results for the median loading of the system have been shown in relative and absolute loadings of lines. The results show that no clear indication is visible that a higher median loading of the lines in the N-1 situations lead to a higher expected load shed. Also, the correlation calculated is small, Table 3.3.

The results for the mean value of loading are presented in Fig. 3.15 and Fig. 3.16. Visually it is difficult to see any correlation between mean value indicators and the expected load shed. However, the correlation computed is 19 %, Table 3.3.

Based on the results, the best indicator for the expected load shed is the highest overloading of a line of the system in the N-1 situation. The
3.5. Results

The results are presented in Fig. 3.17 and Fig. 3.18. The correlation is visible in the latter figure. The correlations of these indicators with the expected load shed are 22 % and 38 %, Table 3.3.

In Table 3.3, correlations of studied post-contingency values with the expected load shed are presented. The results obtained suggest that all post-contingency indicators correlate positively with the expected load shed. However, there is a difference in magnitudes. The results suggest that the median loading of lines of the system is not a good indicator of the expected load shed. Based on the results, the best indicator is the absolute overloading of the lines in the N-1 situation. With absolute values, we obtained a correlation of 38 % and for relative values the correlation is 22 %.

Even though the correlations are positive, the results suggest also that it is difficult to predict the expected load shed from the N-1 situation values, if a cascade is triggered.
Figure 3.15: The expected load shed against the mean loading of lines relative to the capacity of a line in the N-1 situation. Totally 1000 states were studied.

Table 3.3: Correlations of post-contingency indicators with the expected load shed.

<table>
<thead>
<tr>
<th></th>
<th>median</th>
<th>mean</th>
<th>highest overloading</th>
</tr>
</thead>
<tbody>
<tr>
<td>absolute</td>
<td>0.0350</td>
<td>0.1861</td>
<td>0.3757</td>
</tr>
<tr>
<td>relative</td>
<td>0.0712</td>
<td>0.1861</td>
<td>0.2174</td>
</tr>
</tbody>
</table>

3.6 Conclusions

A cascade code has been presented that can be used to model the progress of a cascade in the system. The operation of the cascade code has been demonstrated by modeling the expected load shed for different loading levels of the IEEE RTS96 test system. The results of this chapter state that it might be difficult to state the level of security of the system from the values of N and N-1 situations. The simulations done and results obtained indicate that the expected load shed after the cascade depends on many parameters of the system and it may be difficult to be predicted using the values of N and N-1 situations. Such parameters are, for example, the available capacity margin of lines, lo-
Figure 3.16: The expected load shed against the mean loading of lines of a line in absolute values in the N-1 situation. Totally 1000 states were studied.

cation and amount of loads and generation in the system. These have an effect on the expected load shed, because the overloaded lines in the post-contingency state cause a redistribution of the power flows in the system and parallel lines to the tripped lines are loaded more. This chapter presented also results on computational complexity of security assessment. The analysis has been done using the Big O analysis and the derived results were supported with simulations.
Figure 3.17: The expected load shed against the highest overloading of a line relative to the capacity of the line in the N-1 situation. Totally 1000 states were studied.

Figure 3.18: The expected load shed against the highest overloading of a line in absolute values in the N-1 situation. Totally 1000 states were studied.
Chapter 4

Security Assessment with Fluctuating In-Feed

The share of fluctuating in-feed in total production has increased in power systems and it is expected to increase further in the future. This chapter presents a method for power systems with fluctuating in-feed to classify the system in system security states. Furthermore, a method to assess the risk of the system is presented.

4.1 Introduction

The recent increase in fluctuating generation in Europe, as discussed in Chapter 1, sets new challenges for security assessment. The power flows of lines are not constant for a specific time interval, an hour for example, due to fluctuations in generation and loads. However, the increase of wind and PV generation has amplified these fluctuations. In Fig. 4.1, an illustration about uncertainty, or forecast error, of wind in-feed is presented. There is no uncertainty at the moment of supply $t-0$. However, before the moment of supply, at $t-1$ for example, there is an uncertainty regarding the in-feed at the moment $t-0$. Also, if we look into the future, the uncertainty regarding the in-feed increases as we go far from the current moment.

These fluctuations may cause the system to move out from the normal state, where security criterion is met, to a state where these security lim-
Chapter 4. Security Assessment with Fluctuating In-Feed

4.1.1 Literature Review

In literature, only few publications consider fluctuations of in-feed on security. In [57], the authors have considered branch faults in the probabilistic power flow computation. Earlier, in [58] and [59] the authors have also considered probabilistic load flow computation with line faults.

In [60], the authors emphasize the importance of system security states to provide a basis for decision making in terms of security. McCalley et al. point out that there is no quantitative method to measure the security level, or the membership of the power system in different system security states.

4.1.2 Contribution of Author

This chapter proposes a probabilistic method to classify the power system security state in presence of fluctuations of generation or loads in operational planning or real-time. Moreover, a method to assess the risk associated with security of the system is presented. The method uses load shed to measure severity. The methods proposed contribute to contingency analysis and to classification of the power system security state.
4.2 Probabilistic System Security State Classification

4.2.1 Background

In this section, a probabilistic classification method is proposed. The need for a probabilistic method arises from the fact that many systems have a substantial amount of fluctuating in-feed. The in-feed is not known in the operational planning and may vary during operation also in large extent. Thus, the power flows cannot be presented using a single value but the probability distributions of power flows of lines should be considered.

For the probabilistic system security state classification, the probability distributions of power flows of lines have to be computed for the N situation and for all N-1 situations. From the power flow results of the N situation, the probabilities for the emergency and automatic actions states can be computed. The estimation of probabilities for the normal and alert states needs that we solve the power flow distributions of lines for the N and N-1 situations.

4.2.2 Methods

In the following formulation, it has been assumed that the limits of lines are overloaded 120 % or more in the automatic actions state, and in the emergency state over 100 % but under 120 % in the N situation.

The probability of the automatic actions state, \( P(S_{aa}) \), is the highest observed probability that the power flow of a line is overloaded 20 % or more in the N situation:

\[
P(S_{aa}) = \max_l P(1.2F_{l}^{\text{max}} \leq F_{l}^{N}),
\]

(4.1)

where \( F_{l}^{\text{max}} \) is the thermal limit of the line \( l \) and \( F_{l}^{N} \) is a random variable from the power flow distribution of the line \( l \) in the N situation.

The probability of the emergency state, \( P(S_e) \), is the maximum probability that the random variable generated from the power flow distribution is between the loading levels of 100 % and 120 %:

\[
P(S_e) = \max_l P(F_{l}^{\text{max}} \leq F_{l}^{N} \leq 1.2F_{l}^{\text{max}}).
\]

(4.2)
After calculating the probabilities for the automatic actions and emergency states, the probability that the system is either in the normal or alert state, \( P(S_{n,a}) \), may be computed:

\[
P(S_{n,a}) = 1 - P(S_e) - P(S_{aa}) \tag{4.3}
\]

The probability that the system is in the alert state \( P(S_a) \) is obtained by computing first the probability that the system has an overloaded line in the N-1 situation:

\[
P(\hat{S}_a) = \max P(F_{l}^{\text{max}} \leq F_{l}^{N-1}), \tag{4.4}
\]

where \( F_{l}^{N-1} \) is a random variable generated from the power flow distribution of the line \( l \) in the N-1 situation.

Using this information we may compute the probability that the system is in the alert state:

\[
P(S_a) = P(S_{n,a})P(\hat{S}_a), \tag{4.5}
\]

where \( P(\hat{S}_a) \) is obtained from the power flow solution in the N-1 situation.

The probability of the normal state \( P(S_n) \) may be computed using known values either:

\[
P(S_n) = 1 - P(S_a) - P(S_e) - P(S_{aa}) \tag{4.6}
\]

or

\[
P(S_n) = P(S_{n,a})(1 - P(S_a)), \tag{4.7}
\]

where a similar approach has been used as in calculation of the probability of the alert state.

By calculating the probabilities of different system security states, the following known property may be used to calculate the probability that a power flow \( F_{l}^{N} \) is inside the limits \( a \) and \( b \):

\[
P(a \leq F_{l}^{N} \leq b) = H(b) - H(a), \tag{4.8}
\]

where the following has been used:

\[
H(z) = \int_{-\infty}^{z} h(t)dt, \tag{4.9}
\]

where \( h(t) \) is the power flow distribution of the specific line either in the N or N-1 situation. The random variable \( F_{l}^{N} \) is generated from the power flow distribution \( h(t) \).
4.3. Risk-Based Security Assessment

4.2.3 Probabilistic Interpretation

The obtained probability distribution tells the probability of each system security state. The probabilities fulfills the three properties of a discrete probability distribution listed in [50]. The values of probabilities of states are between 0 and 1:

\[ P(S_n), P(S_a), P(S_e), P(S_{aa}) \in [0, 1] \]  \hspace{1cm} (4.10)

the sum of the probabilities of states is 1:

\[ P(S_n) + P(S_a) + P(S_e) + P(S_{aa}) = 1. \]  \hspace{1cm} (4.11)

and the following is valid for a union of probabilities:

\[ P(S_n + S_a + S_e + S_{aa}) = P(S_n) + P(S_a) + P(S_e) + P(S_{aa}). \]  \hspace{1cm} (4.12)

Therefore, the values obtained indicate the probability of a specific system security state.

4.3 Risk-Based Security Assessment

In the previous Chapter 3, a risk-based security assessment was developed for a system without uncertainties of in-feed. A similar risk-based security assessment may be done for a system with fluctuating in-feed as for a system with (exactly) known generation and load values. This may be done using Monte-Carlo simulations and running realizations of fluctuating in-feed and computing the average of the expected load shed.

With a risk-based security assessment for a system with fluctuating in-feed, the risk associated with customer interruptions may be estimated. Compared with the security assessment in the previous chapter, this method considers also different combinations of wind in-feed realizations and gives an estimate how much is the additional expected load shed if forecast errors are considered.
4.4 Results

4.4.1 Results on System Security State Classification

The method has been illustrated by using one area of the IEEE RTS-96 test system. The fluctuations were compensated with generators in the system. The fluctuating in-feed is located at the nodes 101, 102 and 107. The variance of the forecast error distribution is 20 % from the expected in-feed, or the variance factor is 0.2. It has been assumed that forecast errors are normally distributed. The power flow distributions have been computed using methods presented in Section 1.5.2. The forecasts correlate with each other and the correlation is 80 %. Three different loading levels were considered to illustrate different possible situations in the grid and to demonstrate the value added of the proposed classification method compared to the deterministic classification method.

System with 100 % Loading

For the loading level 100 %, the results of the probabilistic classification have been presented in Fig. 4.2. A comparison with the deterministic classification method has been shown also. The results show that the probabilistic method proposed gives almost the same result with the deterministic classification method. There are two main factors identified that may explain these results: First, the forecast error is relatively small and Second the system is quite unloaded at the loading level of 100 %. Therefore, fluctuations of in-feed do not cause security limit violations in the N or N-1 situations.

System with 120 % Loading

In Fig. 4.3, the classification results for a case for the loading level of 120 % have been presented. In this case, a difference between the probabilistic and deterministic classification methods is visible. The deterministic system security state classification method says that the system is in the alert state. The probabilistic classification method gives additional information that may be useful in decision making. According to the probabilistic classification method, the most probable system state is
4.4. Results

Figure 4.2: Classification results for the test system with a loading level of 100 %. Both methods give identical results. The variance factor is 0.2.

the alert state as the deterministic classification indicates. However, compared with the deterministic classification, the probabilistic classification method shows that there is a substantial probability (about 25%) that the system is in the normal state. Moreover, if the fluctuations of in-feed have the worst possible combination, the system may be even in the emergency state with a small probability (about 2 %).

System with 140 % Loading

The third situation studied is presented in Fig. 4.4. In this case the nominal loading of the test system was increased to 140%. The results obtained show the probabilistic classification method identifies the possibility that the system is in the emergency state or even in the automatic actions state with probabilities 13 % and 1 %, respectively. These possibilities for emergency and automatic actions states are not visible using the deterministic classification method.
Figure 4.3: Classification results for the test system with a loading level of 120%. The variance factor is 0.2.

Figure 4.4: Classification results for the test system with a loading level of 140%. The possibilities for emergency and automatic actions states are identified using the probabilistic classification method. The variance factor is 0.2.
4.4. Results

Figure 4.5: Probability of different system security states for three different forecast errors. The loading of the system is 140 %.

4.4.2 Effect of Forecast Horizon and Accuracy on Results

The forecast error may be decreased by using two main methods: First, by decreasing the forecast horizon or, second, by improving the forecast methods to give more accurate estimates. In simulations we have thus studied the sensitivity of the results with respect to the variance.

The probability of every state for three different forecast error sizes has been presented in Fig. 4.5 when the loading of the system is 140 % from the nominal value. The results show that when the forecast error increases the uncertainty regarding the system security state increases.

The sensitivity of the system security states to the variance of the forecast error has been presented in Fig. 4.6, in Fig. 4.7 and in Fig. 4.8. The results are for the loading levels of 100 %, 120 % and 140 %. For the loading level of 100 % changes are quite small. For the loading levels of 120 % and 140 % the changes are bigger. In Fig. 4.7 the situation for the loading level of 120 % is presented. In Fig. 4.8, the situation for the loading level of 140 % is presented. The probability
Figure 4.6: Change of the probability of the system security state as a function of the forecast error. The loading of the system is 100%.

The results show that the uncertainty regarding the system security state increases as the forecast error increases. Therefore, an improvement of the forecast error makes the decision making easier than in a situation where the in-feed has a big uncertainty.
4.4. Results

Figure 4.7: Change of the probability of the system security state as a function of the forecast error. The loading of the system is 120 %.

4.4.3 Summary

The method proposed has been illustrated using three different situations in the test system. The results show that sometimes the probabilistic method proposed gives almost identical results with the deterministic security assessment as in the first case. In the second case, the deterministic method gives mainly a too pessimistic view because the probability that the system is in the normal state is substantial and the method proposed identifies also the small probability of the emergency state. In the third case, the method proposed identifies the 13 % probability that the system is in the emergency state and the 2 % probability that the system is in the automatic actions state.

The value added of the method proposed is the better understanding of the state of the system under uncertainty. Thus, the possible risks may be identified better.
4.4.4 Results on Risk-Based Security Assessment

Simulations have been run using the IEEE RTS-96 test system. As a consumer side measure, the expected load shed in MW is used as a metric. It has been assumed that the forecast errors follow the normal distribution. The generators have an available capacity of 35 % except the wind power generators that do not have possibility to increase production. The variance of the forecast error distribution of in-feed is 20 % of the expected in-feed. In [61], it has been said that the standard deviation of the forecast error for an aggregation of 30 wind farms is from 12 % to 18 % depending on the forecast horizon. However, in our model the forecast error is for a single wind farm and therefore the forecast error is higher. In [62] it has been stated that aggregation gives benefits that are for example 50 %. Therefore, an assumption that the variance of the forecast error is 20 % of the expected in-feed for a single
4.4. Results

The results for the security assessment using the expected load shed are shown in Fig. 4.9. The results show that even with the loading levels 100% and 120%, the system may be insecure and load has to be shed due to fluctuations of the in-feed.

The probabilities of contingencies have a small effect on the expected load shed. At the loading level of 100%, the expected load shed values are 22 MW and 26 MW for equally distributed probabilities and probabilities based on the length of the line. The latter value is about 18% higher than the first value. For the loading level of 120%, the corresponding values are 231 MW and 251 MW. Also in this case, the expected load shed is higher if the probabilities are based on the length of the line. The difference between the values is about 9% and it is about half of the difference that was obtained at the loading level of 100%.

If the forecast errors are not considered, no load shedding takes place because the system is N-1 secure at the loading levels of 100% and 120% and, therefore, contingencies do not trigger a cascade.

Histogram

The distribution for the load shed after a contingency is presented in Fig. 4.10. The loading level is 100% and the variance of the forecast error distribution is 20%. The histogram has 100 equally spaced bars. There are totally 10 contingencies that do not lead to any load shed with wind scenarios. In additionally, one contingency leads to a very small average load shed and therefore the first bar has 11 observations.

Based on the histogram, the most severe contingencies may be identified. The four most severe contingencies are 91, 92, 54 and 53. The lines can be seen in Fig. A.3. These contingencies have an average load shed of 344 MW, 228 MW, 222 MW and 194 MW, respectively. The most severe contingencies are marked in Fig. A.3. By looking at the location of these contingencies, it might be difficult to find any specific reason why these contingencies lead to most severe load shedding. Most likely, there is no single reason but the load shed is a result of complex cascading failures. Due to the nature of Monte Carlo simulations, the values varied a little bit over runs, but these four contingencies were always the most severe. 1500 Monte Carlo simulations have been used to estimate the load shed.
Figure 4.9: Comparison of results. If no uncertainty of in-feed is considered, the system is N-1 secure at loading levels of 100 and 120 %. If uncertainty is considered, the average of expected load shed is not zero. The variance of the forecast error is 20 % of the expected wind in-feed, \( p_e \) and \( p_l \) refer to equally distributed probabilities and to probabilities proportional to the length of lines.

### 4.4.5 Number of Simulations

The sensitivity of the results to the number of Monte Carlo simulation runs has been presented in Table 4.1. In the simulations, the loading level is 100 % and the variance of the forecast error is 20 % of expected in-feed. The number of simulations was varied from 500 to 1900 runs. The results show that additional simulation runs do not increase accuracy compared to a case with 500 simulation runs in the case of the test system used. The probabilities of contingencies do not affect the convergence.

In general, the number of Monte Carlo runs needed to fulfill a certain
4.4. Results

Figure 4.10: Distribution of average load shed after a contingency.

Confidence interval with a certain probability may be calculated [63]. This is possible because the central limit theorem allows the use of the normal distribution to depict the distribution of the estimated mean[63].

However, a histogram obtained for the contingency 91 is depicted in Fig. 4.11. The distribution does not strictly follow a normal distribution. The two visible bars have 1442 and 58 observations. Due to this reason, the number of Monte Carlo simulations needed may be difficult to estimate from the Monte Carlo simulation outputs and more research is needed to find out if this is the case in general.

4.4.6 Size of Forecast Error

The expected load shed as a function of the variance factor of the forecast error is presented in Fig. 4.12. The variance of the forecast error distribution is the variance factor times the expected in-feed. Results are presented for the loading levels of 100 % and 120 %. The results
Table 4.1: Sensitivity of the expected load shed to the number of Monte Carlo simulations. The variance of the forecast error distribution is 20 % and the loading is 100 %.

<table>
<thead>
<tr>
<th>Number of simulations</th>
<th>Exp. load shed ((p = p_e))</th>
<th>Exp. load shed ((p = p_l))</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>20.81 MW</td>
<td>24.28 MW</td>
</tr>
<tr>
<td>700</td>
<td>21.86 MW</td>
<td>25.12 MW</td>
</tr>
<tr>
<td>900</td>
<td>22.34 MW</td>
<td>24.41 MW</td>
</tr>
<tr>
<td>1100</td>
<td>20.52 MW</td>
<td>23.48 MW</td>
</tr>
<tr>
<td>1300</td>
<td>22.56 MW</td>
<td>25.21 MW</td>
</tr>
<tr>
<td>1500</td>
<td>24.28 MW</td>
<td>28.74 MW</td>
</tr>
<tr>
<td>1700</td>
<td>22.54 MW</td>
<td>25.66 MW</td>
</tr>
<tr>
<td>1900</td>
<td>20.32 MW</td>
<td>23.87 MW</td>
</tr>
</tbody>
</table>

Figure 4.11: Histogram of the load shed after the contingency 91.

show that the higher forecast error leads to a higher expected load shed. For both loading levels, the expected load shed with equally distributed probabilities of contingencies are below the curve obtained with proba-
4.5 Conclusions

The results presented in Fig. 4.9 correspond to the case where the variance factor is 0.2 and the loading level is 120%.

Figure 4.12: Expected load shed as a function of the variance factor of the forecast error for loading levels of 100% and 120%. The results for the loading levels 100% and 120% are not directly comparable because the total load is 20% higher in the second case. The results for a single loading level with different forecast error sizes are comparable because the forecast error is compensated in the rest of the system and, thus, the total load does not change.

4.5 Conclusions

In this chapter, two approaches to security assessment have been presented that consider fluctuations of in-feed in the analysis. First, a method based on the values of N and N-1 situations has been presented
to classify the system security state. Due to fluctuations, the power system security state cannot be classified uniquely in operational planning or operation. The method presented gives a set of indexes that reflect the probability of different security states. The second method can be used to estimate the risk of security failure of the system by considering the cascade triggered and the fluctuations of in-feed in the system. The method gives the expected load shed as a result.
This chapter proposes a method to re-dispatch generators to be robust against fluctuations of in-feed. Moreover, a method to estimate the optimal confidence level is presented.

5.1 Introduction

5.1.1 Background

Based on the results of the security assessment done by the TSOs, a decision on planning and execution of possible remedial actions is done. The remedial actions may be categorized into preventive or curative\(^1\) remedial actions. The preventive actions are executed before the contingency has happened and curative remedial actions are executed after the contingency.

Today, one main challenge is the uncertainty regarding fluctuations of in-feed in the system. In the planning stage, forecasts for in-feed may be used. However, the forecasts almost always have a forecast error. Therefore, the power flows of lines may not be known exactly and possible violations of thermal limits are uncertain. In this chapter, a method to plan a robust re-dispatch of generators is presented. Moreover, a

\(^1\)The term curative action is used in Europe [23]. The term curative action is known also with the term corrective action.
method to decide an optimal probability of overloading used in the robust re-dispatch has been presented.

5.1.2 Literature Review

There is not much literature regarding remedial actions in interconnected power systems. In [64], the authors point out the benefits of improving cross-border re-dispatch in Europe to decrease costs of remedial actions. The authors propose that the participating control areas submit adjustment bids and the re-dispatch of generators is decided based on these bids. The distributed OPF algorithms [28], [29] and [30] were mentioned already in Chapter 2, but they may be used also in planning of remedial actions in interconnected power systems.

In the planning stage, one important aspect is the cost of reliability and security in the system. In order to estimate the value of reliability or security, value of lost load (VOLL) has to be known. Estimation of the value of the VOLL is not a topic of this thesis, and the value is used as given.

The methods to estimate the VOLL may be divided into two categories: Customer surveys and indirect methods. Because VOLL is one of the main factors affecting the planning and execution of remedial actions, several publications to this topic are available. To start with, a good overview is given in [65]. In [66], a customer survey has been used to estimate reliability worth in Canada. The values represent the situation in Canada around the time of publishing in 1994. In [67], the authors have used a survey to estimate the interruption costs in Norway in 2002.

An example of an indirect method is presented in [68], where the worth of reliability is estimated based on the costs of a back-up generation. In many locations where the reliability of electricity supply is critical and VOLL is high, for example in hospitals, back-up generation is available in order to overcome interruption of electrical supply without critical damage.

The reliability level may be optimized by considering the benefits and costs associated with reliability. This method has been used in [69], [65], [70] and [39]. Also the ENTSO-E Operation Handbook states that the reliability should be determined based on the cost benefit analysis [23].
5.2. Coordination of Remedial Actions

5.1.3 Contribution of Author

This chapter presents a robust re-dispatch method of generators in order to meet a given probability in terms of security in presence of fluctuations of generation or loads. Moreover, a method to determine an optimal violation probability in the robust re-dispatch method is presented.

5.2 Coordination of Remedial Actions

In interconnected power systems, the remedial actions have been done normally within responsibility areas. However, there are few issues that motivate that remedial actions should be planned and executed in collaboration. The first is monetary savings if remedial actions are planned and executed in collaboration over borders. The second is that the remedial actions planned by one TSO may disturb other TSOs because the CAs are electrically connected with each other. This means that there is no guarantee if TSOs execute remedial actions separately that the whole system is secure.

Centralized Solution

One way to plan remedial actions in interconnected power systems is to collect all the data and solve the planning problem centrally. When the solution has been found, the member TSOs execute the plans. The costs of remedial actions are shared among participating TSOs. In Europe an agreement on how to share costs has been done among some TSOs [25]. The idea of the centralized solution is depicted in Fig. 5.1.

De-centralized Solution

An alternative for the centralized solution is the decentralized solution. Because the remedial actions are based on a solution of an optimization problem, decomposition algorithms may be used to formulate the problem for CAs. The CAs solve sub-problems independently and a match with the original problem is achieved using coordination. Relevant papers are mentioned in Section 5.1.2. The benefit of the decentralized solutions includes the privacy obtained by all CAs because the
Chapter 5. Remedial Actions

The whole network model does not have to be shared among other TSOs. The drawback relates to the coordination needed and how it could be realized in practice easily. Often, decomposition methods need many iteration rounds and, therefore, an automatic data exchange should be organized among TSOs to make a de-centralized solution realizable.

Another approach is to plan the remedial actions de-centrally without coordination, but no guarantee for the security of the whole system can be given in this case.

5.3 Robust Re-Dispatch of Generators

5.3.1 Introduction

Optimization tools may be used in remedial actions planning. In this section, the remedial actions are based on a solution of a linear program (LP) optimization problem. The cost function has the cost of the adjustments of generators and the constraints are the power balance, thermal limits of lines and technical upper and available up- and downwards adjustments of generators.

Because the adjustment at a node may be negative or positive, the objective function has an absolute value objective function. In the following sections, the absolute value problem and the LP formulation are presented. Moreover, the transformation of the problem to an LP problem is presented.
5.3. Robust Re-Dispatch of Generators

5.3.2 Problem

The needed generator adjustments are selected based on a solution of an optimization problem. The problem is an absolute value optimization problem:

\[
\text{Costs} = \text{minimize } c \sum_g |\Delta P_g|, \quad (5.1)
\]

subject to:

\[
\sum_g \Delta P_g = 0 \quad (5.2)
\]

\[
A_0 P_0 + A_0 \Delta P \leq F \quad (5.3)
\]

\[
A_0 P_0 + A_0 \Delta P \leq F \quad (5.4)
\]

\[
A_c P_0 + A_c \Delta P \leq F \quad (5.5)
\]

\[
A_c P_0 + A_c \Delta P \leq F \quad (5.6)
\]

\[
\Delta P_{\text{min}} \leq \Delta P \leq \Delta P_{\text{max}} \quad (5.7)
\]

where \(c\) is a cost related parameter, \(\Delta P_g\) is the adjustment of the generator \(g\), \(A_c\) is a matrix mapping the net nodal injections to power flows of lines after the contingency \(c\), \(A_0\) is the matrix mapping the net nodal injections to power flows of lines in the N-situation and \(F\) is a vector of thermal limits of lines.

The market dispatch is modeled using the matrices \(A_0\) and \(A_c\) with the net nodal injection vector \(P_0\). The market dispatch gives some initial power flows in the system. The TSO makes the re-dispatching of generators on top of these power flows using the available generators. In practice, the possible generators for adjustments are defined based on an auction or a TSO may require some generators to keep capacity available and pays a compensation on this service.

The problem may not be solved using a standard LP solver because it has an absolute value objective function. However, the absolute value optimization problem may be transformed to a standard LP problem by making substitutions given in the next section.
5.3.3 Linear Program Formulation

The above absolute value optimization problem may be transformed to a standard LP. A method for this type of an optimization problem has been presented in [71]. To apply this method to our problem, the following substitutes have to be made: The adjustment component of generation at every node is divided into two parts $|\Delta P| = \Delta P^+ + \Delta P^-$ and $\Delta P = \Delta P^+ - \Delta P^-$. Moreover, we require that the both adjustment components are positive $\Delta P^+ \geq 0$ and $\Delta P^- \geq 0$.

By considering these substitutes, the following optimization problem is obtained:

$$\text{Costs} = \text{minimize } c\Delta P^+ + c\Delta P^- \quad (5.8)$$

subject to

$$\sum_g (\Delta P^+_g + \Delta P^-_g) = 0 \quad (5.9)$$

$$A_0 P_0 + A_0 \Delta P^+ - A_0 \Delta P^- \leq F \quad (5.10)$$

$$- A_0 P_0 - A_0 \Delta P^+ + A_0 \Delta P^- \leq F \quad (5.11)$$

$$A_c P_0 + A_c \Delta P^+ - A_c \Delta P^- \leq F \quad (5.12)$$

$$- A_c P_0 - A_c \Delta P^+ + A_c \Delta P^- \leq F \quad (5.13)$$

$$0 \leq \Delta P^- \leq \Delta P^-,\text{max} \quad (5.14)$$

$$0 \leq \Delta P^+ \leq \Delta P^+,\text{max} \quad (5.15)$$

where $\Delta P^+$ is a vector of adjustments of generators upwards at the nodes and $\Delta P^-$ is a vector of adjustments of generators downwards at the nodes.

The problem presented is in the standard LP form and it may be solved using commercial solvers, for example the linprog-function of Matlab that uses the Simplex algorithm.

5.3.4 Security Margins

In order to consider the uncertainty of the in-feed at the nodes, the security margins of lines may be increased in order to guarantee that
the thermal limit of the line is not exceeded at the moment of supply with a probability of $\varepsilon$:

$$\mathbb{P}(-F_l^{\text{max}} \leq F_l \leq F_l^{\text{max}}) \geq 1 - \varepsilon,$$

(5.16)

where $F_l$ is a random variable from the normal distribution $N(F_l^{\text{exp}}, \sigma_l^2)$ and $F_l^{\text{max}}$ is the thermal limit of a line $l$, $\sigma_l^2$ is the variance of the power flow distribution of the line $l$.

The size of the adjustment, $\Delta F$, for a given probability of overloading of a line $\varepsilon$ may be solved from the following equation:

$$\int_{-\infty}^{\Delta F_l} \frac{1}{\sigma_l \sqrt{2\pi}} e^{-\frac{x^2}{2\sigma_l^2}} dx = 1 - \varepsilon.$$  

(5.17)

By solving $\Delta F$ from the above equation, the size of line adjustment is achieved. In this thesis, the \texttt{icdf}-function of Matlab has been used to solve $\Delta F$ from Eq. 5.17.

### 5.3.5 Prices

Re-dispatching is a remedial action associated with cost. Because the TSOs do not own generation assets, they have to buy the the capacity of generators for a certain period. Moreover, in case of generator adjustments, the generating companies are compensated for the energy supplied or they may sell energy to the TSO with a price that is smaller than the spot price.

It has been assumed that the TSO has to pay a higher price than the spot price $p_u \geq p_s$ for upward adjustments of generators. In case of downward adjustment, the TSO will get money from the generating company and the price is $p_d \leq p_s$. In order to keep the power balance within the system, the amount of up- and down adjustments have to be equal.

Thus, a TSO pays the difference $C = p_u - p_d$. Due to the spread between up- and downward adjustments, the resulting costs of TSOs are always positive. This means that a TSO has a cost associated to the re-dispatch. The pricing mechanism has been illustrated in Fig. 5.2.
5.4 Security and Reliability

A high level of reliability needs a high level of security. This means that contingencies in the system do not lead to customer interruptions. In addition to security, a high level of reliability requires a low fault rate in the system and/or short restoration times. Formally, the link between security and reliability measured using the EENS may be presented as follows [72]:

\[ EENS = \lambda \sum_c p_c S_c r_c, \]  

(5.18)

where \(p_c\) is the probability of the contingency \(c\), \(S_c\) is the severity of the contingency \(c\), \(\lambda\) is the fault rate in the system and \(r_c\) is the restoration time of after the contingency \(c\).

The probability may be considered in the fault rate of the component. Then \(\lambda_c = \lambda p_c\) and the the equation may be written:

\[ EENS = \sum_c \lambda_c S_c r_c, \]  

(5.19)

where \(\lambda_c\) is the fault rate of the component associated with the contingency \(c\).

The monetary value of EENS is

\[ C_{EENS} = EENS \times VOLL \]  

(5.20)

where \(C_{EENS}\) is the monetary cost associated with the EENS and VOLL is the value of lost load.
5.5 Optimal Reliability Level

Using the robust re-dispatch method, the generators may be dispatched so that the system sustains fluctuations of in-feed without violating the security limits with a probability $1 - \varepsilon$. However, $\varepsilon$ should be chosen so that economic efficiency of the system is maintained. This means that a TSO should not re-dispatch generators more than is needed in order to get a small $\varepsilon$. Because re-dispatching of generators has an associated cost, this should be compared with the benefits obtained due to smaller penalties paid to customer.

An option is to choose $\varepsilon$ by solving an optimal level for reliability by considering the possible cascade triggered and load shed after a contingency and by comparing it with the costs of re-dispatching of generators. In literature, this method of analysis is called the cost-benefit analysis. The idea of this method is illustrated in Fig. 5.3. In the figure, the costs curve represents the re-dispatching costs of a TSO. The penalties curve represents the monetary value of EENS. By summing up these curves, a curve representing the total costs is obtained. The optimal reliability level and an optimal value for $\varepsilon$ is obtained at the point where the total costs curve has the minimum. The cascade simulation may be used to estimate the expected load shed. The cascade simulation is a complex process and the remedial actions executed may affect the progress of the cascade and therefore the expected load shed. This means that the penalties curve does not necessary decrease monotonically as $1 - \varepsilon$ increases.
In order to obtain the curves, a set of simulations by varying $\varepsilon$ has to be performed. The total costs over different values of $\varepsilon$ are calculated and the optimal value for $\varepsilon$ is found at the point where the total costs have a minimum. At the optimal point the penalties due to customer interruptions do not decrease as much as the re-dispatch costs of generators increase.

5.6 Results

5.6.1 Robust Re-Dispatch of Generators

The robust re-dispatch of generators was performed using two areas of the IEEE RTS-96 test system. The location of fluctuating in-feed is at nodes 101, 102, 107 in the first CA and at the nodes 201, 202 and 207 in the second CA. The correlation of in-feeds within CAs is 0.8. The sources of the first area do not correlate with the sources of the second area. All generators except the wind in-feed sources have a possibility to increase their production 15%.

In the simulations, it has been assumed that the TSOs have pooled data and solve the problem with full knowledge about the power system. Otherwise, no guarantee for the security may be given as discussed in Chapter 2.

The results are shown in Fig. 5.4 for loading level of 120%. The system is N-1 secure at the loading level of 120%. There is, however, uncertainty regarding the power flows of lines in the system and, therefore, with $1 - \varepsilon = 0.9$, a re-dispatch of generation costs 30 € to the TSO. After this value, the costs increase exponentially. The last solution was found for the value $\varepsilon = 0.02$. With the value $\varepsilon = 0.01$ no feasible solution was found. The location of the last solution depends on the parameters used in the simulation. The cost parameter $c = 0.2 \times 50$ €/MWh.

The effect of correlation is visible also in the results. The results show that consideration of correlation leads to higher costs of re-dispatch of generation. This may be explained by increased variance of power flow distributions when correlation is considered. Without considering correlation, the re-dispatch costs are zero for all values of $\varepsilon$ studied.
5.6. Results

Figure 5.4: Costs of robust re-dispatch of generation at the loading level 120% of the nominal loading with and without considering correlation of in-feed units.

5.6.2 Optimal Reliability Level

The expected load shed was estimated using Monte Carlo simulations. Five sets of 2500 Monte Carlo simulations were performed with varying $\varepsilon$ and, thus, the total amount of simulation runs used is 12 500. The results of Monte Carlo simulations are presented in Table 5.1. The results show that the differences between different values of $\varepsilon$ are small for the test system used. The results show also that variation within a single $\varepsilon$ value is quite large compared to results obtained with other values of $\varepsilon$ with the test system used. This can be explained by the load shed distribution presented in Chapter 4, Fig. 4.11. The values for 12500 Monte Carlo runs are presented on the last row. These values are used to decide the optimal value for $\varepsilon$.

The results regarding the determination of $\varepsilon$ are presented in Fig. 5.5. The results are obtained using the following parameter values: $\lambda = 0.01$, 

\begin{center}
\begin{tikzpicture}
\begin{axis}[
    width=\textwidth,
    xlabel={$1-\varepsilon$},
    ylabel={Cost (euro)},
    xmin=0.7, xmax=1,
    ymin=0, ymax=500,
    xtick={0.7, 0.75, 0.8, 0.85, 0.9, 0.95, 1},
    ytick={0, 100, 200, 300, 400, 500},
    legend style={at={(0.5,0.95)},anchor=north west},
    legend entries={With correlation, Without correlation},
]
\addplot[black, solid] coordinates {
(0.7, 0)
(0.75, 0)
(0.8, 0)
(0.85, 0)
(0.9, 0)
(0.95, 0)
(1, 500)
};
\addplot[black, dashed] coordinates {
(0.7, 0)
(0.75, 0)
(0.8, 0)
(0.85, 0)
(0.9, 0)
(0.95, 0)
(1, 500)
};
\end{axis}
\end{tikzpicture}
\end{center}
Table 5.1: Estimates for load shed (p.u.) using Monte Carlo simulations. \( \varepsilon \) is the probability that a security limit is violated, i.e. \( 1 - \varepsilon \) represents thus a probability that a security limit is not violated. 1 p.u. = 100 MW.

<table>
<thead>
<tr>
<th></th>
<th>( 1 - \varepsilon = 0.85 )</th>
<th>( 1 - \varepsilon = 0.90 )</th>
<th>( 1 - \varepsilon = 0.95 )</th>
<th>( 1 - \varepsilon = 0.98 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st set</td>
<td>0.9181</td>
<td>0.9530</td>
<td>0.9515</td>
<td>0.9179</td>
</tr>
<tr>
<td>2nd set</td>
<td>0.9240</td>
<td>0.9458</td>
<td>0.9613</td>
<td>0.9076</td>
</tr>
<tr>
<td>3rd set</td>
<td>0.9268</td>
<td>0.9697</td>
<td>0.9684</td>
<td>0.8998</td>
</tr>
<tr>
<td>4th set</td>
<td>0.9342</td>
<td>0.9337</td>
<td>0.9726</td>
<td>0.8779</td>
</tr>
<tr>
<td>5th set</td>
<td>0.9262</td>
<td>0.9679</td>
<td>0.9352</td>
<td>0.8754</td>
</tr>
<tr>
<td>average</td>
<td>0.92586</td>
<td>0.95402</td>
<td>0.9578</td>
<td>0.89572</td>
</tr>
</tbody>
</table>

\( \text{VOLL}=8000 \text{ €/MWh}, \ r = 1h \) and \( P_r = 0.2 \times 50 \text{ €/MWh} \). \( P_r \) is the price of re-dispatch of generation for one MW and for one hour. The multiplier 0.2 is the spread between prices of up and down generation paid. The minimum or minima are located at the start or end of the interval of \( \varepsilon \) or between these points. The results show that the optimal reliability level is achieved with \( 1 - \varepsilon = 0.85 \). This value is obtained without re-dispatching and, therefore, the TSO should not make any actions in order to obtain the optimal reliability level. This is the optimal policy for the TSO because the marginal costs of re-dispatching of generation are greater than the marginal benefits obtained by paying smaller penalties. The cost components of the first case are presented in Fig. 5.6. The yellow bar is the penalty curve for different values of \( \varepsilon \). The green bar is the costs curve that increases as \( \varepsilon \) increases.

The results regarding the optimal reliability level depend on the parameters used. To illustrate this, in Fig. 5.7 results with the parameter values \( \lambda = 0.05, \text{VOLL}=8000 \text{ €/Mwh}, r = 1h \) and \( P_r = 0.2 \times 50 \text{ €/MWh} \). The only parameter value changed was the fault rate compared to the previous case: The fault rate was increased from 1 fault per 100 hours to 5 faults per 100 hours. This increase in the parameter value could represent bad weather conditions, for example. The new set of parameters leads to a result where the TSO should re-dispatch generation to achieve the level where \( \varepsilon = 0.02 \) and, thus, \( 1 - \varepsilon = 0.98 \). This is the maximum value for \( \varepsilon \) that can be achieved. The cost components are presented in Fig. 5.6. The green bar is the costs curve that increases as \( \varepsilon \) increases. From these curves is is also visible that the re-dispatching costs are small compared to the expected penalties to be
5.6. Results

Figure 5.5: Total costs of security. The optimal confidence level is at 0.85 that is obtained without re-dispatching of generation. Re-dispatching of generators is so expensive that it exceeds the benefits (lower interruption costs).

paid. Therefore, a high value of $1 - \varepsilon$ is reasonable.

Effect of Parameters

As illustrated in the results, the optimal reliability level depends on parameters of the cost and penalty curves. The price of re-dispatching of generators affects the cost curve. The parameters VOLL, fault rate and average interruption time affect the penalty curve, see Eq. 5.19 and Eq. 5.20. In Fig. 5.9, the optimal value of $\varepsilon$ is presented as a function of $k$. The ratio $k = C/P$, where $C$ are the costs of re-dispatching of generators and $P$ are the penalties paid. Thus, $k$ tells how much the penalties should increase compared to costs of re-dispatching of generators to change the parameter value $\varepsilon$. The ratio considers the total change of all penalty and cost side parameters. The results show
that if the penalty side parameters have a total increase of 260 %, the optimal value for $1 - \varepsilon$ increases from 0.85 to 0.98.

### 5.7 Conclusions

One of the main goals of TSOs is to maintain a high level of reliability. In order to achieve this goal, the security assessment is done in order to identify the state of the system. After the assessment, remedial actions are planned and executed, if necessary. Within this chapter, a method to perform a robust re-dispatch of generators has been presented. The algorithm considers the uncertainty regarding fluctuating in-feed. The method can be used to consider the uncertainty of loads also. The re-dispatch of generators may be done to consider different probabilities of security limit violations. Within this chapter, also a method to decide
5.7. Conclusions

The optimal violation probability, $\varepsilon$, for the robust re-dispatch algorithm has been presented. The method utilizes the cost/benefit analysis. The cost curve is based on re-dispatch costs of generation and benefits are measured by avoided penalties. The results of this analysis show that a TSO should not consider only the severity of the contingencies in decision making, but also the probability of contingencies, the fault rate of the system, VOLL and an average restoration time. These parameters have an impact on decision making of TSOs.

Figure 5.7: Total costs of security. The optimal confidence level is at 0.98. Re-dispatching of generators is so cheap that the benefits (lower interruption costs) exceed the re-dispatching costs of generators.
Figure 5.8: Costs of re-dispatching (green bars) and interruption (yellow bars).
Figure 5.9: Effect of parameters on the optimal value of $\varepsilon$. The optimal value of $\varepsilon$ has been presented as a function of $k$. The ratio $k = C/P$ describes how much the penalties have to increase in order to change the optimal value of $\varepsilon$. 
Chapter 6

Conclusions

This thesis deals with the security of interconnected power systems. This thesis has demonstrated the importance of exchanging data in order to avoid misleading interpretations regarding the security and regarding a need for remedial actions in interconnected power systems. Due to an increasing share of electricity from fluctuating in-feed sources, fluctuations of wind and solar in-feed may cause substantial uncertainty regarding the power flows also in the neighboring CAs and this issue has been addressed in this thesis. In order to avoid unexpected power flows, the TSOs should exchange data regarding the fluctuating in-feed. For the methods presented in this thesis, the data exchange needed to account for the fluctuations of in-feed comprises of the mean and variance of the forecast error distribution.

Often, security assessment is done using the N-1 security criterion where the values of the N and N-1 situations are used in order to classify the security state of the power system. In this thesis, results on the computational complexity of the security assessment in interconnected power systems have been presented. The results show that from the computational complexity point of view, the TSOs should consider credible contingencies of own areas and monitor consequences on other CAs.

The consequences of contingencies have been considered by studying cascade. This thesis concluded that there is no obvious indication in the post-contingency state that would predict a high amount of expected load shed or major blackout. Therefore, the results suggest that the progress of the cascade in the system should be considered.
The share of fluctuating in-feed in electricity production has increased during the last years and the share is to be expected to increase in the future in order to meet the renewable energy targets. These fluctuations may, however, cause problems in the operational planning and real time in terms of uncertain power flows of lines. In this thesis, a method to classify the power system security state has been presented that takes the fluctuations of in-feed into account. The method gives a probability for every system security state. If the probability of undesired states is too high, TSOs should take appropriate actions.

This thesis presents a method to consider fluctuations of in-feed in the estimation of severity of the contingencies. The results show that even though the traditional N-1 security assessment method states that the system is secure, the fluctuations of in-feed may cause a situation where the lines are overloaded and a cascade is triggered. In the end of the cascade, load may have to be shed. These results emphasize the need to consider also fluctuations or forecast errors of in-feed in the security assessment.

Finally, this thesis presents a method to perform a multi-lateral robust re-dispatch in order to release congestions in interconnected power systems that have fluctuating in-feed sources. The re-dispatch decision is based on an optimization problem that is an LP problem. The LP problem can be solved using standard commercial solvers. The formulation takes the fluctuations of in-feed into account and a violation of security limits is avoided with a certain probability $1 - \varepsilon$. Also a method to decide the optimal violation probability $\varepsilon$ is proposed. By using this optimal violation probability, an optimal operation of the system is achieved in terms of total operation costs of the system.
Chapter 7

Future Research

For the future, the following topics of research may be relevant.

This thesis has considered only thermal limits of lines as potential security limits. In the future, one direction could be to complement the methods presented to consider also voltage limits and dynamic phenomena. Even though, the DC power flow approximation and the thermal limits of lines are mainly the limiting factors in terms of security in Continental Europe, see Chapter 1, these contributions would make the methods proposed more comprehensive and applicable for systems that are not limited only by thermal limits of lines in terms of operation.

In reality, interconnected power systems are large systems that are computationally difficult to handle. Especially if complicated optimizations are run that have integer or binary variables, the computational burden comes high. Therefore, one important topic of further research could be to find ways to solve large optimization problems by applying new methods or by finding reasonable assumptions that make the problem solvable without losing too much in accuracy.
Appendix A

Test Systems

A.1 6-Bus Test System

The 6-bus test system used in simulations is described in this section and illustrated in Fig. A.1. In the system 1 p.u. is 100 MW. The system exports 1 p.u. of electricity to the second CA. The system has a total load of 9 p.u.

Net generation at nodes is

\[
P_{\text{net}} = \begin{bmatrix}
6 \\
1 \\
-6 \\
-1 \\
-2 \\
2
\end{bmatrix}.
\]

The reactance matrix of the system is

\[
\hat{X} = \begin{bmatrix}
8/9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1/9 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1/4 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1/3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1/5 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1/5 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1/6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/4
\end{bmatrix}.
\]
Figure A.1: 6-Bus test system.

The incidence matrix is

\[
T = \begin{bmatrix}
1 & -1 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & 0 & 0 \\
-1 & 0 & 0 & 1 & 0 & 0 \\
0 & -1 & 1 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 1 & 0 & -1 \\
0 & 0 & 0 & 0 & -1 & 1 \\
\end{bmatrix}.
\]

and the matrix \( X \) is used to build the nodal reactance matrix \( \tilde{B} \):

\[
X = \begin{bmatrix}
0 & 8/9 & 1/9 & 1/4 & 0 & 0 \\
8/9 & 0 & 1/3 & 0 & 0 & 0 \\
1/9 & 1/3 & 0 & 0 & 1/5 & 0 \\
1/4 & 0 & 0 & 0 & 1/5 & 1/6 \\
0 & 0 & 1/5 & 1/5 & 0 & 1/4 \\
0 & 0 & 0 & 1/6 & 1/4 & 0 \\
\end{bmatrix}.
\]
A.2 IEEE RTS-96 Test System

The IEEE RTS-96 test system [73] has been used in simulations. A modification done to the system is that the transformers of the system are considered as lines with a length of 10 miles. Moreover, the generation of the test system was decreased to match the load by decreasing output of generators proportional to their original output. These modifications are valid for all setups of this test system.

A.2.1 Three Area System without Wind

The three area system model of the IEEE RTS-96 test system has been presented in Fig. A.2. The model has been used in Chapter 3.

A.2.2 Three Area System with Wind

The three area system model of the IEEE RTS-96 test system with wind has been presented in Fig. A.3. Same assumptions has been used as in the model without wind. The model has been used in Chapter 4 to illustrate the method of security assessment with fluctuating in-feed in the system.

A.2.3 Single Area System

The one area model has been illustrated in Fig. A.4. The model has been used to classify the system security state with presence of fluctuating in-feed.

A.2.4 Two Area System

The two area model of the IEEE RTS-96 test system has been presented in Fig. A.5. The model has been used in simulations to illustrate the data exchange needed in Chapter 2 and in Chapter 5 to illustrate the robust re-dispatch of generators and to estimate the optimal violation probability for this method.
Figure A.2: IEEE RTS-96 test system.
Figure A.3: IEEE RTS-96 test system with wind in-feed.
Figure A.4: One area of the IEEE RTS-96 test system.
Figure A.5: Two areas of the IEEE RTS-96 test system.
Bibliography


Curriculum Vitae

June 18, 1983  Born in Vaasa, Finland

2007  Master of Science, Helsinki University of Technology, Finland

2010  Licentiate of Science, Aalto University, Finland

from 2009 on  PhD Student at ETH Zurich, Switzerland