Doctoral theses at NTNU, 2016:10

Emil Hillberg

Perception, Prediction and Prevention of Extraordinary Events in the Power System

NTNU
Norwegian University of Science and Technology

Doctoral thesis

Emil Hillberg

ISBN 978-82-326-1364-9 (printed ver.)
ISBN 978-82-326-1365-6 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2016:10

NTNU
Norwegian University of
Science and Technology
Thesis for the Degree of
Philosophiae Doctor
Faculty of Information Technology,
Mathematics and Electrical Engineering
Department of Electric Power Engineering

NTNU
Norwegian University of
Science and Technology

NTNU

Emil Hillberg

Perception, Prediction and Prevention of Extraordinary Events in the Power System

Thesis for the Degree of Philosophiae Doctor

Trondheim, January 2016

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

NTNU
Norwegian University of Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Information Technology, Mathematics and Electrical Engineering
Department of Electric Power Engineering

ISBN 978-82-326-1364-9 (printed ver.)
ISBN 978-82-326-1365-6 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2016:10

Printed by NTNU Grafisk senter

To Edith and Egon

Perception, Prediction and Prevention of Extraordinary Events in the Power System

Emil Hillberg

PREFACE

This thesis is submitted to the Norwegian University of Science and Technology (NTNU) in partial fulfilment of the requirements for the degree of *Philosophiae Doctor*, PhD.

This doctoral work has been performed during the period April 2009 – September 2012, at the Department of Electric Power Engineering at NTNU in Trondheim. Professor Kjetil Uhlen, NTNU, has been the main supervisor, with Adjunct Professor Gerd Kjølle, NTNU and SINTEF Energy Research, as the co-supervisor.

This doctoral work has been a part of the research project *Vulnerability and security in a changing power system* which is funded by *The Research Council of Norway* (project number: 191124) and the following Norwegian organisations: *BKK Nett AS, The Directorate for Civil Protection and Emergency Planning (DSB), Eidsiva Nett AS, Energy Norway, Fortum Distribution AS, Hafslund Nett AS, Lyse Elnett AS, NTE Nett AS, Norwegian Water Resources and Energy Directorate (NVE), Skagerak Nett AS, Statnett SF, Troms Kraft AS*.

ACKNOWLEDGEMENTS

This work has been funded through the project: *Vulnerability and security in a changing power system*, with additional financial support from SINTEF Energy Research which is gratefully acknowledged.

First I would like to thank my supervisors Professor Kjetil Uhlen and Adjunct Professor Gerd Kjølle for their continuous support and encouragement throughout this work and their active participation in publications and in the finalising of this thesis.

I would also like to express a special thanks to Associate Professor Trond "Toftis" Toftevaag, who, except for having actively participated in this work, generates a positive and creative working environment with his genuine interest and unsurpassed positive attitude – starting everyday with the question: *Er der liv?*

I am truly grateful for the involvement and the support that I have received during my PhD project, both from my colleagues at the Norwegian University of Science and Technology and at SINTEF Energy Research as well as from the interesting people from other organisations that I have had the opportunity to meet.
I would like to give a special thanks to Jarno Lamponen, Finnish Energy Market Authority and Professor Liisa Haarla, Aalto University School of Electrical Engineering, with whom I have been actively cooperating with during this work.

I would also like to thank everyone who have been contributing to my publications: Professor Emeritus Arne T. Holen and Dr. Til Kristian Vrana, NTNU; Dr. Oddbjørn Gjerde and Dr. Leif Warland, SINTEF Energy Research; Dr. Ritva Hirvonen, Fingrid; Dr. Walter Sattinger, Swissgrid; Agnes Nybø, Statkraft; Vegar Storvann, Frode Trengereid, Stig Løvlund, Jan Ove Gjerde, and Øyvind Breidablikk, Statnett.

Further, I would like to acknowledge: Assistant Professor Luigi Vanfretti, KTH Royal Institute of Technology, for introducing me in the IEEE Power & Energy Society; Professor Olav Fosso, NTNU, and Professor Göran Andersson, ETH Zürich, for involving me in the interesting work of the Hardanger Committee.

I would also like to thank my present employer, STRI, for the support during the finalisation of this thesis.

Finally I would like to thank all my friends and my family for their support and interest in my work – however abstract it may appear in my vain attempts to demystify the power system. A special thanks to my lovely, creative, and supportive wife Emelie.

December 16, 2015, Gamla Köpstad, Sweden

Emil Hillberg

ABSTRACT

Conventional risk and reliability assessment techniques are insufficient when it comes to analysing extraordinary events on-line. The reason for this lies in the nature of extraordinary events, which are the result of dependent or multiple failures leading to an unstable operation. Thus, novel and unconventional techniques are required to analyse and quantify the risk related to extraordinary events.

This thesis describes advances regarding *perception*, *prediction*, and *prevention* of extraordinary events. The focus of this work has been on the operation of the power system, where prediction and prevention of extraordinary events are required on-line and in the day-ahead operation planning.

A central part of the perception of extraordinary events lies in the identification of the transition from a stable to an unstable state being a fundamental and critical characteristic of extraordinary events. Together with the realisation that situational awareness is a requirement for the implementation of remedial actions, this provides a basis for the development of solutions to predict and prevent extraordinary events. A methodology for analysing extraordinary events is presented in this thesis, identifying the requirement to perform transient dynamic multi-level contingency studies to properly address the risk of extraordinary events.

Measures to improve the situational awareness are presented, in form of vulnerability indicators. These measures are of both a predictive and preventive nature, with vulnerability indicators supporting the operator to predict the risk of extraordinary events providing a decision base regarding implementation of manual preventive actions. Furthermore, a concept to assess the transfer capacity of critical power transfer corridors is presented. This concept is proposed to be utilised in the development of automatic controls, to prevent extraordinary events through appropriate mitigating actions.

The predictive and preventive measures presented in this thesis describe conceptual solutions for decreasing the risk of extraordinary events. These measures depend on further development of tools and techniques in order to be integrated in, and supportive for, the tools used for operating the power system.

SAMMANFATTNING

Denna avhandling beskriver forskningsresultat relaterade till stora strömavbrott av ett tekniskt ursprung, d.v.s. avbrott som inte är resultat av extrema väderpåkänningar eller andra icketekniskt relaterade orsaker.

Stora strömavbrott kan innebära kostnader för samhället med upp till flera miljoner kronor per avbrott. Underliggande orsaker till stora störningar i elkraftsystemet är i allmänhet komplexa att analysera då dessa händelser ofta innebär aktivering av många komponentskydd samt bortkoppling av en mängd komponenter i elkraftsystemet.

Avhandlingen ger en beskrivning av underliggande orsaker och händelseförlopp för att ge en ökad förståelse av stora strömavbrott. Då risken för strömavbrott är svår att uppskatta med hjälp av vedertagna verktyg, så innehåller denna avhandling en beskrivning av metoder specifikt utvecklade för att analysera dessa händelser. Avhandlingen innehåller även beskrivning av metoder för att motverka framtida strömavbrott.

En slutsats av denna forskning är att den studerade typen av strömavbrott är ett resultat av att elkraftsystemet blir instabilt. Detta innebär att åtgärder för att öka stabiliteten eller lösningar som snabbt kan tillämpas för att motverka instabilitet är av stor vikt för att hindra framtida strömavbrott. Även verktyg som förbättrar insikten i elkraftsystemets störningskänslighet bidrar till att öka systemoperatörens möjligheter att styra systemet med en godtagbar risknivå.

STRUCTURE OF THE THESIS

The thesis is divided in two parts, where the first part includes a summary and clarification of the concepts and contributions of this work, while the second part consists of appended papers which include the main results and conclusions of the work performed during this PhD project.

PART I – MAIN REPORT

In Chapter 1, the background of the PhD work is described together with the specification of objective, scope and limitations. This chapter also provides an overview of the scientific contributions that are the main outcome of this PhD project.

Perception of extraordinary events is presented in Chapter 2. This provides suggestions on how to classify extraordinary events based on their main attributes related to: sequence, cause, and mitigating solutions. The core contributions to support an increased understanding of extraordinary events originate from the identification and definition of critical characteristics.

Prediction of extraordinary events is described in Chapter 3. Here the criteria from risk, reliability, and stability analyses together with the fundamental characteristic of extraordinary events form a framework for the methodology to predict and assess the risk of extraordinary events.

Measures for *prevention* of extraordinary events are presented in Chapter 4, including results from case studies used to test these solutions.

A summary of the appended papers is provided in Chapter 5. This includes a description of the author’s contribution and the relevance that each paper has to this thesis.

A summary of this thesis is presented in Chapter 6, including conclusions and discussions, as well as suggestions for future work.

Appendices are included at the end of Part I of the thesis, providing information about dynamic models used for studies of the *IEEE Reliability Test System 1996* and the consequence data of historical extraordinary events.

PART II – APPENDED PAPERS

Below follows a list of the papers which are appended at the end of this thesis. In Section 1.3, *Scientific Contributions*, these papers are referred to as Papers I-V, while in the rest of the thesis regular references are used.

Paper I
Emil Johansson, Kjetil Uhlen, Agnes Nybø, Gerd Kjølle, & Oddbjørn Gjerde
*Extraordinary events: understanding sequence, causes, and remedie*s
European Safety & Reliability Conference, 2010, Rhodes, Greece
(Johansson et al. 2010)

Paper II
Emil Johansson, Kjetil Uhlen, Gerd Kjølle & Trond Toftevaag
Reliability evaluation of wide area monitoring applications and extreme contingencies
Power Systems Computation Conference, 2011, Stockholm, Sweden
(Johansson et al. 2011b)

Paper III
Emil Hillberg, Frode Trengereid, Øyvind Breidablik, Kjetil Uhlen, Gerd Kjølle, Stig Løvlund & Jan Ove Gjerde
System integrity protection schemes – increasing operational security and system capacity
CIGRE Session, 2012, Paris, France
(Hillberg et al. 2012c)

Paper IV
Emil Hillberg, Jarno Lamponen, Liisa Haarla & Ritva Hirvonen
Revealing stability limitations in power system vulnerability analysis
Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, 2012, Cagliari, Italy
(Hillberg et al. 2012b)

Paper V
Emil Hillberg & Trond Toftevaag
Equal-area criterion applied on power transfer corridors
IASTED Asian Conference on Power and Energy Systems, 2012, Phuket, Thailand
(Hillberg and Toftevaag 2012)

Paper VI
Jarno Lamponen, Emil Hillberg, Liisa Haarla & Ritva Hirvonen
The change of power system response after successive faults
Power Systems Computation Conference, 2014, Wroclaw, Poland
(Lamponen et al. 2014)

Although not part of this thesis, the author has contributed to the following publications during the PhD project:

Vegar Storvann, Emil Hillberg & Kjetil Uhlen
Indicating and Mitigating Voltage Collapse
IEEE/PES Innovative Smart Grid Technologies, 2012, Berlin, Germany
(Storvann et al. 2012)

J. Pierre, D. Trudnowski, C. Cañizares, L. Dosiek, H. Ghasemi, M. Gibbard, E. Johansson, G. Ledwich, R. Martin, E. Martinez, L. Vanfretti, D. Vowles, R. Wies, N. Zhou
Identification of Electromechanical Modes in Power Systems, Chapter 2: Mode-Meter Analysis Methods
IEEE Task Force Report, Special Publication TP462
(IEEE 2012)

Emil Hillberg, Arne T. Holen, Göran Andersson & Liisa Haarla
Power System Reinforcements – the Hardanger Connection
ELECTRA no. 260, p. 4-15, Feb. 2012
(Hillberg et al. 2012a)

Emil Johansson, Kjetil Uhlen & Gerd Kjølle
Mitigating Extraordinary Events using Wide Area Monitoring Applications
CIGRE International Symposium, 2011, Recife, Brazil
(Johansson et al. 2011a)

Til Kristian Vrana & Emil Johansson
Overview of Analytical Power System Reliability Assessment Techniques
CIGRE International Symposium, 2011, Recife, Brazil
(Vrana and Johansson 2011)

Luigi Vanfretti, Rodrigo García-Valle, Kjetil Uhlen, Emil Johansson, Daniel Trudnowski, John W. Pierre, Joe H. Chow, Olof Samuelsson, Jacob Østergaard & Kenneth E. Martin
Estimation of Eastern Denmark's Electromechanical Modes from Ambient Phasor Measurement Data
IEEE/PES General Meeting, 2010, Minneapolis, Minnesota, USA
(Vanfretti et al. 2010)

NOTATION

HILP	*High Impact Low Probability event* – relating to extraordinary events, extreme contingencies, large disturbances, or blackouts; having a potentially high impact on society and a low probability to occur.
PMU	*Phasor Measurement Unit* – providing synchronised measurements of voltage and current phasors, i.e. measuring the system state which otherwise is estimated.
PTC	*Power Transfer Corridor* – interconnections between areas or systems, where transfer capacities may act as bottlenecks to the system at specific operating scenarios.
SA	*Security Assessment* – methods to evaluate the ability of the power system to remain in stable operation when subjected to pre-defined disturbances, including the analysis of transient phenomena in the power system. Often the term *dynamic security assessment (DSA)* is used when relating to SA based on dynamic simulations.
SCADA	*Supervisory Control And Data Acquisition* – system for collecting measurements and other data to provide the operator with information on the operating state of the power system.
SE	*State Estimator* – estimating the system state, typically based on measurements gathered by the SCADA system.
SIPS	*System Integrity Protection Schemes* – providing protection against system separation and instability, used to increase security and to mitigate extraordinary events. Other terms, such as: *special protection systems* (SPS), *system protection schemes* (SPS), and *remedial action schemes* (RAS), are commonly used in the literature.
WAMS	*Wide Area Monitoring Systems* – system for improved monitoring applications utilising measurements from multiple PMU installations. Acronyms related to *wide area control systems* (WACS), *protection systems* (WAPS), as well as *monitoring-control-and-protection* (WAMPAC) are also found in the literature.

CONTENTS

APPENDICES

PART II APPENDED PAPERS

Paper II: *Reliability evaluation of wide area monitoring applications and extreme contingencies, E. Johansson, K. Uhlen, G. Kjølle & T. Toftevaag*

Paper III: *System integrity protection schemes – increasing operational security and system capacity, E. Hillberg, F. Trengereid, Ø. Breidablik, K. Uhlen, G. Kjølle, S. Løvlund & J. O. Gjerde*

Paper IV: *Revealing stability limitations in power system vulnerability analysis, E. Hillberg, J. Lamponen, L. Haarla & R. Hirvonen*

Paper V: *Equal-area criterion applied on power transfer corridors, E. Hillberg & T. Toftevaag*

Paper VI: *The change of power system response after successive faults, J. Lamponen, E. Hillberg, L. Haarla & R. Hirvonen*

LIST OF FIGURES

PART I
MAIN REPORT

CHAPTER 1
INTRODUCTION

1.1 Background

It is a well-established fact that a reliable supply of electric power is critical for the modern society. Since the function of the power system is to satisfy the system demand, a reliable supply of electric power implies that the power system itself needs to be sufficiently reliable and resilient to failures. It is therefore important to study and understand the risks related to failures that may cause widespread interruptions of the electric power, i.e. extraordinary events. This serves as the motivation behind this PhD work, where focus has been on increasing the understanding of extraordinary events and developing solutions to decrease the risk of future blackouts from an operational perspective.

Extraordinary events in the electric power system refer to disturbances with potentially high societal impact and low probability to occur. Extraordinary events are referred to as blackouts, extreme contingencies, large disturbances, or sometimes as high impact - low probability (HILP) events.

As the power systems become increasingly interconnected, extraordinary events may have an impact over large areas affecting the population of multiple countries. The Nordic power system, shown in Figure 1, is an example of a power system spanning several countries, where Norway, Sweden, Finland, and the eastern part of Denmark are synchronously interconnected. The system is further interconnected to the power systems in the surrounding area through multiple asynchronous connections to the Netherlands, Germany, Poland, Estonia, Russia, and the western part of Denmark.

The consequences of extraordinary events are widespread power interruptions, or even total blackout of an entire power system, resulting in considerable socio-economic losses and costs. Logically, it is impossible to prevent all unforeseen events in the power system; however, there is a high economic incentive to mitigate the consequences of the extraordinary events that do occur. As an example, the blackouts that occurred 2003 in the Eastern Interconnected power system, on August 14, and in the Nordic power system, on September 23, have an estimated cost between 4-10 billion U.S. dollars and 0.5-2 billion Swedish kronor, respectively, (ELCON 2004; Energimyndigheten 2004).

The risk of large disturbances, quantified by probability and consequence, may be of a similar level as the risk of smaller disturbances, as described by (Carreras et al. 2004). However, due to the uncertainties related to the probability and consequence of extraordinary events, there are difficulties to economically justify major reinforcements of the power system only based on decreasing the risk of extraordinary events, (IEEE 2007; CIGRE 2010b). Furthermore, investments in new transmission lines may be highly controversial, where the recent case concerning the Hardanger connection in Norway serves as an illustrative example, (Hillberg et al. 2012a). Solutions to decrease the risk of extraordinary events are therefore often focused on improvements related to the operation and control of the power system in areas such as monitoring and protection related to e.g.: wide area monitoring systems (WAMS), or system integrity protection schemes (SIPS).

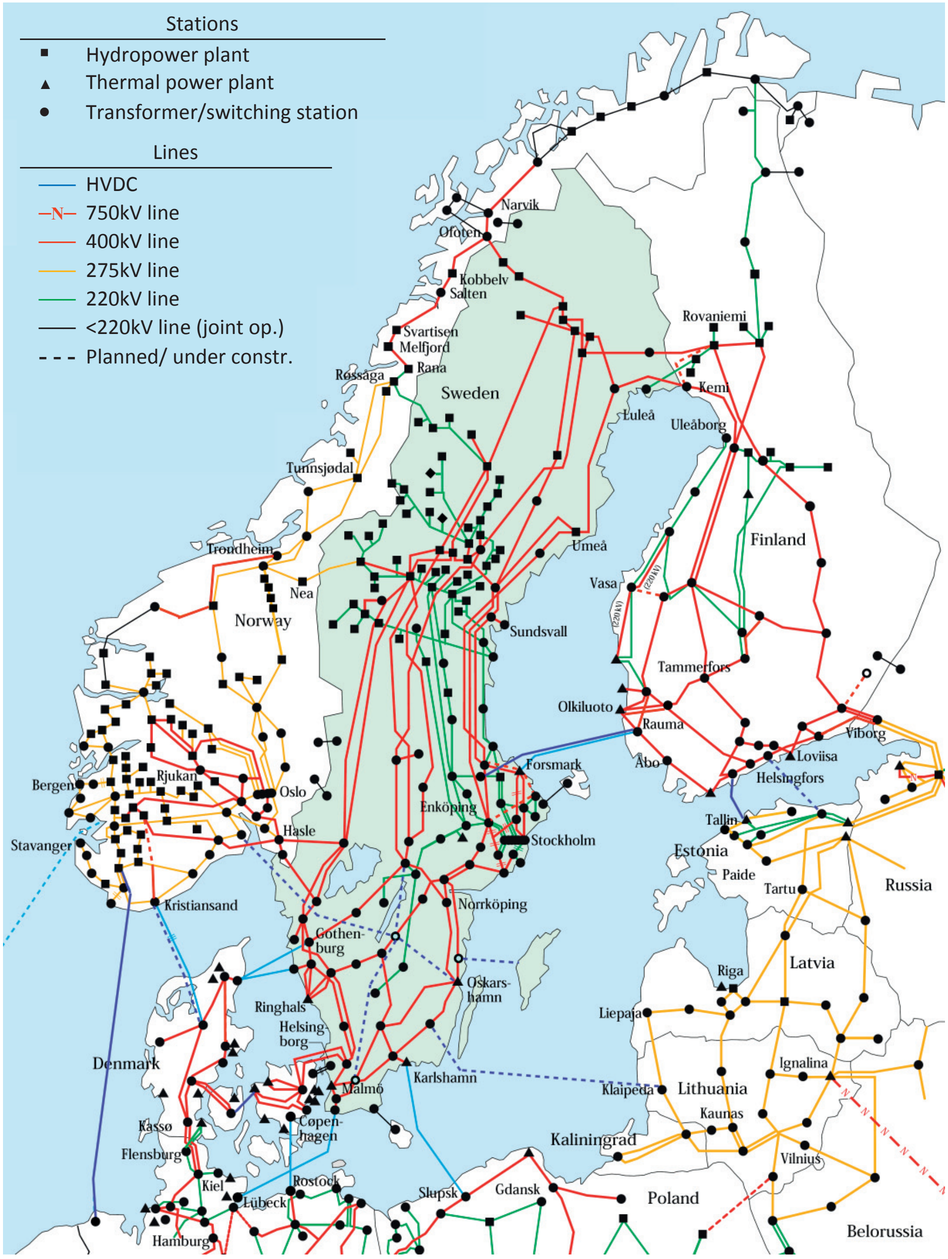

FIGURE 1: MAP OF THE NORDIC POWER SYSTEM, AS PER 2012, FROM (SVK 2012)

1.2 Objective, scope, & limitations

The objective of this PhD project has been to *develop models and methods to analyse the risk of extraordinary events*, having the goal to *increase the security and/or utilisation of the power system*.

In order to meet the objective, it has been necessary to obtain in-depth understanding of extraordinary events as well as knowledge of methods used to analyse the risk and reliability of the power system.

It should be noted that this work has been focusing on the analysis of extraordinary events from an operational point of view, and not from a planning perspective.

The following research questions have been defined:

- *What are the critical characteristics of extraordinary events?*
- *How can the risk of critical characteristics of extraordinary events be addressed?*
- *How can critical characteristics of extraordinary events be averted?*

To be able to answer these questions, the scope of the work has been divided in three main areas:

1. **Perception of extraordinary events**: categorisation of events, analysis of causes, and identification of critical characteristics
2. **Prediction of extraordinary events**: identification of study requirements and the development of a framework and methodology to analyse extraordinary events
3. **Prevention of extraordinary events**: assessment of methods to prevent extraordinary events, including solutions for:
   i. Improved situational awareness of the operating state – through vulnerability indicators.
   ii. Improved instability prevention – through methods for stability assessment and active mitigation using advanced protection and control techniques.

Other promising mitigating solutions, such as advanced islanding schemes and restoration procedures are excluded from the scope of this work.

The work of this thesis has been focusing on the operation of the power system, where prediction and prevention of extraordinary events are required on-line and in the day-ahead operation planning. This means that methods to decrease the risk of extraordinary events from a longer planning perspective, e.g. preventive maintenance, have not been studied.

Further limitations to this work relate to the risk space and the type of events:

- The risk and reliability analyses described in this thesis are limited only to extraordinary events, meaning that they do not reflect the total risk or reliability level of the power system.
- The extraordinary events considered in this thesis are limited to events initiated by factors related to the power system, referred to as *power system initiated extraordinary events*.

1.3 Scientific contributions

Increased understanding of extraordinary events in the electric power system is vital to develop *risk analysis models and methods*, and to implement appropriate remedies in order to limit the presence and consequences of future extraordinary events.

The scientific contributions of this PhD project are summarised in this section, with detailed descriptions provided in Chapters 2, 3, and 4. The scientific contributions are divided into the three research areas:

A. Perception of extraordinary events
B. Prediction of extraordinary events
C. Prevention of extraordinary events

A. PERCEPTION OF EXTRAORDINARY EVENTS

The ability to identify power systems vulnerabilities to extraordinary events lays the foundation to the question of perceiving extraordinary events. This PhD work contributes to improve the perception of extraordinary events with the following aspect, referred to as scientific contribution A_1:

> *Identification of the transition to unstable operation as a fundamental and critical characteristic of extraordinary event.*

Previous studies have identified and described the similarities between many historical extraordinary events, regarding characteristics, sequence, and causes. Many studies describe how instability phenomena have occurred during specific events, and how this may be prevented in the future. However, the instability aspect has not previously been identified as the critical state of any blackout. In Chapter 2, it is described how the response of the power system changes after the transition to unstable operation – illustrating the criticality of the stability aspect for analysing of extraordinary events.

B. PREDICTION OF EXTRAORDINARY EVENTS

The ability to assess how vulnerable a power system is to extraordinary events lays the foundation to the question of predicting extraordinary events. This PhD work contributes to an improved prediction of extraordinary events by providing a methodology and a framework for analysing risk and vulnerability of extraordinary events during on-line operation and in the day-ahead operation planning.

Risk, reliability, and stability of the power system together define the set of requirements for analysis and prediction of extraordinary events. These requirements are presented in Chapter 3 of this thesis, providing the basic framework for the analysis of extraordinary events. These requirements may be summarised into the following statement, which is considered the first contribution to an improved prediction of extraordinary events referred to as scientific contribution B_1:

> *It is a necessity to perform transient dynamic multi-level contingency analyses on-line to be able to assess the risks and vulnerabilities related to extraordinary events during operation of the power system.*

Chapter 3 also provides a description of a methodology to analyse extraordinary events, together with two means to indicate vulnerabilities in the system. These indicators aim to provide on-line information of the systems vulnerabilities to the operator, and are regarded as the second contribution to an improved prediction of extraordinary events referred to as scientific contribution B_2:

> *Vulnerability indicator k_{min} and visualisation of the $N - k$ secure operating region.*

These indicators should not be regarded as operating criteria (such as the $N - 1$ criterion), but as indicators of the systems vulnerability to extraordinary events. Due to the significant uncertainties of assessing the risk of extraordinary events in terms of probability and consequence, this methodology focuses on assessing the shortest distance to undesired events. Implementing this methodology requires tools to perform multilevel transient dynamic contingency analyses on-line, the development of such tools have not been part of the scope of this work.

C. PREVENTION OF EXTRAORDINARY EVENTS

The ability to mitigate the causes of extraordinary events lays the foundation to the question of preventing extraordinary events. This PhD work contributes to the prevention of extraordinary events through solutions related to enhanced situational awareness.

The vulnerability indicators k_{min} *and the $N - k$ secure operating region*, presented as scientific contribution B_2, may be utilised both in the prediction and prevention of extraordinary events. The implementation of k_{min} as an on-line predictor, i.e. a leading vulnerability indicator, would be especially useful in order to provide information on how the vulnerability may develop for future operating states. These indices provide enhanced awareness regarding multiple contingencies related to the actual and the predicted operating states, thus providing the operator with improved possibilities to implement actions to prevent extraordinary events.

The equal-area criterion is utilised to assess the secure power transfer capacity of critical power transfer corridors of the system, presented in Chapter 4. This concept is considered a contribution to preventing extraordinary events, referred to as scientific contribution C_1:

> *The EAC on PTC concept*

This concept is applicable in cases where a sub-system may be identified wherein all machines are defined as critical machines, i.e. where a critical contingency result in the acceleration of all synchronous machines within one sub-system relative the rest of the system. The tie-lines interconnecting the sub- and main systems may then be defined as a critical power transfer corridor on which the *EAC on PTC* concept can be applied.

The *EAC on PTC* concept is not to be regarded as an entirely novel methodology, but as a novel way of utilising previously developed equal-area criteria methods.

Chapter 4 provides a description on how to utilise the *EAC on PTC* concept when developing system integrity protection schemes (SIPS) designed to prevent extraordinary events.

CHAPTER 2
PERCEPTION OF EXTRAORDINARY EVENTS

2.1 Background

Extraordinary events in the electric power system refer to disturbances with potentially high societal impact and low probability to occur. Extraordinary events are referred to as blackouts, extreme contingencies, large disturbances, or sometimes as high impact - low probability (HILP) events.

In order to address the risk of extraordinary events the events themselves need to be understood. This chapter deals with: classification and categorisation of events, identification of event sequences and critical characteristics, as well as analysis of causes and possible remedies.

2.2 Classification of extraordinary events

Extraordinary events in the electric power system refer to disturbances with potentially high societal impact and low probability to occur. Extraordinary events are referred to as blackouts, extreme contingencies, large disturbances, or sometimes as high impact - low probability (HILP) events.

As each extraordinary event is unique, there are many possibilities to classify the events into groups. One possibility to classify the events is their main cause. In this thesis, the following two categories of extraordinary events are defined:

1. ***Natural hazard events****: events caused mainly by factors related to the environment, such as adverse weather (extreme wind, icing etc.) or natural disasters (e.g. forest fires, landslides, earthquakes, or volcanic eruptions).*
2. ***Power system initiated events****: events where the main causes originate from technical or operational failures in the power system (e.g. component malfunction, faulty protective actions, operator errors, or overloading).*

Extraordinary events which are not included in these two categories such as deliberate or accidental actions by a third party are not addressed in this thesis.

Disturbance duration and magnitude may be used for classifying the criticality of extraordinary events in a specific power system, as explained by (Doorman et al. 2004) and (Doorman et al. 2006). These two consequence dimensions, i.e. time and disconnected load, are utilised in Figure 2 to describe the consequences of some historical extraordinary events.

Figure 2 presents events that occurred around the world between 1965 and 2009. The events categorised as natural hazard events or power system initiated events are marked in the figure by a circle or triangle, respectively. The outage data are based on information provided by several studies, where the approximated average duration, disconnected load, and energy not supplied is collected in Appendix B.

As shown in Figure 2, it is possible to differentiate between the two defined event categories. This apparent distribution of events originates mainly from the duration of the event, and is based on the difference between these two event categories, namely their impact on society:

> *Natural hazard events* are often characterised by extensive tripping and destruction of power system components. Such direct impact on the mechanical structures of the power system, as well as on other infrastructures, may significantly delay the restoration process prolonging the duration of the blackout.

> *Power system initiated events* have a relatively short duration, since, if no major mechanical breakdown occurs, restoration mainly relates to the re-energisation and re-synchronisation of power system components.

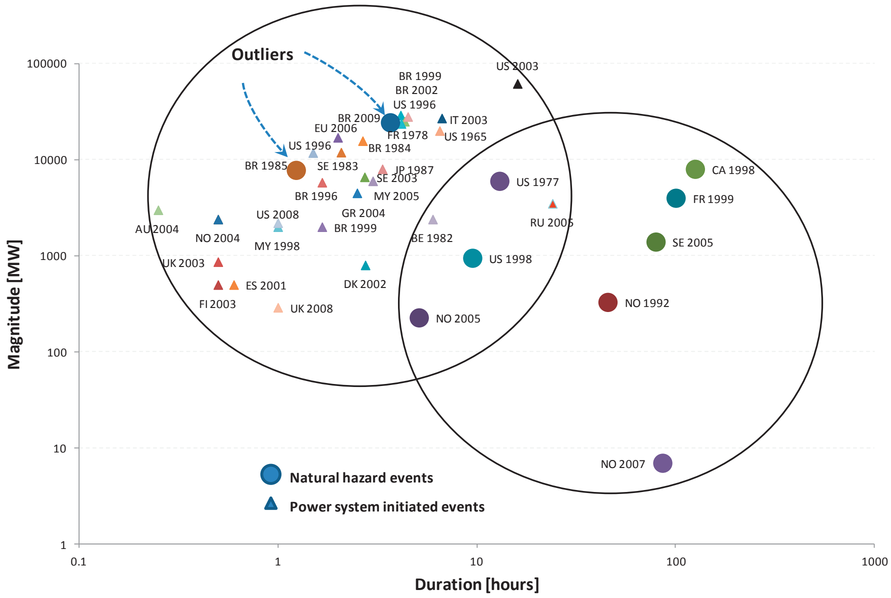

FIGURE 2: HISTORICAL EXTRAORDINARY EVENTS,
CATEGORISED AS NATURAL HAZARD EVENTS OR POWER SYSTEM INITIATED EVENTS,
MARKED BY A CIRCLE OR TRIANGLE, RESPECTIVELY

Since the duration of an event depends on several factors, such as the type and location of faults, the location and availability of resources, and the predefined emergency procedures, there are several outliers to this general distribution of events, as indicated in Figure 2.

Similarly as the causes and duration differentiate the two event categories, so do the most obvious counteractions:

> *Natural hazard events* may in many cases be prevented by increased mechanical dimensioning of power system components and structures, and locating them in a less exposed environment.
>
> *Power system initiated events* may in many cases be prevented by increased electrical dimensioning of power system components, including more backup and parallel connections.

Dimensioning the power system to withstand extraordinary events is normally limited by financial restrictions.

In this thesis, only extraordinary events initiated by factors related to the power system have been studied. Therefore, in the rest of this thesis, the term *extraordinary event* is referring only to *power system initiated events*.

2.3 Sequence of extraordinary events

Many historical extraordinary events have similarities when it comes to the sequence of the event. The possibility to express events following a generic sequence has been proposed in several studies, such as: (Knight 1989; Efimov and Voropai 2006; Lu et al. 2006; Pourbeik et al. 2006; IEEE 2007).

The sequence of extraordinary events presented in this thesis, illustrated in Figure 3, is described by the following stages:

1. Originating from a normal operating state, the sequence of events is triggered by a failure with an unforeseen impact on the operation of the power system. The failure moves the operation into an alert state where the system is vulnerable to further failures. Correct remedial actions are necessary to prevent the system from deteriorating.
2. Depending on the utilisation and topology of the grid, either thermal aspects or stability are the limiting factors in the next phase:
   i. The thermal overloading will lead to protective actions, disconnecting components in a cascaded manner. Remedial actions are required to prevent instability, and often there is enough time to implement such actions manually.
   ii. At a certain point, stability limits are exceeded. **This marks the critical point of the event and from this point onwards the system is unstable.** Remedial actions are imperative to regain stable operation.
3. The instability initiated cascade is characterised by power and frequency oscillations, voltage decay, and a decay or rise in frequency. This leads to the triggering of multiple component protections, and the affected region may be widespread. This phase is very fast and in most cases only predefined automatic remedial actions are able to limit the extent of the cascade.
4. The system will eventually stabilise in a restorative operating state, characterised by several unsynchronised islands, some of which experiencing a total blackout due to the generation facilities of the island being unable to meet the demand.

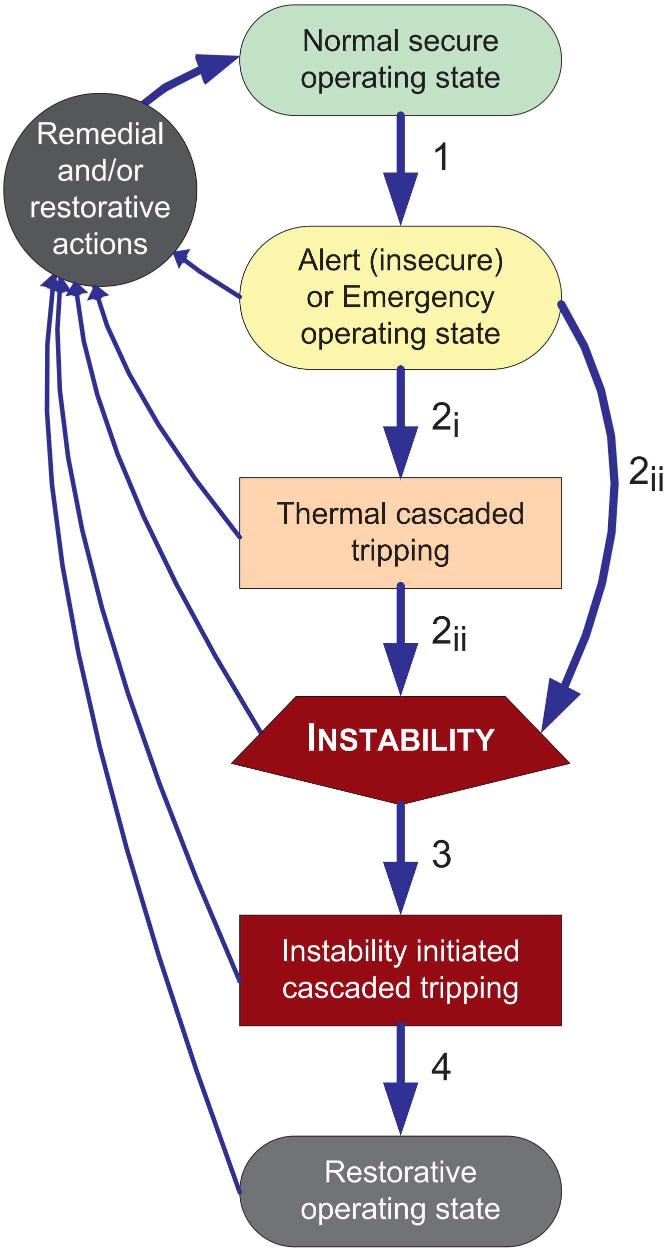

FIGURE 3: GENERIC SEQUENCE OF EXTRAORDINARY EVENTS

The generic sequence presented in Figure 3 provides new insight into the behaviour of extraordinary events in the way that the system always reaches instability before a blackout occurs. In (Hillberg et al. 2012b), it is explained that the violation of stability limits constitutes a fundamental part of any extraordinary event, and that there is a considerable difference between the system response before and after this point.

> Before this point, remedial actions may constitute manually implemented corrective actions. In this way, the consequences of the event may be limited and the system can be restored into another secure operating state.
>
> After stability limits have been violated, remedial actions are only possible through predesigned automatic control and protection systems. Such remedial actions are difficult to design and increases the complexity of the power system, but if an instability initiated cascade is not prevented the system will face a large and uncontrolled disturbance.

Thus, in order to properly understand and analyse extraordinary events it is imperative to acknowledge the criticality of the transition from stable to unstable operation. This implies that the transition from stable to unstable operation should constitute the core in any risk analysis of extraordinary events. Therefore, in this thesis:

The transition from stable to unstable operation *is defined as a fundamental and critical characteristic of an extraordinary event.*

2.4 Causes of extraordinary events

Causes of extraordinary events are complex and several factors influence the final consequences of an event. Causes may be divided into root causes and contributing causes, which are in (DOE 1992) defined as:

> A root cause is *the cause that, if corrected, would prevent recurrence of this and similar occurrences.*
>
> A contributing cause is *a cause that contributed to an occurrence but, by itself, would not have caused the occurrence*.

Hence, identification of the real root causes is important to mitigate future extraordinary events. Differentiation between root and contributing causes can however be difficult, and may also be very case specific. Some general aspects of root and contributing causes are presented in (Johansson et al. 2010):

- Extraordinary events may have several contributing causes but only one single or a few root causes.
- Root causes of power system initiated events are more often related to system operation than to actual equipment failure.
- Contributing causes are often directly related to failure and excessive or premature disconnection of equipment; with hidden failures of protective equipment as a recurrent contributor.

Based on the analysis of historical extraordinary events, presented in (Johansson et al. 2010), the insufficient situational awareness is identified as a root cause of significant importance. The reason for behind the importance lies in the relationship between situational awareness and the implementation of remedial actions:

> If an operator or an automated system is unaware of the vulnerabilities that the system is facing, it is unlikely that the correct remedial actions are taken which could have mitigated the consequences of an event.

Thus, insufficient situational awareness makes the system increasingly vulnerable to extraordinary events since the system may be exposed to completely other threats than those that the operator are aware of. From the studies of historical blackouts, it is clear that enhancements of the situational awareness may contribute significantly to decrease the power systems vulnerability to extraordinary events. Therefore, in this thesis:

The lack of situational awareness *is defined as a significantly important cause of extraordinary events.*

2.5 Mitigation of extraordinary events

As indicated in Figure 3, remedial actions are important at every stage of an extraordinary event. Remedial actions are here referring to actions, either manual or automatic, taken to limit the consequences of an event and maintain the integrity and stability of the power system.

The possibility to implement remedial actions to prevent a large disturbance lies in the situational awareness of the operator or the dedicated control or protection system. This means that enhanced monitoring solutions, enabling improved situational awareness, can provide essential contributions to reduce the vulnerabilities in the power system and to decrease the risk of extraordinary events.

Uncontrolled system sectioning, as a result of instability, often leads to a blackout due to insufficient awareness and control of the islanded power systems. This implies that controlled islanding can limit disturbance propagation and the consequences of extraordinary events. A well functioning automated islanding scheme may be the difference between total system blackout and controlled load shedding.

Automated actions to mitigate extraordinary events are often implemented as system protections, here referred to as system integrity protection schemes (SIPS)[1].

The functionality of various SIPS controls is explained in e.g. (CIGRE 2007a), including actions such as: *generation rejection, turbine fast valving, fast unit start-up, automatic generation control (AGC) action, under frequency load shedding (UFLS), under voltage load shedding (UVLF), remote load shedding, automatic shunt switching, braking resistor, generator voltage set point change, controlled system separation, tap changer blocking, SVC voltage control, HVDC special control*.

As illustrated by Figure 4, the response time of SIPS actions has a similar time frame as the transient stability phenomena of the power system, implying the possibility of SIPS actions to improving the transient stability of the power system.

[1] Several other terms and acronyms are used when referring to this kind of protection scheme, such as *special protection systems*, *system protection schemes*, or *remedial action schemes*, (Anderson and LeReverend 1996; CIGRE 2001; Madani et al. 2010). Due to the different terminology found in the literature, the use of these expressions has become rather mixed. In this thesis, the expression *system integrity protection schemes* is used since there is a tendency in the literature to use this more precise term, and I consider this as best reflecting the functionality of these protection schemes.

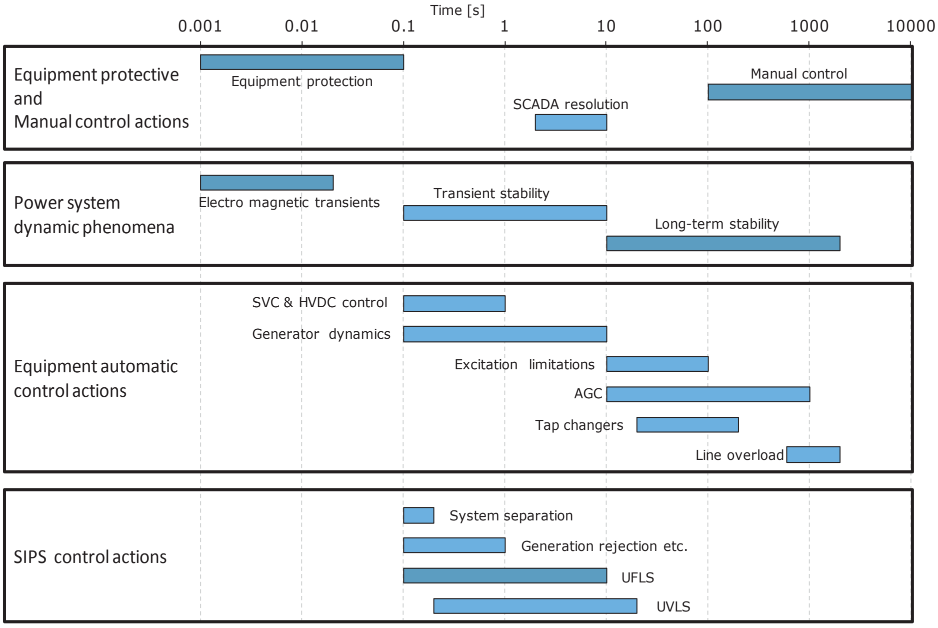

FIGURE 4: TIME FRAME OF POWER SYSTEM RELATED PHENOMENA, BASED ON (CIGRE 2001; NOVOSEL ET AL. 2004)

System integrity protection schemes are increasingly utilised in power systems worldwide to provide additional power transfer capacity and enhanced reliability. In the Norwegian power system, SIPS implementation has been progressing since the 1980s and today generation rejection schemes control 20% of the installed capacity (Hillberg et al. 2012c). This intensified SIPS penetration implies an augmented operational demand in terms of both utilisation and complexity of the power system.

As noted by (Patel et al. 2004), it is important that any SIPS implemented actions are sufficiently coordinated with component protection in order to achieve the required remedial action to mitigate an extraordinary event.

In many ways, the installation of phasor measurement units (PMU) provides the means of improvements based on synchronous monitoring of voltage and current phasors throughout the power system. This is described by e.g. (Phadke et al. 1983) and (Phadke and Thorp 2006).

2.6 Summary

Each extraordinary event is unique; hence, there are many possibilities to classify the events into groups. The group of extraordinary events studied in this thesis is referred to as *power system initiated extraordinary events.*

Power system initiated extraordinary events originate from technical or operational failures in the power system, such as component malfunction, faulty protective actions, human errors, or overloading. This type of events can be characterised by the relatively short duration of the interruption. Since the events do not involve major mechanical breakdown, the restoration procedure is normally fast and mainly concerns re-energisation and re-synchronisation of power system components. In this thesis, only *power system initiated extraordinary events* are studied. Therefore, the term extraordinary event is used in this thesis to refer to *power system initiated extraordinary events* if not stated otherwise.

From the study of historical events, a generic sequence of events is presented in this chapter which emphasises the criticality of the state of instability as a fundamental part of extraordinary events. In this thesis, the *transition from stable to unstable operation* is defined as a fundamental and *critical characteristic of extraordinary events*. This reflects new insights into the behaviour and characteristics of extraordinary events and is therefore referred to as scientific contribution A_1.

As each extraordinary event is unique, the generic root causes of extraordinary events are difficult to identify, but the number of root causes of a single event are typically very low and more often related to the operation of the system than to actual equipment failure. Inadequate situational awareness is identified as a root cause to many events, and should be regarded as a main vulnerability to the system when it comes to extraordinary events. Remedial actions are important to prevent extraordinary events. The possibility to implement remedial actions lies in the situational awareness of the operator or the dedicated control or protection system as well as in the impact of the action taken. This implies that enhanced monitoring solutions, enabling improved situational awareness, as well as improved functionality of automated actions can provide essential contributions to decrease the risk of extraordinary events in the power system.

CHAPTER 3
PREDICTION OF EXTRAORDINARY EVENTS

3.1 Background

In order to predict extraordinary events, tools and techniques able to identify and analyse critical event characteristics are required. From the perception of extraordinary events, described in Chapter 2, the transition to unstable operation is identified as a fundamental characteristic of extraordinary events. With stability being an aspect of reliability, which is one of several aspects incorporated in the general concept of risk, these three interrelated disciplines are in focus when it comes to the possibility of predicting extraordinary events.

Sections 3.2-3.4 provide general descriptions of risk, reliability, and stability concepts, as well as on their relevance to the analysis of extraordinary events. The introduction to risk, reliability, and stability forms the basic framework and requirements to analyse extraordinary events. This framework is utilised to develop the methodology for analysing risk of extraordinary events presented in section 3.5. Two means of indicating vulnerabilities in the system are presented, referred to as: the k_{min}*-index* and the $N-k$ *secure operating region*.

3.2 Power system risk

Power system risk relates to multiple aspects, such as: safety, reliability, environmental, financial, and reputational. In this thesis, the focus is on risk related to reliability, and specifically to *power system initiated extraordinary events*. The risk of such events reflects only a subset of the *total* risk space, as illustrated by Figure 5. This means that the risk and reliability analyses described in this thesis are limited only to extraordinary events; hence, these studies do not describe the total risk or reliability level of the power system.

In this section, general concepts of risk are described, including different definitions of risk and the description of two conventional risk assessment methods. The section also provides a discussion of power system risk in relation to the analysis of extraordinary events.

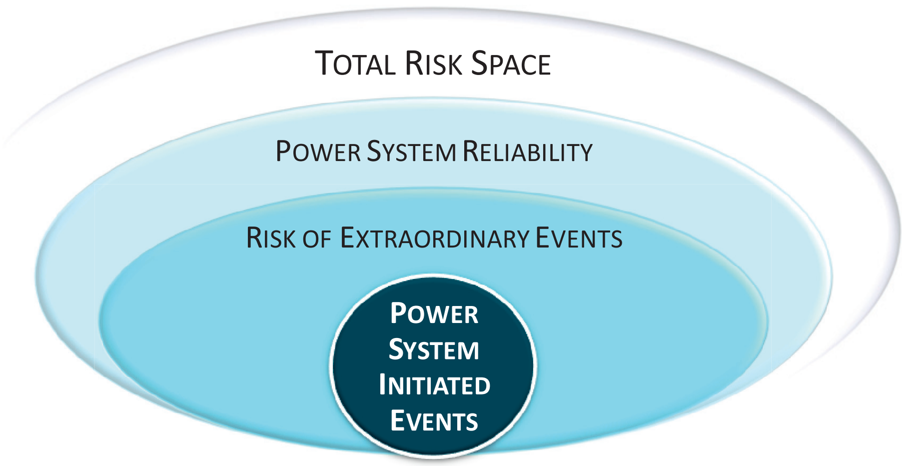

FIGURE 5: RISK OF POWER SYSTEM INITIATED EXTRAORDINARY EVENTS, A SUBSET OF THE TOTAL RISK SPACE

3.2.1 Definitions of risk

There are various definitions of risk, where an example is the definition in (ISO 2009) stating that *risk is the effect of uncertainty on objectives*. (Nordgård 2010) presents a list of risk definitions, which is partly reproduced here:

Risk is:

- *a situation of uncertain outcome, where something of human value is at stake.*
- *the uncertainty of: outcome, actions and events.*
- *the expected loss.*
- *the expected disutility.*
- *the probability of adverse outcome.*
- *the uncertain consequence of an event.*
- *the two-dimensional combination of consequences and uncertainty.*
- *a set of scenarios, each with a probability and a consequence.*

These relatively wide definitions imply that risk may be interpreted, expressed and assessed in various ways.

In this thesis, no specific risk definition is preferred; instead risk is identified as the quantifiable danger depending on: the point of view of the beholder, the focus of the study, and the extent of the modelled system.

Vulnerability may be defined as *an expression of the problems a system will face maintaining its function when exposed to threats, and the problems the system faces resuming its activities after the event occurred*, (Kjølle et al. 2012). As vulnerability is considered a component of risk, vulnerability indicators may be utilised to quantify risk from a certain perspective.

3.2.2 Risk assessment methods

As the variety of risk definitions implies, risk may be quantified by different parameters. In (ISO 2009), it is noted that risk is often expressed as a combination of the *probabilities* and the *consequences* of the event.

Two conventional risk assessment methods, which utilise probability and consequences to quantify risk, are the *fault tree* and *event tree* methods. Figure 6 illustrates the fault and event trees in a bow-tie model, where threats lead to an undesired event further resulting in consequences. As the figure implies, the undesired event defines the interconnection between the fault and event trees; hence the definition of the undesired event is a key factor in this type of risk assessment method.

> In a fault tree analysis, the probability of the undesired event is assessed, based on threats, barriers, and logical interrelations (marked in Figure 6 as $T_{1\text{-}3}$, B_{F1}, and AND-/OR- gates, respectively). Barriers, also referred to as function events (Pottonen 2005), may be explicitly expressed in the tree each having a probability to prevent the undesired event from occurring. The logical interrelations, together with the barriers, build the fault tree leading from threats to an undesired event.
>
> The event tree consists of barriers branching the undesired event into various consequence levels (marked in Figure 6 as $B_{E1\text{-}2}$ and $C_{1\text{-}3}$, respectively). The probability of each consequence level may be assessed

by the probability of the respective branch and the probability that the undesired event occurs.

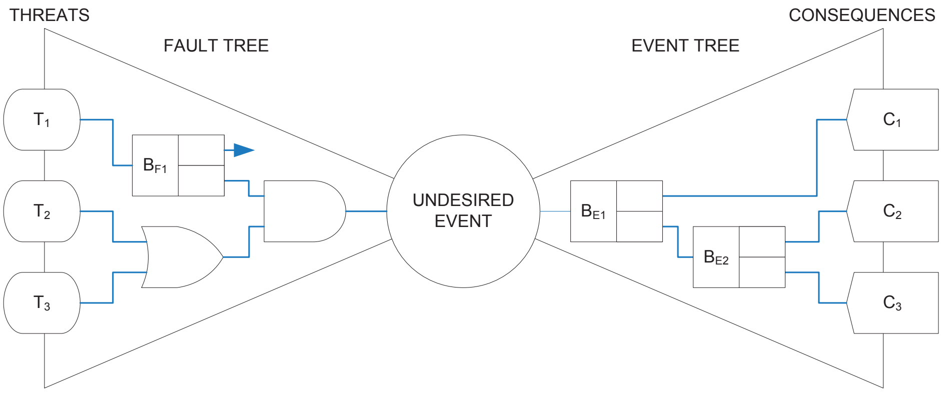

FIGURE 6: CONCEPTUAL BOW-TIE MODEL,
USED FOR RISK ASSESSMENT AND QUANTIFICATION, ILLUSTRATING INTERRELATIONS BETWEEN: THREATS, UNDESIRED EVENT, AND CONSEQUENCES

Barriers in the fault and event trees may for example be different kind of protection systems. Such protection systems could be designed to prevent a threat to result in an undesired event (i.e. a barrier in the fault tree) or to limit the consequences of an undesired event (i.e. a barrier in the event tree). See section 4.1 for examples of threats, barriers, consequences, and undesired events which may be used in the analysis of extraordinary events.

There are several challenges related to this type of risk assessment method, such as:

- *Identification of threats*: the assessed risk level only reflects the risk of identified threats, not the risk of unidentified or hidden threats.
- *Identification of logical interrelations and barriers, and assessing the effect of barriers*: the effect that a single fault has the system and on the course of an event may depend on multiple system parameters and may differ considerably from one scenario to the other.
- *Assessment of the probabilities of threats and barriers*: the probability of events, which might never have occurred previously, must be defined to quantify the risk level
- *Definition of the undesired event*: as the undesired event is the interlink between cause and effect its definition is vital in order to correctly analyse the risk in question
- *Predicting the extent of consequences*: with the consequences being the final outcome of an event, it provides an essential part of the risk assessment; however, the extent of the consequences is highly dependent on the assumptions made in other parts of the analysis, and may therefore involve a large level of uncertainty.

(Aven 2010) describes the importance of including the uncertainty perspective in risk analysis, since large uncertainties, related to e.g. probability and consequences, may undermine the credibility of quantified risk levels and thus their value as support in a decision process. Performing sensitivity analysis using e.g. fuzzy set theory is one way of considering the uncertainty perspective.

3.2.3 Power system risk and extraordinary events

In this thesis, the focus is on the risk related to power system initiated extraordinary events. This implies that risk assessment in this thesis is focusing only on extraordinary events; hence, this thesis does not consider the total risk level in the power system.

The undesired event is the link between cause and effect in risk analysis, as illustrated by the bow-tie model shown in Figure 6. Thus, accurate identification and definition of undesired events is vital in order to correctly analyse the risk in question. The characteristics of the undesired events should represent the fundamental behaviour of the studied phenomena, reflecting:

- a common result of identified threats, and
- a critical point of the event which may lead to undesired consequences.

Thus, the following question must be raised in order to specify the undesired events in a risk analysis:

Which are the common critical characteristics of the studied phenomena?

As described in Section 2.3, the transition from stable to unstable operation is identified as a critical point in the generic sequence of extraordinary events. The reason behind its criticality lies in the criterion that in order for the power system to operate, it is required to be stable. Since the transition from stable to unstable operation implies a breach of stability limits, if no remedial actions are implemented, this will result in an uncontrolled disconnection of generation and/or load, system separation, voltage collapse, and eventually blackout. Such events are likely to be widespread, and may affect the integrity of the whole power system. Based on studies of historical events and on the criterion of stable operation, it follows that the violation of stability limits constitutes a fundamental part of any power system initiated extraordinary event. Thus, the transition from stable operation to the state of instability may be defined as the undesired event for risk analysis of extraordinary events.

Conventional risk assessment methods often quantify risk as a combination of probabilities and consequences, with the undesired event being a vital part as illustrated in the bow-tie model. Such methods rely on the precise assessment of probabilities and consequences to provide sufficiently accurate risk levels. Unfortunately, there are in general a multitude of challenges related specifically to the assessment of probability and consequences.

Utilising conventional risk assessment methods to quantify the risk of extraordinary events requires the precise assessment of probabilities and consequences related to extraordinary events. Such assessment faces two main obstacles:

> Since power systems are normally considered to be operating in accordance with the $N-1$ criterion, extraordinary events typically involve: simultaneous occurrence of multiple faults, the presence of hidden faults or threats, maloperations, or that the system is actually operated outside the secure region. Thus, extraordinary events are rare but there are significant uncertainties related to the probability of their occurrence.
>
> As the consequence of an extraordinary event depends on the response of an unstable system, it may be characterised by oscillations and/or decay in voltage, frequency, and/or power, resulting in the triggering of multiple component protections. The region in the power system that is affected by such an event is complex to asses, and the final outcome of the event is thus highly uncertain.

Thus, conventional risk assessment methods are not able to adequately assess the risk of extraordinary events. Unconventional risk assessment techniques and vulnerability indicators are therefore required to describe a systems risk of extraordinary events.

3.3 Power system reliability

Risk related to power system reliability is an important part of the operation and planning of the power system. Power system reliability is often classified in two aspects: adequacy and security, with power system stability being a part of the latter, as illustrated by Figure 7.

Power system *reliability*, *adequacy*, and *security* are defined and described in this section, which also includes a discussion of the relevance of power system reliability in the analysis of extraordinary events.

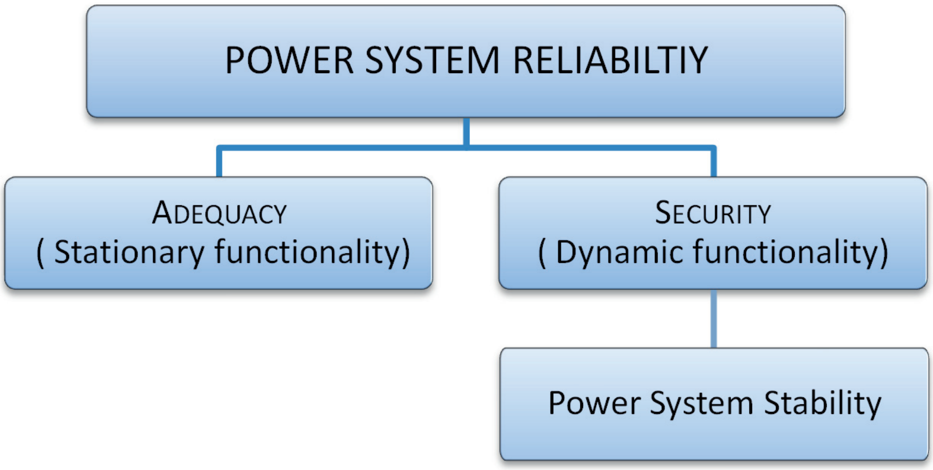

FIGURE 7: CLASSIFICATION OF POWER SYSTEM RELIABILITY

3.3.1 Definitions of reliability

Several proposals to define power system reliability can be found in the literature and some examples are provided below.

"Reliability is considered as referring to the probability (in the heuristic sense of relative frequency over the long run) of satisfactory performance", (Fink and Carlsen 1978). (Billinton and Allan 1984) state that: *"the ability of the system to provide an adequate supply of electrical energy is usually designated by the term reliability"*. While (IEC 1990) defines reliability of an electric power system as the: *"probability that an electric power system can perform a required function under given conditions for a given time interval"*, noting that *"reliability quantifies the ability of an electric power system to supply adequate electric service on a nearly continuous basis with few interruptions over an extended period of time"*.

A common element among these three definitions is the use of the expression *adequate*, and that reliability is considered a measure *over the long run* or *extended period of time*. (Fink and Carlsen 1978) clearly state that reliability *"is a function of the time-average performance of the system and its achievement is a system planning problem"*. As described in the following section, these definitions do not suitably cover the *security* aspect of reliability.

Other definitions are wider, which may also encompass operational aspects:

"Reliability, in a bulk power electric system, is the degree to which the performance of the elements of that system results in power being delivered to consumers within accepted standards and in the amount desired", (NERC 1985).

Reliability is *"a general concept encompassing all the measures of the ability to deliver electricity to all points of utilization within acceptable standards and in the amount desired"* (CIGRE 1987).

(Billinton and Allan 1984) in a way also cover this, with the statement that power system reliability *"is extremely broad and covers all aspects of the ability of the system to satisfy the consumer requirements."*

In this thesis, these wider definitions of reliability are favoured, and the definition used is: ***power system reliability is the overall objective of the system to perform its function***.

3.3.2 Adequacy & security

Common among many reliability definitions is the subdivision of power system reliability in two aspects: adequacy and security, as illustrated in Figure 7. In this thesis, these aspects are defined as:

Adequacy (or stationary functionality) *is the ability of the power system to satisfy the consumer load demand. Adequacy considerations include component ratings and voltage limits under <u>steady-state conditions</u>. Adequacy relates to planned and unplanned component outages.*

Security (or dynamic functionality) *is the ability of the power system to maintain interconnected operation. Security considerations include component ratings, voltage and frequency limits, loss of load, and <u>instability</u>. Security relates to disturbances and system failures, such as short circuits and the loss of system components.*

These definition are based on the definitions in (Guertin et al. 1978; Billinton and Allan 1984; NERC 1985; CIGRE 1987; IEC 1990; CIGRE 1997). Even though these references differ considerably in their definitions of reliability, their definitions of adequacy and security are all very similar. (Fink and Carlsen 1978) show a major difference here: considering reliability a pure planning aspect while distinguishing security as an operating issue.

As the above definition of security includes stability, an operating scenario is only secure against a set of disturbances if it remains in stable operation when exposed to any of these disturbances (e.g. an $N-1$ secure operating scenario implies that no single contingency results in instability). Thus, a requirement for security is power system stability, meaning that analyses of the power system stability are imperative when assessing reliability.

There is a multitude of expressions relating to security and adequacy, and the different terminology is often confusing and is definitely a basis for misinterpretation. Below are some examples of the terminology used in the literature:

> *Security* may be referred to as *operational security, operational reliability, dynamic reliability, transient security,* or *dynamic security*. The two latter are used when referring to methods for assessing security, making the distinction with methods for *adequacy* referred to as *steady-state* or *static security* assessment methods (CIGRE 1987; Balu et al. 1992; EURELECTRIC 2004b; CIGRE 2007b; NERC 2010).
>
> (Fosso 1989) notes a difference between the interpretation and use of *adequacy* and *security* in planning compared with operation: In planning, *adequacy* refers to steady state and *security* refers to transient, while in operation, the expressions *steady-state security* and *transient security* are used.
>
> Operating states may be referred to as *secure* or *insecure*. (CIGRE 1997) identifies that the meaning of an insecure state is different in Europe (*insecure* = *alert* = potentially unstable and/or potentially inadequate, i.e. *potentially unreliable*) compared to North America (*insecure* = *potentially unstable*). Similarly, (IEC 1990) notes that in North America security *"is usually defined with reference to instability, voltage collapse and cascading only"*. This seems to imply that European literature does not consider both aspects of reliability to the same extent as American literature does.

In German, adequacy and security are referred to as the ***stationary*** and ***dynamic functionality*** of the power system[2], respectively. These expressions include the most significant attributes of the two aspects of reliability – namely:

- *adequacy* is associated only with *stationary conditions*, while
- *security* is associated with the *dynamic system response*.

As noted by (Støa 1986), the techniques required to assess the aspects of reliability differ: adequacy can be assessed using *steady-state techniques* while security assessment requires *dynamic techniques*. Thus, the expressions *stationary* and *dynamic functionality* seem more appropriate than *adequacy* and *security* and are therefore included in the definitions in this thesis.

It is important to realise that both adequacy and security play a role in the reliability of the power system, as pointed out in (CIGRE 1997) where it is stated that: *"equal*

[2] *Stationäre / dynamische Funktionsfähigkeit (eines Elektrizitätsversorgungssystems), (DKE-IEV 2007).*

consideration must be given to what state the system ends up in after, say, the loss of a component, and how it gets there, if it can get there at all", implying the requirement of considering transient simulations in reliability studies. Adequacy and security are also identified to contribute to reliability in different ways: *"adequacy mostly with minor local interruptions, and security predominantly with large widespread ones"*, (Støa 1986).

3.3.3 Security of electricity supply

Sometimes the expression security of electricity supply is used, which in (IEC 1990) is defined as the: *"ability of an electric power system to provide electric power and energy to end-users with evaluation of existing standards and contractual agreements at the point of supply"*. A shorter definition can be found in the European directive (EU 2006): *"the ability of an electricity system to supply final customers with electricity"*.

Security of electricity supply may be seen as a broader concept than power system reliability, encompassing also aspects such as energy availability and market structure. Power system reliability is, however, extremely broad – covering all aspects of the ability of the system to satisfy its consumers, (Billinton and Allan 1984); hence, security of electricity supply is in many ways a synonym for power system reliability, (Pérez-Arriaga 2007). Furthermore, the expression security of electricity supply is yet another source of misinterpretation of the aspect of security.

Therefore, security of electricity supply is an expression that should be used with caution, and if used it should be clearly specified what it covers.

3.3.4 Reliability assessment methods and the $N-1$ criterion

Power system operating states, introduced by (Dy Liacco 1967) and revised by (Fink and Carlsen 1978), are widely used in operation planning and design of remedial emergency actions. Figure 8 provides examples of how the operating states are interpreted in the Continental European and Nordic power systems. Various terms are used to express the states of operation, but during normal operation (i.e. normal state) the power system is considered to be able to withstand any single contingency that the system operator considers credible.

In many power systems, the $N-1$ criterion is used as a reliability criterion for both planning and operation purposes, with the implication that the power system should be planned and operated in a state where no single contingency will result in the disconnection of load.

The $N-1$ criterion is based on the basic probabilistic idea that: the loss of any single component is pretty likely, while the simultaneous loss of multiple components is quite unlikely. The $N-1$ criterion is commonly used in a deterministic manner, with no regard to the relative probability or the consequence of a specific outage. Sometimes however, semi-probabilistic approaches are used, based on e.g. decreased transfer capacities during adverse weather conditions or analysis of extreme contingencies based on experience, (CIGRE 2010b) and (Qi 2011).

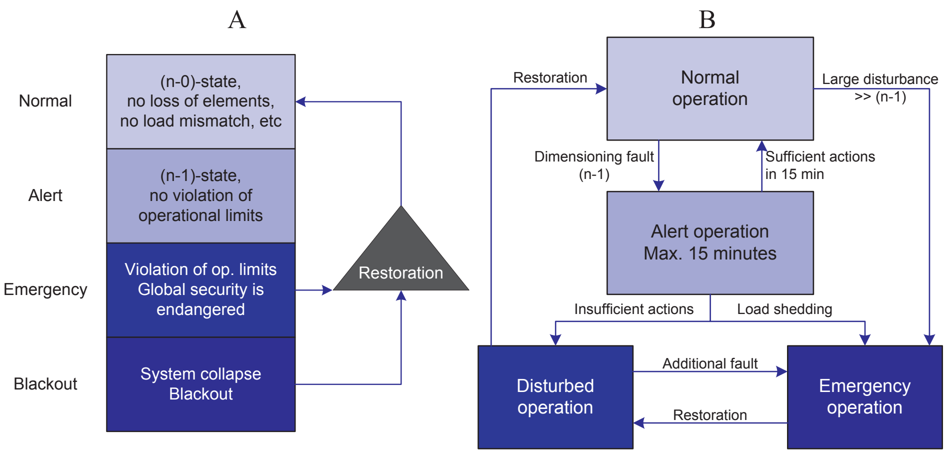

FIGURE 8: INTERPRETATION OF POWER SYSTEM OPERATING STATES, FROM (A) THE ENTSO-E OPERATION HANDBOOK (ENTSO-E 2010), AND (B) THE NORDIC GRID CODE (NORDEL 2007)

Varieties of the $N-1$ criterion exist, such as: $N-G-1$ and $N-2$, implying that the system should withstand a pre-specified selection of multiple contingencies, (CIGRE 2010b). In cases where the $N-1$ criterion is not fulfilled, expressions such as $N-0$ or $N-½$ can be found, (Breidablik et al. 2003).

$N-0$ operation may imply a radial operating scenario, where any single failure (of a set of components) results in the outage of an area[3].

$N-½$ operation reflects an operating scenario that is more reliable than $N-0$, but less reliable than $N-1$. Such a situation implies the dependency of system integrity protection schemes (SIPS), which have automated remedial actions that are designed to prevent blackout[4].

The $N-1$ criterion has different interpretations in the planning and operation of the power system. In planning, each foreseen operating scenario should be able to cope with any single outage in order to be considered $N-1$ reliable. Under operation, the $N-1$ criterion also involves the time aspect. In the Nordic power system, if two or more faults occur within a time frame of 15 minutes, they may be categorised as $N-2$ faults and outside the dimensioning criteria of the system (Nordel 2007). This implies that preventive actions should be implemented within 15 minutes after a fault has occurred. Thus, the operator needs to be aware of the actual state of operation with a minimum latency in order to identify and implement sufficient actions within the stipulated time frame. Hence, in operation the $N-1$ criterion has limited value during operation without sufficient situational awareness.

[3] Since only a highly limited set of components affect the reliability of a radially operated area, a more precise expression for this operating scenario could be: $M-0$, where typically $M<<N$.

[4] To properly reflect the dependency of the power systems on the automated response of a system integrity protection scheme, this operating scenario could be expressed as: $N-SIPS$.

The $N-1$ criterion is a reliability criterion, used in both planning and operation, reflecting both the adequacy and security of the system. However, $N-1$ contingency analyses are often performed using steady-state simulations, i.e. assessing the adequacy of the power system, with dynamic studies only performed on a limited number of contingencies, (CIGRE 1997). This means that if fulfilment of the criterion is based on conventional $N-1$ contingency analyses, it may be difficult to verify if the operation is $N-1$ secure.

Conventional reliability assessment techniques often neglect the *security* aspect of reliability, (Vrana and Johansson 2011). This may be a remnant from the historical perspective of reliability studies – being on long-term planning. A main reason for this still being the case might be the simpler and faster means of evaluating adequacy compared with security, (CIGRE 1997), and a reluctance to define a study as an *adequacy* study. There is a trend towards the development and implementation of on-line security assessment methods (referred to as dynamic or transient security assessment methods), as the value of secure operation is increasingly recognised by the power industry (CIGRE 2007b; Cirio et al. 2008). An example of work in this area is the R&D project *iTesla: Innovative Tools for Electrical System Security within Large Areas* (2012-2015), with the development of a toolbox to provide the system operator with security information based on semi-online dynamic security assessment.

3.3.5 Power system reliability and extraordinary events

Power system reliability is defined here as *the overall objective of the system to perform its function*, and is composed by the two aspects *adequacy* and *security*. Adequacy is typically associated with static conditions, while security is associated with the stability and dynamic response of the power system. Even though reliability is often considered as having these two aspects, conventional reliability assessment techniques are often limited to steady-state studies – thus assessing only the adequacy aspect of reliability.

Since stability is identified as a critical attribute of extraordinary events, identification of contingencies leading to instability is fundamental when studying extraordinary events. Thus, in order to address the reliability of extraordinary events, the security aspect cannot be neglected. This implies that dynamic reliability assessment techniques are required, meaning that contingency analyses must be based on dynamic simulations.

The criticality of exceeding stability boundaries constitutes the requirement of identifying stability limitations also in a system where limitations are defined by thermal capacities. This means that independent of the nature of the constraints during normal operation, after a number of consecutive contingencies the power system will face instability. This behaviour is illustrated in Figure 9, describing how multiple contingencies may affect the thermal and stability limits of a power transfer corridor. This figure is only conceptual and does not imply that stability limits necessarily are exceeded before thermal limits. On the contrary, thermal limits might be exceeded after only one or a few contingencies, but when the stability limits are exceeded the critical point of an extraordinary event is reached.

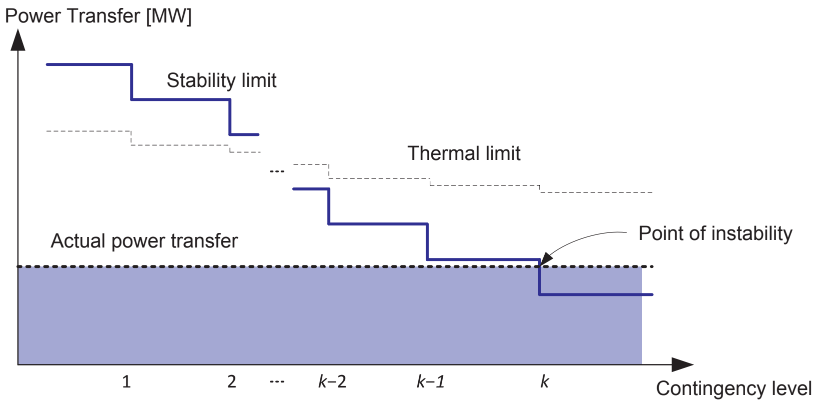

FIGURE 9: INDICATING THE POINT OF INSTABILITY AFTER MULTIPLE CONTINGENCIES, MODIFIED FROM (HILLBERG ET AL. 2012B)

Power systems are normally considered operating in accordance with the $N-1$ criterion, which is a reliability criterion used for both planning and operation purposes. If the $N-1$ contingency analyses are mainly based on steady-state simulations, it is uncertain if the operating state is $N-1$ secure. Furthermore, ordinary $N-1$ contingency analyses fail to identify the vulnerabilities related to events caused by multiple contingencies, as illustrated in Figure 9. Thus, in order to address the reliability related to extraordinary events, it is required to assess the dynamic functionality (i.e. security) of the system when exposed to multi-level contingencies.

3.4 Power system stability

Since the dynamic functionality (or security) of the power system depends on the stability, it is important to understand the phenomena related to power system stability when assessing the reliability of the power system.

Power system stability is defined by the dynamic response of all components in the system, and may be classified into three separate phenomena: rotor angle stability, frequency stability, and voltage stability, as illustrated in Figure 10. Each of these phenomena is separately described in this section, which also includes a discussion of the relevance of power system stability in the analysis of extraordinary events.

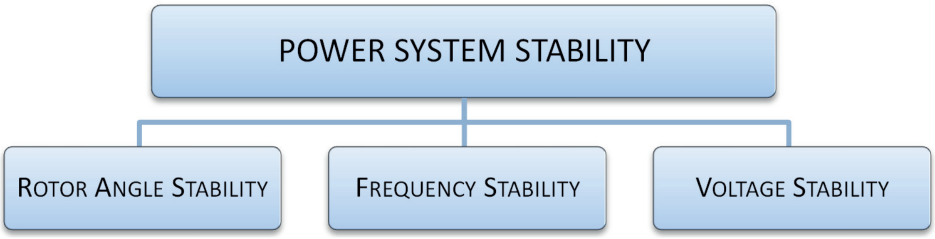

FIGURE 10: CLASSIFICATION OF POWER SYSTEM STABILITY, BASED ON (KUNDUR ET AL. 2004)

3.4.1 Rotor angle stability

Rotor angle stability reflects the ability of the power system to maintain its synchronism, defined by the amount of damping and synchronizing torque available for each synchronous machine, (Kundur et al. 2004).

Every disturbance in the system affects the operating point of the synchronous generators. The location, type and duration of the disturbance, as well as the transient behaviour of generators, are crucial to the rotor angle stability. The simplified power-angle characteristics presented in Figure 11 can be used to illustrate different types of rotor angle stability phenomena.

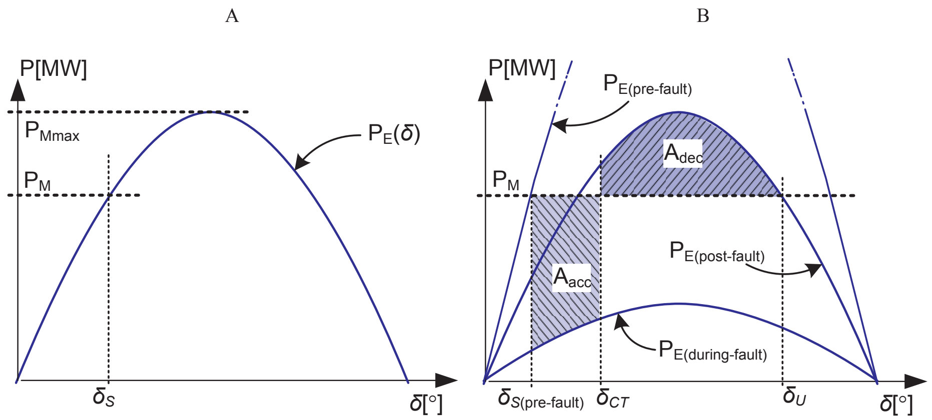

FIGURE 11: POWER-ANGLE CHARACTERISTICS,
(A) SMALL- DISTURBANCE ROTOR ANGLE STABILITY
(B) LARGE-DISTURBANCE ROTOR ANGLE STABILITY

Small disturbances perturb the system around the steady-state operating point, (P_M, δ_S) in Figure 11A. The amount of damping torque controls the decay of the post-fault oscillations on the $P_E(\delta)$ curve. The maximum steady-state power production, P_{Mmax}, defines the theoretical limit of the small-disturbance rotor angle stability.

Large-disturbance rotor angle stability is defined by the transient behaviour of the machine and the system, where sufficient decelerating torque (A_{dec}) is needed to stabilise the post-fault system as illustrated in Figure 11B. During a fault, the machine accelerates due to the difference between mechanical and electric power, P_M and P_E, respectively. If, at fault clearing (δ_{CT}), the accumulated accelerating torque of the machine (A_{acc}) is larger than the available decelerating torque, the machine will accelerate past the unstable equilibrium point (P_M, δ_U) and lose synchronism with the rest of the system. This condition is the basis of the well-known transient stability equal-area criterion: $A_{acc} \leq A_{dec}$.

In (Kundur et al. 2004), rotor angle stability is classified as a short-term phenomenon. However, rotor angle stability phenomena may also be present as sustained power oscillations. Such long-term phenomena occur due to insufficient damping torque, and may be found especially in systems with long transmission distances. For the transmission network to cope with such oscillations, limitations may be invoked on the transfer capacity of the exposed connections.

3.4.2 Voltage stability

Voltage stability reflects the ability of the power system to maintain steady-state bus voltages, (Kundur et al. 2004), and is defined by the equilibrium of the power-voltage characteristics of each transmission connection in the power system.

Voltage stability is mainly related to the amount of power transfer, the availability of reactive power, and the voltage dependency of loads.

Similarly as with rotor angle stability, voltage stability can be divided in small-disturbance and large-disturbance phenomena as illustrated by the power-voltage characteristics shown in Figure 12. Here, the characteristics are shown for active power, but the same principles and similar characteristics are valid for reactive power.

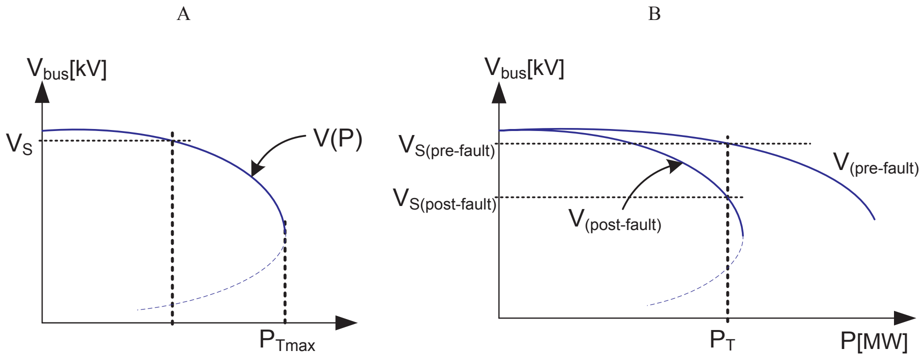

FIGURE 12: POWER-VOLTAGE CHARACTERISTICS,
(A) SMALL-DISTURBANCE VOLTAGE STABILITY,
(B) LARGE-DISTURBANCE VOLTAGE STABILITY

Small disturbances perturb the system around the steady-state operating point, (V_S,P_T) in Figure 12A. The maximum steady-state power transfer, P_{Tmax}, defines the theoretical limit of the small-disturbance voltage stability.

Large-disturbance voltage stability is defined by the possibility of the system to achieve a post-fault steady-state operating point ($V_{S(post\text{-}fault)}$,P_T), see Figure 12B. This implies that the post-fault power-voltage characteristic is needed to be considered for the system to be operated in a state which is stable against large disturbances.

Voltage instability may arise as short- or long-term phenomena, and may develop over several minutes depending on the time constants of loads, controls, and protection systems.

3.4.3 Frequency stability

Frequency stability reflects the ability of the power system to maintain a steady-state frequency (Kundur et al. 2004), defined by the generation-load balance of the entire system.

Since the system load is always in a state of change, the frequency stability is heavily influenced by the amount of available frequency containment reserves, the equivalent speed-droop of the system, the system inertia, and the response of each turbine-governor.

The piecewise linear equivalent speed-droop characteristics of the generators, $f(P_G)$, and the frequency dependency of the load, $f(P_L)$ are illustrated in Figure 13. The steady-state frequency of any operating scenario is defined by the intersection between the load and generation in the frequency-power plane, implying that any change in load or generation will result in a new equilibrium point or an unstable scenario in case the new curves fail to intersect.

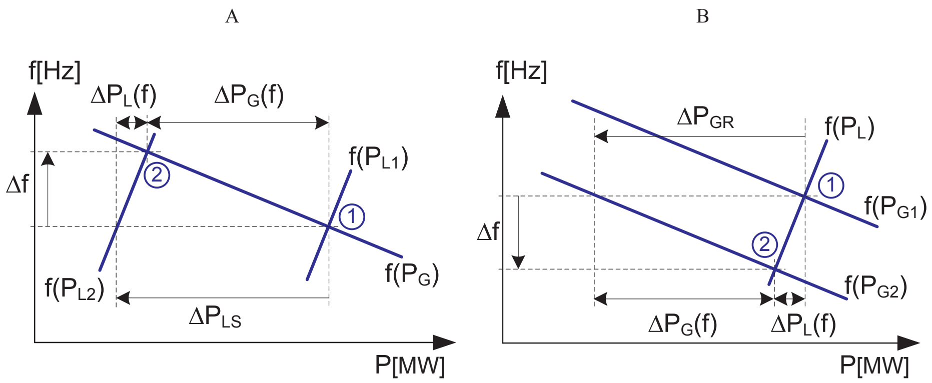

FIGURE 13: SPEED-DROOP CHARACTERISTICS,
(A) FREQUENCY INCREASE AS A RESULT OF LOAD SHEDDING,
(B) FREQUENCY DECREASE AS A RESULT OF GENERATION REJECTION

The change in frequency and generation as a result of load shedding, ΔP_{LS}, is illustrated by Figure 13A. Here, the load curve changes from the pre-disturbance, $f(P_{L1})$, to the post-disturbance, $f(P_{L2})$. The new intersecting point (2) leads to an increase in frequency, Δf, as a function of the frequency dependency of the load and generation. The final decrease in generation, $\Delta P_G(f)$, and total system demand, $\Delta P_{LS} - \Delta P_L(f)$, is the result of the load shedding.

Correspondingly, generation rejection, ΔP_{GR}, leads to a decrease in frequency, as illustrated by Figure 13B, where the intersecting equilibrium point changes from (1) to (2), in the pre-disturbance and post-disturbance system, respectively. The final decrease in generation, $\Delta P_{GR} - \Delta P_G(f)$, and total system demand, $\Delta P_L(f)$, is the result of the generation rejection.

These characteristics define the short-term frequency stability, and are related to the primary control of the generators. When analysing slower phenomena, the secondary and tertiary frequency control should also be considered.

Frequency instability is often an issue after a system is separated into several asynchronous islands; hence, transfer capacity limits based on frequency stability may be enforced on corridors which fully separate two areas of a power system.

3.4.4 Stability expressions and analysis methods

Other expressions than the ones described above are commonly found in the literature, such as: *small-disturbance stability, small-signal stability, large-disturbance stability,* and *transient stability*. Since these expressions are sometimes used in a confusing manner, their descriptions are included here.

Stability related to disturbances having only a minor impact on the operating state of the system is defined as *small-disturbance stability* (also referred to as *small-signal stability*). Power system *small-disturbance stability* relates to the dynamic response of the power systems, and is often studied using modal-analysis methods on linearised models of the power system. The validity of such studies is limited to the relatively close vicinity of the operating point at which the system is linearised, implying that a *small disturbance* may only perturb the system to a minor extent from the pre-disturbance operating point. Simulation models and tools used to study *small-disturbance stability* need to realistically reproduce the dynamic behaviour of the power system.

Stability related to disturbances having a significant impact on the operating state of the system is referred to as *large-disturbance stability*. Power system *large-disturbance stability* relates to the transient response of the power system when exposed to large-disturbances, which may considerably alter the power flow and transfer capacity of the post-disturbance steady-state system. *Large-disturbance rotor angle stability* is the phenomenon typically intended when using the expression *transient stability*. Sometimes however, *short-term voltage stability* is also referred to as *transient stability*. It should also be noted that the transient phase of a disturbance refers to the dynamic state between the pre- and post-disturbance steady states. To assess the *large-disturbance stability*, it is essential to study the behaviour of the power system during fault, i.e. the *transient behaviour.* Due to the non-linear nature of the transient behaviour during such disturbances, non-linear models are required to study *large-disturbance stability*.

The expressions *steady-state stability* and *dynamic stability* are found in the literature. These expressions may be misleading, since the former might be interpreted to relate to steady-state tools and the latter is sometimes used to represent different stability phenomena. Therefore, it is recommended that neither *steady-state stability* nor *dynamic stability* are used to express stability phenomena in the power system.

3.4.5 Power system stability and extraordinary events

With the transition to an unstable state defined as a fundamental characteristic of extraordinary events, the stability of the power system needs to be analysed to assess the risk of extraordinary events. As described in (Hillberg et al. 2012c), studying the transient behaviour of the power system, i.e. the behaviour between the pre- and post-disturbance states, is required when analysing extraordinary events:

> *Power flow calculations can only give information on the pre- and post-contingency states, and not whether the transition from one state to the next is stable. Only when the transition is stable and the system finds a post-fault steady-state, the analysis of a post-fault state is meaningful. Therefore, relying only on steady-state power flow calculations, inherently underestimates the vulnerability of the system.*

In order to cope with the underestimated vulnerabilities, utilities often operate with a *safety margin* to the *steady-state stability limit*. (Savulescu 2009) states that *"no* *contingency, no matter how severe, would cause transient instability"* when a system is operated according to the *safety margin*, concluding that *"given the current operating conditions and a dynamically selected set of major, yet credible, contingencies, there is no risk of blackout"*. Concerning extraordinary events, however, there are fatal limitations of relying solely on a margin which is basically only supported by steady-state calculations. As extraordinary events often include multiple successive or simultaneous contingencies, resulting in significant changes in the system operation, the transient dynamic impact on the system may be considerable. This is especially the case with increased fault clearing time, as a consequence of a protection system failure, which has a highly destabilising effect that is completely ignored in a steady-state study. Thus, a contingency regarded as non-critical in an analysis based only on power flow calculations, may be identified as leading to instability in a dynamic simulation. This implies that the models and simulation tools used for stability analysis of extraordinary events are required to properly reproduce the dynamic response of the power system exposed to disturbances, comprising also the transient behaviour. Furthermore, if considering only credible contingencies when assessing the risk of blackouts, it is likely that low probability events are neglected. Since blackouts are often caused by low probability events, such analysis would underestimate the risk of extraordinary events.

3.5 Methodology for analysing risk of extraordinary events

As described in this chapter, risk, reliability, and stability are three disciplines that are interrelated in the process of predicting extraordinary events. These three disciplines together formulate the requirement of performing transient dynamic multi-level contingency analyses on-line to be able to study the risks and vulnerabilities related to extraordinary events during operation of the power system. These requirements form the framework of the risk assessment methodology developed during this PhD work, where the following definitions have been made when referring to contingencies in extraordinary events:

Critical contingencies *are defined as contingencies leading to instability*

Critical contingency level *is defined as the level of subsequent contingencies where critical contingencies occur*

Undesired event *is defined as the transition from stable operation to a state of instability*

Due to the significant uncertainties of assessing the risk of extraordinary events in terms of probability and consequence, other measures and techniques are required. Therefore, the methodology presented here focuses solely on the distance to undesired events.

The following sub-sections describe how a risk analysis of extraordinary events may be realised utilising this methodology and provide two different means to convey the shortest distance to undesired events: the k_{min}*-index* and the $N-k$ *secure operating region.*

3.5.1 Realisation of risk analysis of extraordinary events

This methodology is focusing on the distance to undesired events, hence the identification of undesired events. From a bow-tie model perspective, the distance to undesired events implies the left-hand side of the bow-tie, i.e. the fault tree, as indicated in Figure 14. This figure is intended to illustrate how this unconventional methodology to quantify the risk of extraordinary events can be seen in a conventional risk analyses perspective.

In order to assess this distance, the following requirements are part of the risk analysis:

- identification of threats
- identification of logical interrelations and barriers
- assessing the effect of barriers

For power system initiated extraordinary events, to assess the distance to system instability it is required to:

- identify a comprehensive list of contingencies
- specify a set of operating scenarios
- perform contingency analysis to the critical contingency level

As a result of the requirements from stability, reliability, and risk analyses, transient dynamic contingency studies are identified as imperative to analyse extraordinary events. The undesired events, i.e. the transition to instability, are identified through multi-level contingency analyses. The required analysis depth of the contingency analyses is defined as the critical contingency level. Threats may be defined as the critical contingencies which, at the critical contingency level, lead to an unstable system.

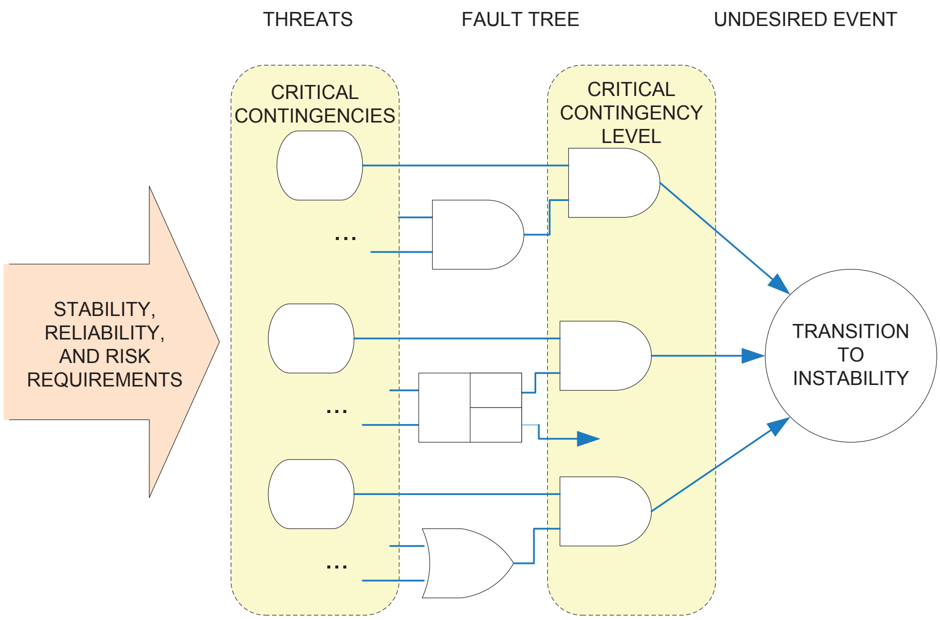

FIGURE 14: METHODOLOGY FOR RISK ANALYSIS OF EXTRAORDINARY EVENTS, ILLUSTRATED IN THE BOW-TIE MODEL PERSPECTIVE

See sections 3.2.2 and 4.1 for further description of the fault tree and the bow-tie model.

As previously stated, neither the probability identification nor the consequence assessments are explicitly included in this methodology, due to the significant uncertainties related to these quantities when considering extraordinary events.

The required multi-level dynamic contingency analysis is in the following referred to as an $N-k$ *security analysis*, where k is the critical contingency level. Thus, an $N-1$

security analysis refers to a dynamic contingency analysis including only single level failures.

To perform an $N-k$ *security analysis*, a basic necessity is to define the study scope. This section provides a description of how the scope of the study may be defined, considering the following aspects:

1. Selection of a representative set of operating scenarios.
2. Definition of a list of independent single component failures.
3. Identification of a comprehensive list of dependent failures.

Depending on the goal of the study, it might be relatively easy to identify a limited set of operating scenarios (e.g. during operation, the actual scenario is provided by the state estimator). In operation planning however, it might be necessary to utilise clustering techniques to identify a limited set of operating scenarios.

The number of required independent single component contingencies to study depends on the size of the power system, and on the critical contingency level. The possible independent $N-k$ contingencies may be identified as a selection of k contingencies from a set of n contingencies. In mathematics, this is defined as the binomial coefficient indexed by n and k, denoted $\binom{n}{k}$ and calculated as:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

In the context of this methodology (where $k \ll n$), the above expression may be approximated to: $\frac{n^k}{k!}$. This approximation clearly illustrates how the selected set of $N-1$ contingencies (n) significantly impacts the required number of simulations in a multi-level contingency analysis. For example, if the number of components considered potentially critical is decreased from 100% to 10%, the number of required simulations are reduced to: 10% ($N-1$), 1% ($N-2$), and 1‰ ($N-3$).

In Table I, the total number of components in the *IEEE Reliability Test System 1996* is presented, together with the set of independent multi-level contingencies. These contingencies have been calculated according the binomial coefficient, with all the listed components considered potentially critical.

TABLE I. COMPONENTS AND INDEPENDENT CONTINGENCIES OF THE *IEEE RELIABILITY TEST SYSTEM 1996 (IEEE 1999)*

Number of power system components	
Lines[5] (l)	100
Transformers[6] (t)	16
Generators[7] (g)	96
Compensation[8] (c)	6
Total no of components	**218**

Number of independent $N-k$ contingencies	
$N-1$ (n)	318
$N-2$ $\binom{n}{2}$	5.0×10^4
$N-3$ $\binom{n}{3}$	5.3×10^6
$N-4$ $\binom{n}{4}$	4.2×10^8

Since the fault location on a line has an impact on the dynamic result, single failures are considered on both sides of each line and the set of single component contingencies are calculated as:

$$n = 2 \times l + t + g + c.$$

In a real system, the number of installed components is often considerably larger than in a test system, resulting in an extremely high number of multi-level contingencies. For illustrative purposes, Table II lists the number of independent multi-level contingencies for a model of the Nordic power system. The contingencies listed here are calculated in the same manner as in Table I. The considered number of components includes 4000 branches and 1100 generators, and is based on information of the Nordic power system model presented in (Johansson et al. 2009). This model includes lines down to 50kV as well as small scale generation; thus, it is likely that only a fraction of these components, e.g. lines >200kV and generation >100MVA, would be considered potentially critical.

TABLE II. INDEPENDENT CONTINGENCIES OF THE NORDIC POWER SYSTEM

Number of independent $N-k$ contingencies	
$N-1$	9100
$N-2$	4.1×10^7
$N-3$	1.3×10^{11}
$N-4$	2.9×10^{14}

[5] Including AC overhead lines and cables, and merging lines which are fully in parallel.
[6] Including only transformers in the transmission system, i.e. not generator or load transformers.
[7] Generators which are identical and located at the same main bus may be merged if they are operated equally. As the generator operation depends on the studied scenario, this merging has not been done here.
[8] Synchronous condensers and shunt reactors.

The occurrence of dependent contingencies, such as common cause failures or cascaded component overloading, resulting in disconnection of multiple components may have substantial impact on the resilience of the system. Therefore, the analysis of dependent contingencies is of vital importance for a multi-level contingency analysis in order to assess the risk of extraordinary events. Dependent contingencies are subject to the system structure, and their identification requires knowledge of actual construction and location of system components.

As the above description implies, the proposed methodology presents significant challenges due to the extensive requirements to dynamically study a large quantity of cases and contingencies. There are several techniques to reduce the number of necessary simulations, such as contingency screening techniques and operating scenario clustering techniques, as described by e.g. (Singh et al. 2006; Kile and Uhlen 2012). In order to properly assess the risk of extraordinary events, the loss of important information must be limited when using techniques to expedite the contingency analyses. Development and testing of such techniques are however outside the scope of this work.

3.5.2 k_{min} vulnerability indicator

The distance to instability may be indicated by various parameters: regarding transient instability, the distance to instability may be represented by the *critical clearing time* or the *transient stability margin*, while voltage instability might be represented using the *S-difference indicator* or the *impedance stability index*, for information on these and other stability indices, see e.g. (Xue et al. 1988; Storvann et al. 2012). These stability indices are useful when specifying operational limits on power transfer capacities, as they provide information regarding the distance to instability of a specific operating state. However, since power systems are typically operated according to the requirement to fulfil the $N-1$ criterion, indices based only on studies of the steady-state or single-contingencies do not provide any information regarding the risk of multi-contingency events.

When studying extraordinary events, multi-level contingency analysis are in focus and the shortest distance to instability can therefore be represented by the minimum number of subsequent contingencies that will lead to instability. In this PhD work, the shortest distance to instability is expressed by the k_{min}*-index* defined as:

$$k_{min} = \min(s_i)\,, \forall i$$

where i is the set of contingencies that leads to an unstable state for a specific operating scenario, and s is the contingency level of each such set. In this way, k_{min} provide information on the risk of extraordinary events of the studied operating scenario and may be referred to as a vulnerability indicator.

The main purpose of the k_{min}-*index* is to provide information on the vulnerability of the system regarding extraordinary events. Conventional measures of providing system loadability limits, based on $N - 1$ security assessment, fail to provide information regarding extraordinary events due to several reasons:

1. If only single contingencies are assessed, the effect of multi-level contingencies is neglected.
2. If multi-level contingencies are considered, studies are typically limited to a list of major contingencies, thus neglecting other contingencies.
3. If probabilities of contingencies are considered, low probability events are normally neglected.
4. If basing the security assessment only on steady-state studies, transient stability phenomena are neglected.

In order to assess the vulnerability to extraordinary events, it is required to analyse the transient behaviour related to low probability multi-level contingencies. The k_{min}-*index* may then be utilised to address the risk of extraordinary event for a system during different operating scenarios.

The requirements for computing k_{min} are the same as the previously mentioned requirements for analysing extraordinary events: the execution of transient dynamic multi-level contingency analyses. As described earlier, such analyses involve a great number of simulations and it may therefore be necessary to utilise different kind of computational methodologies to be able to compute and present k_{min} as an online indicator. However, the described indicator does have an intrinsic reduction to some extent, since it is not necessary to identify all critical contingencies in order to find the critical contingency level. This implies that it is highly unlikely that all $\binom{n}{k}$ simulations are required to identify k_{min}, especially if the set of contingencies is ranked in a fairly plausible order of criticality.

A proposal to further develop k_{min} and to visualise the vulnerability level of the operating scenario is presented as the *$N - k$ secure operating region*.

3.5.3 $N - k$ secure operating region

(CIGRE 1997; Uhlen et al. 2002; Morison et al. 2004; Sarmiento et al. 2009) suggest that a *secure operating region* may be defined based on different criteria, such as the power transfer capacity limitations on corridors or the secure generation within a specific part of the system.

The secure operating region is basically determined by the thermal and stability constraints of the system, which, in fact, spans a multi-dimensional space. Thus, it may be complex to conceive the secure operating region without losing vital information. Furthermore an immense number of simulations are required to fully specify the distance to the security limit in all dimensions. However, it is theoretically possible to identify in which dimensions the system is most vulnerable. Assuming that a limited number of critical dimensions can be identified, these dimensions can be used to visualise a limited number of two-dimensional secure operating regions.

In this PhD work, the concept of the secure operating region have been expanded to multi-level contingencies, defined as the $N - k$ *secure operating region.* Dynamic multi-level contingency analysis may be referred to as $N - k$ *security analysis*, where $N - k$ *secure* implies that the system can withstand k subsequent failures. Thus, the $N - k$ *secure operating region* implies an operating region within which the system is secure against k subsequent failures. The $N - k$ *secure operating region* is conceptually illustrated in Figure 15, where it is assumed that the power flow over two power transfer corridors (PTC) is identified as critical dimensions in the secure operating space.

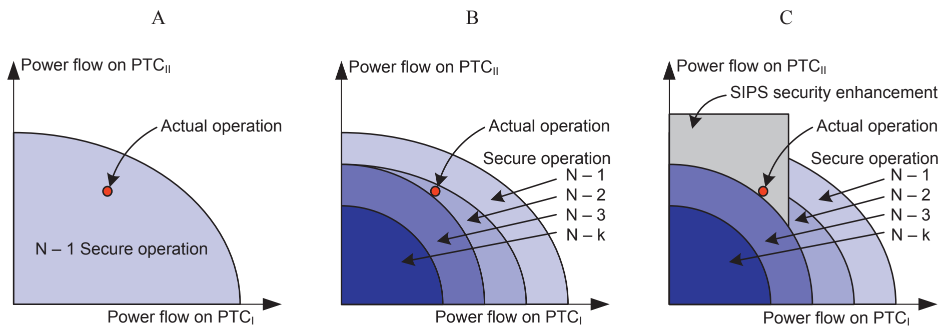

FIGURE 15: *N-K SECURE OPERATING REGION*,
VISUALISING THE ACTUAL OPERATION FROM THE PERSPECTIVE OF:
(A) *N*-1 SECURITY, (B) *N-K* SECURITY, AND (C) SIPS SECURITY,
FROM (HILLBERG ET AL. 2012C)

Figure 15A illustrates the $N - 1$ *secure operating region*, including the actual operating state, in the two-dimensional space defined by the power flow over two power transfer corridors. Expanding this region to consider the effect of multiple contingencies, visualising the $N - 2$, $N - 3$, and a general $N - k$ *secure operating region* as illustrated in Figure 15B. The $N - k$ *secure operating region* would thus provide insight into the security level of the actual operating state related to multiple contingencies. This information could be utilised to assess the necessity to plan for different kinds of remedial actions to limit the risk of extraordinary events. In this way, the increased security related to activated/installed SIPS could also be included in the visualisation as illustrated in Figure 15C.

Critical contingencies that define the secure operating region may be identified from the dynamic contingency analysis; thus specifically identifying vulnerable components or regions in the power system which may require increased attention in order to reduce the risk or extraordinary events.

3.6 Summary

This thesis deals with risk and vulnerability of extraordinary events in the power system from an operational perspective. These events involve multiple contingencies and instability, where the transition to an unstable state is identified as a fundamental characteristic and constitutes the core in the analysis of extraordinary events. Conventional risk and reliability assessment techniques are unable to provide sufficient information regarding the risks and vulnerabilities related to extraordinary events, one of the main reasons for this being the limitation of steady-state simulations, concluding that:

> *Power flow calculations can only give information on the pre- and post-contingency states, and not whether the transition from one state to the next is stable. Only when the transition is stable and the system finds a post-fault steady-state, the analysis of a post-fault state is meaningful. Therefore, relying only on steady-state power flow calculations, inherently underestimates the vulnerability of the system.*

Risk, reliability, and stability of the power system together define the set of requirements for analysis and prediction of extraordinary events during operation, resulting in the following prerequisites on analysis of extraordinary events:

- dynamic reliability assessment techniques are required, since the instability of the power system is of critical importance
- multi-level contingencies are needed to be analysed, to be able to assess the involvement of multiple contingencies
- transient dynamic studies are required, since the instability phenomena involve large-disturbance instability

This set of requirements can be summarised by the following statement:

> *It is a necessity to perform transient dynamic multi-level contingency analyses on-line to be able to assess the risks and vulnerabilities related to extraordinary events during operation of the power system.*

This reflects new insights into the analysis of extraordinary events and is therefore referred to as scientific contribution B_1.

These requirements form the foundation of the methodology to analyse risks and vulnerabilities related to extraordinary events, where the following definitions are used when referring to contingencies in extraordinary events:

Critical contingencies *are defined as contingencies leading to instability*

Critical contingency level *is defined as the level of subsequent contingencies where critical contingencies occur*

***Undesired event** is defined as the transition from stable operation to a state of instability*

Due to the significant uncertainties of assessing the risk of extraordinary events in terms of probability and consequence, this methodology focuses on assessing the distance to undesired events. Utilising this methodology, two means to indicate the vulnerability of specific operating scenarios have been developed:

> the vulnerability indicator k_{min} and the visualising of the $N-k$ *secure operating region.*

These indicators should not be regarded as operating criteria (such as the $N-1$ criterion), but as indicators of the systems vulnerability to extraordinary events. These indicators aim to provide information of the systems vulnerabilities to the operator on-line or for the day-ahead planning, thus contributing to an improved prediction of extraordinary events, and are referred to as scientific contribution B_2.

Implementing this methodology and indices require tools that are able to perform multilevel transient dynamic contingency analyses on-line for operation or in the day-ahead planning. Development of such tools has not been part of the scope of this work.

CHAPTER 4
PREVENTION OF EXTRAORDINARY EVENTS

4.1 Background

During this PhD work, measures have been developed for improvement of the on-line prevention of extraordinary events. The developed solutions are focusing on improvements of the situational awareness for the system operator and in the day-ahead planning. With the definition of the undesired event being the transition from stable to unstable operation, situational awareness may be related to the bow-tie model in several ways, as illustrated in Figure 16:

1. Threat: contingencies may result in undesired events if the operating state is less secure than the operator is aware of
2. Fault tree barrier: utilising a vulnerability indicator, such as k_{min}, the awareness regarding multiple contingencies can be improved and preventive manual actions may be implemented accordingly
3. Event tree barrier: large consequences may only be prevented by automatic actions, where successful operation of implemented SIPS depend on their awareness of the criticality of the situation

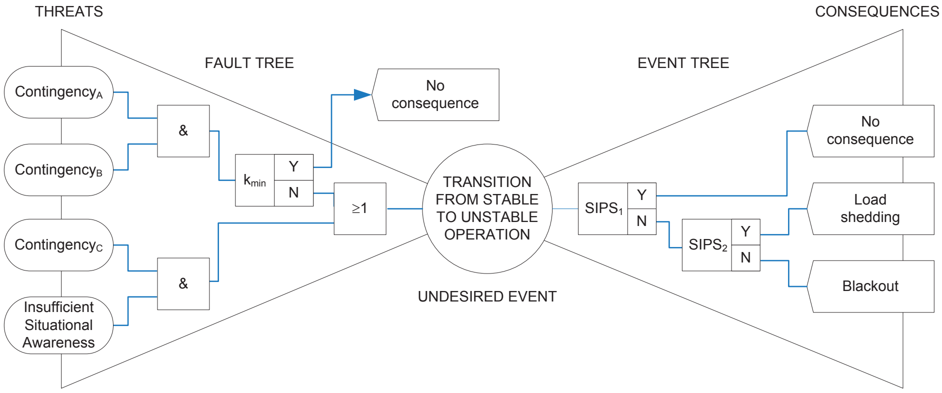

FIGURE 16: SITUATIONAL AWARENESS IN THE BOW-TIE MODEL

This chapter include description of concepts as well as results from case studies of the *IEEE Reliability Test System 1996* and of historical events. The solutions for improvement of the on-line prevention of extraordinary events are presented in two categories:

– Indicating risk of extraordinary events: providing enhanced awareness of the risk of extraordinary events utilising the vulnerability indicator k_{min} and the visualisation technique $N-k$ *secure operating region*, during online operation.
– Transfer capacity assessment of critical corridors: providing enhanced situational awareness based on the concept of utilising the equal-area criterion on power transfer corridors and in the designing of SIPS.

4.2 Indicating risk of extraordinary events

Utilising the previously described vulnerability indicator k_{min} and the visualisation technique *$N-k$ secure operating region*, a part of the total risk space related to extraordinary events may be assessed. Acknowledging the lack of situational awareness as a significantly important cause to extraordinary events, the proposed indicators provide information to the operator so that the vulnerabilities of the system state may be identified.

This chapter includes descriptions on how the *k_{min}-index* may be incorporated into the on-line operation to improve the system operator's awareness of the actual state of the system and off-line for day-ahead planning. The chapter also includes two case studies, illustrating the vulnerability level of historical events as well as for the *IEEE Reliability Test System 1996*.

4.2.1 Utilising k_{min} during operation

The *k_{min}-index* is expected to provide most value if computed during operation and in the operation planning phase. In this case, the indicator may be an integrated part of a (dynamic) security assessment (SA) module, as suggested in Figure 17.

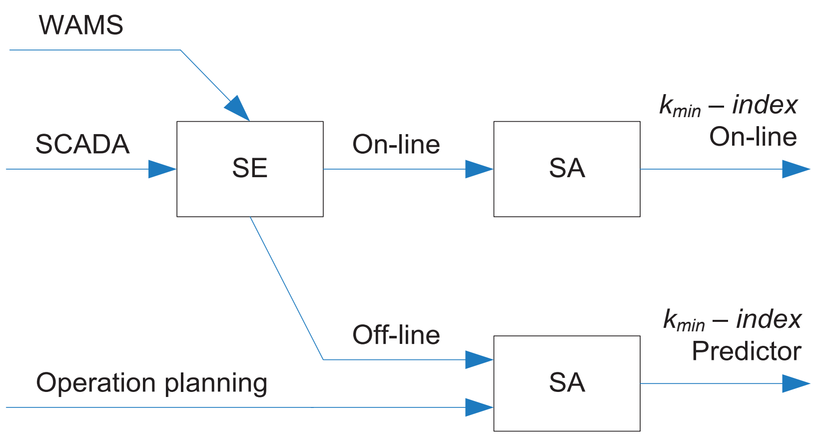

FIGURE 17: COMPUTING THE K_{MIN}-INDEX, AS AN INTEGRATED PART OF SECURITY ASSESSMENT (SA) MODULES, DEPENDING ON INFORMATION FROM THE STATE ESTIMATOR (SE)

The input to the SA is based on data of the operating state, mainly based on the results from the state estimator (SE). A conventional state estimator utilises measurement data gathered through the SCADA system to estimate the state of the system.

PMU data available through WAMS may be used to provide an enhanced state estimator, which may be especially beneficial when performing on-line (dynamic) security assessment. A decreased time delay and an improved accuracy of the estimated state may provide the possibility to identify extreme states where the system is most vulnerable and where the risk for extraordinary events is most significant.

Suggestions of how the k_{min}-*index* could be used, as available from the on-line and off-line SA modules, are illustrated in Figure 18-Figure 20. These figures are included for illustration purposes, with fictive data which does not reflect the result of any study.

The on-line SA module provides a continuously updated k_{min}-*index* which could be monitored during operation, as exemplified by Figure 18. In this way, the vulnerability regarding extraordinary events of the actual operating point is clearly shown in relation to the vulnerability level of the preceding hours. The on-line k_{min}-*index* is proposed to be updated with the same frequency as the on-line (dynamic) security assessment. Figure 18 presents the fictive on-line k_{min}-*index* as a trend curve for the previous 24 hours.

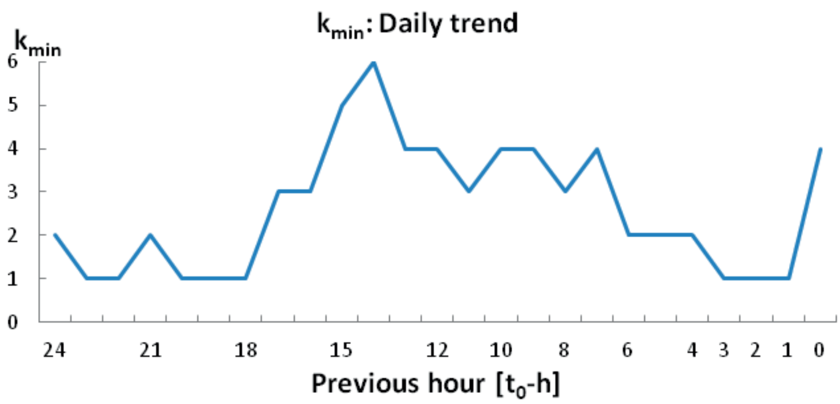

FIGURE 18: ON-LINE K_{MIN}-*INDEX,*
DISPLAYING THE TREND CURVE OF THE PRECEDING 24-HOUR PERIOD

An off-line SA module may utilise information based on both the actual operating state, provided by the state estimator, and the future states as forecasted in the day-ahead operation planning phase, including forced alterations due to unforeseen occurrences during operation. Such module could thus provide k_{min} as an indicator predicting vulnerabilities of future states, as illustrated in Figure 19. Here, particularly vulnerable future operating scenarios may be identified for which the predicted indicator is below a pre-defined "acceptable" k_{min} level. In this way, the operator can be made aware of vulnerabilities of future scenarios and measures can be taken to decrease the risk of extraordinary events. This utilisation may be especially useful in the day-ahead planning to prevent such vulnerable scenarios when possible.

As a predictor, k_{min} may be referred to as leading indicator, providing information on how vulnerability and risk develop in the future, as described by (Kjølle et al. 2012).

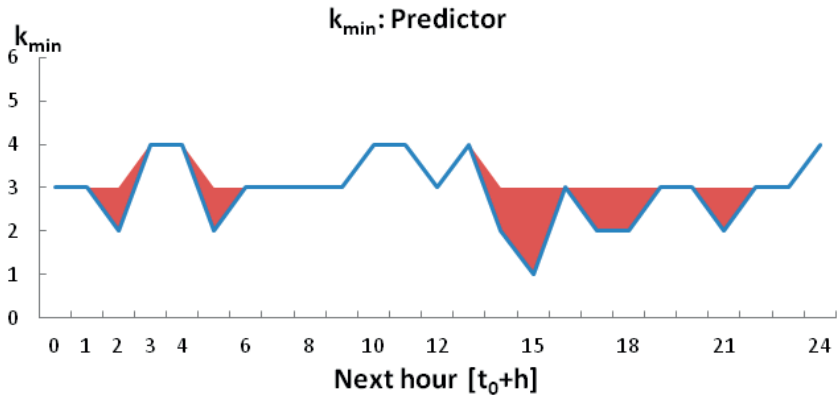

FIGURE 19: PREDICTED K_{MIN}-*INDEX*,
DISPLAYING THE TREND CURVE OF THE SUCCEEDING 24-HOUR PERIOD,
HIGHLIGHTING INTERVALS WITH ELEVATED RISK (K_{MIN}<3)

The computed k_{min}-*index* could easily be related to the distribution of the vulnerability level from historical data, as illustrated in Figure 20. In this way, the on-line or predicted k_{min}-*index* can give information of the *relative vulnerability level* of the actual or forecasted operating scenario. The utilisation of k_{min} in relation to historical levels may prove a useful indicator for operation planning, to define procedures for cases where the relative vulnerability level is increased.

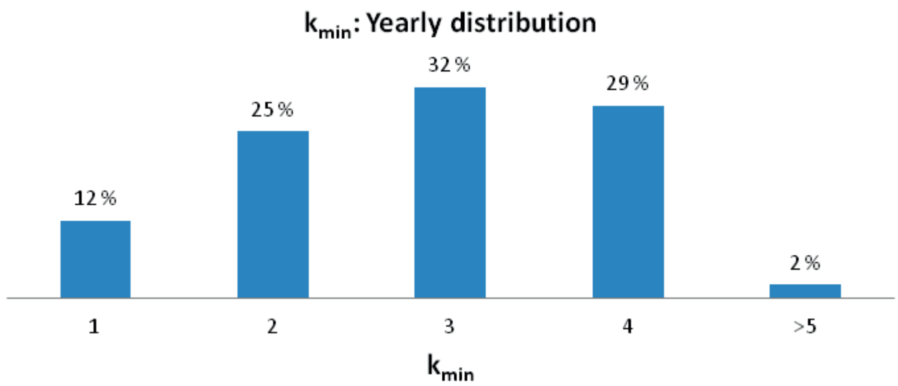

FIGURE 20: HISTORICAL K_{MIN}-*INDEX,*
DISPLAYING THE DISTRIBUTION OF THE K_{MIN}-*INDEX* ON A YEARLY BASIS

The above described proposals illustrate how the k_{min}-*index* can be used as an indicator of the risk of extraordinary events. During operation, the k_{min}-*index* provides the system operator with improved situational awareness of the actual operation and a predictor of the risk level of the coming hours. In a similar manner, the k_{min}-*index* may be used during the day-ahead planning phase to assess the relative vulnerability level of the planned operation and to analyse the arming requirements of SIPS.

The risk level shown in Figure 18-Figure 20 is intended for illustration purposes only, and the actual values of the k_{min}-*index* will vary between different power systems. A valid question is if any power system is operated to withstand as much as four or five major contingencies without becoming unstable, and what could be considered an acceptable vulnerability level. The number of contingencies that a system can withstand is system specific, and depends highly on: how densely meshed the grid is, the location and amount of reserves, the power transfer level, and on the severity and timing of the contingencies. In order to be able to define an acceptable vulnerability level it is important to quantify economical impacts in the system: comparing the cost of a blackout with the benefit of more relaxed operational criteria. Such regulatory considerations have not been part of the scope of this thesis.

Utilising the on-line k_{min}-*index*, it will be possible to identify operation scenarios with an increased risk level. It may also be possible to identify operational patterns, such as daily or seasonal, which could be used to improve the operational planning procedures.

4.2.2 Case study of k_{min} for historical events

The k_{min}-*index* may be calculated from the factual contingencies of historical events, providing information on the actual risk level at the time of the event. For such circumstances, the indicator only reflects the actual event, which may or may not have been the worst case. (Hillberg et al. 2012b) present an overview of the sequence of events of three historical extraordinary events: blackout in Sweden and Denmark 23 September 2003, blackout of Italy 28 September 2003, and the disturbance in Europe 4 November 2006. This overview is partly reproduced in Table III-Table V, and the sequence of the blackout in Brazil 10 November 2009 is included in Table VI.

As can be identified from the description of these events, the actual contingency levels at which the systems became unstable were not very high. In the Italian blackout the risk level can be quantified as $k_{min} \leq 2$, while in the other three events this is $k_{min} \leq 3$. Thus, this study illustrates the importance of assessing the power systems vulnerability to multiple contingencies.

Note that it is not possible to identify the critical contingency level without a multi-level contingency analysis, thus indicating k_{min} as less than or equal to the factual contingency level.

The indicated k_{min} levels may be considered controversial since analysing the information from different perspectives may result in other conclusions. However, the conclusions drawn here are based on event descriptions provided by: (Elkraft 2003; SvK 2003; UCTE 2004; UCTE 2007; ONS 2009; Chipp 2010; Filho 2010).

TABLE III. SEQUENCE OF EVENTS LEADING TO BLACKOUT IN SOUTHERN SWEDEN AND EASTERN DENMARK, 23 SEPTEMBER 2003, (ELKRAFT 2003; SVK 2003)

Time	Event
12:30	An internal fault in a power plant led to the disconnection of 1.2 GW of generation in southern Sweden.
12:35:00	A double-busbar failure resulted in the disconnection of two 400 kV transmission lines and an additional 1.8 GW generation in southern Sweden.
12:35:00 – 12:35:10	This resulted in a significant frequency decrease and massive oscillations of voltage and reactive power flow, leading to additional transmission line trips bringing the system to the verge of short-term voltage instability within ten seconds.
12:35:10 – 12:35:20	The decreased voltage level led to disconnection of load and an overall load decrease, which had a positive effect and stabilized the frequency at an appropriate level.
12:35:20 – 12:36:40	Insufficient reactive power support in the south led to a continuous slow voltage decay. After approximately 100 seconds, this resulted in the isolation of southern Sweden and eastern Denmark from the rest of the Nordic power system.
12:36:40	The large production deficit in the islanded system, led to a total blackout of southern Sweden and eastern Denmark.

Relating the above description to the definition of an undesired event being the transition from stable to unstable operation, to which the distance may be quantified by the k_{min} vulnerability indicator, the following should be noted:

- This event is governed by two consecutive faults, after which the system experiences voltage instability resulting in a partial blackout.
- The second fault is generally considered a double-contingency, thus from a multilevel contingency perspective this may be defined as a three-level contingency, i.e. $k_{min} \leq 3$.

TABLE IV. SEQUENCE OF EVENTS LEADING TO BLACKOUT OF ITALY, 28 SEPTEMBER 2003, (UCTE 2004)

Time	Event
03:01:42	An earth fault due to excessive sagging and inadequate vegetation management caused the trip of a 400 kV transmission line in the corridor between the Italian power system and the rest of the continental European power system. After the line tripped, the excessive phase angle difference across the breaker prohibited reclosing of the line. This caused overloading of other lines in the same corridor.
03:25:21	After around 25 minutes, a second 400 kV transmission line tripped, caused by thermal overload leading to excessive sagging and a flashover.
03:25:25 – 03:25:34	The system experienced rotor angle and voltage instability, simultaneously with several line trips due to heavy overloading. This resulted in the disconnection of the remaining transmission lines between Italy and the rest of the continental European power system.
03:28:00	The high initial imbalance between load and production in Italy, together with instability phenomena, tripping of generation, and an insufficient load shedding, ultimately resulted in a total blackout of the Italian power system.

Relating the above description to the definition of an undesired event being the transition from stable to unstable operation, to which the distance may be quantified by the k_{min} vulnerability indicator, the following should be noted:

- This event is governed by the consecutive disconnection of two 400 kV transmission lines, after which the system experiences separation (i.e. rotor angle instability) and a blackout of the islanded part of the system.
- Since the transmission circuits at lower voltage levels are not designed to carry the power of parallel circuits at higher voltage levels, from a multilevel contingency perspective this may be defined as a two-level contingency, i.e. $k_{min} \leq 2$.

TABLE V. SEQUENCE OF EVENTS LEADING TO THE DISTURBANCE IN EUROPE, 4 NOVEMBER 2006, (UCTE 2007)

Time	Event
21:38 – 21.39	The manual disconnection of two 380 kV transmission lines in Germany led to increased loading of a third 380 kV line close to its protective limit.
22:10:11	Manual actions to relieve the highly loaded line were implemented after around 30 minutes, but with adverse effect.
22:10:13 – 22:10:28	The highly loaded line tripped on overloading, triggering fast cascading failure leading to system separation in only 15 seconds.
22:10:28 – 22:49	The continental European power system operated as three unsynchronized islands for almost 40 minutes before successfully resynchronized.

Relating the above description to the definition of an undesired event being the transition from stable to unstable operation, to which the distance may be quantified by the k_{min} vulnerability indicator, the following should be noted:

- This event is governed by the consecutive disconnection of three 380 kV transmission lines, after which the system experiences separation (i.e. rotor angle instability).
- Even though the first line was manually disconnected, from a multilevel contingency perspective the event may be defined as a three-level contingency, i.e. $k_{min} \leq 3$.

TABLE VI. SEQUENCE OF EVENTS LEADING TO BLACKOUT IN BRAZIL, 10 NOVEMBER 2009, (ONS 2009; CHIPP 2010; FILHO 2010)

Time	Event
22:13:06	Three almost simultaneous single phase to ground faults led to the disconnection of two out of three 765 kV transmission lines. The third 765 kV line was disconnected after only an instant, by the residual over-current protection of shunt reactors.
22:13:06 – 22:13:07	The disconnection of the three lines led to activation of a SIPS which rejected 3.1 GW of generation. This action was however insufficient to prevent the instability.
22:13:07 – 22:13:22	Several transmission lines and generating units tripped because of power oscillations, resulting in voltage collapse and system separation.
22:13:22	Approximately 40% of the Brazilian system load was interrupted.

Relating the above description to the definition of an undesired event being the transition from stable to unstable operation, to which the distance may be quantified by the k_{min} vulnerability indicator, the following should be noted:

- This event is governed by the almost simultaneous disconnection of three 765 kV transmission lines, after which the system experiences separation (i.e. rotor angle instability) and a partial blackout.
- From a multilevel contingency perspective this may be defined as a three-level contingency, i.e. $k_{min} \leq 3$.

4.2.3 Vulnerability of the IEEE Reliability Test System 1996

The risk of extraordinary events in the *IEEE Reliability Test System 1996* is assessed based on studies performed together with PhD candidate Jarno Lamponen presented in (Lamponen et al. 2014) and is partly reproduced here.

The study was performed on a model of the *IEEE Reliability Test System 1996*, with modelling details presented in Appendix A. Dynamic contingency analyses were performed on approximately 50 different operating scenarios. These contingency analyses include 3-phase short-circuit faults on transmission lines, transformers, and generators, with 100ms duration, followed by the disconnection of the affected unit. Partial $N-2$ contingency analyses were performed in this study, where second-level contingencies were considered only for primary contingencies related to the inter-area tie-lines. Furthermore, the system was assumed to have reached a stable equilibrium before the second-level contingencies occurred.

Regarding component modelling, synchronous machines are the main contributors to the dynamic behaviour and stability of the power system. This means that sufficiently detailed and realistic synchronous machine models are required to be able to identify contingencies that could result in an unstable system. In order to use the *IEEE Reliability Test System 1996* for benchmark risk analysis of extraordinary events, dynamic models of synchronous machines are required. During this PhD work, dynamic models suitable for the *IEEE Reliability Test System 1996* have been developed for the synchronous machines, as well as for turbine-governor and excitation systems. These models are provided in Appendix A and have been used in several studies, presented in (Johansson et al. 2011a; Johansson et al. 2011b; Hillberg et al. 2012b; Hillberg and Toftevaag 2012; Hillberg et al. 2012c; Storvann et al. 2012; Lamponen et al. 2014). Further improvements of the dynamic models, specifically related to load recovery dynamics and excitation system limiters are found in (Storvann 2012). Other components and controls, such as tap-changers and power system stabilisers, also affect the system stability and need to be considered to realistically reproduce the response of the system to different contingencies. Furthermore, protection systems have a tremendous impact on the consequences of an unstable scenario; thus, protection systems (component as well as system protection) are necessary to include if attempting to study the breakdown sequence and the consequences of an extraordinary event.

The results from the dynamic contingency analyses are utilised to identify a secure operating region for the *IEEE Reliability Test System 1996*. Due to the weak interconnections between the three meshed areas, see single-line diagram in Figure A-1 in Appendix A, it is possible to identify critical transfer corridors from the system topology. These transfer corridors may then be used to visualise the secure operating regions of the system. Here, the secure operating region is visualised as the two-dimensional space spanned by the power flow between areas A and B ($P_{\text{A-B}}$) and the power export from area C (P_{Cexport}), as shown in Figure 21.

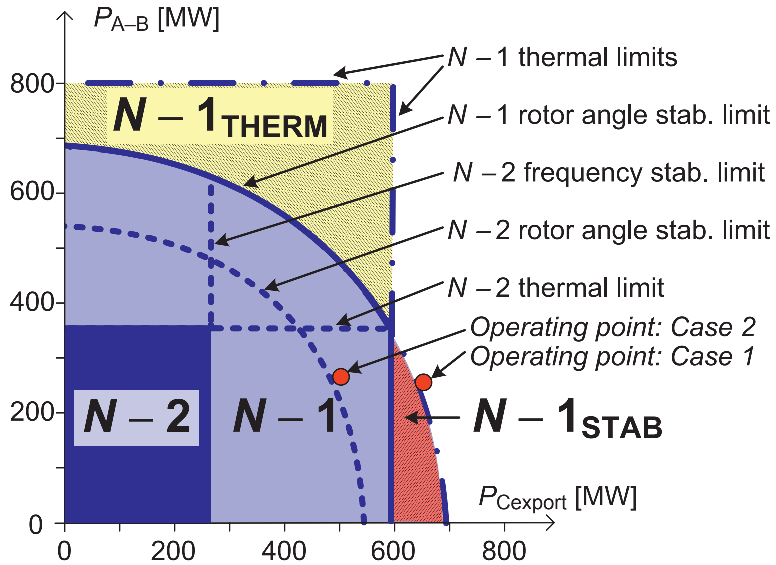

FIGURE 21: SECURE OPERATING REGIONS OF THE *IEEE RELIABILITY TEST SYSTEM 1996*, VISUALISING *N*-1 AND *N*-2 THERMAL AND STABILITY LIMITATIONS, ADAPTED FROM (LAMPONEN ET AL. 2014)

Thermal and stability limitations related to the inter-area power transfer are visualised in Figure 21. Thermal limits are here defined by the long term emergency ratings of lines, as specified in (IEEE 1999). Frequency stability limits are based on the assumption that the frequency controlled instantly activated reserves (i.e. spinning reserves) equals the largest generator of the system. It is also assumed that these reserves are divided evenly between the three areas, implying frequency stability limitations on the inter-area transfer capacity for contingencies leading to islanded sub-systems. Rotor angle stability limits are represented by arcs in Figure 21. The *N – 1 secure region* is filled as a light blue area, inside which none of the studied single contingencies resulted in the violation of neither thermal nor stability limits.

Figure 21 also illustrates how the *N – 1 secure region* may be subdivided in regions which are more or less secure against *N – 2* events (dotted lines) and the fully *N – 2 secure region*. Similarly, the *N – 1 secure region* can be extended with semi-secure regions (dash-dotted lines), where the *N – 1 stable but outside thermal limits* and *N – 1 unstable but inside thermal limits* regions are marked $N-1_{STAB}$ and $N-1_{THERM}$, respectively.

It should be noted that the presented rotor angle stability limits presented as arcs in Figure 21, are approximations based on the result from approximately 30000 dynamic simulations.

Two of the studied operating scenarios are marked in the figure as *case 1* and *2*. A description of these cases is included in Appendix A, and some of the results related to these cases are presented below.

For the operating scenario referred to as *case 1*, the following contingency was especially noted since it provides important findings related to the difference in result between dynamic and steady-state studies:

> Solving the power flow after disconnecting the tie-line between area A and C resulted in a stable solution, although with approximately 135 % overload of the B-C tie-line. If assuming that the overloaded line would trip, the system separates into two islands which could remain in stable operation depending on islanding control and the level of reserves available in each island. In a time domain simulation however, when applying a fault on the same tie-line followed by the disconnection of the line, the system is experiences rotor-angle instability which may lead to a large disturbance.

These findings demonstrate an important difference between dynamic and power flow simulations. Thus, when considering performing contingency analysis using only steady-state tools, it should be taken into account that this disregards the transient phenomena of the power system. It may therefore be concluded that:

> *Steady-state studies provide insufficient information to identify all critical contingencies.*

The operating scenario referred to as *case 2* is secure against any of the single contingencies studied, and is well within the *N – 1 secure region* as shown in Figure 21. If system reserves follow the assumption above, this case would be outside the *N – 2 frequency stability limits*. If the system reserves are distributed differently, the frequency stability limits will change accordingly. However, the case is also outside the *N – 2 rotor-angle stability limits* with a critical event identified by the *N – 2* contingency analysis. This critical event consist of the fault and trip of the tie-line between areas B and C (BLOCH-CLARK line) and the trip of the largest generator in area B (generator 221), where results from the dynamic simulation are presented in Figure 22. These results describe the value of performing multi-level contingency analyses to assess the risk of extraordinary events and to identify threats in the system.

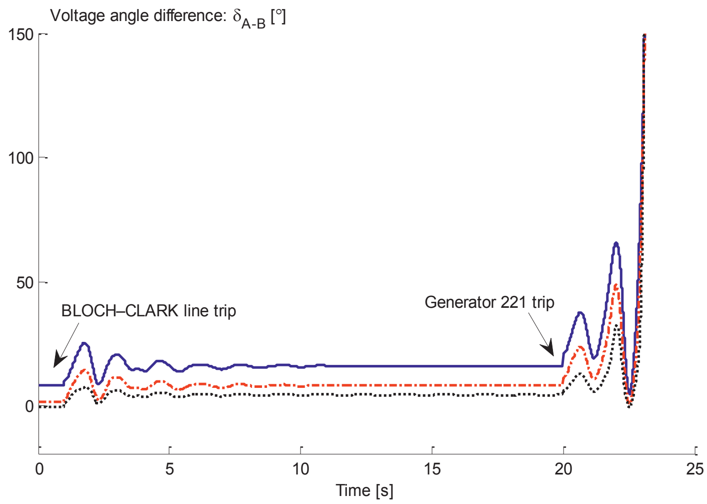

FIGURE 22: *N – 2* CONTINGENCY ANALYSIS RESULTS,
SHOWING THE VOLTAGE ANGLE DIFFERENCE BETWEEN AREA A AND B
FOR THE CRITICAL EVENT IDENTIFIED IN CASE 2, FROM (LAMPONEN ET AL. 2014)

Since the transition to the state of instability is identified as the critical characteristics of extraordinary events, it is the stability constraints that are of main importance when analysing the risk of extraordinary events. Thus, if only stability constraints are considered when determining the *N – k secure region*, such an *N – k* ***stable*** *region* indicates the vulnerability of extraordinary events of an operating region in the same manner as the k_{min}*-index* does for a specific operating state. This concept is illustrated in Figure 23, where the k_{min}*-index* of the *IEEE Reliability Test System 1996* is visualised. Here, the *N – 1 secure region* from Figure 21 is extended with semi-secure *N – 1 stable but outside thermal limits* region ($N – 1_{STAB}$), and similarly for the *N – 2 secure region*. Thus, the $k_{min} \geq 2$ region is larger than the *N – 1 secure region.* It should be noted that thermal limitations may not be completely ignored, but the system response is completely different when violating thermal limits compared by the violation of stability limits.

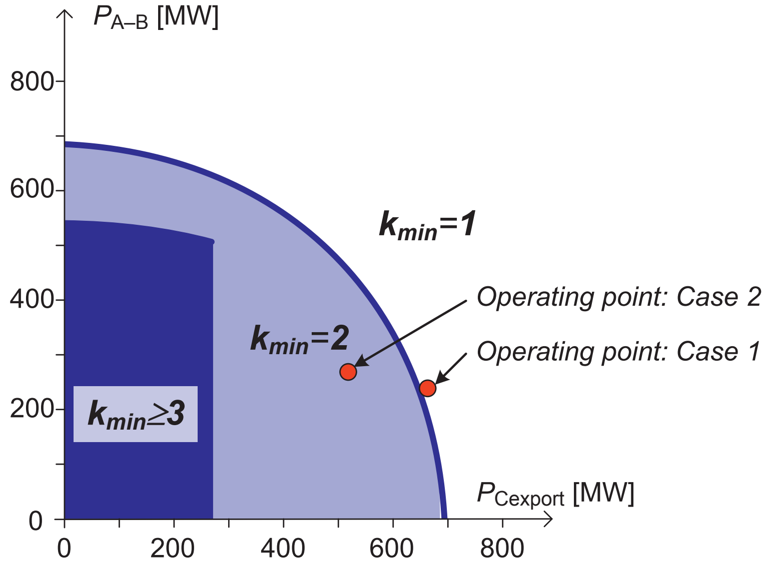

FIGURE 23: STABLE OPERATING REGIONS OF THE *IEEE RELIABILITY TEST SYSTEM 1996*, VISUALISING THE *K_{MIN}-INDEX*, ADAPTED FROM (LAMPONEN ET AL. 2014)

4.3 Transfer capacity assessment of critical corridors

With the transition to an unstable state considered the critical characteristic of extraordinary events, identification of the stability limitations in the power system are of major importance to assess the risk of extraordinary events. As extraordinary events often include multiple contingencies resulting in significant changes in the system operation, instability phenomena often involve large-disturbance stability meaning that transient dynamic studies are required to analyse extraordinary events. This chapter presents measures related to transient stability assessment. The concepts are based on applying the equal-area criterion on critical power transfer corridors in the power system, and may be used to define secure power transfer capabilities and design solutions to prevent instability.

4.3.1 PTC capacity assessment using the equal-area criterion

Transient rotor angle stability is often analysed using equivalent modelling, such as single-machine infinite-bus equivalent models, where stability margins are determined using the renowned equal-area criterion (EAC) of a synchronous machine. Since stability stipulates that every machine needs to fulfil the equal-area criterion, several studies focus on the identification of *critical machines* which are likely to loose synchronism with the remaining system (Xue et al. 1988; Dong and Pota 1993; Haque 1994; Ernst and Pavella 2000; Yi-qun et al. 2002; Ruiz-Vega and Pavella 2003a; Ruiz-Vega and Pavella 2003b; Glavic et al. 2007; Huan et al. 2008).

The EAC is based on the definition of the steady-state operating point of a synchronous machine. In the P-δ -plane, the intersection between the electric power transmitted to the system, P_E, and the mechanical power of the machine, P_M, result in a steady-state voltage angle, δ_S, between the machine and the system equivalent, as illustrated in Figure 24.

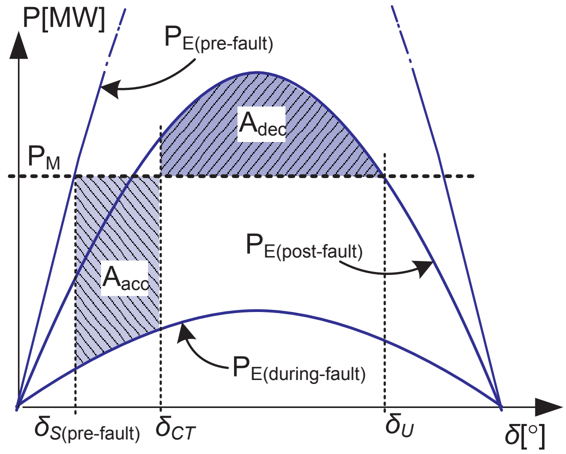

FIGURE 24: THEORETICAL EQUAL-AREA CRITERION,
USED IN TRANSIENT STABILITY ASSESSMENT STUDIES, WITH THE STABILITY REQUIREMENT DEFINED AS: $A_{ACC} \leq A_{DEC}$

The EAC specifies that the available decelerating torque, required for a synchronous machine to maintain in synchronism with the remaining system when exposed to a contingency, needs to be at least as large as the accelerating torque that the machine acquires throughout the fault duration, i.e.:

$$A_{acc} \leq A_{dec}.$$

Which also implies that the maximum rotor angle, δ_{Max}, must be smaller the post-fault unstable equilibrium angle, δ_U,:

$$\delta_{Max} \leq \delta_U.$$

From the theoretical power-angle characteristics described by Figure 24, it is clear that the accelerating and decelerating areas can be calculated as:

$$A_{acc} = \int_{\delta_{S(pre-fault)}}^{\delta_{CT}} \left(P_M - P_{E(post-fault)}(\delta)\right)$$

$$A_{dec} = \int_{\delta_{CT}}^{\delta_{Max}} \left(P_{E(post-fault)}(\delta) - P_M\right)$$

A machine which loses synchronism with the system is referred to as a critical machine. In the case with multiple critical machines, it is possible to cluster these into an equivalent one-machine-infinite-bus (OMIB) system. As described by e.g. (Xue et al. 1988), it is possible to assess the transient stability margins against an equivalent of the remaining system utilising the extended equal-area criterion (EEAC). A single machine equivalent method (SIME) is proposed by (Zhang et al. 1997), which differs from other

EEAC based methods by considering the time variance of machine parameters such as powers and speed.

Another utilisation of the traditional equal-area criterion is suggested in (Dong and Pota 1993; Haque 1994), where the transient stability margin and critical clearing time of critical machines are assessed without equivalent models.

In this PhD work, the equal-area criterion is utilised to assess the secure power transfer capacity between two interconnected systems. In this manner, the EAC provide means of assessing the capacity of critical power transfer corridors (PTC) and of specifying the secure power transfer capacity of the interconnected power system. The *EAC on PTC* concept is applicable in cases where the topology of the network and the impact of a critical contingency may be described as:

> *A sub-system may be identified wherein all machines are defined as critical machines. I.e. a critical contingency result in the acceleration of all synchronous machines within one sub-system relative the rest of the system. The tie-lines interconnecting the sub- and main systems may then be defined as a critical power transfer corridor.*

Figure 25 illustrates a power system where the *EAC on PTC* concept may be applied. The sub-system and main systems are interconnected through a corridor with *m* tie-lines. As shown in Figure 25B, all generators within the sub-system accelerate against the main system after a critical contingency.

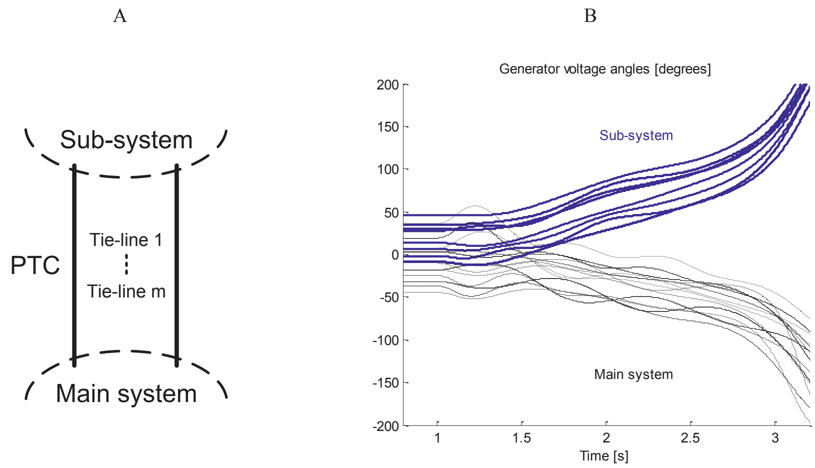

FIGURE 25: TRANSIENT INSTABILITY OF A PTC
(A) A PTC WITH *M* TIE-LINES CONNECTING A SUB-SYSTEM TO THE MAIN SYSTEM,
(B) ACCELERATION OF ALL GENERATORS IN A SUB-SYSTEM (RELATIVE THE REST OF THE SYSTEM) AFTER A CRITICAL CONTINGENCY,
FROM (HILLBERG AND TOFTEVAAG 2012)

In a similar manner as the steady-state operating point of a machine may be defined in the P-δ -plane, the steady-state operating point of a sub-system can be defined by the level of electric power that flows across a corridor between the sub-system and the main system, and the equivalent mechanical power of the sub-system resulting in the steady-state voltage angle between the systems.

The main difference between the *EAC on PTC* approach and other EAC based methods is the utilisation of the actual power flow and angle differences over a set of transmission lines, instead of assessing the power and angles of equivalent models. The benefit by this approach is the direct assessment of transfer capacity limitations, instead of focusing on the transient stability margins of critical machines.

A difficulty that this approach faces is the approximation of the mechanical power of the sub-system. Figure 26 illustrates the significant difference in the calculated accelerating torque depending on assumptions regarding mechanical power. In theoretical descriptions of the equal-area criterion, mechanical power (or torque) is typically assumed to be constant. This assumption provides an easy means of assessing the accelerating (as well as decelerating) torques, which is illustrated in Figure 26A. In reality, the mechanical power of a single machine is depending on the speed-droop characteristics of the turbine-governor of the machine – i.e. typically frequency dependent. The equivalent mechanical power of a system consists of the mechanical power of the machines as well as of the loads in the system, which further complicates assessment of the accelerating torque. In Figure 26B, the accelerating torque is assessed using an approximation of the speed-droop of the system. This approximation of the response of the system is further described in the case study presented in section 4.3.3.

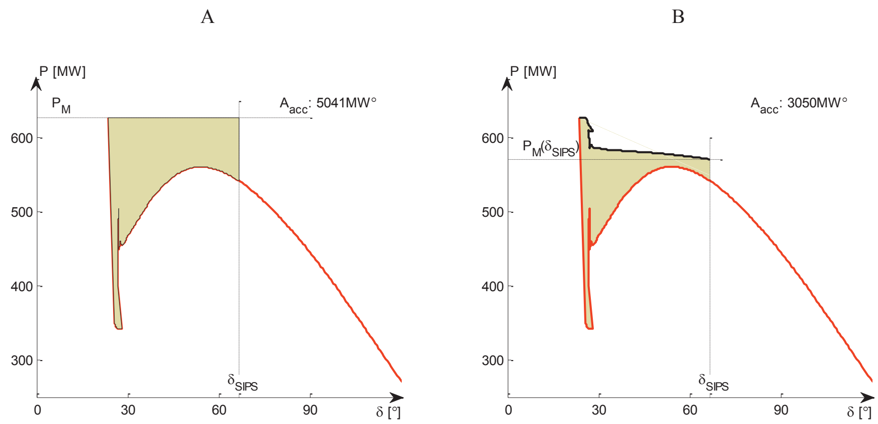

FIGURE 26: ASSESSMENT OF ACCELERATING TORQUE, ASSUMING: (A) CONSTANT MECHANICAL POWER, (B) FREQUENCY DEPENDENT MECHANICAL POWER, FROM (HILLBERG AND TOFTEVAAG 2012)

Figure 26 illustrates how the dynamics and control of the power system act as obstacles (or challenges) to the apparent straightforward manner of assessing the equal-area criterion implied by theoretical descriptions as illustrated in Figure 24.

Utilising the equal-area criterion on a PTC, the transient stability margin and the secure power transfer capacity of the PTC can be assessed during operation. The concept could thus provide an enhanced awareness of the operating state. A requirement for the online assessment is the availability of phasor measurements to monitor the voltage angle differences over the PTC as well as other synchronous measurements required to assess the areas of the equal-area criterion. This use of the equal-area criterion could be applied in multi-level dynamic contingency analyses, when studying the response from subsequent contingencies and the risk of extraordinary events. There are several possible application areas of the *EAC on PTC* approach, and one of these is related to the design and utilisation of SIPS which is further described in the following section.

4.3.2 SIPS design using the equal-area criterion

System integrity protection schemes (SIPS) are often designed to provide mitigating actions to prevent an extraordinary event from occurring. For such schemes, it is imperative that the mitigating actions are sufficient for the system to remain stable after an undesired event. The monitoring improvements provided by the implementation of PMUs can be used to enhance the situational awareness of conventional SIPS, providing robustness towards unforeseen disturbances. General improvements of this kind are discussed in (Johansson et al. 2011a; Hillberg et al. 2012c).

Techniques for preventive and emergency transient stability control, based on the utilisation of the EAC, are described in (Ernst and Pavella 2000; Rosales et al. 2000; Ruiz-Vega and Pavella 2003a; Ruiz-Vega and Pavella 2003b), where the single-machine-equivalent (SIME) method is used. The emergency control actions are defined on the basis of identifying critical machines, which are tripped in an iteratively manner until the system reaches stable operation. Other solutions, with emergency controls based on online PMU based measurements, are suggested in (Yi-qun et al. 2002; Glavic et al. 2007; Huan et al. 2008), where the EAC is utilised for identifying critical machines and assessing the adequacy of emergency control actions.

Based on the *EAC on PTC* concept described in the previous section, a SIPS design method has been developed. The general approach of this method is presented here, and a feasibility study of the method is presented in the next section. Figure 27 illustrates how this method may be applied in the design and utilisation of SIPS. Here, the electrical power represents the flows across a corridor between the sub-system and the main system, while the mechanical power represents the equivalent mechanical power of the sub-system. The voltage angle represents the angle between the systems, i.e. over the PTC.

In the case where a contingency decreases the power-angle characteristics of the PTC below the equivalent mechanical power of the sub-system, the power system will be unstable in the post-fault state, as illustrated by Figure 27A. This corresponds to an insecure operating scenario, where a critical contingency result in the continuous acceleration of the sub-system until it loses its synchronism with the remaining system. Considering the possibility of applying actions to prevent instability, a SIPS solution may be designed based on the equal-area criterion of the PTC. As a SIPS will have an inherent time delay, the corresponding SIPS activation angle and theoretical accelerating torque may be calculated and illustrated as shown in Figure 27B. The minimum level of SIPS remedial actions, required to prevent instability, may then be assessed as the maximum post-SIPS equivalent mechanical power of the sub-system that satisfies the equal-area criterion. In this way, the resulting post-fault-post-SIPS steady-state can be identified as illustrated in Figure 27C.

A

B

C

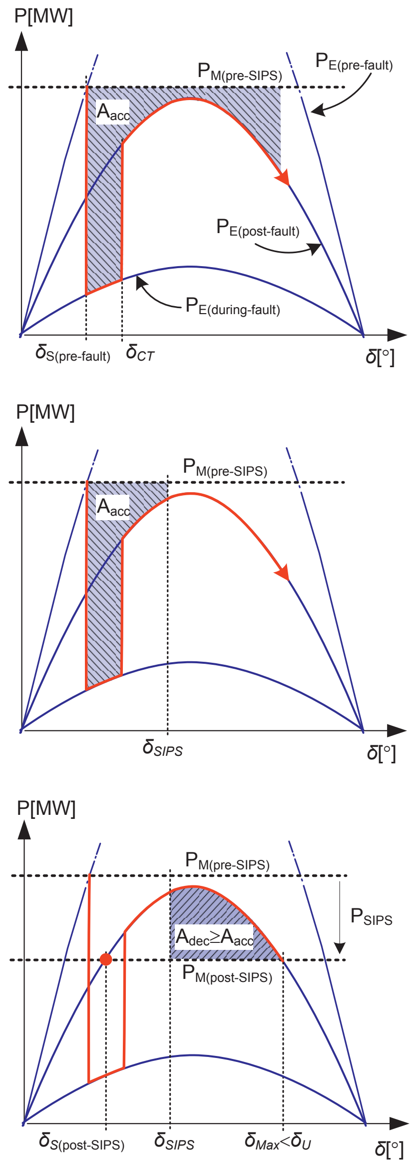

FIGURE 27: EQUAL-AREA CRITERION USED IN SIPS DESIGN,
(A) AN INSECURE OPERATING SCENARIO, I.E. THE POST-FAULT SYSTEM IS UNABLE TO REGAIN STABLE OPERATION
(B) THE INTRINSIC TIME DELAY OF A SIPS IS USED TO IDENTIFY THE CORRESPONDING ROTOR ANGLE AND THE ACCELERATION TORQUE
(C) THE REQUIRED LEVEL OF SIPS REMEDIAL ACTION TO PREVENT INSTABILITY MAY BE ASSESSED BASED ON THE EQUAL AREA CRITERION

4.3.3 Transient stability assessment of the IEEE Reliability Test System 1996

A case study has been performed to test the feasibility of the presented *EAC on PTC* concept and the SIPS design method. The study was performed on a model of the *IEEE Reliability Test System 1996*, with modelling details presented in Appendix A. The studied operating scenario is referred to as *case 1* and is also presented in Appendix A. A dynamic $N-1$ contingency analysis has been performed, including 3-phase short-circuit faults on transmission lines, transformers, and generators, with 100ms duration, followed by the disconnection of the affected unit. In this analysis, faults have been studied with the short-circuit applied on either end of a transmission line.

Results from the $N-1$ contingency analysis are presented in Figure 28; showing power flow (P), angle difference (δ), and frequency difference (f), between areas B and C. The dynamic contingency analyses indicate that fault and trip of the A-C tie-line result in rotor angle instability; hence this is defined as a critical contingency. The dashed red curves in Figure 28B and Figure 28C represent contingencies where the short-circuit is on the C-side of the A-C tie-line. These contingencies have a significantly higher impact on the system than contingencies where the short-circuit is on the other side of the line. In Figure 28A, results from contingencies involving the A-C tie-line are not included.

Further analysis of the critical contingency shows that all machines in area C accelerate out of synchronism relative the rest of the system. These results are presented in Figure 25B, showing the generator terminal voltage angles of all machines in the studied test system. Hence, for this contingency all machines in area C are considered critical.

It is possible to design SIPS to improve the security of the analysed case. Here, the efficiency of three different types of arming and activation/triggering signals is assessed for a scheme based on generator rejection:

- $SIPS_{CB}$: Event-based, monitoring the trip signal of circuit breakers on the A-C tie-line
- $SIPS_{\delta}$: Response-based, monitoring the voltage angle differences over the B-C tie-line
- $SIPS_{f}$: Response-based, monitoring the bus frequency at both sides of the B-C tie-line

A manual (or automatic) arming is assumed to limit the operating scenarios where the SIPS can be triggered. A thorough assessment of the arming procedures and activation signals is necessary to limit the risk of inappropriate SIPS actions. Arming procedures can be designed through identification of the operating criteria that defines the secure operating area, while an extensive dynamic analysis is needed to identify appropriate activation signals and their magnitude. Here, the analysis is limited to the presented case and contingencies.

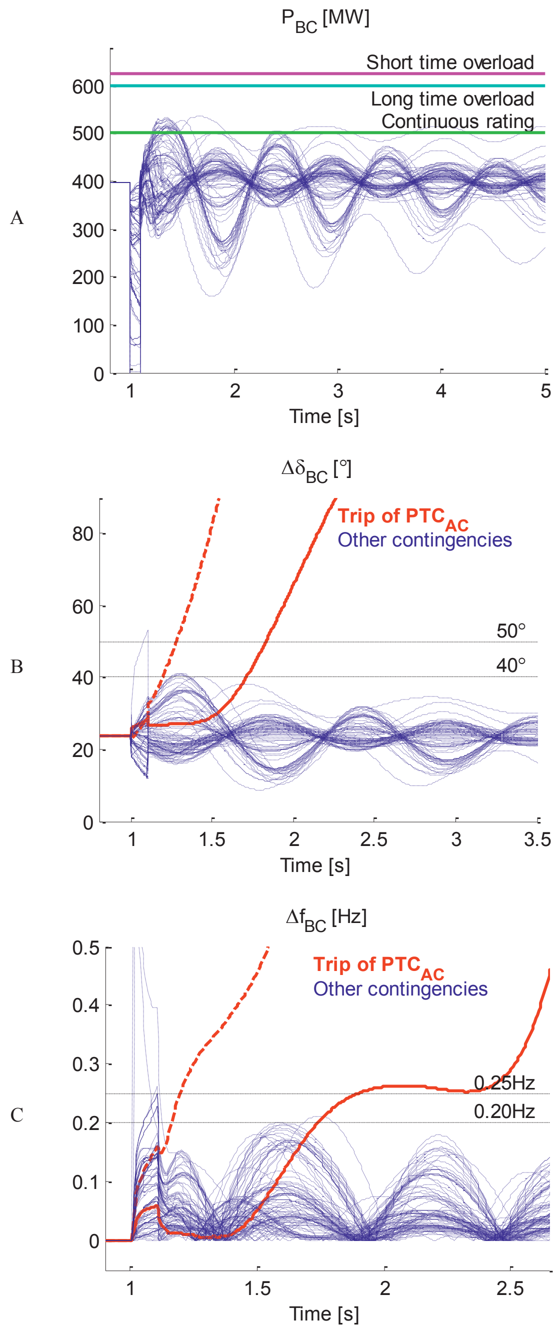

FIGURE 28: $N-1$ CONTINGENCY ANALYSIS RESULTS,
(A) POWER FLOW, (B) ANGLE DIFFERENCE, AND (C) FREQUENCY DIFFERENCE,
BETWEEN AREA B AND C

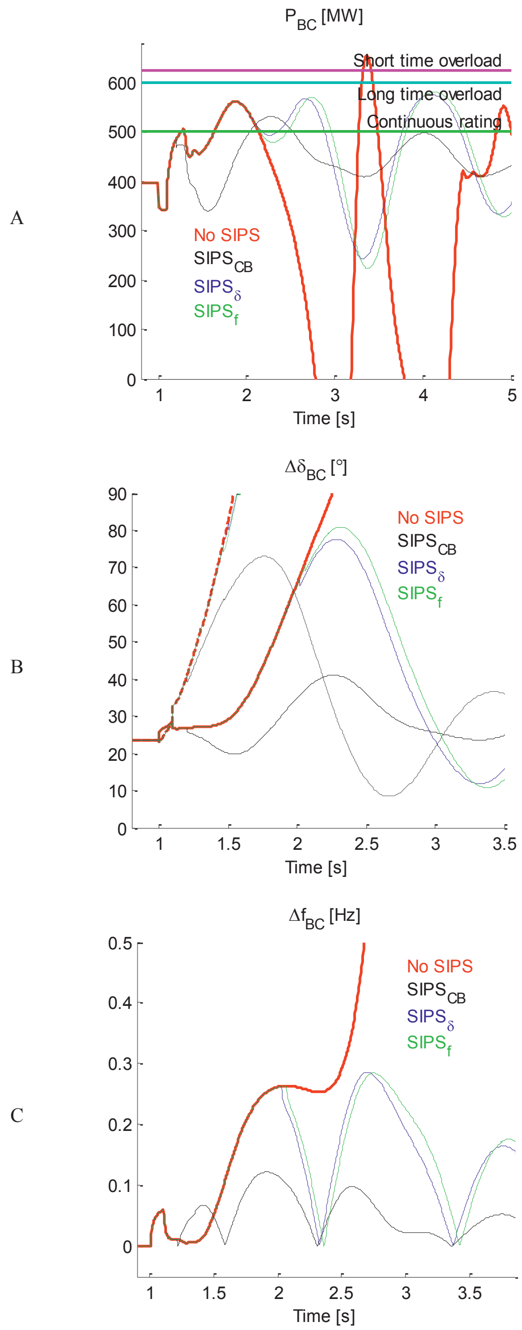

FIGURE 29: SECURITY ENHANCEMENT OF *CASE 1* USING SIPS, (A) POWER FLOW, (B) ANGLE DIFFERENCE, AND (C) FREQUENCY DIFFERENCE, BETWEEN AREA B AND C

From Figure 28, the unstable contingencies are easily distinguishable in both $\Delta\delta_{BC}$ and Δf_{BC}, supporting their potential as SIPS activation signals. It is suggested that an internal arming is used together with a time delay, to prevent unwanted SIPS action during switching events. Based on the results of the dynamic contingency analysis, the suggested arming and activation signal magnitudes, as marked in Figure 28, are:

$\Delta\delta_{BC}$ - arming: 40° for 200ms, activation: 50°
Δf_{BC} - arming: 0.2Hz for 200ms, activation: 0.25Hz

δ and f measurements are considered to be available, from e.g. a WAMS. The total delay between measurement and the implementation of mitigating action is assumed to be no longer than 100 ms which seams realistically achievable, based on actual measurements of a PMU based Wide Area Power Oscillation Controller as well as the delays of a Wide Area Monitoring and Control System presented in (Chenine et al. 2009).

The response after the trip of PTC_{AC}, with and without the suggested SIPS, are presented in Figure 29 including the power flow, angle, and frequency difference between areas B and C. The dashed curves in Figure 29B, represent the fault with the short-circuit occurring at the C-side of the line. The system response of this contingency is too rapid for the $SIPS_{\delta}$ and $SIPS_{f}$ solutions to act before the system becomes unstable, and only $SIPS_{CB}$ results in a stable solution. All other curves in the figure represent the fault with the short-circuit occurring at the A-side of the line. For this fault, all the studied SIPS solutions results in a stable post-fault system, however, the event-based $SIPS_{CB}$ scheme shows lower levels of oscillations due to the more rapid activation than the response-based schemes.

In order to minimise the vulnerability of the operation of the post-SIPS steady state system, it is important that the SIPS action is adapted to suit the actual operating scenario. Different solutions to identify appropriate levels of SIPS action are possible, and here the $SIPS_{\delta}$ actions are designed based on the EAC on PTC concept. The equal-area assessment of the PTC for the identified critical contingency is done in three steps:

1. Identifying the instant of SIPS activation
2. Assessing the accelerating torque of the PTC before SIPS activation
3. Assessing the minimum necessary level of rejected generation to fulfil the equal-area criterion

Based on the arming levels and time delays described above it is possible to identify the instant (t_{SIPS}) and the corresponding activation angle (δ_{SIPS}) of the SIPS, as illustrated in Figure 30,

δ_{SIPS}: $\delta_{BC} \leq 67°$
t_{SIPS}: $t_0 + 1.0\text{s}$

where t_0 is the instant of the occurrence of the fault.

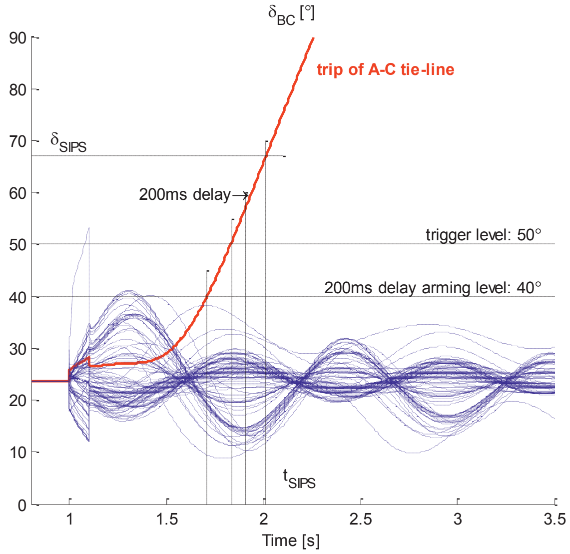

FIGURE 30: SIPS ACTIVATION ANGLE AND INSTANT, FROM (HILLBERG AND TOFTEVAAG 2012)

The power-angle characteristics of the PTC (the B-C tie-line) after exposed to the critical contingency is shown in Figure 31. Utilizing the identified SIPS activation angle (δ_{SIPS}) it is possible to assess the accelerating torque of the PTC at the instant of SIPS activation. Assuming a constant mechanical power of the system (P_{0M}), the accelerating torque before SIPS activation (A_{acc}), as shown in Figure 31A, is approximated to:

$$A_{acc}|P_{0M} = 5000\text{MW}^{\circ}$$

Here, the notation *"|"* is used to imply the restriction on accelerating torque based on the assumption of mechanical power. In reality, the mechanical power is not constant during a disturbance and the above assumption results in an over-conservative SIPS design. To assess the change in mechanical power, the frequency during the disturbance need to be considered. Assuming that the response of each turbine governor control may be approximated by the speed-droop, the system response can be approximated by a piece-wise linear speed-droop, R. The mechanical power of the system, as a function of the frequency change ($\Delta\omega$), can thus be approximated as

$$P_M(\Delta\omega) = \left(1 - {}^{\Delta f}/_{R}\right) \times P_{0M} \tag{1}$$

where Δf is the per unit change in frequency and P_{0M} is the mechanical power at the pre-fault instant. The speed-droop of the system can be assessed during operation, studying the frequency response of a known disturbance, e.g. the trip of a generator, as:

$$R = -{}^{\Delta f}/_{\Delta P_G} \times P_G \tag{2}$$

where ΔP_G is the production change and P_G is the total system production. Analysing responses of generator tripping, the speed-droop of the test system is approximated to:

$$R=4.3\%$$

Based on the frequency measurement in area C, presented in Figure 32, and the calculated speed-droop of the system, the approximate equivalent mechanical power of the sub-system, $P_M(\Delta\omega)$, can be derived from equation (1). The accelerating torque before the SIPS activation, as shown in Figure 31B, is approximated to:

$$A_{acc}|P_M(\Delta\omega) = 3000\text{MW}°$$

This area is drastically smaller than the area calculated using constant mechanical power. This implies that the impact of simplified assumptions is large, thus in order to design appropriate SIPS solutions sufficient details are needed to be considered.

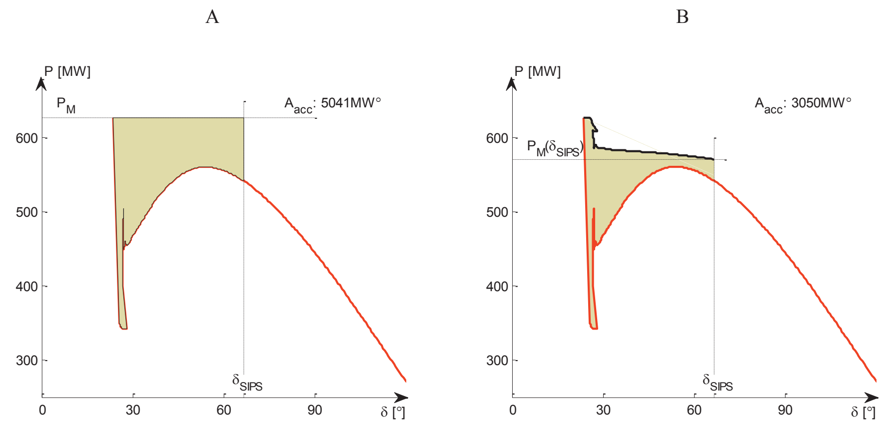

FIGURE 31: POWER-ANGLE CHARACTERISTICS AND ACCELERATING TORQUE OF PTC WHEN EXPOSED TO A CRITICAL CONTINGENCY, ASSUMING:
(A) CONSTANT MECHANICAL POWER,
(B) FREQUENCY DEPENDENT MECHANICAL POWER,
FROM (HILLBERG AND TOFTEVAAG 2012)

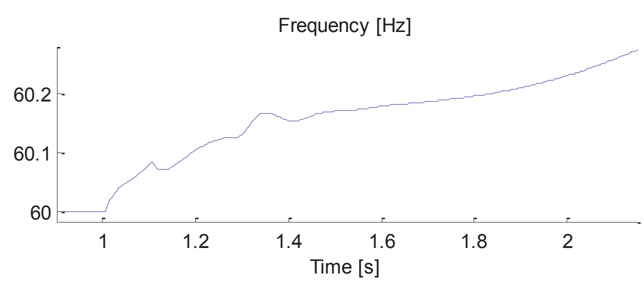

FIGURE 32: FREQUENCY IN AREA C DURING THE CRITICAL DISTURBANCE MEASURED AT THE B-C TIE LINE, FROM (HILLBERG AND TOFTEVAAG 2012)

To check the validity of the assumption that during the transient phase of the disturbance the mechanical power of the sub-system can be approximated using the speed-droop, the mechanical power of all machines in area C is reproduced in Figure 33.

A

B

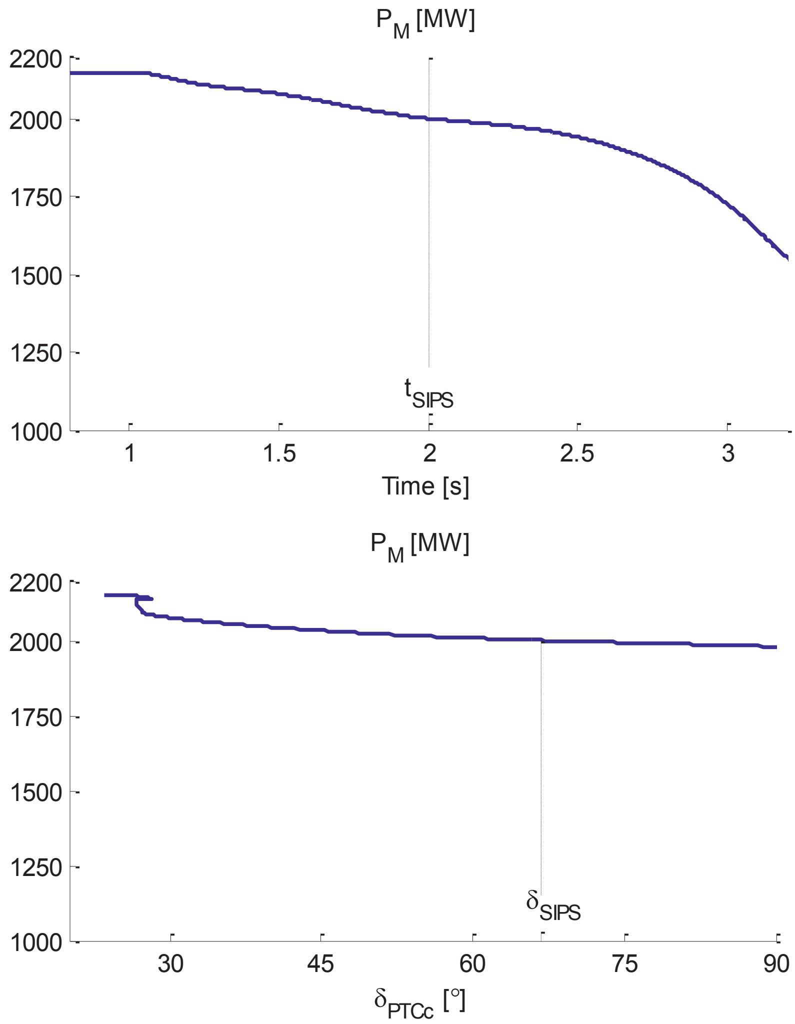

FIGURE 33: TOTAL MECHANICAL POWER OF MACHINES IN AREA C (P_{MG}), AS A FUNCTION OF TIME (A), AND ANGLE DIFFERENCE OVER PTC_C (B).

It is noticed that the response of the machines result in a continuous decay in mechanical power (P_{MG}) during the studied time interval. The activation instant of the SIPS is assumed as previously mentioned, resulting in a decrease in P_{MG} between 5-10% from the pre-fault state to the SIPS activation instant. Relating the mechanical power of all machines in area C to the voltage angle difference over PTC_C, P_{MG} shows a more rapid decay during the first part of the increase in angle. This behaviour is similar to the approximation of $P_M(\Delta\omega)$, shown in Figure 31B. Normalising P_{MG} on the pre-contingency steady-state power exchange from area C, the results from Figure 33B and Figure 31B may be compared, as shown in Figure 34. This comparison shows a similar behaviour in the decay, however the decay in P_{MG} is less than for $P_M(\Delta\omega)$. This difference results in a higher accelerating torque, which is approximated to:

$$A_{acc}|P_{MG} = 3700\text{MW}°$$

The main reason for this difference lies in the time delays of governors, which has been neglected when calculating $P_M(\Delta\omega)$. The accelerating torque is however considerably less than for P_{0M}.

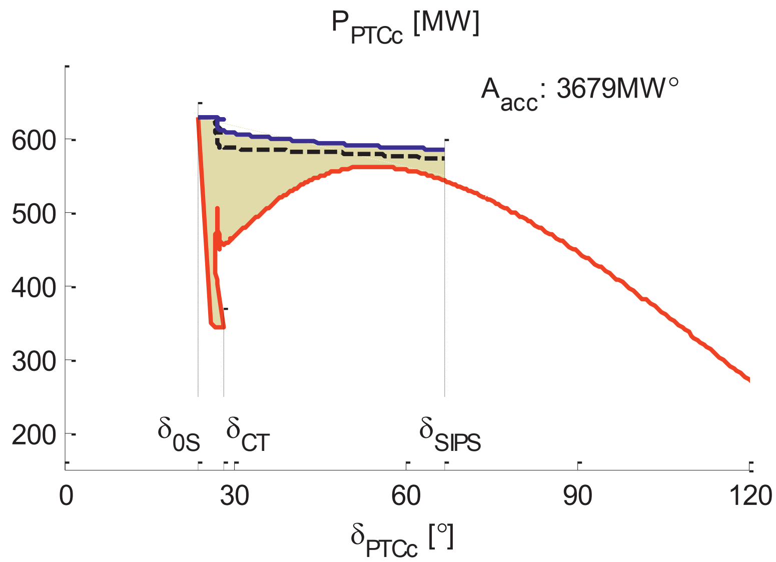

FIGURE 34: ACCELERATING TORQUE ASSESSMENT FOR P_{MG}, INCLUDING CURVE FOR $P_M(\Delta\omega)$

The conclusions from this validity check is that:

> *Assuming constant mechanical power of machines (i.e. $P_M = P_{0M}$) during the transient phase of a disturbance results in a largely conservative SIPS solution.*

The assumption that the response of the system can be approximated by a speed-droop, i.e. $P_M = P_M(\Delta\omega)$, provides results similar to when considering the total governor dynamics – however, with a more optimistic calculation of the accelerating torque. It should be noted that the equivalent mechanical power of a system may also depend on the loads in the system, which further complicates assessment of the true accelerating and decelerating torques.

In the following study, it is considered that the assumption $P_M = P_M(\Delta\omega)$ can be used to calculate the accelerating area with sufficient details to decide whether the system can return to a stable state of operation. Therefore, the continued design of the SIPS is based on an accelerating torque equal to 3000MW°.

Assuming that the effect on the frequency in area C by the SIPS activation can be approximated by a linear decay, where nominal frequency is reached at the maximum angle, δ_M, the decelerating area can be assessed as shown in Figure 35. The minimum level of rejected generation that fulfils the equal-area criterion is then approximated to:

$$P_{SIPS} \geq 206\text{MW}$$

resulting in a maximum angle equal to:

$$\delta_M = 99°$$

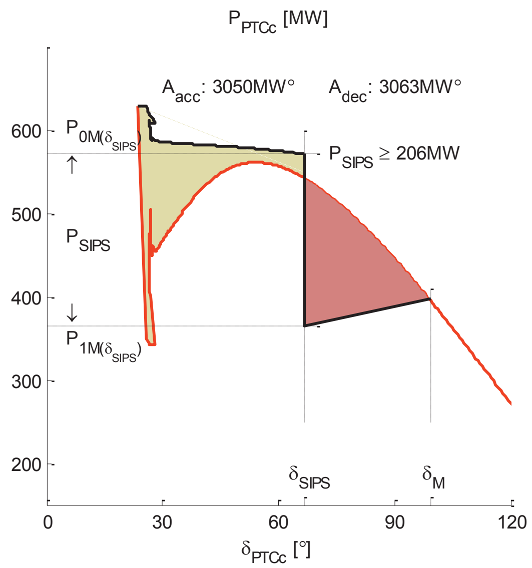

FIGURE 35: DECELERATING TORQUE ASSESSMENT, FROM (HILLBERG AND TOFTEVAAG 2012)

The functionality of eight different SIPS schemes have been assessed utilising the identified minimum level of rejected generation. All generations in area C have been considered during the selection process, and Table VII lists the available generators together with their pre-fault steady state production level and the related SIPS schemes.

There are two criteria in the selection procedure of generators that should be addressed:

1. The generators should have a power production level corresponding at least to the minimum level of mitigating actions.
2. The impact on the sub-system and on the PTC characteristics should be limited in order for the equal-area criterion to be utilised.

For SIPS schemes with rejection of a single generator, only the machines on bus 321 and 323 (G3) have sufficient production, i.e. $P_G \geq P_{SIPS}$. These machines are selected to represent the schemes $SIPS_{A1}$ and $SIPS_{A2}$, respectively. Various generator selections are possible for SIPS schemes based on tripping several generators. Here three schemes have been selected: $SIPS_{B1\text{-}B3}$. The schemes $SIPS_{C1\text{-}C3}$ are based on single machines with production less than the identified minimum P_{SIPS} level.

TABLE VII. SIPS SCHEMES FOR GENERATORS IN AREA C,
FROM (HILLBERG AND TOFTEVAAG 2012)

Bus number and generator ID	Pre-fault production (MW)	SIPS ID	
302 G1	10		B3
302 G2	10		
313 G1	197		B3
313 G2	197	C1	
313 G3	197		
315 G1-5	5x12		
315 G6	155	C2	B2
316 G1	114	C3	B2
321 G1	400	A1	
322 G1-6	6x25		
323 G1	155		B1
323 G2	155		B1
323 G3	350	A2	

The selected SIPS schemes are based only on the criteria of sufficient production level of the selected generators. The machines' impact on the PTC and the sub-system can be difficult to anticipate, but the machines' reactive power capability and the relative closeness to the PTC may be used to determine their influence on the voltage level of the PTC busses. From the single-line diagram, presented in Appendix A, it is noticed that bus 321 ($SIPS_{A1}$) is relatively close to the PTC bus, thus this scheme might cause voltage instability in the sub-system.

The system response to the selected SIPS schemes have been analysed, with results shown in Table VIII, Figure 36 and Figure 37.

TABLE VIII. SIPS ACTIVATION RESULTS,
FROM (HILLBERG AND TOFTEVAAG 2012)

SIPS ID	Rejected power P_{SIPS} (MW)	Maximum angle δ_M (°)	Decelerating area A_{dec} (MW°)	Post-SIPS PTC power transfer P_{M1} (MW)
A1	400	- (unstable)		
A2	350	76	3000	420
B1	310	77	2800	450
B2	269	82	3100	470
B3	207	83	2000	500
C1	197	84	1800	500
C2	155	84	1400	520
C3	114	- (unstable)		

As anticipated, $SIPS_{A1}$ results in an unstable system. This is due to the location and size of the generator that is rejected in this scheme, leading to a significant voltage drop at the PTC and the system is not able to regain stability. Also $SIPS_{C3}$ proved insufficient, which was expected from the insufficient level of rejected power.

$SIPS_{A2,\ B1,\ B2}$, shown in Figure 36, all respond as expected, resulting in stable operation with calculated decelerating torque approximately equal to the assessed accelerating torque. Better approximations of the accelerating and decelerating torque may be achieved by considering how the demand is affected by voltage changes in the sub-system. Furthermore, the participation of each machine in the acceleration of the sub-system also affects the results. Since the accelerating area of the PTC consists of the participation of each machine, the contribution of the rejected machines should be deducted from the total acceleration.

It should be noted that the schemes $SIPS_{B3,\ C1,\ C2}$, shown in Figure 37, have decelerating areas considerably smaller than expected. This is related to the reactive power capability of the machines participating in these schemes. The generators in these schemes were at their under-excitation limit, thus disconnecting these generators resulted in a voltage rise at the buses in the surrounding area affecting the total load of area C. Following the dynamic representation of loads, described in Appendix A, a rise in bus voltage on the load buses lead to increased active and reactive load. In this way, these SIPS schemes also increase the load of the sub-system, resulting in further decrease of the equivalent mechanical power of the sub-system. Hence, in order to properly assess the decelerating areas, also the SIPS affect on the load needs to be considered in the equivalent mechanical power.

From the results presented here, two main conclusions may be drawn:

1. It is possible to utilise the concept of applying the equal-area criterion on a power transfer corridor to design the functionality of SIPS.
2. It is not as straightforward to assess the accelerating and decelerating torques as simplified theoretical models would imply, meaning that:
   i. Realistic dynamic modelling, of e.g. turbine-governor systems, is required to simulate and assess transient stability margins.
   ii. Voltage and frequency dependencies of load, production, and losses, are needed to be considered when assessing the equivalent mechanical power of a system.

Assumptions regarding the equivalent mechanical power of the sub-system prove to be of high importance for the success of the proposed concept. The speed-droop characteristic and reactive power capabilities of generators, as well as the voltage dependency of loads, have significant impact on the results. The uncertainties in the approximation of sufficient rejected production, as well as the system impact by the rejected machines, may constitute a challenge during SIPS design in this context. SIME based approaches solve this difficulty by assuming that measurements of electrical and mechanical power, speed, acceleration, etc. are made available for all machines. The equivalent accelerating power of the OMIB is then calculated in the SIME, based on the machine inertia together with machine angles, electrical and mechanical powers measured at all generators in the system. One limitation to such approach is that it is unlikely that all measurements are available from all machines in a large power system.

Utilising this SIPS design concept, based on the *EAC on PTC* concept, it is possible to identify sufficient SIPS actions to prevent instability. This concept has the benefit of direct identification of the secure power transfer capacity, from the transient stability margins of the system including SIPS action.

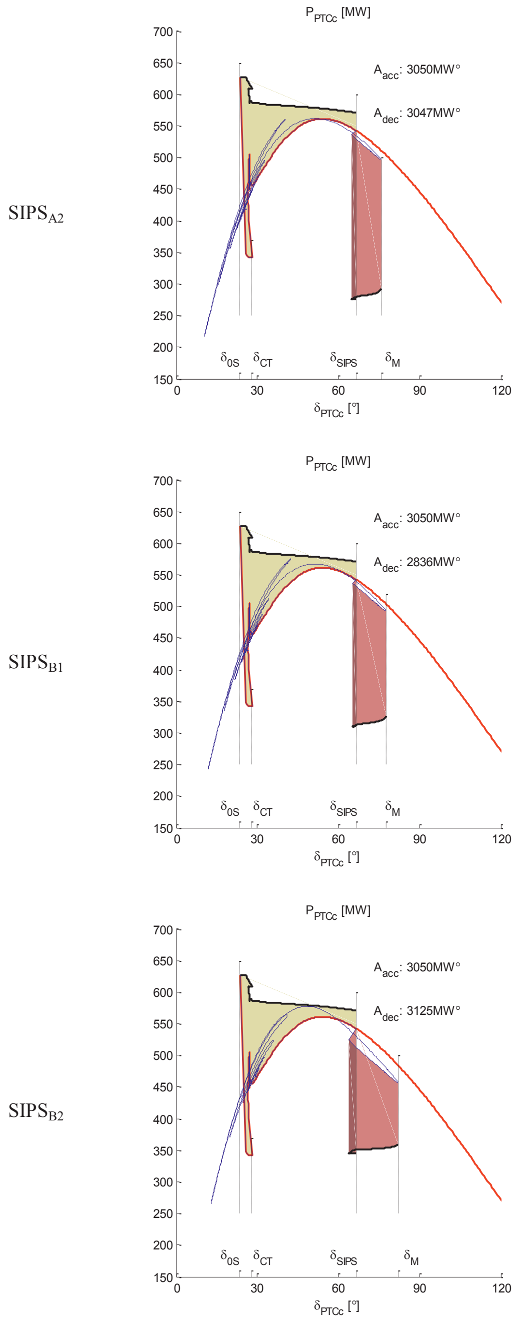

FIGURE 36: RESULTS FROM SIPS SOLUTIONS A2, B1 & B2, FROM (HILLBERG AND TOFTEVAAG 2012)

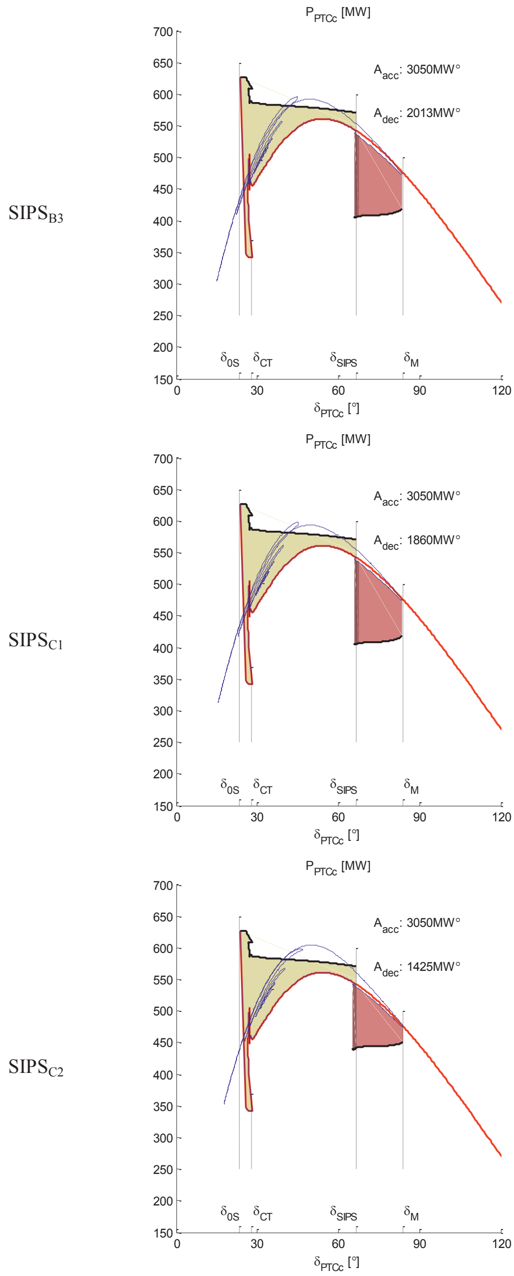

FIGURE 37: RESULTS FROM SIPS SOLUTIONS B3, C1 & C2, FROM (HILLBERG AND TOFTEVAAG 2012)

4.4 Summary

Power system initiated extraordinary events may be prevented by various means, and the most obvious solution is over-dimensioning. More economically viable solutions are often related to the operation and control of the power system, focusing on areas such as enhanced monitoring and protection. In this thesis, solutions related to improved situational awareness have been in focus since insufficient situational awareness makes the system increasingly vulnerable to extraordinary events.

Through the methodology for analysing extraordinary events, the k_{min} vulnerability indicator and the *$N-k$ secure operating region* are proposed to provide the operator with information related to multiple contingencies for specific operating scenarios. These vulnerability indicators provide information on the distance to instability, and this chapter presents suggestions on how they could be utilised during operation and in the day-ahead planning. The main value of these indicators is to increase the awareness of vulnerabilities related to the actual and to the predicted future operating states.

The results from the case studies presented in this chapter highlight the value of dynamic analyses, and illustrate that *analyses based on steady-state tools may overestimate the security of the system as they do not reveal vulnerabilities related to the dynamic response of the system*. The results also illustrate the value of analysing multi-level contingencies to identify changes in system response and to raise the awareness of vulnerabilities to extraordinary events.

As analyses of extraordinary events require transient dynamic studies, solutions related to the awareness of transient stability limits have been studied. Novel concepts are presented in relation to the transient stability equal-area criterion: the utilisation of the EAC on power transfer corridors. The *EAC on PTC* concept, utilised to assess secure power transfer capacities and to design SIPS to prevent instability, represents an improved defence against extraordinary events and is referred to as scientific contribution C_1.

CHAPTER 5
SUMMARY OF APPENDED PAPERS

5.1 Paper I

Extraordinary events: understanding sequence, causes, and remedies

Emil Johansson, Kjetil Uhlen, Agnes Nybø, Gerd Kjølle, & Oddbjørn Gjerde
European Safety & Reliability Conference, Rhodes, Greece
(Johansson et al. 2010)

This paper was written mainly by the author. Co-authors have actively contributed with comments, restructuring, text improvements and rephrasing.

This paper is based on a literature study of extraordinary events, including a generalised sequence of events which has been further revised by the author as presented in Chapter 2. The identification of situational awareness as a root cause in many events has been an important factor during the work, focusing on possibilities to improve the operators' awareness to decrease the vulnerability to extraordinary events in the power system.

ABSTRACT

Increased understanding of extraordinary events in the electric power system is vital in order to develop and assign appropriate remedies to limit the presence and consequences of such events in the future. In this paper, extraordinary events are analysed in order to identify general patterns in the sequence of event, causes, and potential remedies. The generalised discussion is supported by a case study of historical events from the U.S.-Canadian and continental European power systems. Results show that there are correlating factors between the proposed generalised structure of events and the events analysed in the case study, supporting the generalisation of extraordinary events. Improvements of monitoring systems and controlled islanding schemes are remedial actions identified to have considerable potential for decreasing the vulnerability of extraordinary events. Such actions may lead to increased situational awareness and limitation of disturbance propagation and the consequences of extraordinary events.

5.2 Paper II

Reliability evaluation of wide area monitoring applications and extreme contingencies

Emil Johansson, Kjetil Uhlen, Gerd Kjølle & Trond Toftevaag
Power Systems Computation Conference, Stockholm, Sweden
(Johansson et al. 2011b)

This paper was written mainly by the author. Co-authors contributed with the development of the final model, as well as with comments, text improvements and rephrasing.

This paper describes the importance of the dynamic model when assessing the reliability of a power system, and includes a proposed improvement of the dynamic model of the reliability test model *IEEE Reliability Test System 1996*. The developed dynamic models have been utilised in the studies described in Paper III (Hillberg et al. 2012c) and Paper V (Hillberg and Toftevaag 2012).

ABSTRACT

In order to perform reliability assessment studies involving the influence of WAMS with regard to extreme contingencies, it is essential to have a good representation of the dynamic behaviour of the system. This paper describes a proposed improvement of the benchmark model *IEEE Reliability Test System 1996*. The dynamic behaviour of the proposed model is illustrated with results from dynamic simulations.

5.3 Paper III

System integrity protection schemes – increasing operational security and system capacity,

Emil Hillberg, Frode Trengereid, Øyvind Breidablik, Kjetil Uhlen, Gerd Kjølle, Stig Løvlund & Jan Ove Gjerde

CIGRE Session 44, Paris, France
(Hillberg et al. 2012c)

This paper was written mainly by the author. Frode Trengereid has contributed to the overview and statistics regarding the Norwegian SIPS installations. Further text improvements were based on input from the co-authors and the Norwegian CIGRE reviewing committee.

The importance of transient stability is described in this paper, suggesting the incorporation of dynamic simulations in security assessment studies. An $N-k$ secure operating region is suggested to be used as a visualising aid to improve the operators' awareness of the vulnerability of the system to extraordinary events. The paper includes a case study of the *IEEE Reliability Test System 1996*, utilising the dynamic models developed in Paper II (Johansson et al. 2011b).

ABSTRACT

System Integrity Protection Schemes (SIPS) are increasingly utilised in power systems worldwide to provide additional power transfer capacity and enhanced operational security. The implementation of Phasor Monitoring Units (PMU) and Wide Area Monitoring Systems (WAMS) provide opportunities to improve the conventional system integrity protection. These improvements can increase the awareness of the protection schemes to the system state, providing robustness towards unforeseen disturbances and enhanced operational security with regard to extraordinary events.

This paper describes a technique of how to assess the security to extraordinary events, where the concept of a secure operating region is extended to involve multiple contingencies, referred to as the *$N-k$ secure operating region*. This paper also includes an overview of the SIPS in the Norwegian power system, and a security assessment study performed using the *IEEE Reliability Test System 1996*. The study includes conventional and WAMS- based SIPS solutions, and demonstrates the importance of incorporating dynamic contingency analysis when assessing the security of a power system.

5.4 Paper IV

Revealing stability limitations in power system vulnerability analysis

Emil Hillberg, Jarno Lamponen, Liisa Haarla & Ritva Hirvonen
Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, Cagliari, Italy
(Hillberg et al. 2012b)

This paper was written in cooperation with Jarno Lamponen, PhD candidate, and Professor Liisa Haarla, both with the Aalto University School of Electrical Engineering, Espoo, Finland, and Dr Ritva Hirvonen with Fingrid Oyj, Helsinki, Finland. There has been a very close cooperation during the whole process of writing the paper, where the three first authors have actively contributed to most parts of the paper. Dr. Hirvonen has actively contributed with comments, text improvements and rephrasing.

The development of the $N-k$ *vulnerability* concept, the k_{min}*-index*, and the definition of the *blackout process* are the result of joint work by Emil Hillberg and Jarno Lamponen.

In this paper, the correlation between instability and blackout is analysed, concluding that all extraordinary events occur as the result of loss of stability. This leads to the development of the $N-k$ *vulnerability* concept and the k-index, which defines the closeness of the system to instability as a function of consecutive outages. This has further influenced the development of the $N-k$ *secure operating region* used in Paper III (Hillberg et al. 2012c) as well as the *visualisation of the* $N-k$ *secure operating domain*.

ABSTRACT

Creating defence plans against extreme contingencies requires knowledge of the principal vulnerabilities of power systems. This paper describes the blackout phenomenon as a process with separate phases and distinctive transitions. The paper proposes two indicators that can help to identify vulnerabilities in a specific operating scenario and recommends that the dynamic behaviour of a power system after successive faults should be analysed. This analysis would reveal vulnerabilities connected to high impact low probability contingencies where the system response can change after several successive contingencies. These vulnerabilities cannot be captured by steady state analyses. Analyses of some recent large European blackouts, presented in the paper, indicate that a power system may collapse after only a limited number of contingencies, implying that these power systems are more vulnerable to multiple contingencies than the system operators may be aware of.

5.5 Paper V

Equal-area criterion utilised in system integrity protection scheme design

Emil Hillberg & Trond Toftevaag
IASTED Asian Conference on Power and Energy Systems, Phuket, Thailand
(Hillberg and Toftevaag 2012)

This paper was written mainly by the author. Trond Toftevaag contributed to the development of concepts, as well as with comments, text improvements and rephrasing

The concept of applying the equal-area criterion on a critical PTC is described in this paper, providing a novel measure to assess the secure power transfer of critical power transfer corridors. The concept is tested and applied in the design procedure of a SIPS, using the *IEEE Reliability Test System 1996* with the dynamic models developed in Paper II (Johansson et al. 2011b).

ABSTRACT

This paper presents a novel adaptation of the equal-area criterion. The adapted criterion provides a new possibility to study the stability criteria of critical power transfer corridors, supporting the specification of the secure power transfer capacity of the interconnected power system.

Furthermore, the authors describe how the adapted equal-area criterion can be employed in the design of System Integrity Protection Schemes to prevent instability and mitigate consequences of extraordinary events. The concept is tested on the benchmark model: *IEEE Reliability Test System 1996*.

5.6 Paper VI

The change of power system response after successive faults

Jarno Lamponen, Emil Hillberg, Liisa Haarla & Ritva Hirvonen
Power Systems Computation Conference, Wroclaw, Poland
(Lamponen et al. 2014)

This paper was written in cooperation with Jarno Lamponen, PhD candidate, and Professor Liisa Haarla, both with the Aalto University School of Electrical Engineering, Espoo, Finland, and Dr Ritva Hirvonen with Fingrid Oyj, Helsinki, Finland. There has been a very close cooperation during the whole process of writing the paper, where the three first authors have actively contributed to most parts of the paper. Dr. Hirvonen has actively contributed with comments, text improvements and rephrasing.

The methodology development and case study are the result of joint work by Emil Hillberg and Jarno Lamponen.

This paper is a continuation of the work presented in (Hillberg et al. 2012b), where the k_{min} vulnerability indicator is presented as a mean to quantify vulnerabilities to large disturbances. In (Hillberg et al. 2012b), this indicator is utilized in an analysis of large European blackouts. In this paper, the k_{min} vulnerability indicator is utilized for a case study of the *IEEE Three Area Reliability Test System 1996* to quantify vulnerabilities related to dynamic instability.

ABSTRACT

This paper illustrates the usefulness of visualizing the secure operating domains and the value of dynamic analyses when considering the vulnerability of a power system. The paper includes studies of the secure power transfer limits and vulnerabilities of the *IEEE Reliability Test System 1996*. The limits and vulnerabilities are determined by simulating the dynamic response of single and multiple faults. The results are presented by visualizing the secure transfer domains as a function of the power flow on critical transfer corridors. The paper also provides an estimate for the frequency of blackouts related to the different operating domains. The results show how the vulnerability of the power system increases in steps as the amount of power transfer over a corridor increases.

CHAPTER 6
SUMMARY OF THE THESIS

6.1 Conclusions & discussion

The objective of this PhD project has been to *develop models and methods to analyse the risk of extraordinary events*, limited to study only extraordinary events which are initiated by power system related factors.

This work has been focusing on the analysis of extraordinary events from an operational point of view, and not from a planning perspective.

Conventional risk and reliability assessment techniques are insufficient when it comes to analysing extraordinary events online. With extraordinary events being the result of dependent or multiple failures leading to an unstable operation, conventional techniques are unable to identify and quantify their risk. Thus, novel and unconventional techniques are required to analyse and quantify the risk related to extraordinary events.

This thesis describes advances regarding *perception*, *prediction*, and *prevention* of extraordinary events.

6.1.1 Perception of extraordinary events

In order to address the risk of extraordinary events, the events themselves need to be understood. Therefore, this part of the project has been focusing on answering the research question:

- *What are the critical characteristics of extraordinary events?*

As any extraordinary event is unique, there is no simple answer to this question. Furthermore, the perspective and objective of the perceiver all influence how critical characteristics are interpreted. This PhD work has been studying extraordinary events from the perspective of the system operator, with the objective to improve the security and the capacity of the power system. Therefore, the characteristics of extraordinary events having critical impact on the operation and control of the power system have been in focus here.

Perception of extraordinary events is described in Chapter 2, including a description of a generic sequence of event. The transition to unstable operation is a part of this sequence, and is identified as a point in the event sequence after which the response of the system completely changes. From the system operator's perspective, the most important objective during operation is to prevent instability in order to maintain a steady-state operation of the power system. Therefore, in this thesis:

- *The transition from stable to unstable operation is defined as a fundamental and critical characteristic of extraordinary event.*

This implies that it is imperative to identify events leading to instability in order to assess how vulnerable the actual operation is to extraordinary events. Investigating extraordinary events from other perspectives, different characteristics are likely to be considered as critical – where timely and adequate preventive maintenance may be considered a critical aspect from a long-term planning perspective. Such investigations have however not been part of the scope of this work.

6.1.2 Prediction of extraordinary events

In order to predict extraordinary events, the critical characteristics of the events must be studied. Therefore this part of the project has been focusing on answering the research question:

- *How can the risk of critical characteristics of extraordinary events be addressed?*

From the working perspective of this thesis, this question is rephrased to:

- *How can the risk of transition to an unstable operation be addressed?*

Implying the need to assess events leading to instability. In the case where the power system is operated according to the $N-1$ reliability criterion, this question relates to the systems reliability with regard to multiple contingencies. It is obvious that this question relates to a connection between the three expressions: *risk*, *reliability*, and *stability*. With risk being an all-embracing expression, this thesis only addresses risk from a highly limited viewpoint: first of all, only risk related to extraordinary events from an operational perspective is considered; secondly, due to the significant uncertainties related to the terms probability and consequence of extraordinary events, risk is only addressed through vulnerability indicators.

The question also opens the discussion regarding the risk that the actual operating state of the system is unknown to the operator. It is likely that there are limitations to the situational awareness of the operator. The extent of such limitations impact the level of unknown vulnerabilities that the system is in fact exposed to. This is a factor that largely impacts the possibilities for the operator to implement appropriate actions to prevent a large disturbance. Sufficient situational awareness is thus a basic requirement to be able to predict and prevent extraordinary events.

In Chapter 3, the interrelation between risk, reliability, and stability is presented, identifying requirements related to the analysis of extraordinary events. One of the main conclusions from these requirements is that: *Relying only on steady-state power flow calculations inherently underestimates the vulnerability of the system.* The framework that these requirements form, with regard to extraordinary events, specify that:

- *In order to address the risk of transition to an unstable operation, it is required to perform transient dynamic multi-level contingency analyses.*

Based on this requirement, the risk of transition to an unstable operation may be addressed through the two proposed vulnerability indicators: the k_{min}*-index* and the visualising of the $N-k$ *secure operating region.* These indicators should not be regarded as operating criteria (such as the $N-1$ criterion), but as indicators of how vulnerable the system is to extraordinary events. Utilising these indicators, system vulnerabilities may be identified thus predicting extraordinary events during operation.

Implementing the proposed indices require tools that are able to perform multilevel transient dynamic contingency analyses on-line, which is highly complex and computer intense. There are to this date no commercial tools available to perform such task.

6.1.3 Prevention of extraordinary events

The focus of this part of the project has been on answering the research question:

- *How can critical characteristics of extraordinary events be averted?*

Averting extraordinary events may be done by various means, where the most obvious solution may be over-dimensioning. More economically viable solutions are often related to the operation and control of the power system, focusing on areas such as enhanced monitoring and protection. Situational awareness is identified as a basic requirement to be able to prevent extraordinary events, thus improved situational awareness may provide possibilities to prevent extraordinary events.

As described by the sequence of extraordinary events presented in Chapter 2, manual prevention techniques are possible to implement if the operator is aware of the vulnerability of the situation in a timely manner. Studies of historical events show that after the triggering failure there is often sufficient time to implement manual actions to prevent the system from further deterioration. However, due to insufficient situational awareness the system may continue to operate in a state where the system is highly vulnerable and further failures may result in large disturbances.

After the system has passed from stable to an unstable operation, manual actions are no longer possible to prevent an extraordinary event. This is due to the change in system response, where the state of an unstable system changes too fast for the operator to manually identify the actions which would be able to take the system back to another steady state. Therefore, at this stage remedial actions are only possible through predesigned automatic control and protection systems, i.e. SIPS. Such remedial actions are difficult to design and increase the complexity of the power system. However, with insufficient remedial actions the instability of the system will lead to the triggering of multiple component protections, resulting in a large and uncontrolled disturbance which may affect a widespread region.

The methodology presented in Chapter 3 provides possibilities to enhance the situational awareness related to extraordinary events. Here, the k_{min} and the $N-k$ *secure operating region* are suggested to indicate the vulnerabilities of the situation. It is also possible to utilise k_{min} as an on-line predictor, i.e. a leading vulnerability indicator, to provide information on how the vulnerability may develop for future states. Other vulnerability indicators may be identified, but to provide information on the vulnerability of the operating state with regard to extraordinary events, it is required to study the systems dynamic response to multi-level contingencies during operation.

The equal-area criterion may be utilised to define transfer capacities of critical power transfer corridors, as presented in Chapter 4. This *EAC on PTC* concept is suggested to be utilised to improve the design of SIPS to prevent instability in the cases where critical contingencies may result in the separation of a system. However, it is necessary to further refine this method to be able to implement it in a real system – specifically regarding assessment of the equivalent mechanical power which has a large impact on the method. Many similar approaches have been developed previously, based on e.g. the SIME method. The main difference between the *EAC on PTC* approach and other EAC based methods is the direct utilisation of actual power flow and angle differences over a set of transmission lines, instead of the assessing power and angles between equivalent models. Even though not explicitly studied here, it may be assumed that the *EAC on PTC* concept is valid in cases where out-of-step relays are designed to act in order to actively sectionise a system which is subject to a disturbance resulting in the loss of synchronism within the system. This kind of relays is implemented in many power systems, and the *EAC on PTC* concept would in many cases be able to provide another solution than system separation to prevent the loss of synchronism thus preventing large disturbances.

6.2 Suggestions for future work

Perception, prediction, and prevention of extraordinary events are broad research areas where many challenges and opportunities are still to be found. Conventional risk and reliability assessment techniques provide limited value in the analysis of extraordinary events from an operational perspective, thus the development and implementation of novel and unconventional methods and techniques are of paramount importance in order to predict and prevent future extraordinary events. In this section, some thoughts are gathered concerning valuable areas for further research and development.

The predictive and preventive measures presented in this thesis describe conceptual solutions for decreasing the risk of extraordinary events. These measures depend on further development of tools and techniques in order to be integrated in, and supportive for, the existing tools used in operation of the power system.

- With instability being a critical characteristic of extraordinary events, it is important to carry out online stability analyses to provide information on the distance to instability after sudden changes in the power system. To be able to perform multi-level dynamic contingency analyses during operation, increased requirements are placed on component modelling, simulation tools, as well as on state estimation.
- Due to the complexity of performing dynamic simulations, it is needed to further explore solutions for limiting the number of simulations required to identify critical contingencies.
- PMU and WAMS are identified as enabling technologies, and their implementation in the power system is a necessity for measures to improve the situational awareness as well as for the future development of the power system.
- The utilisation and dependency of SIPS in the operation of the power system involve additional risk aspects and may add complexity to the everyday work of the system operator. Identifying and assessing these risks, as well as identifying the pros and cons of specific SIPS, are important tasks to perform before deciding on implementation of new protection systems.
- The limitations of relying on the $N-1$ criterion to limit the risk of extraordinary events opens up the discussion on the value of developing other operating criteria, based for example on stability and reliability aspects.
- If consequence analysis is to be considered in the analysis of extraordinary events, the consequences of system instability needs to be studied. This places considerable requirements on the modelling of component protections as well as other automatic actions of the power system.

– Analysing actual or realistic event sequences, to study and identify system criticalities, is an important topic which forms a formidable task. The timing of actual faults and protective actions is highly complex where, for example, faults occurring due to excessive sagging of overloaded lines depend on the actual distance to the ground and the thermal heating of the line, which depends on the loading of the line and the wind speed among many other parameters.

The need to perform dynamic contingency analysis on-line is not only a requirement to assess the risk of extraordinary events, but it will become a necessity when operating the power systems closer to their limits. In these cases, relying on safety margins based on steady state simulations becomes increasingly risky and blackouts may no longer be so extraordinary.

REFERENCES

Anderson, P.M., LeReverend, B.K. (1996), *Industry experience with special protection schemes, IEEE/CIGRÉ Committee Report,* IEEE Transactions on Power Systems, Vol. 11, p. 1166-1176

Aven, T. (2010), *On how to define, understand and describe risk,* Reliability Engineering & System Safety, Vol. 95, p. 623-631

Balu, N., Bertram, T., Bose, A., Brandwajn, V., Cauley, G., Curtice, D., Fouad, A., Fink, L., Lauby, M.G., Wollenberg, B.F., Wrubel, J.N. (1992), *On-Line Power System Security Analysis,* Proceedings of the IEEE, Vol. 80, p. 262-280

Barkans, J., Zalostiba, D. (2009), *Protection against Blackouts and Self-Restoration of Power Systems*, Riga, RTU Publishing House

Billinton, R., Allan, R.N. (1984), *Power-system reliability in perspective,* Electronics and Power, Vol. 30, p. 231-236

Breidablik, Ø., Giæver, F., Glende, I. (2003), *Innovative Measures to Increase the Utilization of Norwegian Transmission*, IEEE Power Tech Conference, Bologna, Italy

Carreras, B.A., Newman, D.E., Dobson, I., Poole, A.B. (2004), *Evidence for self-organized criticality in a time series of electric power system blackouts,* IEEE Transactions on Circuits and Systems-I: Regular Papers, Vol. 51, p. 1733-1740

Chenine, M., Karam, E., Nordström, L. (2009), *Modeling and simulation of wide area monitoring and control systems in IP-based networks*, IEEE/PES General Meeting

Chipp, H. (2010), *The Brazilian Blackout, November 10th 2009*. Cigré Session, Workshop on Large Disturbances, Paris; Available from: www.cigre.org/

CIGRE (1987), *Power system reliability analysis, Application guide,* CIGRE Working Group: 38.03, Technical Brochure: 026

CIGRE (1997), *Power system security assessment: A position paper,* CIGRE Task Force: 38.03.12, ELECTRA, no. 175, Dec.

CIGRE (2001), *System Protection Schemes in Power Networks,* CIGRE Task Force: 38.02.19, Technical Brochure: 187

CIGRE (2007a), *Defence Plan Against Extreme Contingencies,* CIGRE Task Force: C2.02.24, Technical Brochure: 316

CIGRE (2007b), *Review of On-line Dynamic Security Assessment Tools and Techniques,* CIGRE Working group C4.601 Technical Brochure 325

CIGRE (2010a), *Planning to manage power interruption events,* CIGRE Working Group: C1.17, Technical Brochure: 433

CIGRE (2010b), *Review of the Current Status of Tools and Techniques for Risk-Based and Probabilistic Planning in Power Systems,* CIGRE Working Group: C4.601, Technical Brochure: 434

Cirio, D., Lucarella, D., Massucco, S. (2008), *On-line dynamic security assessment to mitigate the risk of blackout in the Italian power system,* European Transactions on Electrical Power, Vol. 18, p. 784-801

Cooke, D. (2005), *Learning from the Blackouts - Transmission System Security in Competitive Electricity Markets,* International Energy Agency (IEA)

DKE-IEV (2007), *Deutsche Online-Ausgabe des IEV (German on-line edition of the International Electrotechnical Vocabulary IEC 60050)*. Available from: www.dke.de

DOE (1992), *Root Cause Analysis Guidance Document,* U.S. Department of Energy DOE-NE-STD-1004-92

Dong, Y., Pota, H.R. (1993), *Transient stability margin prediction using equal-area criterion,* Generation, Transmission and Distribution, IEE Proceedings C, Vol. 140, p. 96-104

Doorman, G., Kjølle, G., Uhlen, K., Huse, E.S., Flatabø, N. (2004), *Vulnerability analysis of the Nordic power system - Main Report - Report to the Nordic Council of Ministers,* SINTEF Energy Research, Technical Report: A5962

Doorman, G., Uhlen, K., Kjølle, G., Huse, E.S. (2006), *Vulnerability analysis of the Nordic power system,* IEEE Transactions on Power Systems, Vol. 21, p. 402-410

Dy Liacco, T.E. (1967), *The Adaptive Reliability Control System,* IEEE Transactions on Power Apparatus and Systems, Vol. PAS-86, p. 517-531

Efimov, D.N., Voropai, N.I. (2006), *Blackouts Analysis and Generalization*, 3rd Int. Workshop on Liberalization and Modernization of Power Systems - Risk Assessment and Optimization for Asset Management, Irkutsk, Russia

ELCON (2004), *The Economic Impacts of the August 2003 Blackout,* Electricity Consumers Resource Council

Elkraft (2003), *Power failure in Eastern Denmark and Southern Sweden on 23 September 2003 - Final report on the course of events,* Elkraft System

Energimyndigheten (2004), *Consequences of the power failure in southern Sweden (in Swedish: Konsekvenser av elavbrottet i Sydsverige den 23 september 2003),* Statens energimyndighet ER 4:2004

ENTSO-E (2010), *Operation Handbook Policy 5: Emergency Operation, v1,* The European Network of Transmission System Operators for Electricity

Ernst, D., Pavella, M. (2000), *Closed-loop transient stability emergency control*, IEEE/PES Winter Meeting

EU (2006), *Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment,*

EURELECTRIC (2004a), *Power Outages in 2003,* Union of the Electricity Industry, Task Force on: Power Outages, Ref: 2004-181-0007

EURELECTRIC (2004b), *Security of Electricity Supply,* Union of the Electricity Industry, Working Group: Security of Electricity Supply, Ref: 2004-180-0019

Filho, J. (2010), *Brazilian Blackout 2009,* PAC World Magazine, March,

Fink, L.H., Carlsen, K. (1978), *Operating under stress and strain,* IEEE Spectrum, Vol. 15, p. 48-53

Fosso, O.B. (1989), *Power System Operation in Normal and Alert State - With Emphasis on Stedy State Security Assessment and Control*, Trondheim, Norwegian Institute of Technology

Glavic, M., Ernst, D., Ruiz-Vega, D., Wehenkel, L., Pavella, M. (2007), *E-SIME - A method for transient stability closed-loop emergency control: achievements and prospects*, Bulk Power System Dynamics and Control - VII

Gomes, P. (2004), *New strategies to improve bulk power system security: lessons learned from large blackouts*, IEEE/PES General Meeting, Denver, Colorado, USA

Guertin, M.B., Albrecht, P.F., Bhavaraju, M.P., Billinton, R., Jorgensen, G.E., Karas, A.N., Masters, W.D., Patton, A.D., Reppen, N.D., Spence, R.P. (1978), *Reliability indices for use in bulk power supply adequacy evaluation,* IEEE Transactions on Power Apparatus and Systems, Vol. PAS-97, p. 1097-1103

Haque, M.H. (1994), *Equal-area criterion: an extension for multimachine power systems,* Generation, Transmission and Distribution, IEE Proceedings, Vol. 141, p. 191-197

Hillberg, E., Holen, A.T., Andersson, G., Haarla, L. (2012a), *Power System Reinforcements – the Hardanger Connection,* ELECTRA no. 260, Feb., p. 4-15

Hillberg, E., Lamponen, J., Haarla, L., Hirvonen, R. (2012b), *Revealing stability limitations in power system vulnerability analysis*, 8th Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, Cagliari, Italy

Hillberg, E., Toftevaag, T. (2012), *Equal-Area Criterion Applied on Power Transfer Corridors*, IASTED Asian Conference on Power and Energy Systems, Phuket, Thailand: ACTA Press

Hillberg, E., Trengereid, F., Breidablik, Ø., Uhlen, K., Kjølle, G., Løvlund, S., Gjerde, J.O. (2012c), *System Integrity Protection Schemes – Increasing operational security and system capacity*, 44th CIGRE Session, Paris, France

Huan, X., Bao-Hui, Z., Hao, T.Z.G., Wang, C.G., Peng, L., Cheng, L.Y., You, M., Bo, Z.Q., Klimek, A. (2008), *Study on closed-loop transient stability emergency control based on Wide Area Measurement*, IEEE/PES Transmission and Distribution Conference and Exposition: Latin America

IEC 600050 (1990), *International Electrotechnical Vocabulary (IEV)*

IEEE 1110 (1991), *IEEE Guide for Synchronous Generator Modeling Practices in Stability Analyses*

IEEE (1999), *The IEEE reliability test system - 1996,* Reliability Test System Task Force IEEE Transactions on Power Systems, Vol. 14, No.3

IEEE (2005), *IEEE Recommended Practice for Excitation System Models for Power System Stability Studies*

IEEE (2007), *Blackout Experiences and Lessons Best Practices for System Dynamic Performance, and the Role of New Technologies,* IEEE Task Force on: Blackout Experiences, Mitigation, and Role of New Technologies, Special Publication: 07TP190

IEEE (2012), *Identification of Electromechanical Modes in Power Systems,* IEEE Task Force on: Modal Identification of Electromechanical Modes, Special Publication: TP462

ISO Guide 73 (2009), *Risk management — Vocabulary*

Johansson, E., Uhlen, K., Kjølle, G. (2011a), *Mitigating Extraordinary Events using Wide Area Monitoring Applications*, CIGRE International Symposium, Recife, Brazil

Johansson, E., Uhlen, K., Kjølle, G., Toftevaag, T. (2011b), *Reliability evaluation of wide area monitoring applications and extreme contingencies*, 17th Power Systems Computation Conference, Stockholm, Sweden

Johansson, E., Uhlen, K., Leirbukt, A.B., Korba, P., Gjerde, J.O., Vormedal, L.K. (2009), *Coordinating Power Oscillation Damping Control using Wide Area Measurements*, IEEE/PES Power Systems Conference and Exposition, Seattle, Washington, USA

Johansson, E., Uhlen, K., Nybø, A., Kjølle, G., Gjerde, O. (2010), *Extraordinary events: Understanding sequence, causes, and remedies*, European Safety & Reliability Conference, Rhodes, Greece

Kile, H., Uhlen, K. (2012), *Supervised and Unsupervised Learning in Composite Reliability Evaluation*, IEEE/PES General Meeting, San Diego, California, USA

Kjølle, G., Gjerde, O., Hoffman, M. (2012), *Monitoring Vulnerability in Power Systems - Extraordinary Events, Analysis Framework and Development of Indicators*, 12th International Conference on Probabilistic Methods Applied to Power Systems, Istanbul, Turkey

Kjølle, G., Mogstad, O., Samdal, K. (2006a), *Analysis of faults and disruptions in the power system 1989-2005 (Norwegian: Analyser av feil of avbrudd i kraftnettet 1989-2005),* SINTEF Energy Research, Technical Report: A6451

Kjølle, G., Refsnæs, S., Nordgård, D.E. (2007), *Maintenance and security of supply in Nord-Salten (Norwegian: Vedlikehold og forsyningssikkerhet i Nord-Salten),* SINTEF Energy Research, Technical Report: A6555

Kjølle, G., Uhlen, K., Rolfseng, L., Stene, B. (2006b), *Vulnerability in power systems – a pre-study (Norwegian: Sårbarhet i kraftnett – en forstudie),* SINTEF Energy Research, Technical Report: A6223

Knight, U.G. (1989), *The Control of Power Systems During Disturbed and Emergency Conditions,* CIGRE Study Committee: 39, Technical Brochure: 36

Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C., VanCutsem, T., Vittal, V. (2004), *Definition and classification of power system stability,* IEEE Transactions on Power Systems, Vol. 19, p. 1387-1401

Lamponen, J., Hillberg, E., Haarla, L., Hirvonen, R. (2014), *The Change of Power System Response after Successive Faults*, 18th Power Systems Computation Conference, Wroclaw, Poland

Lu, W., Bésanger, Y., Zamaï, E., Radu, D. (2006), *Blackouts: Description, Analysis and Classification*, WSEAS International Conference on Power Systems, Lisbon, Portugal

Madani, V., Novosel, D., Horowitz, S., Adamiak, M., Amantegui, J., Karlsson, D., Imai, S., Apostolov, A. (2010), *IEEE PSRC Report on Global Industry Experiences With System Integrity Protection Schemes (SIPS),* IEEE Transactions on Power Delivery, Vol. 25, p. 2143-2155

Morison, K., Lei, W., Kundur, P. (2004), *Power system security assessment,* IEEE Power & Energy Magazine, Vol. 2, p. 30-39

NERC (1985), *Reliability concepts in bulk power systems,* North American Electric Reliability Corporation (NERC)

NERC (2010), *Reliability Assessment Guidebook, ver. 2.1,* North American Electric Reliability Corporation (NERC)

Nordel (2007), *The Nordic Grid Code,* Nordel

Nordgård, D.E. (2010), *Risk Analysis for Decision Support in Electricity Distribution System Asset Management*, Trondheim, Norwegian University of Science and Technology

Novosel, D., Begovic, M., Madani, V. (2004), *Shedding Light on Blackouts,* IEEE Power & Energy Magazine, Vol. 2, p. 32-43

ONS (2009), *Disturbance analysis report,* Operador Nacional do Sistema Elétrico (In Portuguese: Análise da Perturbação do dia 10/11/2009 às 22:13 Envolvendo o Desligamento dos Três Circuitos da LT 765 kV Itaberá-Ivaiporã), ONSRE-3-252/2009

Patel, S., Stephan, K., Bajpai, M., Das, R., Domin, T.J., Fennell, E., Gardell, J.D., Gibbs, I., Henville, C., Kerrigan, P.M., King, H.J., Kumar, P., Mozina, C.J., Reichard, M., Uchiyama, J., Usman, S., Viers, D., Wardlow, D., Yalla, M. (2004), *Performance of Generator protection during major system disturbances,* IEEE Transactions on Power Delivery, Vol. 19, p. 1650-1662

Pérez-Arriaga, I. (2007), *Security of electricity supply in Europe in a short, medium and long-term perspective,* European Review of Energy Markets, Vol. 5

Phadke, A.G., Thorp, J.S. (2006), *History and applications of phasor measurements*, IEEE/PES Power Systems Conference and Exposition, Atlanta, Georgia, USA

Phadke, A.G., Thorp, J.S., Adamiak, M.G. (1983), *A New Measurement Technique for Tracking Voltage Phasors, Local System Frequency, and Rate of Change of Frequency,* IEEE Transactions on Power Apparatus and Systems, Vol. PAS-102, p. 1025-1038

Pottonen, L. (2005), *A method for the probabilistic security analysis of transmissin grids*, Espoo, Helsinki University of Technology, Power Systems and High Voltage Engineering

Pourbeik, P., Kundur, P.S., Taylor, C.W. (2006), *The Anatomy of a power grid blackout,* IEEE Power & Energy Magazine, Vol. 4, p. 22-29

Qi, D. (2011), *Defense schema against large disturbances in China Southern Power grid,* ELECTRA, Vol. 257, p. 4-16

Rosales, R.A., Ruiz-Vega, D., Ernst, D., Pavella, M., Giri, J. (2000), *On-line transient stability constrained ATC calculations*, Power Engineering Society Summer Meeting, 2000. IEEE

Ruiz-Vega, D., Pavella, M. (2003a), *A comprehensive approach to transient stability control. I. Near optimal preventive control,* Power Systems, IEEE Transactions on, Vol. 18, p. 1446-1453

Ruiz-Vega, D., Pavella, M. (2003b), *A comprehensive approach to transient stability control. II. Open loop emergency control,* Power Systems, IEEE Transactions on, Vol. 18, p. 1454-1460

Sarmiento, H., Pampin, G., Barajas, R., Castellanos, R., Villa, G., Mirabal, M. (2009), *Nomograms for assistance in voltage security visualization*, IEEE/PES Power Systems Conference and Exposition, Seattle, Washington, USA

Savulescu, S. (2009), *Real-time stability assessment in modern power system control centers*. IEEE Press Series on Power Engineering, New Jersey, Wiley

Singh, C., Luo, X., Kim, H. (2006), *Power System Adequacy and Security Calculations Using Monte Carlo Simulation incorporating Intelligent System Methodology*, International Conference on Probabilistic Methods Applied to Power Systems, Stockholm, Sweden

Storvann, V. (2012), *Maintaining Voltage Stability: An Analysis of Voltage Stability Indicators and Mitigating Actions*, Trondheim, Norwegian University of Science and Technology, Department of Electrical Power Engineering

Storvann, V., Hillberg, E., Uhlen, K. (2012), *Indicating and Mitigating Voltage Collapse*, IEEE/PES Innovative Smart Grid Technologies, Berlin, Germany

Støa, P. (1986), *Reliability in a Bulk Power System - A Conceptual Study*, Trondheim, Norwegian Institute of Technology

SvK (2003), *The power failure 23 September 2003 – events and actions,* Svenska Kraftnät (In Swedish: Elavbrottet 23 september 2003 – händelser och åtgärder)

SvK (2012), *Kraftsystemet 2012, by Svenska Kraftnät*. Available from: www.svk.se

TaskForce (2004), *Final Report on the 2003 Blackout in the United States and Canada: Causes and Recommendations,* U.S.-Canada Power System Outage Task Force

UCTE (2004), *Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy,* Union for the Coordination of Transmission of Electricity (UCTE)

UCTE (2007), *Final Report - System Disturbance on 4 November 2006,* Union for the Coordination of Transmission of Electricity (UCTE)

Uhlen, K., Pálsson, M., Time, T.R., Kirkeluten, Ø., Gjerde, J.O. (2002), *Raising stability limits in the Nordic power transmission system*, 14th Power Systems Computation Conference, Sevilla, Spain

Vanfretti, L., García-Valle, R., Uhlen, K., Johansson, E., Trudnowski, D., Pierre, J.W., Chow, J.H., Samuelsson, O., Østergaard, J., Martin, K.E. (2010), *Estimation of Eastern Denmark's Electromechanical Modes from Ambient Phasor Measurement Data*, IEEE/PES General Meeting, Minneapolis, Minnesota, USA

Vournas, C.D., Nikolaidis, V.C., Tassoulis, A.A. (2006), *Postmortem analysis and data validation in the wake of the 2004 Athens blackout,* IEEE Transactions on Power Systems, Vol. 21, p. 1331-1339

Vrana, T.K., Johansson, E. (2011), *Overview of Analytical Power System Reliability Assessment Techniques*, CIGRE International Symposium, Recife, Brazil

Xue, Y., Van Cutsem, T., Ribbens-Pavella, M. (1988), *Real-time analytic sensitivity method for transient security assessment and preventive control,* Generation, Transmission and Distribution, IEE Proceedings C, Vol. 135, p. 107-117

Yi-qun, L., Lin, T., Wang-shun, L., Jian-fei, L. (2002), *The study on real-time transient stability emergency control in power system*, IEEE Canadian Conference on Electrical and Computer Engineering

Zhang, Y., Wehenkel, L., Rousseaux, P., Pavella, M. (1997), *SIME: A hybrid approach to fast transient stability assessment and contingency selection,* International Journal of Electrical Power & Energy Systems, Vol. 19, p. 195-208

APPENDICES

APPENDIX A: IEEE RELIABILITY TEST SYSTEM 1996

The *IEEE Reliability Test System 1996* is used in several studies during this PhD work, presented in (Johansson et al. 2011a; Johansson et al. 2011b; Hillberg et al. 2012b; Hillberg and Toftevaag 2012; Hillberg et al. 2012c; Storvann et al. 2012; Lamponen et al. 2014). The dynamic models and parameterisation used are provided in this appendix. Further improvements of the dynamic models, specifically related to load recovery dynamics and excitation system limiters, can be found in (Storvann 2012).

The *IEEE Reliability Test System 1996*, defined in (IEEE 1999), consists of 73 buses in three sub-systems, area A, B, and C, as shown in Figure A-1. Each area has approximately 3.4 GW of installed production and a peak load of 2.8 GW. The areas are interconnected by five tie-lines and one optional DC-link (which has been excluded in these studies).

Several different operating scenarios have been studied, with various levels of total system demand and inter-area power transfer. Detailed case studies have been performed on two of these cases. In these two cases, the system is operated at low load, corresponding to a total system demand of approximately 50 % of the peak demand. This low load scenario belongs to the lower 25 percentile of the annual demand, as described by the probability distribution of the annual demand duration shown in Figure A-2. The inter-area power transfer of these cases is listed in Table A-I. In both cases, area A is a region with a low level of power interchange, while areas B and C are import and export regions, respectively.

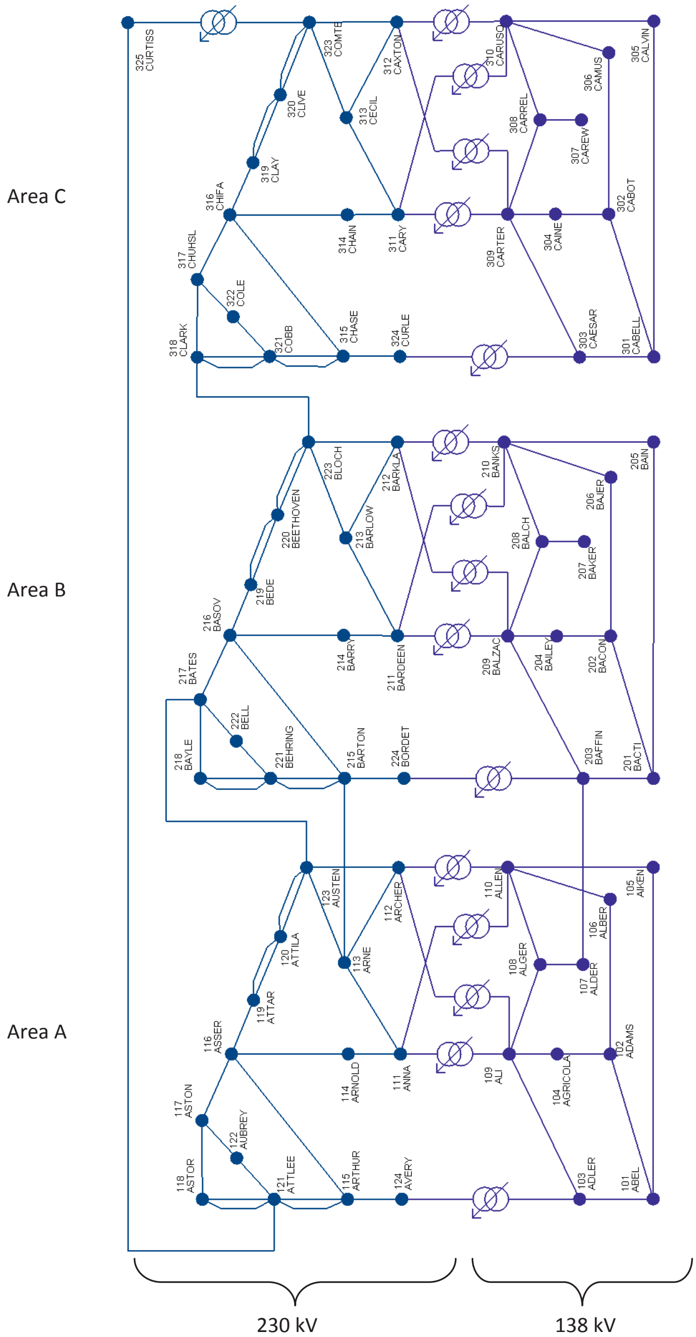

FIGURE A-1: SINGLE LINE DIAGRAM OF THE *IEEE RELIABILITY TEST SYSTEM 1996*

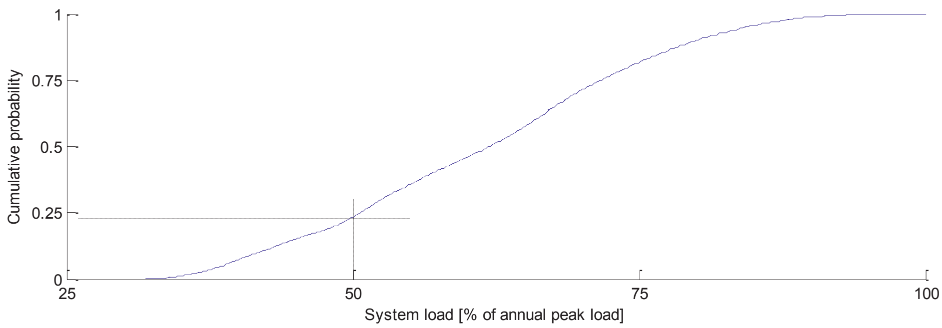

FIGURE A-2: ANNUAL DEMAND DURATION OF THE *IEEE RELIABILITY TEST SYSTEM 1996*, BASED ON (IEEE 1999)

TABLE A-I. INTER-AREA POWER EXCHANGE FOR STUDY CASES 1 & 2

	Case 1	*Case 2*
Power flow from area A to B(MW)	220	255
Power flow from area A to C (MW)	-240	-150
Power flow from area B to C (MW)	-420	-365
Area A Power export (MW)	15	-105
Area B Power export (MW)	-640	-620
Area C Power export (MW)	655	515

The loads in the system are represented by steady-state and dynamic load models, based on a composite of constant power, constant current and constant admittance, as defined by equations (3)-(6):

$$P_0 = P_N \left({U_0}/{U_N}\right)^2 \tag{3}$$

$$P_d = P_0 \, {U_d}/{U_0} \left(0.4 + 0.6 \, {U_d}/{U_0}\right) \tag{4}$$

$$Q_0 = Q_N \tag{5}$$

$$Q_d = Q_0 \left({U_d}/{U_0}\right)^2 \tag{6}$$

where the sub-indices *N*, *0*, and *d* represent nominal, steady-state, and dynamic values, respectively. *P* and *Q* refer to the active and reactive power of the load, with *U* as the bus voltage.

Synchronous condensers are represented as SVCs, and the machine parameters and dynamic models and parameterisation used in the studies of this PhD work are presented in the tables and figures below.

TABLE A-II. MACHINE DATA, FROM (JOHANSSON ET AL. 2011B)

Parameter \ Unit Type	Thermal			Hydro
	Oil	Coal	Nuclear	
Model Type[9]	2.2			2.1
H [s] [10]	2.8	3	5	3.5
T_{d0}' [s]	8	8	8	6
T_{d0}'' [s]	0.05	0.05	0.05	0.03
T_{q0}' [s]	1	1	1	-
T_{q0}'' [s]	0.05	0.05	0.05	0.06
T_a [s]	0.2	0.2	0.2	0.2
X_d [pu]	1.8	1.7	2.0	1.1
X_d' [pu] [10]	0.32	0.3	0.4	0.28
X_d'' [pu]	0.2	0.18	0.23	0.19
X_q [pu]	1.8	1.7	2.0	0.7
X_q' [pu]	0.55	0.52	0.65	-
X_q'' [pu]	0.23	0.21	0.26	0.22
X_l [pu]	0.15	0.13	0.18	0.11

[9] Model type classification as in the *Guide for Synchronous Generator Modeling Practices in Stability Analyses*, (IEEE 1991).
[10] Data as given in *The IEEE reliability test system - 1996*, (IEEE 1999)

TABLE A-III. EXCITATION SYSTEM MODEL PARAMETERS, FROM (JOHANSSON ET AL. 2011B)

Parameter \ Unit Type	All generator types
Model Type[11]	AC4A
T_A [s]	0.1
T_B [s]	10
T_C [s]	1
K_A	100[12]
V_{RMAX} [pu]	3
V_{RMIN} [pu]	0

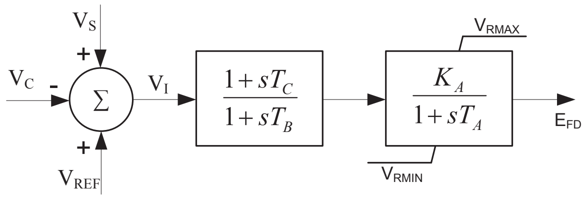

FIGURE A-3: BLOCK DIAGRAM OF EXCITATION SYSTEM MODEL, FROM (JOHANSSON ET AL. 2011B)

[11] Model type classification as in the *Recommended Practice for Excitation System Models for Power System Stability Studies*, (IEEE 2005).
[12] This value is corrected from (Johansson et al. 2011b), where K_A is erroneously listed as 400.

TABLE A-IV. STEAM TURBINE-GOVERNOR SYSTEM MODEL PARAMETERS, FROM (JOHANSSON ET AL. 2011B)

Unit Type / Parameter	Thermal
T_1 [s]	0.5
R	0.05
P_{MAX} [pu]	1
P_{MIN} [pu]	0.3

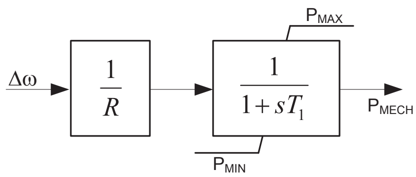

FIGURE A-4: BLOCK DIAGRAM OF STEAM TURBINE-GOVERNOR SYSTEM MODEL, FROM (JOHANSSON ET AL. 2011B)

TABLE A-V. HYDRO TURBINE SYSTEM MODEL PARAMETERS, FROM (JOHANSSON ET AL. 2011B)

Parameter \ Unit Type	Hydro
D	0.5
T_W [s]	1.3
A_t	1.1
q_{nL}	0.08

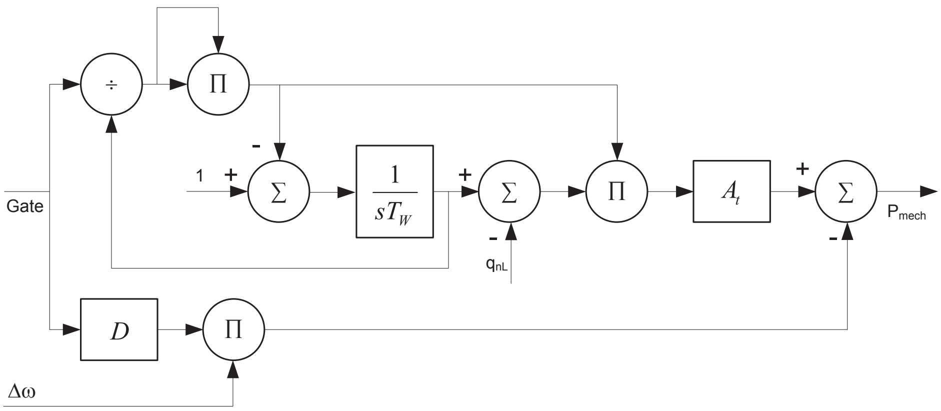

FIGURE A-5: BLOCK DIAGRAM OF HYDRO TURBINE SYSTEM MODEL, FROM (JOHANSSON ET AL. 2011B)

TABLE A-VI. HYDRO GOVERNOR SYSTEM MODEL PARAMETERS, FROM (JOHANSSON ET AL. 2011B)

Parameter \ Unit Type	Hydro
R	0.05
r	0.3
T_F [s]	0.05
T_R [s]	5.2
T_G [s]	0.5
V_{ELMAX} [pu]	0.2
G_{MAX} [pu]	1
G_{MIN} [pu]	0

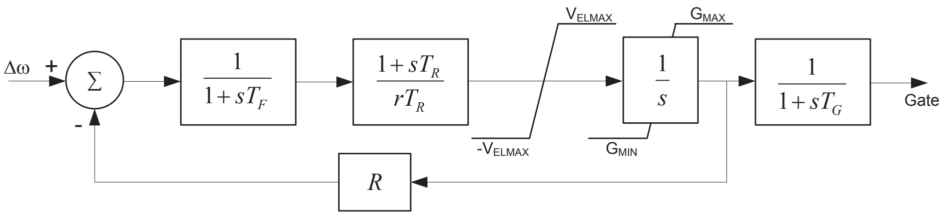

FIGURE A-6: BLOCK DIAGRAM OF THE HYDRO GOVERNOR SYSTEM MODEL, FROM (JOHANSSON ET AL. 2011B)

APPENDIX B: HISTORICAL EXTRAORDINARY EVENTS

The consequences of several historical extraordinary events are illustrated in the consequence diagram shown in Figure 2, and repeated below in Figure B-1. The outage data are based on information provided by several studies, where the approximated average duration, disconnected load, and energy not supplied is gathered in the tables in this appendix.

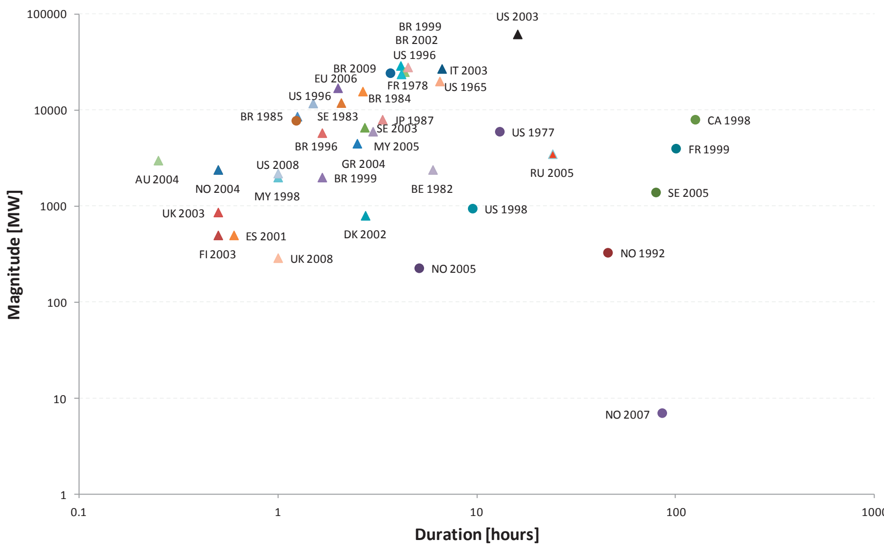

FIGURE B-1: HISTORICAL EXTRAORDINARY EVENTS,
CATEGORISED AS NATURAL HAZARD EVENTS OR POWER SYSTEM INITIATED EVENTS,
MARKED BY A CIRCLE OR TRIANGLE, RESPECTIVELY

TABLE B-I. LIST OF HISTORICAL NATURAL HAZARD EVENTS

Event name in Figure 2 and Figure B-1	Approx. average duration [hours]	Approx. disc. load [MW]	Approx. energy not supplied [MWh]	Affected Country	Year	References
BR 1985	1.2	7800	9620	Brazil	1985	(Gomes 2004)
BR 2009	3.7	24400	90000	Brazil	2009	(Filho 2010)
CA 1998	125	8000	1000000	Canada	1998	(Kjølle et al. 2006b)
FR 1999	100	4000	400000	France	1999	(Kjølle et al. 2006b)
NO 1992	45.5	330	15000	Norway	1992	(Kjølle et al. 2006a)
NO 2005	5.1	228	1165	Norway	2005	(Kjølle et al. 2006a)
NO 2007	85.7	7	600	Norway	2007	(Kjølle et al. 2007)
SE 2005	79.3	1400	111000	Sweden	2005	(Kjølle et al. 2006b)
US 1977	13	6000	78000	USA	1977	(TaskForce 2004)
US 1998	9.5	950	9025	USA	1998	(TaskForce 2004)

TABLE B-II. LIST OF HISTORICAL POWER SYSTEM INITIATED EVENTS

Event name in Figure 2 and Figure B-1	Approx. average duration [hours]	Approx. disc. load [MW]	Approx. energy not supplied [MWh]	Affected Country	Year	References
AU 2004	0.3	3000	750	Australia	2004	(Cooke 2005)
BE 1982	6	2400	14400	Belgium	1982	(Barkans and Zalostiba 2009)
BR 1984	2.7	15700	42000	Brazil	1984	(Gomes 2004)
BR 1994	1.3	8600	10750	Brazil	1994	(Gomes 2004)
BR 1996	1.7	5800	9667	Brazil	1996	(Gomes 2004)
BR 1999	4.3	25000	108000	Brazil	1999	(Gomes 2004)
BR 1999	1.7	2000	3300	Brazil	1999	(Gomes 2004)
BR 2002	4.2	23700	98750	Brazil	2002	(Gomes 2004)
CL 1997	0.5	2400	1200	Chile	1997	(IEEE 2007)
DK 2002	2.75	800	2200	Denmark	2002	(EURELECTRIC 2004a)
ES 2001	0.6	500	300	Spain	2001	(EURELECTRIC 2004a)
EU 2006	2	17000	34000	EU	2006	(IEEE 2007)
FI 2003	0.5	500	250	Finland	2003	(IEEE 2007)
FR 1978	4.1	29000	120000	France	1978	(IEEE 2007)
GR 2004	2.5	4500	11250	Greece	2004	(Vournas et al. 2006)
IT 2003	6.7	27000	180000	Italy	2003	(IEEE 2007)
JP 1987	3.4	8000	26800	Japan	1987	(IEEE 2007)
MY 1998	1.0	2000	2000	Malaysia	1998	(IEEE 2007)
MY 2005	3.0	6000	18000	Malaysia	2005	(IEEE 2007)
NO 2004	0.5	2400	1200	Norway	2004	(IEEE 2007)
RU 2005	24	3500	84000	Russia	2005	(Barkans and Zalostiba 2009)
SE 1983	2.1	11920	25000	Sweden	1983	(IEEE 2007)
SE 2003	2.7	6600	18000	Sweden	2003	(Elkraft 2003; SvK 2003)
UK 2003	0.5	870	430	UK	2003	(EURELECTRIC 2004a)
UK 2008	1.0	290	290	UK	2008	(CIGRE 2010a)
US 1965	6.5	20000	130000	USA	1965	(TaskForce 2004)
US 1996	1.5	11800	17700	USA	1996	(TaskForce 2004)
US 1996	4.5	28000	126000	USA	1996	(TaskForce 2004)
US 2003	16	61800	988800	USA	2003	(TaskForce 2004)
US 2008	1	2200	2200	USA	2008	(CIGRE 2010a)

PART II
APPENDED PAPERS

Johansson, E., Uhlen, K., Nybø, A., Kjølle, G., Gjerde, O.
Extraordinary events: understanding sequence, causes, and remedies
European Safety & Reliability Conference, 2010, Rhodes, Greece

I

Johansson, E., Uhlen, K., Kjølle, G., Toftevaag, T.
Reliability evaluation of wide area monitoring applications and extreme contingencies
17th Power Systems Computation Conference, 2011, Stockholm, Sweden

II

Hillberg, E., Trengereid, F., Breidablik, Ø., Uhlen, K., Kjølle, G., Løvlund, S., Gjerde, J.O.
System integrity protection schemes – increasing operational security and system capacity
44th CIGRE Session, 2012, Paris, France

III

Hillberg, E., Lamponen, J., Haarla, L., Hirvonen, R.
Revealing stability limitations in power system vulnerability analysis
8th Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, 2012, Cagliari, Italy

IV

Hillberg, E., Toftevaag, T.
Equal area criterion applied on power transfer corridors
5th IASTED Asian Conference on Power and Energy Systems, 2012, Phuket, Thailand

V

Lamponen, J., Hillberg, E., Haarla, L., Hirvonen, R.
The change of power system response after successive faults
18th Power Systems Computation Conference, 2014, Wroclaw, Poland

VI

I

Paper I:

Extraordinary events: understanding sequence, causes, and remedies
Johansson, E., Uhlen, K., Nybø, A., Kjølle, G., Gjerde, O.

Proceedings of the European Safety & Reliability Conference, 2010, Rhodes, Greece
ESREL 2010
Reliability, Risk and Safety – Back to the Future, Ale, Papazoglou & Zio (eds)
Taylor & Francis Group, London
ISBN 978-0-415-60427-7

Is not included due to copyright

II

Paper II:

Reliability evaluation of wide area monitoring applications and extreme contingencies
Johansson, E., Uhlen, K., Kjølle, G., Toftevaag, T.

Proceedings of the 17th Power Systems Computation Conference, 2011, Stockholm, Sweden
PSCC 2011
Curran Associates, Inc.
ISBN 978-1-61-839227-5

RELIABILITY EVALUATION OF WIDE AREA MONITORING APPLICATIONS AND EXTREME CONTINGENCIES

Emil Johansson
NTNU
Trondheim, Norway
emil.johansson@ntnu.no

Kjetil Uhlen,
NTNU
Trondheim, Norway
kjetil.uhlen@ntnu.no

Gerd Kjølle,
SINTEF Energy Research
Trondheim, Norway
gerd.kjolle@sintef.no

Trond Toftevaag,
SINTEF Energy Research
Trondheim, Norway
trond.toftevaag@sintef.no

Abstract – In order to perform reliability assessment studies involving the influence of WAMS and extreme contingencies, it is essential to have a good representation of the dynamic behaviour of the system. This paper describes a proposed improvement of the benchmark model IEEE Reliability Test System 1996. The dynamic behaviour of the proposed model is illustrated with results from dynamic simulations.

Keywords: System security, Extreme contingencies, Wide Area Monitoring Systems, Dynamic modelling

1 INTRODUCTION

Power system operation and management requirements are escalating due to society's increased dependency on electricity as well as a continued evolution of the power system. A reliable supply of electricity is recognized as vital for the society, to which extreme contingencies pose a severe threat.

Reliability of the power system is traditionally assessed using adequacy techniques. However, when it comes to the reliability assessment of consequences of extreme contingencies as well as possible remedies using Wide Area Monitoring Systems, the dynamics in the system cannot be neglected. Hence adequacy techniques are inadequate in such analysis.

The IEEE Reliability Test System 1996 [1] is a power system model intended to be used for testing reliability assessment techniques. However, the models' limitations are obvious when it comes to the analysis of dynamic phenomena.

In this paper, an improved dynamic model of the IEEE Reliability Test System 1996 is proposed. The improved dynamic model is suggested to be used for benchmark testing of security assessment techniques.

In this manner, the test system can be used in studies involving consequences of extreme contingencies and the development of various remedial applications based on Wide Area Monitoring Systems.

The paper is organised in the following manner: Section 2 gives an introduction to reliability assessment with regard to extreme contingencies and prospective applications of wide area monitoring systems. The proposed improvement of the dynamic model for the IEEE Reliability Test System 1996 is described in section 3, while analysis and results of a dynamic study are described in section 4. Discussion and further work is included in section 5.

2 A SMART TRANSMISSION GRID

Smart grid issues have mainly been focusing on making the distribution grid and the demand side smarter, examples on areas of interest are:

- simplified system integration of distributed generation
- demand side management and response
- interaction between many/all components
- smart metering

However, the smart grid approach also relates to improvements of the transmission grid. Such improvements are essential in order to maintain a reliable power supply in a changing power system, of which the society is increasingly dependent. An area of special concern is the power systems' robustness to extreme contingencies.

2.1 Power System Reliability Assessment

Reliability of a power system is composed by two aspects, adequacy and security, where adequacy relates to the ability of the system to satisfy the demand while security is related to the systems capability to withstand disturbances [2, 3]. A comprehensive elaboration on the concepts of power system adequacy and security can be found in [4].

When addressing the reliability of power systems, the attention is often towards the steady state adequacy in supply and demand, rather than towards the dynamic robustness and contingency ride through capabilities of the system. One of the reasons for this might be the complexity involved in a proper representation of the dynamic behaviour of the power system. Hence, many reliability assessment techniques are neglecting the dynamic aspect of reliability and only focusing on steady-state security and adequacy assessment of the power system.

Several security assessment techniques are available, with many of the online dynamic security assessment techniques described in [5]. There is, however, a need to further define security assessment indices [6]. Challenges are also related to the modelling requirements for performing adequate dynamic analysis and to the assessment of consequences of extreme contingencies from a simulation point of view.

2.2 Extreme Contingencies

An extreme contingency refers to a disturbance in the power system with a potentially High societal Impact and a Low Probability to occur (also called HILP events), often leading to a wide-area interruption (or blackout).

Due to the unpredictable nature of HILP events, difficulties arise to economically justify major reinforcements on the power systems to prevent such events from occurring [6]. However, with consequences resulting in considerable socio-economic costs, mitigation of extraordinary events has a high social, economical, and political benefit.

Increased insight into and understanding of these events is an important step in order to develop and assign appropriate remedies to limit the consequences of future events. Analyses of historical extreme contingencies, e.g. [7-9], describe several factors identified as root causes to the events. Two aspects of special importance recognised in [10] are:

- insufficient situational awareness
- inadequacy of implemented schemes for controlled islanding

2.3 Wide-Area Situational Awareness

An improved situational awareness of the operating state of the power system on a system wide basis implies an improved system security by e.g. increased operator decision support and enhanced emergency control. In this way, the risk of blackouts can be decreased through more accurate identification of system vulnerabilities. Improved monitoring is one solution to enhance the wide-area situational awareness.

2.4 Wide Area Monitoring Systems

Wide Area Monitoring Systems (WAMS) is identified as a field where applications could be efficiently utilised in order to increase the system security to extreme contingencies without major economical investments. The breakthrough in wide area monitoring arrived with the development and installation of fast, reliable, and highly accurate Phasor Measurement Units, PMUs [11]. PMUs are utilised to supply a WAMS with time synchronised phasor data from a widely dispersed system. Typically WAMS have a relatively low time delay, providing almost real-time observability either of selected parts of the power system, such as vital transfer corridors, or of the entire power system if sufficient PMU installations are available.

The enhanced information made available by a WAMS enables improvements in many fields, related to monitoring, control, and protection of the power system, some of them being:

- Post-mortem analysis
- State estimation & prediction
- Situational awareness
- Security assessment
- System utilization
- Robustness & coordination of protection and control

3 DYNAMIC MODEL OF THE IEEE RELIABILITY TEST SYSTEM 1996

In order to properly perform benchmark reliability assessment of various WAMS applications and extreme contingencies, the widely known IEEE Reliability Test System 1996 is used as a starting point.

3.1 Background

The IEEE Reliability Test System 1996, described in [1], (hereinafter referred to as the test system) is designed with the purpose to be used for benchmark studies on new and existing reliability evaluation techniques. The test system is an extended successor of the original IEEE Reliability Test System 1979, see [12], and consists of an interconnected power system with three areas and six sub-areas. The test system is described by a generation and transmission system supplying loads represented at bulk load points. The representation of a power system by its generation and transmission systems, neglecting the effects of the distribution systems, is often referred to as hierarchical level 2 model, HL-II, which is a usual level of modelling when performing power system reliability assessment.

Several studies have been made on this system, where e.g. [13] presents a reliability (adequacy) assessment of the system and compares the results with the predecessor from 1979, and [14] proposes a full three-phase description of one of the areas of the test system. As far as the authors are aware of, there are no publications available where the limitations of the dynamic model presented in [1] are discussed or the implications this might have when assessing the reliability, including security, of the test system.

3.2 Dynamic modelling

The description in [1] lacks vital information on the dynamical behaviour of the test system; hence the description is mainly useful when addressing the steady state adequacy of generation and transmission rather than the dynamic robustness of the system related to various contingencies. In order to utilise this system for security analysis, further definition of the dynamic parts of the test system is needed.

Depending on the goal of a dynamic power system study, the modelling of the physical behaviour of various items is important, such as: generators, loads, tap-changers, and control & protection systems.

In the following sub-section, the modelling of synchronous generators is discussed, and an improved dynamic model of the generators in the test system is proposed.

3.3 Generator system dynamic models

Several generating plants are defined in [1], where the dynamic generator models are grouped into four unit types: oil, coal, nuclear, and hydro.

The generators are described using the so called classical machine model, i.e. a constant voltage behind a transient reactance. The generators are parameterised using the parameters: H (inertia constant), D (damping constant), and X_d' (transient reactance). The damping constant D is used to represent electrical damping in the classical model, where the effect of damper windings is not included. When the damping constant is set to zero, the model fully neglects any electrical and mechanical damping of the machine.

The dynamic generator data presented in [1] is based on the study described in [15], where the classical machine model is introduced for assessing the security of the IEEE Reliability Test System 1979. It should be noticed that the classical machine model is a highly simplified model, lacking much valuable information of the machines' non-stationary behaviour, and when neglecting the damping of the machines the model may produce highly conservative results in a dynamic simulation.

Hence, in order to more properly reproduce the transient and sub-transient behaviour of the generators, models representing the rotor circuits are proposed. Including the field winding together with one damper circuit in each of the d- and the q-axes, respectively, sub-transient effects and rotor related magnetic saliency are considered. To further increase model accuracy, it is common to include one additional circuit in the q-axis. These model types are in [16] referred to as *Model 2.1* and *Model 2.2*, respectively. Model 2.1 is normally considered sufficiently detailed to represent machines of salient pole type, which typically is the case with generator units in hydro plants. Generator units in thermal plants are often of round-rotor type, for which model 2.2 is normally considered suitable.

The parameters needed in order to represent the generators in the test system with machine models 2.1 and 2.2 are listed in Table 1. The selected data is based on data from [17] and [18], and is supposed to represent typical machine parameter values.

Unit Type / Parameter	Thermal			Hydro
	Oil	Coal	Nuclear	
Model Type[1]	2.2			2.1
H [s] [2]	2.8	3	5	3.5
T_{d0}' [s]	8	8	8	6
T_{d0}'' [s]	0.05	0.05	0.05	0.03
T_{q0}' [s]	1	1	1	-
T_{q0}'' [s]	0.05	0.05	0.05	0.06
T_a [s]	0.2	0.2	0.2	0.2
X_d [pu]	1.8	1.7	2.0	1.1
X_d' [pu][2]	0.32	0.3	0.4	0.28
X_d'' [pu]	0.2	0.18	0.23	0.19
X_q [pu]	1.8	1.7	2.0	0.7
X_q' [pu]	0.55	0.52	0.65	-
X_q'' [pu]	0.23	0.21	0.26	0.22
X_l [pu]	0.15	0.13	0.18	0.11

Table 1: Proposed data for machine models

An example of the differences in dynamic behaviour between the classical machine model and models 2.1 and 2.2 is illustrated by Figure 1. In this figure, the speed deviation (from nominal speed) is shown for three different machine models, after a 100 ms 3-phase short-circuit applied at bus 119. The red curve describes the response when all machines in the test system are modelled using the classical model with parameters as described in [1]. The blue and black curves describes the response when modelling the machines as suggested in Table 1, with the governor and excitation systems explicitly modelled in the system described by the black curve.

It is obvious that the speed deviation in the case with the classical machine model oscillates in an undamped manner. Hence, this contingency would result in instability and loss of load in a study where the machines were modelled using this type of model parameterised as in [1].

See [19] for further description on how the complexity of the machine model influences the dynamic response of the modelled power system.

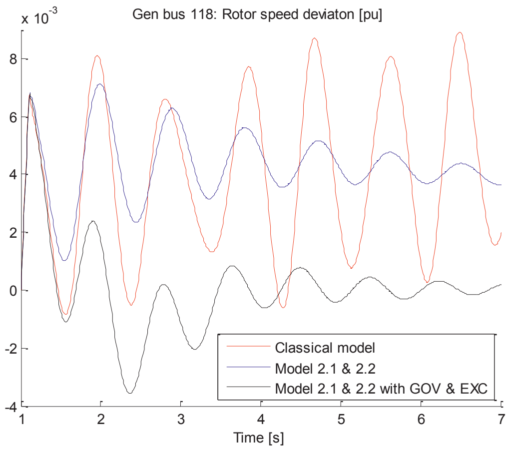

Figure 1: Rotor speed deviation of the machine at bus 118 for different dynamical models, when the system is exposed to a 3-phase fault on bus 119

3.4 Governor and Excitation system models

A brief description of the governor and excitation system models is included in this sub-section. As shown in Figure 1, the governor and excitation systems have a significant impact during the transient state of a dynamic simulation, and it can be shown that the stability of the power system is greatly affected by these controls. In order to include the dynamic effects of governors and excitation systems, simplified models together with rather typical data are presented here.

The excitation system model used for all generators is represented by a simplified version of the model referred to as Type AC4A described in [20]. The following simplifications are made: the regulator input filter time constant (T_R) is set to zero, the under excitation limiter (V_{UEL}) and the commutating reactance (K_C) are neglected, and no limit is set on the regulator input (V_I). This simplified model can be represented by

---

[1] Model type classification as in the *Guide for Synchronous Generator Modeling Practices in Stability Analyses*, [16].

[2] Data as given in *The IEEE reliability test system - 1996*, [1]

the block diagram shown in Figure 2, with suggested typical parameters listed in Table 2.

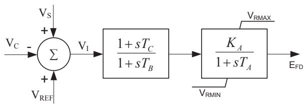

Figure 2: Excitation system model

Unit Type / Parameter	All generator types
Model Type[3]	AC4A
T_A [s]	0.1
T_B [s]	10
T_C [s]	1
K_A	400
V_{RMAX} [pu]	3
V_{RMIN} [pu]	0

Table 2: Excitation system model parameters

The turbine and governor system model used for the thermal units is a very simple model, only describing the droop and governor time constant. The model can be represented by the block diagram shown in Figure 3. The parameters suggested for this model are listed in Table 3.

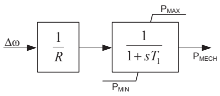

Figure 3: Steam turbine-governor system model

Unit Type / Parameter	Thermal
T_1 [s]	0.5
R	0.05
P_{MAX} [pu]	1
P_{MIN} [pu]	0.3

Table 3: Steam turbine-governor system model parameters

For the hydro units, a more elaborate turbine and governor system model is used. The turbine is modelled as a non-linear model with a non-elastic water column, as described in [21], with the simplification that the penstock head losses (f_P) are ignored. The simplified model can be represented by the block diagram shown in Figure 4.

The governor system includes temporary and permanent droop, filter-, governor-, and servo- time constants, together with gate velocity and position limiters. The governor system can be represented by the block diagram shown in Figure 5. The parameters of the hydro turbine and governor systems used in the study are listed in Table 4 and Table 5.

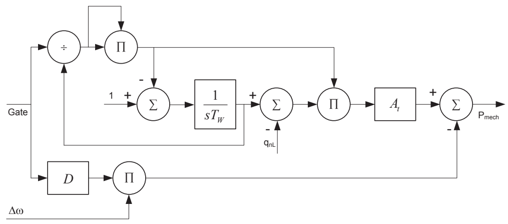

Figure 4: Hydro turbine system model

Unit Type / Parameter	Hydro
D	0.5
T_W [s]	1.3
A_t	1.1
q_{nL}	0.08

Table 4: Hydro turbine system model parameters

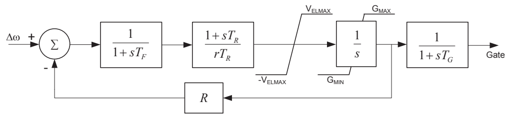

Figure 5: Hydro governor system model

Unit Type / Parameter	Hydro
R	0.05
r	0.3
T_F [s]	0.05
T_R [s]	5.2
T_G [s]	0.5
V_{ELMAX} [pu]	0.2
G_{MAX} [pu]	1
G_{MIN} [pu]	0

Table 5: Hydro governor system model parameters

4 ANALYSIS & RESULTS

In this section, the dynamic response of the test system is discussed. The studied scenario corresponds to a high transfer scenario, with load and production distributed as described in Figure 6. The system load is approximately 75 % of the peak load scenario described in [1], with implemented dynamic models as proposed in the previous section. All other data and information regarding the test system are found in [1].

[3] Model type classification as in the *Recommended Practice for Excitation System Models for Power System Stability Studies*, [20].

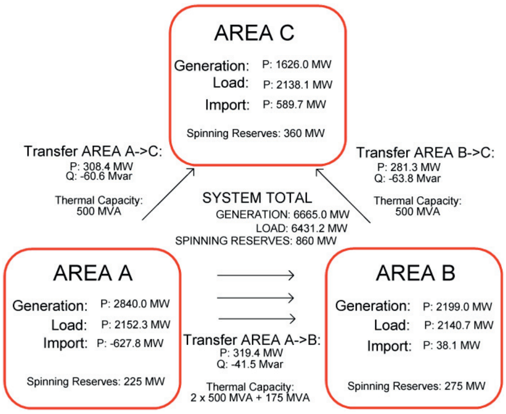

Figure 6: Overview of the IEEE Reliability Test System 1996 showing distribution of load and generation in the studied operating scenario

Important dynamic aspects are studied by linearising the test system. The eigenvalues related to the electro-mechanical oscillatory modes of the linearised system are displayed in Figure 7, where the most influencing modes are seen to be in the range of 0.8–1.5 Hz with damping ratio of around 5 %. Table 6 lists further information on the five lowest damped modes, together with the equipment having the highest participation factor of each mode.

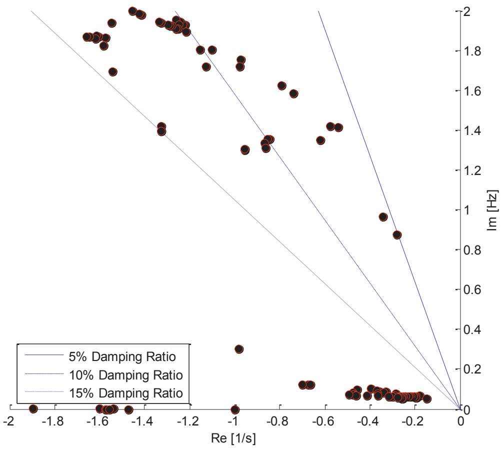

Figure 7: Electro-mechanical modes

no	f [Hz]	Damping [%]	Participation Factor
1	0.87	5.1	Gen1, bus 321
2	0.96	5.6	Gen1, bus 118
3	1.41	6.1	Gen3 & 4, bus 202
4	1.42	6.4	Gen3 & 4, bus 302
5	1.35	7.3	Gen1, bus 218

Table 6: Low damped oscillatory modes

A mode shape plot, describing the observability level using bus voltage angles for the 0.96 Hz mode is displayed in Figure 8. This mode is identified as an interarea mode, where mainly generators in Area A and B are swinging against each other. The 0.87 Hz mode is mainly observable as generators in Area C are swinging against the rest of the system.

Utilising the observability information, it is possible to identify optimal monitoring quantities and locations in order to best observe the level of oscillations in the system. With voltage angles as monitoring unit, the optimal measurements to observe the 0.87 Hz mode is identified as the angle difference between buses 222 (Area B) and 322 (Area C), while the 0.96 Hz mode is best observed as the angle difference between buses 118 (Area A) and 222 (Area B). Such information could be used in a wide area monitoring system to keep track on power oscillations in the system, with possibilities to monitor damping levels of different modes.

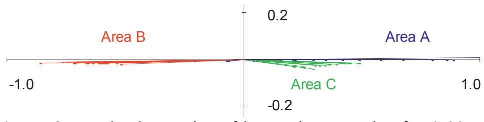

Figure 8: Mode shape plot of bus voltage angles for 0.93 Hz oscillatory mode

The low damped modes are easily triggered, and in Figure 9 the voltage angle difference between buses 222 and 322 is displayed in the wake of a small disturbance, where the oscillatory frequency can be approximated to 0.9 Hz, with damping of around 7 %.

For the same disturbance, Figure 10 depicts the speed deviation of the generators in the system. After a couple of seconds, the 0.87 Hz mode is the most significant mode in the oscillation, with most participation from the generators in Area C, which are distinctly swinging in opposite phase to the generators in Area A and B.

It should be noticed that the damping of the low damped modes could be improved by the implementation of properly tuned power system stabilisers at the generators in the system.

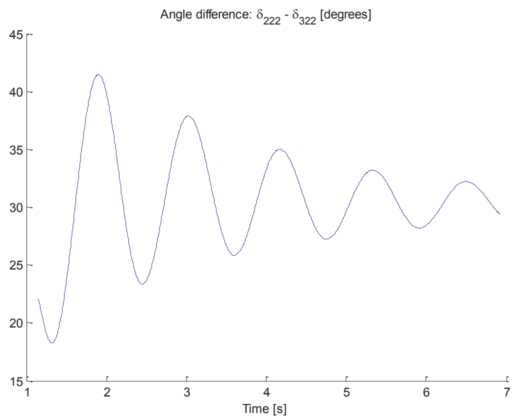

Figure 9: Voltage angle difference between bus 222 and 322

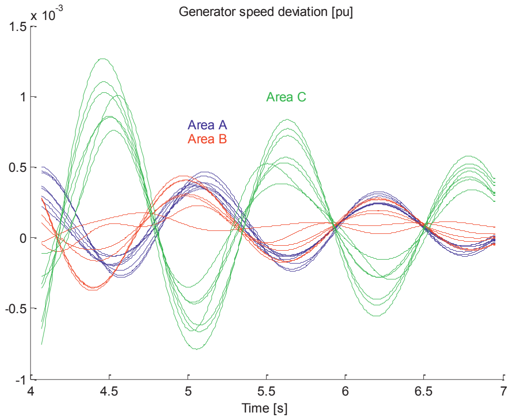

Figure 10: Generator speed deviation (showing inter-area oscillations identifying three groups of generators)

The proximity to voltage collapse can be studied using various indices and calculation techniques. In [22] and [23], it is described how local measurement can be used to estimate the stability margin. At any given bus in the system, the Thevenin equivalent impedance of the network (Z_{NET}) is estimated using phasor measurements and compared to the apparent load impedance of the bus (Z_{APP}). Maximum power transfer to the bus occurs when $Z_{NET} = Z_{APP}$, hence the proximity to voltage collapse can be estimated by studying these two impedances.

Figure 11 displays the impedance ratio Z_{APP} / Z_{NET} (equal to the ratio of short-circuit apparent power and load apparent power) at bus 109. As the system load increases, the voltage stability margin is decreasing. Although the system is far from voltage collapse, the outage of the two transformers connecting bus 109 with buses 111 & 112, respectively, moves the system towards voltage collapse, showing a significant effect on the impedance ratio of the bus.

In this case the apparent load impedance at bus 109 is equal to the local bulk load impedance. However also other impedances could be monitored for example the equivalent impedance of the sub-systems on each side of a tie line.

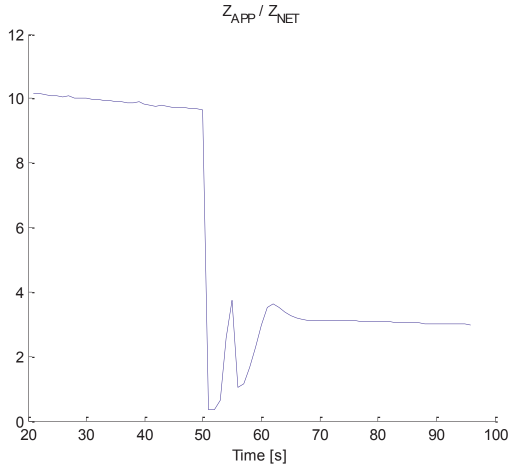

Figure 11: Impedance ratio between load and system at bus 109 during outage of transformers 109-111 & 109-112

This technique is useful in order to improve voltage collapse proximity estimation of a widely distributed system. Using a wide area monitoring system, this information could also be made available on an operator level, where key buses in the system could be specifically monitored as described in [24].

5 DISCUSSION

Development of a wide area monitoring, protection, and control system is a topic of high interest. However, the R&D community need good power system models to develop relevant applications. The main contribution in this paper is the development of a test system for dynamic system analysis based on the well-known IEEE Reliability Test System 1996.

Further work includes specification of improved models, describing: dynamic behaviour of loads, reactive power compensation, power system stabilisers, tap-changer control, and equipment protection.

Planned studies involve security assessment analysis of the impact of WAMS applications as well as HVDC interconnections between the areas of the test system.

REFERENCES

[1] Reliability Test System Task Force, *The IEEE reliability test system - 1996,* IEEE Transactions on Power Systems, Vol. 14, No.3, 1999

[2] IEEE Working Group on Performance Records for Optimizing System Design, *Reliability indices for use in bulk power supply adequacy evaluation,* IEEE Transactions on Power Apparatus and Systems, Vol. 97, No.3, 1978

[3] Billinton, R., Allan, R.N., *Power-system reliability in perspective,* Electronics and Power, 1984, Vol. 30, p. 231-236

[4] CIGRE Task Force: 38.03.12,, *Power system security assessment: A position paper,* ELECTRA, no. 175, Dec., 1997

[5] CIGRE Working group C4.601, *Review of On-line Dynamic Security Assessment Tools and Techniques,* Technical Brochure 325, 2007

[6] CIGRE Working Group: C4.601,, *Review of the Current Status of Tools and Techniques for Risk-Based and Probabilistic Planning in Power Systems,* Technical Brochure: 434, 2010

[7] Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., Vittal, V., *Causes of the 2003 major grid blackouts in north America and Europe, and recommended means to improve System Dynamic Performance,* IEEE Transactions on Power Systems, 2005, Vol. 20, p. 1922-1928

[8] Union of the Electricity Industry, Task Force on: Power Outages,, *Power Outages in 2003,* Ref: 2004-181-0007, 2004

[9] IEEE Task Force on: Blackout Experiences, Mitigation, and Role of New Technologies,, *Blackout Experiences and Lessons Best Practices for System Dynamic Performance, and the Role of New Technologies,* Special Publication: 07TP190, 2007

[10] Johansson, E., Uhlen, K., Nybø, A., Kjølle, G., Gjerde, O. *Extraordinary events: Understanding sequence, causes, and remedies*, European Safety & Reliability Conference, 2010, Rhodes, Greece

[11] Phadke, A.G., Thorp, J.S. *History and applications of phasor measurements*, IEEE/PES Power Systems Conference and Exposition, 2006, Atlanta, Georgia, USA

[12] Reliability Test System Task Force, *The IEEE reliability test system,* IEEE Transactions on Power Apparatus and Systems, Vol. 98, No.6, 1979

[13] Pinheiro, J.M.S., Dornellas, C.R.R., Schilling, M.T., Melo, A.C.G., Mello, J.C.O., *Probing the new IEEE Reliability Test System (RTS-96): HL-II assessment,* IEEE Transactions on Power Systems, 1998, Vol. 13, p. 171-176

[14] Dam, Q.B., Meliopoulos, A.P.S., Heydt, G.T., Bose, A., *A Breaker-Oriented, Three-Phase IEEE 24-Substation Test System,* IEEE Transactions on Power Systems, 2010, Vol. 25, p. 59-67

[15] Porretta, B., Kiguel, D.L., Hamoud, G.A., Neudorf, E.G., *A comprehensive approach for adequacy and security evaluation of bulk power systems,* IEEE Transactions on Power Systems, 1991, Vol. 6, p. 433-441

[16] IEEE, *IEEE Guide for Synchronous Generator Modeling Practices in Stability Analyses*, in *IEEE Std 1110-1991*, 1991

[17] Kundur, P., *Power system stability and control*. The EPRI power system engineering series, 1994, New York: McGraw-Hill

[18] Johannesen, A., *Fault calculations and stability analysis of electric power systems*, 1974, Trondheim: EFI, (in Norwegian)

[19] Johansson, E., Persson, J., Lindkvist, L., Söder, L. *Location of Eigenvalues Influenced by Different Models of Synchronous Machines*, IASTED International Conference Power and Energy Systems, 2002, Marina del Rey, California, USA

[20] IEEE, *IEEE Recommended Practice for Excitation System Models for Power System Stability Studies*, in *IEEE Std 421.5-2005*, 2005

[21] IEEE Working Group on Prime Mover and Energy Supply Models for System Dynamic Performance Studies, *Hydraulic turbine and turbine control models for system dynamic studies,* IEEE Transactions on Power Systems, Vol. 7, No.1, 1992

[22] Vu, K., Begovic, M.M., Novosel, D., Saha, M.M., *Use of local measurements to estimate voltage-stability margin,* IEEE Transactions on Power Systems, 1999, Vol. 14, p. 1029-1034

[23] Warland, L., *A Voltage Instability Predictor Using Local Area Measurements VIP++*, 2002, Trondheim: NTNU

[24] Leirbukt, A., Uhlen, K., Palsson, M.T., Gjerde, J.O., Vu, K., Kirkeluten, O. *Voltage monitoring and control for enhanced utilization of power grids*, IEEE/PES Power Systems Conference and Exposition, 2004

III

Paper III:

System integrity protection schemes – increasing operational security and system capacity

Hillberg, E., Trengereid, F., Breidablik, Ø., Uhlen, K., Kjølle, G., Løvlund, S., Gjerde, J.O.

Proceedings of the 44th CIGRE Session, 2012, Paris, France
CIGRE 2012
Conseil International des Grands Réseaux Électriques
International Council on Large Electric Systems
ISBN 978-2-85873-204-3

21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

C2-201

CIGRE 2012

System Integrity Protection Schemes – Increasing operational security and system capacity

**E. HILLBERG[1], F. TRENGEREID[2], Ø. BREIDABLIK[2],
K. UHLEN[1], G. KJØLLE[1], S. LØVLUND[2], J.O. GJERDE[2]**
**[1] Norwegian University of Science and Technology, [2] Statnett
Norway**

SUMMARY

System Integrity Protection Schemes (SIPS) are increasingly utilised in power systems worldwide to provide additional power transfer capacity and enhanced operational security. The implementation of Phasor Measurement Units (PMU) and Wide Area Monitoring Systems (WAMS) provide opportunities to improve the conventional system integrity protections. These improvements can increase the protection schemes' awareness of the system state, providing robustness towards unforeseen disturbances and enhanced operational security to extraordinary events.

In this paper, a technique of how to assess the security to extraordinary events is described, where the concept of a secure operating region is extended to involve multiple contingencies, referred to as *the $N-k$ secure operating region*. This paper also includes an overview of the SIPS in the Norwegian power system, and a security assessment study performed on the IEEE Reliability Test System 1996. The study includes conventional and WAMS based SIPS solutions, and demonstrates the importance of incorporating dynamic contingency analysis when assessing the security of a power system.

KEYWORDS

System Integrity Protection Schemes – Operational security – Power transfer capacity – Extraordinary events – $N-k$ security assessment – IEEE Reliability Test System

Emil.Hillberg@ntnu.no

1. INTRODUCTION

Power transfer capacity limits are set in order to maintain a reliable operation of the power system. Typically, power transfer capacities between areas, or sub-systems of an interconnected power system, are defined by limitations on one or several power transfer corridors (PTC). A PTC can be identified as a set of transmission circuits that form an interface in a power system, which may impose a bottleneck in the system during a specific operating scenario. Limitations are often related to the thermal capacities of transmission lines and other equipment; however, the stability of the power system may as well constitute limiting factors. In the Continental European power system, main limitations are typically on thermal capacities, while stability limiting factors are of high concern in the less densely interconnected Nordic power system, [1, 2].

Maintaining a reliable operation of the power system implies that the system should be both adequate and secure. The adequacy of the power system can be defined as the existence of sufficient facilities in the system to satisfy its demand [3], referring mainly to the level of available generation and transmission capacity. Power system security reflects a systems ability to withstand disturbances, [3], where a contingency during insecure operation could result in instability. Extraordinary events (large disturbances or blackouts) are often caused by system instability, where the degraded system collapses after stability limits are violated, [4]. Since many power systems are operated according to the $N-1$ security criterion, stability limits are rarely violated by a single contingency. This further implies that the security to extraordinary events can be expressed as the security to multiple contingencies, i.e. $N-k$ security.

System Integrity Protection Schemes (SIPS) are implemented in many power systems worldwide. According to [5], approximately half of the globally installed SIPS can be classified as applications related to increasing the transfer capacity, while the other half is classified as increasing the operational security. SIPS are, in contrast to common component protection, designed to preserve the power system integrity during abnormal conditions. Another possible classification of SIPS is on the type of activation signal, which can be either event-based (detecting of predefined events, such as breaker tripping signals) or response-based (measuring electrical parameters, e.g. frequency or voltage), [6]. Most SIPS tend to be of the event-based type, [5], and are characterised by taking predefined actions to predefined events. Event-based SIPS are fast acting and designed to improve transient rotor angle stability and short-term voltage stability, they are, however, without protection against unforeseen events and consequence of SIPS action might be hard to anticipate for all operating scenarios. An example of commonly used response-based SIPS is the under-frequency load-shedding scheme (UFLS), which often is implemented on a system wide basis in order to prevent the collapse of a system due to frequency instability. Approximately 75% of all SIPS are intended to prevent instability, and corrective actions are in more than 50% of the cases related to load shedding or generation tripping, [5].

This paper is organised as follows:
Section 2 holds a description of SIPS in the Norwegian power system. Section 3 describes a technique for assessing the security to extraordinary events, and a security assessment analysis is included in section 4. Discussion and conclusions are provided in section 5.

2. SYSTEM INTEGRITY PROTECTION SCHEMES IN NORWAY

2.1 Background

The Norwegian transmission system is normally operated according to the $N-1$ security criterion. However, this criterion cannot always be fulfilled and Statnett (the Norwegian TSO) has therefore defined a minimum acceptable operational security level, where: *a contingency should not have consequences beyond the disconnection of 200 MW load with duration up to 1 hour during normal operation, or 500 MW up to 2 hours during maintenance,* [7]. In such cases, the sub-system is referred to as being $N-0$ or $N-½$ secure, depending on the consequences of a probable contingency:

- $N-0$ secure operation refers to cases where a single outage leads to uncontrolled loss of load, e.g. in the case of radial operation in the transmission network
- $N-½$ secure operation reflects the mitigating impact by armed SIPS. In this way, the consequences of an event can be limited to a controlled load shedding, as described by [8]. This does, however, not automatically imply that an islanded system will be able to continue in stable operation, even though local load and generation are in balance after the SIPS action.

There are around twenty different SIPS installed in the Norwegian power system, affecting over 6 GW of production (approximately 20% of the total installed production) and more than 1.3 GW of load (this is event-based and amounts to approximately 5% of the maximum peak load). On top of this, there is a response-based under-frequency load shedding scheme implemented in the Nordic system, which in Norway is activated for frequencies below 48.7 Hz, where load is disconnected in steps summing up to a total of 7 GW.

The SIPS are utilised to increase transfer capacities of almost 20 different PTCs during normal operation and to improve the operational security during strained situations. In this section, the functionality and experience of some of these schemes are described.

2.2 Classification, objective & functionality

The installed SIPS in the Norwegian power system can, based on the nature of their corrective actions, be structured into four categories: generation tripping, load shedding, system separation, and HVDC emergency power. Both event-based and response-based activation signals are used, varying from local measurements of frequency, voltage, or power oscillation, to trip signals from remote breaker protection and over-current relays.

In many cases, SIPS are utilised to increase power transfer capacities, either to enhance system utilisation during normal operation or in scenarios with high load or insufficient local production. SIPS are also used to increase the security in situations with strained operation, e.g. during maintenance of an important transmission line, with the purpose to limit consequences of contingencies while sustaining a sufficient transmission capacity. All of the SIPS are manually armed by the transmission system operator (TSO), with the decision based on analysis made during the operation planning phase. Actual outcome of mitigating actions of armed SIPS is continuously updated in the control centre, based on state estimator data.

2.3 Operation experience & future trends

Since the 1980s, the Norwegian TSO has employed an increased number of SIPS, implying a more demanding operation of the power system in terms of both utilisation and complexity.

Statistics collected from the national control centre, describing the initiation of SIPS in Norway, limited to generation tripping schemes, are displayed in the figures below. Figure 1 shows the annual number of SIPS initiations together with the amount of disconnected generation. The number of affected units, together with the cost (including both annual unit participation fees as well as activation fees), are shown in Figure 2 . The economical gain from utilisation of SIPS has not been included here, due to the difficulty in acquiring quantifiable data such as: earnings from increased energy exchange, savings from mitigated cost of energy not supplied, value of delayed investments, etc.

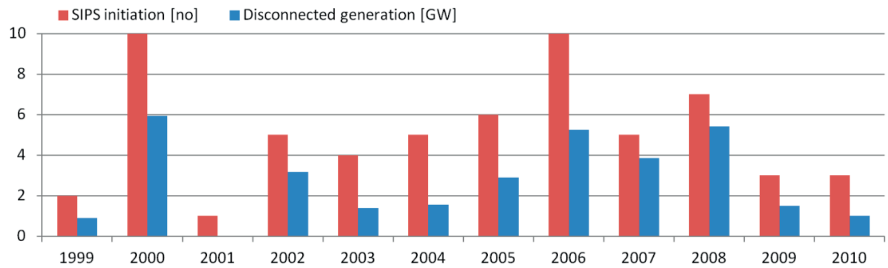

Figure 1: Annual number of SIPS initiations and resulting disconnected generation in Norway.

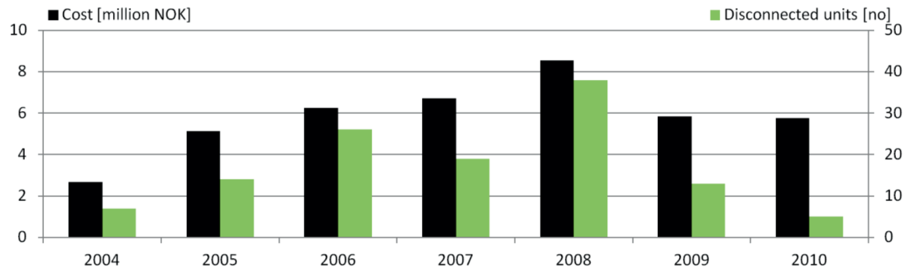

Figure 2: Annual cost and number of disconnected units by SIPS initiation in Norway.

There are some negative operational experiences reported, and an example is described in [9]. The report describes an event where the delayed operation of one SIPS initiated a system separation, leading to approximately 2 GW of production deficit in the main Nordic system. Automatic production increase led to overload and the triggering of another SIPS, which, however, failed to operate. The missed operation actually prevented a production disconnection, which likely would have led to an unstable scenario. This example shows the high complexity of SIPS control and operation, as well as the difficulty in designing protections against unforeseen event. It is therefore important to consider the risks involved when the operating scenarios largely rely on the performance of a number of SIPS.

According to [7], no further load shedding schemes[1] will be employed, stating that investments in new transmission capacity are imperative to increase future transfer capacity while maintaining a satisfactory level of operational security.

[1] Several other schemes (generation tripping and HVDC emergency power) are, however, planned to be installed in the near future.

3. SECURITY TO EXTRAORDINARY EVENTS

3.1 Background

Many historical blackouts have been the result of the progression of cascaded events, followed by system separation and instability, [4]. The system operators' lack of situational awareness has been identified as one of the root causes, as well as the system's insufficiency to regain stable operation in the post-contingency state, [10, 11]. In this section, improved security to extraordinary events is proposed through enhanced awareness by means of visualisation of the secure operating region related to single and multiple contingencies as well as the arming of SIPS.

3.2 N – 1 secure operating region

The $N-1$ secure operation, limited by aspects described in the introduction, can be assessed through contingency analysis. In some power systems it is possible to identify power transfer corridors with critical influence on the available secure transfer capacity. Such PTC could be utilised to visualise a region defining the secure operation, as suggested by [3, 12] and exemplified in Figure 3-I. Since a secure operation is of a multi dimensional nature, it is important to identify relevant quantities when visualising the secure region. In a power system with several critical PTCs, it might be reasonable to visualise several regions defined by different PTCs. In Figure 3-I, the secure operating region is visualised, together with the actual operating point, using the $N-1$ secure power transfer capacity of PTC_{I} relative to the capacity of PTC_{II}. The size and shape of the secure region will vary for different operating scenarios, since modifications of the network topology and other aspects influence the security of the power system.

3.3 N – k secure operating region

Similarly as suggested in the previous sub-section, the secure operating region related to multiple contingencies can be visualised as exemplified in Figure 3-II. Assessing the $N-1$ to $N-k$ secure operating region can be done by contingency analysis to the k^{th} subsequent contingency level. Such contingency analysis can be very tedious, and screening techniques might be necessary to identify contingencies which affect the critical PTC. Representation of a multiple contingency security region can be beneficial to assess the operating scenarios' vulnerability to extraordinary events. This may be further improved by explicit monitoring of vulnerability indices, where an example is the k_{min}*-index*. This index describes a distance to the stability limits of a system, determined by the minimum number of subsequent contingencies that lead to instability. A continuously updated estimation of the k_{min}*-index,* quantifying the vulnerability of the actual operating scenario, can improve the situational awareness of the operator when considered in relation with a historical perspective.

3.4 SIPS security enhanced operating region

The effects of arming a specific SIPS can be visualised as exemplified in Figure 3-III. The figure shows how arming of a SIPS enhances the security around the actual operating point. In cases where the desired operating point is outside the $N-1$ secure region, the SIPS can be used to provide an acceptable level of security. Utilising the secure operating region related to multiple contingencies, the efficiency of specific SIPS can be assessed regarding the improvement of the system's resilience to extraordinary events.

Showing the full region of secure operation, i.e. not limiting to the first quadrant as in Figure 3, will display both positive and negative effects of armed SIPS. In this way, the decision procedures may be influenced to reduce the number of simultaneously armed SIPS. Such reduction may also decrease the risk of adverse effects in case of events unforeseen when designing the SIPS.

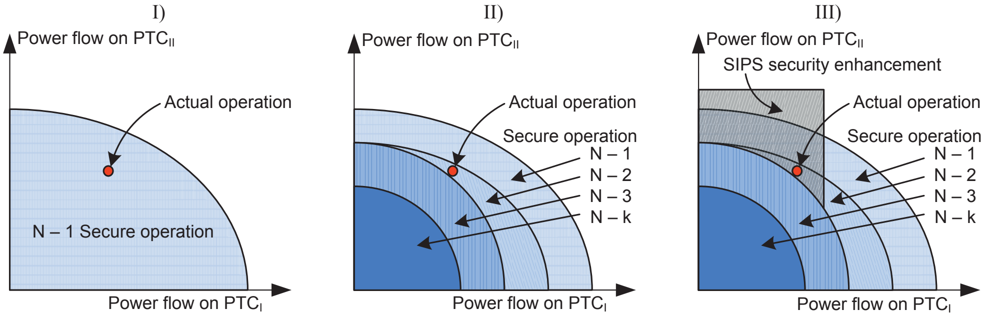

Figure 3: Visualising actual operating point and the secure region of operation[2] for a specific operating scenario, using the power flow on PTC_I relative to the flow on PTC_{II}: I) $N-1$ secure operation, II) $N-1$ to $N-k$ secure operation, II) SIPS security enhancement

4. SECURITY ASSESSMENT ANALYSIS

This section describes a security assessment of the transmission capacity across specific interfaces of a power system. The study is performed on the IEEE Reliability Test System 1996, which is a benchmark model for reliability assessment studies.

4.1 Study model

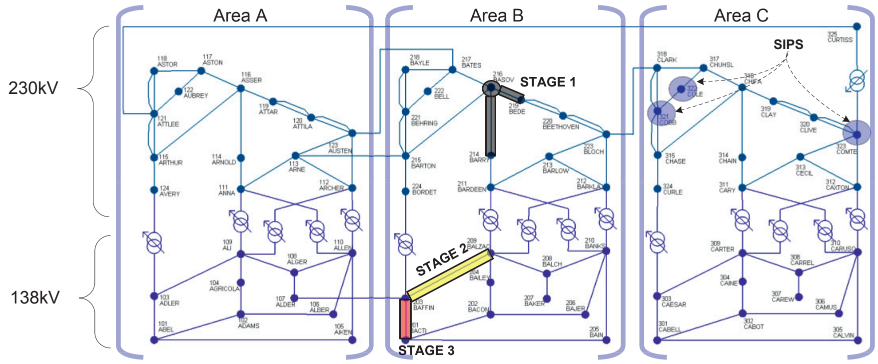

Figure 4: Single line diagram describing the IEEE Reliability Test System 1996, the dimensions does not reflect the line lengths. The markings *STAGES* and *SIPS* relate to the studies described in subsections 4.3 and 4.4, respectively.

The IEEE Reliability Test System 1996, defined in [13], consists of 73 buses in three equally designed areas, as shown in Figure 4. Each area has approximately 3.4 GW of installed

[2] In order to simplify the interpretation of the figures, the complexity is reduced with respect to the shapes in Figure 3; the more realistic shapes of a secure operating region is highly irregular.

production and a peak load of 2.8 GW. The areas are interconnected by five tie-lines, here referred to as the A-B, A-C, and B-C tie-lines, forming the inter-area power transfer corridors: PTC_{AB}, PTC_{AC}, and PTC_{BC}, respectively. In the analysed model, the optional DC-link is excluded, synchronous condensers are exchanged to SVCs, and the dynamic models suggested in [14] are used to represent the synchronous generators.
The studied operating scenario is a low load scenario, corresponding to a total system demand of approximately 50 % of the peak demand. Two cases of power exchange are studied, with power transfer between areas listed in Table I. In both cases, area A is a region with a low level of power interchange, while areas B and C are import and export regions, respectively.

Table I: Inter-area power exchange of the studied operating scenarios

	Case 1	Case 2
PTC_{AB} Power flow(MW) (rating: 175 + 2×500 MVA[3])	220	255
PTC_{AC} (MW) (rating: 500 MVA[3])	240	150
PTC_{BC} (MW) (rating: 500 MVA[3])	420	365
Area A Power export (MW)	15	-105
Area B Power export (MW)	-640	-620
Area C Power export (MW)	655	515

4.2 N – 1 security assessment

The $N-1$ security of both cases is assessed through dynamic contingency analysis, studying faults on transmission lines, transformers, and generators, where a 3-phase short-circuit is applied for 100 ms followed by disconnection of the affected unit.

Case 1 is identified to be insecure for the following contingencies: fault and trip of either of the A-C and B-C tie-lines (PTC_{AC}, PTC_{BC}). Since the desired power export from area C (655 MW) is well above the short term $N-1$ thermal rating of the tie-lines to area C, tripping one of these lines would result in an excessive overload of the remaining line. The dynamic analyses indicate that tripping PTC_{AC} results in rotor angle instability, which might lead to a large disturbance[4]. Hence, Case 1 can not be considered secure, from an $N-1$ perspective. Some of the results from the $N-1$ contingency analysis are shown in Figure 5. Parts I and IV describe the power flow on PTC_{BC} and PTC_{AC}: P_{BC} and P_{AC}, for all stable contingencies. Parts II-III and V-VI include the voltage angle and frequency difference over the same PTCs: $\Delta\delta_{BC}$, Δf_{BC} and $\Delta\delta_{AC}$, Δf_{AC}, for all studied contingencies (except when the PTC itself is tripped). The analysis includes contingencies with the short-circuit applied on either end of a line, hence two cases where A-C and B-C tie-line trips can be seen in the figure. The dashed red curves represent contingencies where the short-circuit is on the C-side of the line. These contingencies have a significantly higher impact on the system than contingencies where the short-circuit is on the other side of the line, as can be seen in parts II and III of the figure.

[3] The thermal overload capabilities of all lines are 120 % for 24 hours and 125 % for 15 minutes.
[4] It should be noted that in a power flow simulation, the disconnection of PTC_{AC} resulted in a stable solution, although with approximately 135 % overload of PTC_{BC}. Assuming the PTC_{BC} would trip, the system separates into two islands which could remain in stable operation depending on islanding control and the level of reserves available in each island. These results demonstrate an important difference between dynamic and power flow simulations, where the latter disregards the transient phenomena and therefore may not be able to identify the criticality of the contingency.

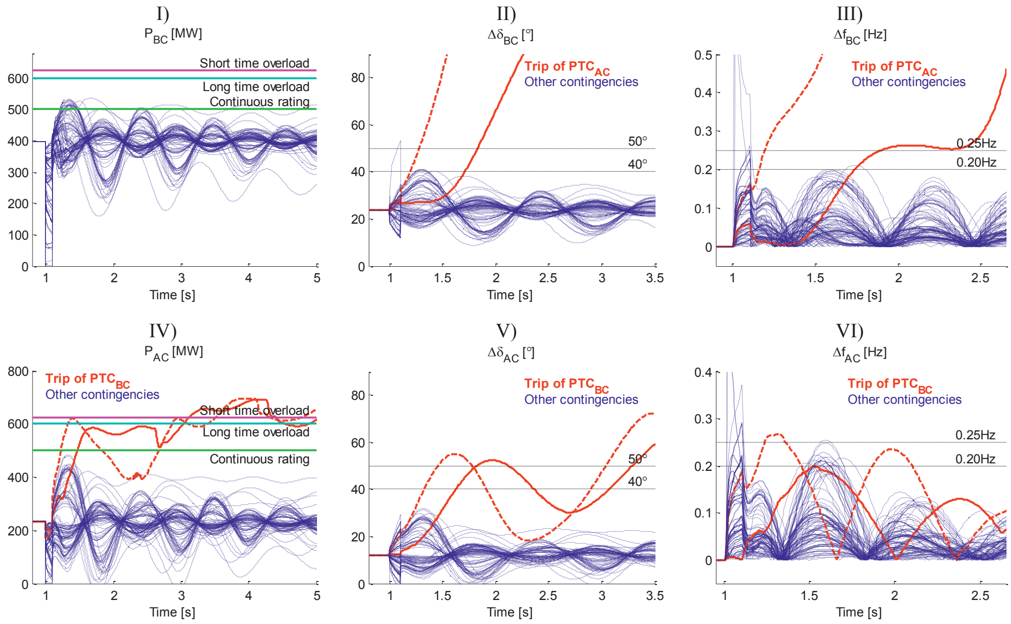

Figure 5: Results from the $N-1$ contingency analysis of Case 1, showing power flow, angle difference and frequency difference of PTC_{BC} (I-III) and PTC_{AC} (IV-VI)

Case 2 has been found secure for all the analysed contingencies, even though the desired power export from area C (520 MW) is above the continuous $N-1$ thermal rating of the tie-lines from area C, it is well below their long term overload capability.

4.3 N – k security assessment

The $N-k$ security of Case 2 has been assessed through both an $N-k$ contingency analysis and an analysis of common cause failures.

The $N-k$ contingency analysis is performed with consecutive contingencies, where the subsequent contingency occurs after the system has reached a steady state, but before any generation re-dispatch has taken place. A set of contingencies including the largest generation unit in area B (located on bus 221, see Figure 4) and PTC_{BC} is identified to cause instability. Independently of which contingency is occurring first, the system cannot regain stable operation after the second contingency. This suggests that Case 2 can be considered $N-1$ secure, but $N-2$ insecure[5].

Common cause failures, where the failure of a single item leads to the disconnection of several components, are not always a part of an ordinary $N-1$ contingency analysis. The consequences of such failure may have high impact on the system, and an example of this is described here.
The breaker-and-a-half configuration shown in Figure 6, describes the layout of substation 216, where a failure of the midsection breaker results in the disconnection of the outgoing lines to buses 214 and 219.

[5] Other contingency sets leading to instability can be identified through a more extensive $N-k$ contingency analysis, however, the number of subsequent contingencies will be minimum two.

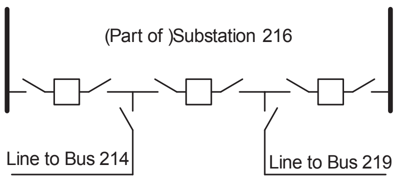

Figure 6: Single line diagram describing substation 216, with breaker-and-a-half configuration feeding lines to buses 214 and 219, according to [13].

In both Case 1 and 2, such failure leads to thermal overload of lines, followed by a thermal cascade, resulting in instability. The first part of the event can be separated in three stages, as marked in Figure 4:

- Stage 1 includes the failure at bus 216 and the trip of lines 216-214 and 216-219
- Stage 2 represents the overload and trip of line 203-209
- Stage 3 represents the overload and trip of line 203-201.

The thermal capacity of each of the lines in stages 2 and 3 is 175 MVA[6].

In Case 2, the overload in Stage 2 (124%) is just below the short-term emergency rating of the line, implying that there might be time to implement manual remedial actions before any protection disconnects the line. If such actions are not taken, or if the actions are insufficient, the line is likely tripped. In Stage 3, the line load (153 %) is far beyond its short-term emergency rating, which might lead to a fast protective disconnection of this line. If the line is tripped, the main part of area B is fed only through PTC_{BC}, and the system experiences instability. Case 2 can thus be considered $N-1$ secure, but $N-1$ inadequate when considering common cause failures.

This study reveals both the importance in identifying failures to include in the contingency analysis of a security assessment study, and that insufficient remedial actions, to mitigate the overload of a line which might seem to be of minor importance to the system state, may cause instability.

4.4 SIPS security enhancement

It is possible to design System Integrity Protection Schemes to improve the security of the analysed cases. Here, a study is made of a generator tripping scheme in area C and its influence on the $N-1$ security of Case 1. The efficiency of three different types of arming and activation/triggering signals is assessed:

I. Event-based, monitoring the trip signal of circuit breakers in PTC_{AC}: $SIPS_{CB}$
II. Response-based, monitoring the voltage angle differences over PTC_{BC}: $SIPS_{\delta}$
III. Response-based, monitoring the bus frequency at both sides of PTC_{BC}: $SIPS_{f}$

A manual (or automatic) arming is assumed to limit the operating scenarios where the SIPS can be triggered, and that, e.g., the level of inter-area power transfer is used to identify an appropriate level of generation tripping in each scenario. The mitigating action studied here, is acting on sources in the production dense 230 kV region of area C, as marked in Figure 4.
A thorough assessment of the arming procedures and activation signals is necessary to limit the risk of inappropriate SIPS actions. Arming procedures can be designed through identification of the operating criteria that defines the secure operating area, while an

[6] The thermal overload capabilities of all lines are 120 % for 24 hours and 125 % for 15 minutes.

extensive dynamic analysis is needed to identify appropriate activation signals and their magnitude. Here, the analysis is limited to the cases and contingencies described previously.

From Figure 5, the unstable contingencies are easily distinguishable in both $\Delta\delta_{BC}$ and Δf_{BC}, supporting their potential as SIPS activation signals. It is suggested that an internal arming is used together with a time delay, to prevent unwanted SIPS action during switching events. Based on the results of the dynamic contingency analysis, the suggested arming and activation signal magnitudes, as marked in Figure 5, are:

$\Delta\delta_{BC}$ - arming: 40° for 200ms, activation: 50°

Δf_{BC} - arming: 0.2Hz for 200ms, activation: 0.25Hz

δ and f measurements are considered to be available, from e.g. a WAMS, and the total delay between measurement and the implementation of mitigating action is assumed to be no longer than 100 ms.

Figure 7 describes the response, after the trip of PTC_{AC}, with and without the suggested SIPS, including the power flow, angle, and frequency difference over PTC_{BC}. The dashed curves in part II represent the fault with the short-circuit occurring at the C-side of the line. The system response of this contingency is too rapid for the $SIPS_{\delta}$ and $SIPS_{f}$ solutions to act before the system becomes unstable, and only $SIPS_{CB}$ results in a stable solution. All other curves in the figure represent the fault with the short-circuit occurring at the A-side of the line. For this fault, all the studied SIPS solutions results in a stable post-fault system, however, the event-based $SIPS_{CB}$ scheme shows lower levels of oscillations due to the more rapid activation than the response-based schemes.

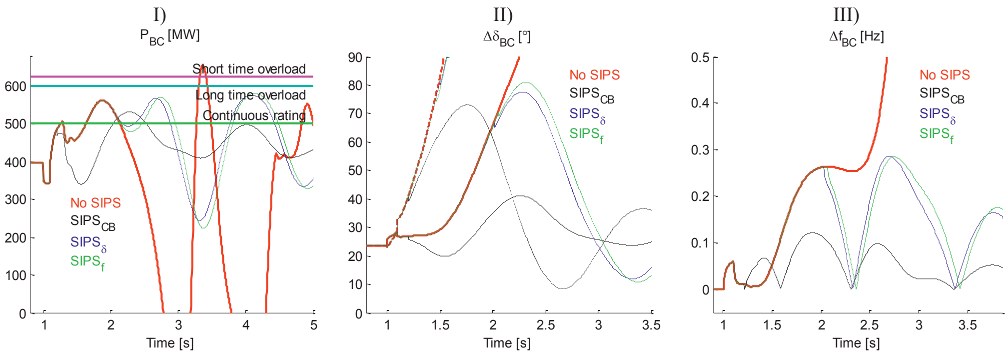

Figure 7: Results for different SIPS activation signals after trip of PTC_{AC}, in Case 1: I) P_{BC}, II) $\Delta\delta_{BC}$, III) Δf_{BC}

In Figure 8, the characteristics of PTC_{BC} are included in the form of the power-voltage, the power-angle, and the rotor motion curves. According to the equal-area criterion, passing the unstable equilibrium point, here approximated by (P_S, $\Delta\delta_U$), would result in instability since the decelerating torque was not able to sufficiently decelerate the machine before it starts to accelerate out of synchronism. This behaviour is seen in the scenario without SIPS, where the angle increases beyond $\Delta\delta_U$. For the scenarios with SIPS, the maximum angles ($\Delta\delta_{CBmax}$ and $\Delta\delta_{\delta fmax}$) are lower than $\Delta\delta_U$ and the system stabilises at a post-contingency stable equilibrium point (represented by V_S, P_S, and $\Delta\delta_S$). It is, however, complex to identify the actual unstable equilibrium point, since: the mechanical power is not constant but depending on the response of the governor controller, and the voltage dependency of loads will affect the electrical power flow. Through simulations with increased delay in SIPS mitigating actions, the actual $\Delta\delta_U$ is approximated to 110degrees for the studied scenario.

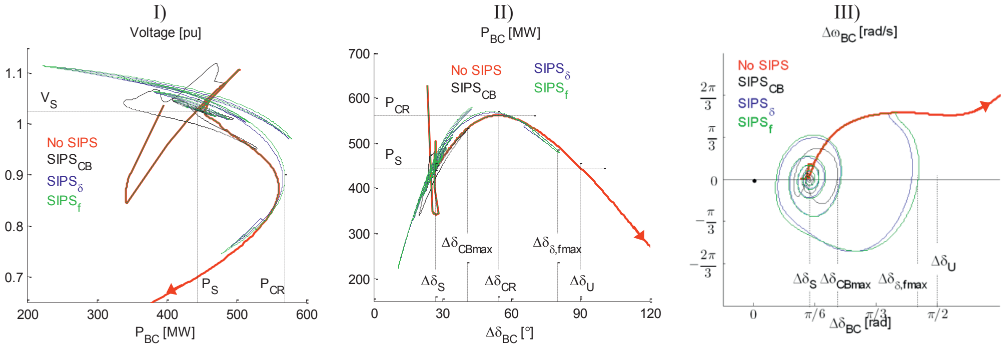

Figure 8: Results for different SIPS activation signals after trip of PTC_{AC}, in Case 1: I) Power-voltage (nose) curve, II) Power-angle characteristics, III) Rotor motion trajectory

5. DISCUSSION AND CONCLUSIONS

This study gives examples of SIPS solutions utilising monitoring parameters provided by a WAMS. The studied SIPS solutions are, however, not the most optimal ones, and other schemes can further improve the $N-1$ security of the studied cases. Response-based solutions, as the suggested $SIPS_\delta$ and $SIPS_f$ will not be as fast as event-based SIPS, but they will be able to provide increased protection against multiple or unforeseen contingencies that event-based protections can not. Improvements in SIPS activation can be done using adaptive response, providing optimal protection in each operating scenario. The sufficient amount of mitigating actions depends on the required actions for the system to remain stable. In the case of generation tripping, factors such as the level of spinning reserves and reactive power capabilities available after the SIPS action are needed to be considered. It is also possible to select the mitigating actions through a sensitivity analysis, assessing the stabilising effects of each component.

This study also demonstrates that thermal overloading of a line, which seems to be of minor importance to the system state, can cause instability if mitigated actions are not implemented. Furthermore, it is shown that power flow simulations might not be able to identify critical contingencies, since transient phenomena are disregarded. These findings underline the importance of performing dynamic contingency analysis during a security assessment study, also in power systems where thermal capacities is the normal limitation on the power transfer capacity.

The described visualisation of an $N-k$ secure operating region, together with a continuous monitoring of the *k-index*, could provide improved awareness of the power system's vulnerability to extraordinary events. This does however imply the need of continuously performed $N-k$ contingency analysis to properly identify the vulnerabilities as the operating scenario of the system changes.

6. ACKNOWLEDGEMENT

The authors would like to thank PhD candidate J. Lamponen and Professor L. Haarla, both at Aalto University School of Electrical Engineering, Espoo, Finland, for the cooperation in developing the concept of dynamic $N-k$ vulnerability assessment and in the work of modelling and simulation of the IEEE Reliability Test System 1996.

The support provided by T. Toftevaag at SINTEF Energy Research, related to power system dynamic phenomena, is gratefully acknowledged.

BIBLIOGRAPHY

[1] Nordel, *The Nordic Grid Code*. 2007; Available from: www.entsoe.eu/
[2] IAEW, CONSENTEC, *Analysis of Electricity Network Capacities and Identification of Congestion, Final Report*. 2001; Available from: ec.europa.eu
[3] CIGRE Task Force 38.03.12, *Power system security assessment: A position paper,* ELECTRA, no. 175, Dec., 1997
[4] IEEE Task Force on Blackout Experiences, Mitigation, and Role of New Technologies, *Blackout Experiences and Lessons Best Practices for System Dynamic Performance, and the Role of New Technologies,* Special Publication 07TP190, 2007
[5] Madani, V., Novosel, D., Horowitz, S., Adamiak, M., Amantegui, J., Karlsson, D., Imai, S., Apostolov, A., *IEEE PSRC Report on Global Industry Experiences With System Integrity Protection Schemes (SIPS),* IEEE Transactions on Power Delivery, 2010, Vol. 25, p. 2143-2155
[6] CIGRE Task Force 38.02.19, *System Protection Schemes in Power Networks,* Technical Brochure 187, 2001
[7] Statnett, *Nettutviklingsplan 2010. Nasjonal plan for neste generasjon kraftnett (in Norwegian)*. 2010; Available from: www.statnett.no
[8] Breidablik, Ø., Giæver, F., Glende, I. *Innovative Measures to Increase the Utilization of Norwegian Transmission*, IEEE Power Tech Conference, 2003, Bologna, Italy
[9] Walseth, J.Å., Eskedal, J., Breidablik, Ø., *Analysis of Misoperations of Protection Schemes in the Nordic Grid - 1st of December 2005,* Protection, Automation & Control World, 2010,
[10] Johansson, E., Uhlen, K., Nybø, A., Kjølle, G., Gjerde, O. *Extraordinary events: Understanding sequence, causes, and remedies*, European Safety & Reliability Conference, 2010, Rhodes, Greece
[11] CIGRE Study Committee 39, *The Control of Power Systems During Disturbed and Emergency Conditions,* Technical Brochure 36, 1989
[12] Uhlen, K., Pálsson, M., Time, T.R., Kirkeluten, Ø., Gjerde, J.O. *Raising stability limits in the Nordic power transmission system*, 14th Power Systems Computation Conference, 2002, Sevilla, Spain
[13] Reliability Test System Task Force, *The IEEE reliability test system - 1996,* IEEE Transactions on Power Systems, Vol. 14, No.3, 1999
[14] Johansson, E., Uhlen, K., Kjølle, G., Toftevaag, T. *Reliability evaluation of wide area monitoring applications and extreme contingencies*, Power Systems Computation Conference, 2011, Stockholm, Sweden

IV

Paper IV:

Revealing stability limitations in power system vulnerability analysis
Hillberg, E., Lamponen, J., Haarla, L., Hirvonen, R.

Proceedings of the 8th Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, 2012, Cagliari, Italy
MedPower 2012
IET - The Institution of Engineering and Technology
ISBN 978-1-84919-715-1

Is not included due to copyright

V

Paper V:

Equal area criterion applied on power transfer *corridors*
Hillberg, E., Toftevaag, T.

Proceedings of the 5th IASTED Asian Conference on Power and Energy Systems, 2012, Phuket, Thailand
AsiaPES
International Association of Science and Technology for Development
Power and Energy Systems, 2012, I. Ngamroo (ed)
ACTA Press

EQUAL-AREA CRITERION APPLIED ON POWER TRANSFER CORRIDORS

Emil Hillberg[1)], Trond Toftevaag[2)]
1) Norwegian University of Science and Technology, 2) SINTEF Energy Research
Trondheim, Norway
1) emil.hillberg@ntnu.no, 2) trond.toftevaag@sintef.no

ABSTRACT

This paper presents a novel adaptation of the equal-area criterion. The adapted criterion provides a new possibility to study the stability criteria of critical power transfer corridors, supporting the specification of the secure power transfer capacity of the interconnected power system.

Furthermore, the authors describe how the adapted equal-area criterion can be employed in the design of System Integrity Protection Schemes to prevent instability and mitigate consequences of extraordinary events. The concept is tested on the benchmark model IEEE Reliability Test System 1996.

KEY WORDS

Equal-Area Criterion, Power System Stability, Wide Area Monitoring, Protection and Control, Security Assessment, Power Transfer Corridor

1. INTRODUCTION

Extraordinary events in the electrical power system refer to disturbances with potentially high societal impact and low probability to occur. As both probability and consequences of extraordinary events are highly unpredictable, there are difficulties to economically justify major power system reinforcements based on their prevention, [1].

Extraordinary events are often characterised by instability phenomena, [2], leading to the triggering of component protections, resulting in a wide-spread interruption or blackout,where the affected region is difficult to anticipate. As the system becomes unstable, only pre-designed automatic remedies, such as System Integrity Protection Schemes (SIPS), are able to prevent the un-controlled disconnection of power system components and splitting of the system.

SIPS are increasingly utilized in power systems worldwide, providing both increased transfer capacity and security [3]. The improved situational awareness provided by Phasor Measurement Units (PMU) and Wide Area Monitoring Systems (WAMS) opens for further improvements of conventional SIPS, providing robustness against unforeseen disturbances. The main purpose of SIPS is to prevent instability and to maintain an interconnected operation of the power system.

Stability phenomena related to extraordinary events are mainly large-disturbance voltage and rotor angle stability, where the latter is often referred to as transient (rotor angle) stability [4]. Frequency instability may also be an issue, typically related to the shortage of spinning reserves in island operation. Although the different stability phenomena are interrelated, the concerns of this paper are limited to aspects of transient rotor angle stability only.

Transient rotor angle stability is often analysed using simplifications, such as single-machine infinite-bus equivalent models, where stability margins are determined using the renowned equal-area criterion of a synchronous machine.

Since stability stipulates that every machine needs to fulfil the equal-area criterion, several studies focus on the identification of *critical machines* which are likely to loose synchronism with the remaining system [5-13]. In the case with multiple critical machines, it is possible to cluster these into an equivalent one-machine-infinite-bus (OMIB) system, as described in [5]. An extension of the traditional equal-area criterion is suggested in [6, 7], where the transient stability margin and critical clearing time of critical machines are assessed without equivalent models. Techniques for preventive and emergency transient stability control are described in [8-10]. Here, the single-machine-equivalent (SIME) method is utilised, and the emergency control actions are defined on the basis of identifying critical machines, which are tripped in an iteratively manner until the system reaches stable operation. Emergency controls based on online measurements provided by PMUs are suggested in [11-13]. Here, the equal-area criterion is used to identify critical machines and assess the adequacy of emergency control actions.

This paper presents a novel adaptation of the equal-area criterion, providing new possibilities to study the stability criteria of critical power transfer corridors (PTC) and specifying the secure power transfer capacity of the interconnected power system. The authors describe how the adapted equal-area criterion can be employed in the design of adequate mitigating actions of SIPS, to limit the consequences of extraordinary events.

The paper is organized in the following manner: Chapter 2 holds the theoretical background of the equal-area criterion, including a description of the concept to apply the criterion on a PTC. The utilization of the adapted equal-area criterion in SIPS design is described in chapter 3. Chapter 4 holds a case study made on the IEEE Reliability Test System 1996. Discussion and conclusions are included in chapter 5.

2. THEORETICAL BACKGROUND

2.1 Equal-Area Criterion of a single machine

The equal-area criterion of a single synchronous machine, in a multi-machine system exposed to a disturbance, can be formulated as:

$$A_{acc} - A_{dec} \leq 0 \tag{1}$$

where A_{acc} and A_{dec} are the accelerating and decelerating areas as depicted in the synchronous machine power-angle characteristics illustrated in Fig 1. Equality occurs if the maximum rotor angle, δ_M, coincides with the post-fault unstable equilibrium angle, δ_U, i.e. for the machine to remain stable, the following criteria needs to be fulfilled:

$$\delta_M \leq \delta_U \tag{2}$$

From in Fig 1, it is clear that the accelerating and decelerating areas can be calculated as:

$$A_{acc} = \int_{\delta_S}^{\delta_{CT}} \left(P_M - P_f(\delta)\right) \mathrm{d}\delta \tag{3}$$

$$A_{dec} = \int_{\delta_{CT}}^{\delta_M} (P_E(\delta) - P_M) \, \mathrm{d}\delta \tag{4}$$

where δ_S *and* δ_{CT} are the rotor angles at the pre-fault steady-state equilibrium and at the time of fault clearing, respectively. P_M is the mechanical power of the turbine (assumed constant), and $P_f(\delta)$ and $P_E(\delta)$ are the under-fault and post-fault electrical power of the machine, respectively.

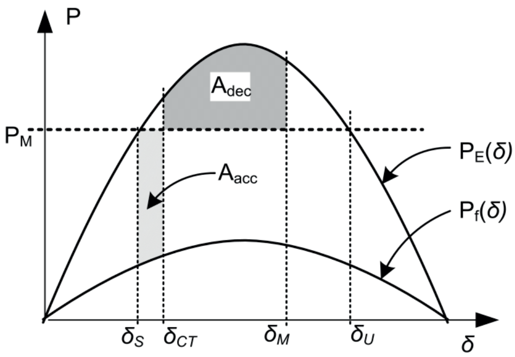

Fig 1. Simplified power-angle characteristics of a synchronous machine, during and after a temporary fault.

The rotor angle δ needs to be related to a reference, and often a centre of angle reference is used, [5], but theoretically any angle reference can be used.

2.2 Equal-Area Criterion of a Power Transfer Corridor

Fig 2 shows a power system, consisting of a sub-system and a main system, interconnected via a single power transfer corridor (PTC). In this system, it is possible that all synchronous machines inside the sub-system can be identified as critical for certain contingencies. This is exemplified by Fig 3, where all generators in the sub-system accelerate relative the main system after a critical contingency.

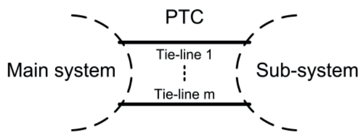

Fig 2. A power system where one sub-system is connected to the rest of the system through a single power transfer corridor.

Clustering all critical machines into an equivalent model, as described in [5], the entire sub-system can be assessed against the main system. This implies that, at steady state, the equivalent mechanical power of the sub-system equals the power flow of the PTC. Together with the angle difference between the equivalents of the sub- and main systems, the equal-area criterion of the PTC can be assessed.

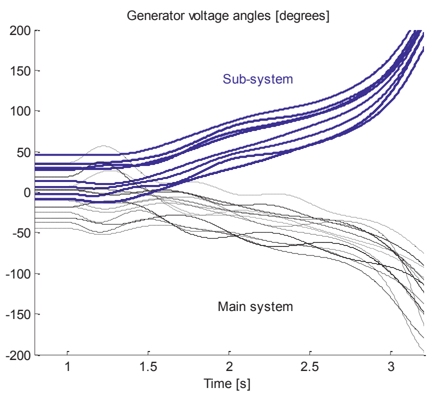

Fig 3. Generator terminal voltage angles, where all generators in a sub-system accelerate (relative the rest of the system) after a critical contingency.

If the PTC consists of only a single tie-line, the rotor angle reference can be selected so that δ corresponds to the voltage angle difference over the PTC. Thus, the power-angle characteristics of the sub-system and main system equivalents correspond to the power flow and angle over the PTC. The equal-area criterion of the PTC can then be described by equations (1)-(4).

The loss of a line or generator in close vicinity of a PTC may prove to be especially critical: significantly decreasing the power-angle characteristics of the PTC, resulting in an equivalent mechanical power which exceeds the critical loading level of the post-fault system. This scenario is exemplified by Fig 4, where a SIPS is suggested to decrease the equivalent mechanical power of the post-fault system to a new stable operation point.

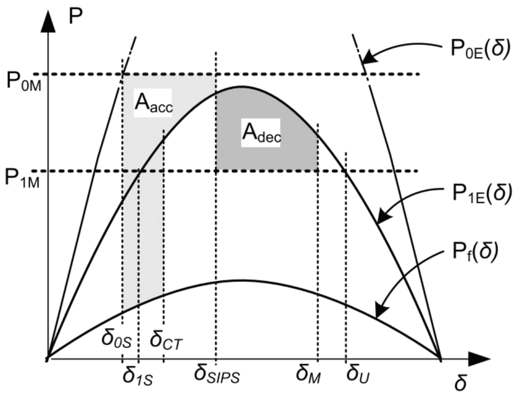

Fig 4. Simplified power-angle characteristics of a PTC, describing pre-fault, $P_{0E}(\delta)$, under-fault, $P_f(\delta)$, and post-fault, $P_{1E}(\delta)$, characteristics. P_{0M} and δ_{0S} represent the pre-fault steady-state operating point. δ_{SIPS} represent the angle difference at the instant when the SIPS is activated, with P_{1M} and δ_{1S} as the post-SIPS stable equilibrium point and δ_U as the corresponding unstable equilibrium.

At the pre-fault state, the steady-state operation point is characterized by the PTC power flow, $P_{0E}(\delta)$, the PTC equivalent mechanical power of the sub-system, P_{0M}, and the voltage angle between the equivalents of the sub- and main systems, δ_{0S}. A critical contingency moves the system to an unstable state, since the pre-fault mechanical power is higher than the critical level of the post-fault power-angle characteristics, $_{\max}\{P_{1E}(\delta)\}$. At $\delta = \delta_{SIPS}$, the mitigating action of a SIPS system is assumed to decrease the mechanical power to a potentially stable post-fault level, P_{1M}.

In the scenario described by Fig 4, equations (3) and (4) require the following modifications:

$$A_{acc} = \int_{\delta_{0S}}^{\delta_{CT}} \left(P_{0M} - P_f(\delta)\right) \mathrm{d}\delta + \int_{\delta_{CT}}^{\delta_{SIPS}} \left(P_{0M} - P_{1E}(\delta)\right) \mathrm{d}\delta \tag{5}$$

$$A_{dec} = \int_{\delta_{SIPS}}^{\delta_M} \left(P_{1E}(\delta) - P_{1M}\right) \mathrm{d}\delta \tag{6}$$

The equal-area criterion of a PTC can thus be further utilised in contingency analysis, where assessing the stability margins of a critical PTC can provide an improved overview of the system operation. In the case when assessing the system response after multiple sub-sequent contingencies, the PTC stability margins can be used to identify the systems vulnerability of extraordinary events.

3. EQUAL-AREA CRITERION APPLIED ON SIPS DESIGN

The main purpose of the SIPS is to regain a stable steady-state operation of the power system. A sufficient level of mitigating action is needed in order for the system to maintain in stable operation in accordance with the equal-area criterion. The SIPS system introduced in the previous section could be based on for example load-shedding or generation-rejection. In the following, the suggested design procedure of a generation-rejection scheme is described.

The SIPS design, having the goal to identify suitable generators to achieve sufficient stabilizing performance, is proposed to be done by:

1. Identification of critical contingencies
2. Equal-area criterion assessment of critical contingencies
3. Selection of suitable generators to participate in SIPS action

This procedure is described in the following sub-sections and tested in the power system analysis described in chapter 4.

3.1 Identification of critical contingencies

The critical contingencies referred to here, are the contingencies leading to rotor-angle instability in the sense that all machines within a specific sub-system are identified as critical.

Critical contingencies can be identified through a standard contingency analysis, assessing the consequences of e.g. all $N-1$ contingencies. The contingency analysis should be based on dynamic simulations, rather than steady-state power flow calculations, since the transient stability of the system is to be assessed.

3.2 PTC equal-area assessment of critical contingencies

For each identified critical contingency, the SIPS activation instant and corresponding angle needs to be assessed. In this way, the size of the accelerating area of can be calculated, which defines the minimum size of the decelerating area that fulfils the equal-area criterion. Thus, the minimum level of mitigating actions necessary to maintain stable operation can be identified.

3.3 Selection of suitable generators to participate in SIPS action

There are two criteria in the selection procedure of generators that have to be addressed: firstly, the generators should have a power production level corresponding at least to the minimum level of mitigating actions, secondly, the impact on the sub-system and on the PTC characteristics should be limited in order for the equal-area criterion to be utilised.

A suitable set of generators needs to be selected among the critical machines as a basis to perform desired SIPS actions, in order to assess the reliability of the new steady-state scenario.

4. CASE STUDY

4.1 System model

The study is performed on the IEEE Reliability Test System 1996, which is a benchmark model for reliability assessment studies.

The IEEE Reliability Test System 1996, defined in [14], consists of 73 buses in three sub-systems, area A, B, and C, as shown in Fig 5. Each area has approximately 3.4GW of installed production and a peak load of 2.8GW. The areas are interconnected by five tie-lines, where the A-C and B-C tie-lines form a power transfer corridor between area C and the rest of the system, referred to as PTC_C.

The studied scenario is a low load scenario, with total demand approximately 50% of the system peak demand. The power exchange between areas is listed in Table I, with area A as a transit region, and areas B and C as import and export regions, respectively.

The loads in the system are represented by steady-state and dynamic load models, based on a composite of constant power, constant current and constant admittance, as defined by equations (7)-(10):

$$P_0 = P_N \left({U_0}/{U_N} \right)^2 \tag{7}$$

$$P_d = P_0 \, {U_d}/{U_0} \left(0.4 + 0.6 \, {U_d}/{U_0} \right) \tag{8}$$

$$Q_0 = Q_N \tag{9}$$

$$Q_d = Q_0 \left({U_d}/{U_0} \right)^2 \tag{10}$$

where the sub-indices N, 0, and d represent nominal, steady-state, and dynamic values, respectively. P and Q refer to the active and reactive power of the load, with U as the bus voltage.

In this study, the optional DC-link is excluded, synchronous condensers are exchanged with SVCs, and the dynamic models suggested in [15] are used to represent the synchronous generator and turbine systems.

TABLE I
INTER-AREA POWER EXCHANGE OF THE STUDIED OPERATING SCENARIO

Area A→B Power flow(MW)	220
Area C→A Power flow (MW)	240
Area C→B Power flow (MW)	420
Area A Power exchange (MW)	15
Area B Power exchange (MW)	-640
Area C Power exchange (MW)	655

4.2 Identification of critical contingencies

Critical contingencies are identified through an $N-1$ contingency analysis, including 3-phase short-circuit faults on transmission lines, transformers, and generators,

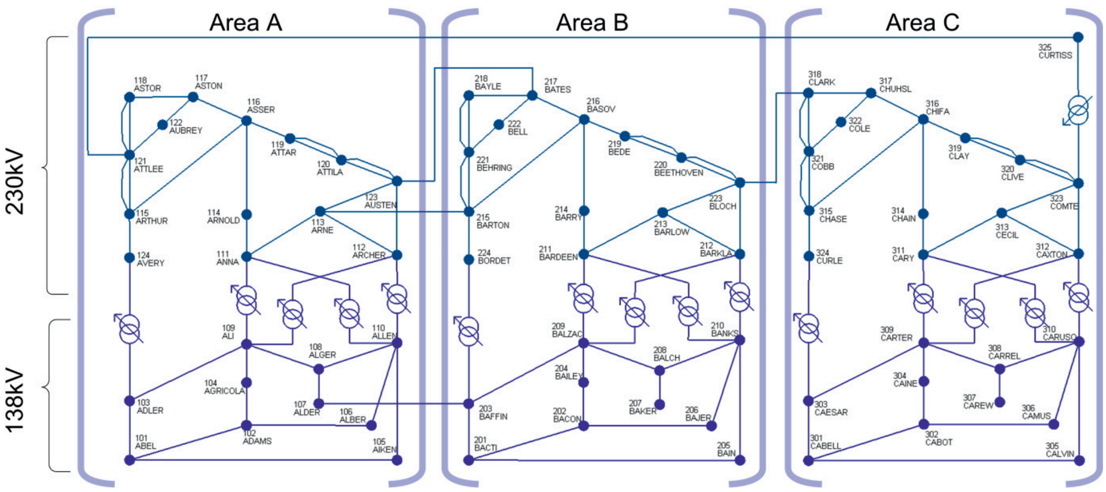

Fig 5. Single-line diagram describing the IEEE Reliability Test System 1996. The dimensions do not reflect the line lengths.

with 100ms duration, followed by the disconnection of the affected unit. The results show that the trip of the A-C tie-line leads to instability, as shown in Fig 6.

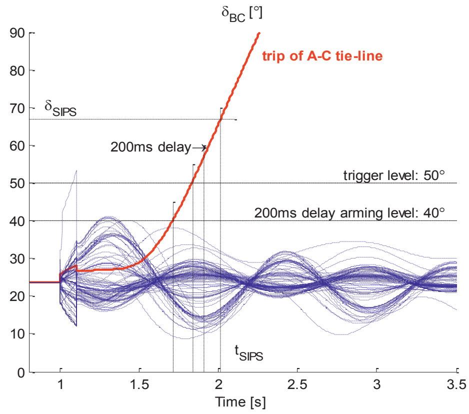

Fig 6. Results of the $N-1$ contingency analysis, showing angle difference over PTC$_C$, δ_{BC}. Trip of the A-C tie-line results in an increasing angle difference.

Further analysis of the critical contingency, shows that all machines in area C accelerate out of synchronism relative the rest of the system, as described by the generator terminal voltage angles shown in Fig 3. Hence, for this contingency, the machines in area C are considered critical and can be clustered into a single-machine equivalent to analyze the transient stability of the system.

4.3 PTC equal-area assessment of critical contingencies

The equal-area assessment of the PTC for the identified critical contingency is done in three steps:

1. Identifying the instant of SIPS activation
2. Assessing the accelerating area of the PTC before SIPS activation
3. Assessing the minimum necessary level of rejected generation to fulfil the equal-area criterion

4.3.1 Identifying the instant of SIPS activation

A generation-rejection SIPS is considered to be utilized to prevent instability if the A-C tie-line is tripped. Measurement data from a WAMS are used as input to the SIPS, where δ_{BC}, the voltage angle difference over PTC$_C$ shown in Fig 6, is utilised as activation signal.

The total inherent time delay of the SIPS, from PMU measurement to execution of mitigating action, is assumed to be no longer than 100ms. This seams realistically achievable, based on actual measurements of a PMU based Wide Area Power Oscillation Controller as well as the delays of a Wide Area Monitoring and Control System presented in [16].

By studying the results of the $N-1$ contingency analysis, presented in Fig 6, appropriate trigger levels for arming and activation of the SIPS are identified:

δ_{arming}: $\delta_{BC} \geq 40°$

$\delta_{activation}$: $\delta_{BC} \geq 50°$

To prevent unwanted SIPS action during switching events, the internal time delay between arming and earliest activation is set to 200ms.

The specified SIPS trigger levels and delays are displayed in Fig 6, together with the resulting activation angle of the SIPS and corresponding instant:

δ_{SIPS}: $\delta_{BC} \leq 67°$

t_{SIPS}: $t_0 + 1.0$s

where t_0 is the instant of the occurrence of the fault.

4.3.2 Assessing the accelerating area of the PTC before SIPS activation

The power-angle characteristics of the PTC is shown in Fig 8, together with the identified SIPS activation angle, δ_{SIPS}, for the critical contingency (the trip of the A-C tie-line).

Assuming a constant mechanical power of the system, the accelerating area before the SIPS activation, as shown in Fig 8-I, is then approximated to:

$A_{acc}|P_{0M} = 5000\text{MW}$

The mechanical power of the turbines is, however, not constant but depending on the response of the governor controllers. Assuming that the response of each machine can be approximated by its speed-droop, then the response of the system can be approximated by a piece-wise linear speed-droop, R. The mechanical power of the system, as a function of the frequency change, can thus be approximated as:

$$P_M(\Delta\omega) = \left(1 - {}^{\Delta f}/_{R}\right) \times P_{0M} \tag{11}$$

where Δf is the per unit change in frequency and P_{0M} is the mechanical power at the pre-fault instant.

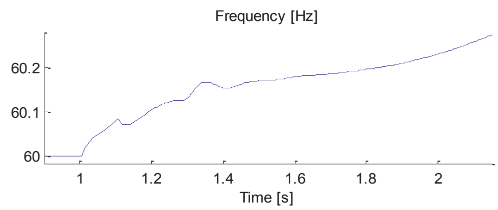

Fig 7. Area C frequency response for the critical contingency.

The speed-droop of the system can be assessed during operation, studying the frequency response of a known disturbance, e.g. the trip of a generator, as:

$$R = -{}^{\Delta f}/_{\Delta P_G} \times P_G \tag{12}$$

where ΔP_G is the production change and P_G is the total production of the system. In the studied scenario, the speed-droop of the system is approximated to:

R=4.3%

The frequency in area C, measured at the B-C tie-line, is shown in Fig 7.

From this frequency measurement and the calculated speed-droop of the system, the approximate equivalent mechanical power of the sub-system, $P_M(\Delta\omega)$, is derived from equation (11), and illustrated in Fig 8-II.

The PTC$_C$ accelerating area can then be approximated to:

$$A_{acc}|P_M(\Delta\omega) = 3000\text{MW}$$

This area is drastically smaller than the area calculated using constant mechanical power. This implies that the impact of simplified assumptions is large, thus to design appropriate SIPS solutions sufficient details are needed to be considered.

4.3.3 Assessing the minimum level of rejected generation to fulfil the equal-area criterion

Assuming that the SIPS action affect on the frequency in area C can be approximated by a linear decay, with nominal frequency reached at the maximum angle, δ_M, the decelerating area can be assessed as shown in Fig 8-III. The minimum SIPS action that fulfil the equal-area criterion is then approximated to:

$P_{SIPS} \geq 206$MW

The resulting maximum angle equals:

$\delta_M = 99°$

4.4 Selection of suitable generators to participate in SIPS action

Table II lists all generators in operation in area C.

TABLE II
GENERATORS IN SUB-SYSTEM C

Bus number and generator ID	Pre-fault production (MW)	Selected SIPS solutions	
302 G1	10		B3
302 G2	10		
313 G1	197		B3
313 G2	197	C1	
313 G3	197		
315 G1-5	5x12		
315 G6	155	C2	B2
316 G1	114	C3	B2
321 G1	400	A1	
322 G1-6	6x25		
323 G1	155		B1
323 G2	155		B1
323 G3	350	A2	

If basing the SIPS solution on the rejection of a single generator, only the machines on bus 321 and 323 (G3) have sufficient production, i.e. $P_G \geq P_{SIPS}$. These machines are selected to represent the solutions SIPS$_{A1}$ and SIPS$_{A2}$, respectively.

Various generator selections are possible for SIPS solutions based on tripping several generators. Here three solutions have been selected: SIPS$_{B1\text{-}B3}$.

Solutions SIPS$_{C1\text{-}C3}$ are based on single machines with production less than the identified minimum P_{SIPS} level.

The selected SIPS solutions are based only on the first criteria defined in section 3.3: the production level of the selected generators. The second criteria relates to the machines' impact on the PTC and the sub-system, which can be difficult to anticipate. The machines' reactive power capability and the relative closeness to the PTC determine their influence on the voltage level of the PTC bus. From the single-line diagram in Fig 5, it is noticed that bus 321 (SIPS$_{A1}$) is relatively close to the PTC bus, thus this solution might cause voltage instability in the sub-system. This has however not been further investigated in this study.

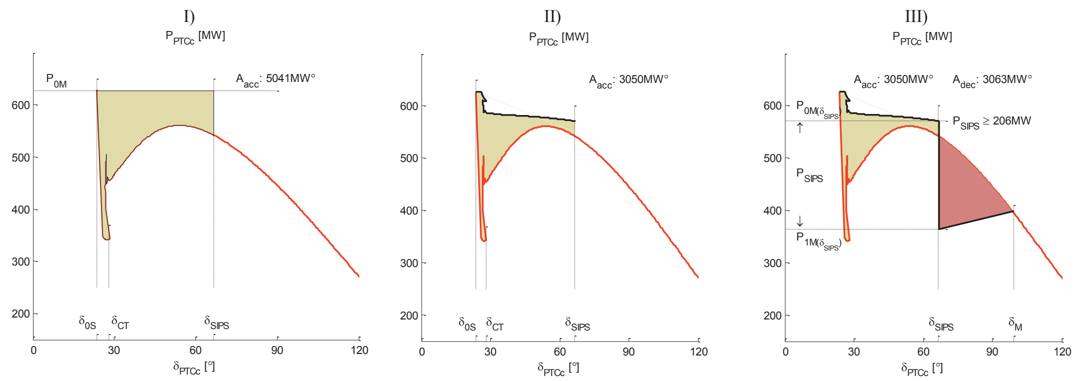

Fig 8. Assessment of PTC$_C$ accelerating area for the critical contingency, assuming: I) constant mechanical power, II) mechanical power as a function of the frequency deviation. III) Assessment of minimum generation rejection level to fulfill the equal area criterion.

4.5 Results from SIPS activation

The response of the selected SIPS solutions are analysed in this section, showing simulation results in Table III.

TABLE III
RESULTS OF SIPS ACTIVATION

SIPS ID	Rejected power P_{SIPS} (MW)	Maximum angle δ_M (°)	Decelerating area A_{dec} (MW°)	Post-SIPS PTC power transfer P_{M1} (MW)
A1	400		- (unstable)	
A2	350	76	3000	420
B1	310	77	2800	450
B2	269	82	3100	470
B3	207	83	2000	500
C1	197	84	1800	500
C2	155	84	1400	520
C3	114		- (unstable)	

As anticipated, solution A1 results in an unstable solution. This is due to the location and size of the generator that is rejected in this scheme, leading to a significant voltage drop at the PTC and the system is not able to regain stability. Also solution C3 proved insufficient, which was expected from the insufficient level of rejected power.

Solutions A2, B1, and B2, shown in Fig 9, all respond as expected, with stable solutions and the calculated decelerating areas are approximately equal to the accelerating area. For these solutions, the approximate accelerating and decelerating areas are quite similar. Better approximations are possible to achieve, if considering also the effects of the voltage changes in the sub-system. Furthermore, the participation of each machine in the acceleration of the sub-system should also be considered. Since the accelerating area of the PTC consists of the participation of each machine, the contribution of the rejected machines should be deducted from the total acceleration.

It should be noted that solutions B3, C1, and C2, shown in Fig 10, have decelerating areas considerably smaller than expected. The reason behind this is related to the reactive power capability of the rejected machines. In these three cases, the generators in question were at their under-excitation limit, implying that their disconnection would lead to a voltage rise at the buses in the surrounding area affecting the load of area C. As defined by the dynamic representation of loads, described by equations (8) and (10), a rise in voltage on the load buses lead to an increase in active and reactive load. Thus, the

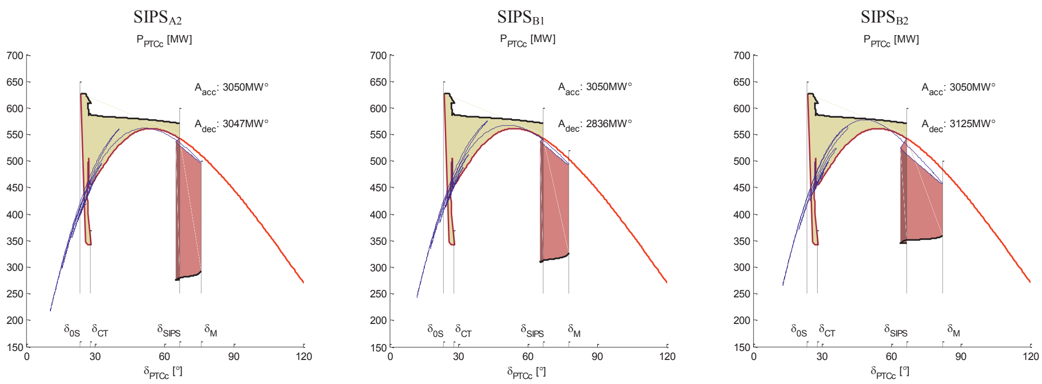

Fig 9. Results from the stable SIPS solutions: A2, B1, and B2.

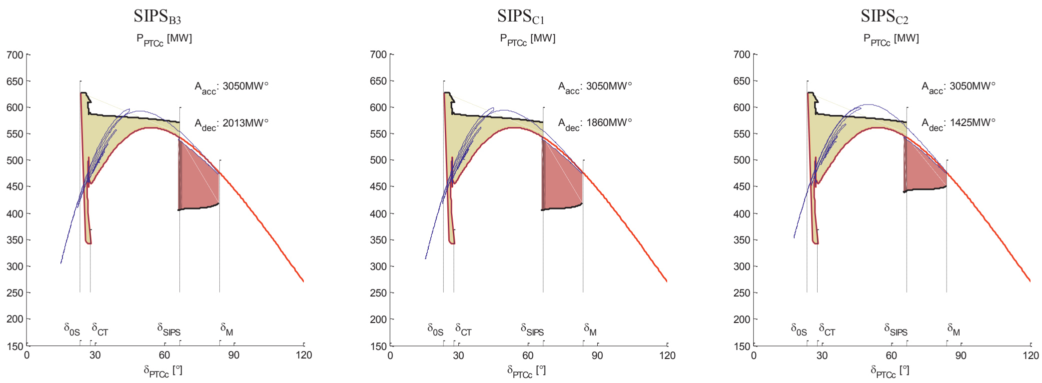

Fig 10. Results from the stable SIPS solutions: B3, C1, and C2.

actions of these three SIPS solutions result in increased load of the sub-system, meaning that the equivalent mechanical power of the sub-system further decreases due to the voltage rise. Hence, in order to properly assess the decelerating areas, also the SIPS affect on the load needs to be considered in the equivalent mechanical power.

5. CONCLUSIONS AND DISCUSSION

The concept of applying the equal-area criterion on critical power transfer corridors appears theoretically feasible. The results from computer simulations show that it is possible to utilise this concept when designing a System Integrity Protection Scheme.

Assumptions regarding the equivalent mechanical power of the sub-system prove to be of high importance for the success of the proposed concept. The speed-droop characteristic and reactive power capabilities of generators, as well as the voltage dependency of loads, have significant impact on the results.

The uncertainties in the approximation of sufficient rejected production, as well as the system impact by the rejected machines, may constitute a challenge during SIPS design in this context. The SIPS functionality and potential voltage and frequency stability problems should be appropriately tested through dynamic analysis.

Utilising data from a Wide Area Monitoring System, the proposed adaptation of the equal-area criterion provide promising applications. In this way, the situational awareness can be enhanced, thus improving the security level of system operation. Furthermore, the proposed concept can be used to increase the efficiency as well as proving the adequacy of existing System Integrity Protection Schemes.

ACKNOWLEDGMENT

The authors would like to thank Professor K. Uhlen and Adjunct professor G. Kjølle at the Norwegian University of Science and Technology for constructive discussions and comments.

REFERENCES

[1] CIGRE Working Group: C4.601,, *Review of the Current Status of Tools and Techniques for Risk-Based and Probabilistic Planning in Power Systems,* Technical Brochure: 434, 2010

[2] IEEE Task Force on: Blackout Experiences, Mitigation, and Role of New Technologies,, *Blackout Experiences and Lessons Best Practices for System Dynamic Performance, and the Role of New Technologies,* Special Publication: 07TP190, 2007

[3] Madani, V., Novosel, D., Horowitz, S., Adamiak, M., Amantegui, J., Karlsson, D., Imai, S., Apostolov, A., *IEEE PSRC Report on Global Industry Experiences With System Integrity Protection Schemes (SIPS),* IEEE Transactions on Power Delivery, 2010, Vol. 25, p. 2143-2155

[4] Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C., VanCutsem, T., Vittal, V., *Definition and classification of power system stability,* IEEE Transactions on Power Systems, 2004, Vol. 19, p. 1387-1401

[5] Xue, Y., Van Cutsem, T., Ribbens-Pavella, M., *Real-time analytic sensitivity method for transient security assessment and preventive control,* Generation, Transmission and Distribution, IEE Proceedings C, 1988, Vol. 135, p. 107-117

[6] Dong, Y., Pota, H.R., *Transient stability margin prediction using equal-area criterion,* Generation, Transmission and Distribution, IEE Proceedings C, 1993, Vol. 140, p. 96-104

[7] Haque, M.H., *Equal-area criterion: an extension for multimachine power systems,* Generation, Transmission and Distribution, IEE Proceedings, 1994, Vol. 141, p. 191-197

[8] Ernst, D., Pavella, M. *Closed-loop transient stability emergency control*, IEEE/PES Winter Meeting, 2000

[9] Ruiz-Vega, D., Pavella, M., *A comprehensive approach to transient stability control. I. Near optimal preventive control,* Power Systems, IEEE Transactions on, 2003, Vol. 18, p. 1446-1453

[10] Ruiz-Vega, D., Pavella, M., *A comprehensive approach to transient stability control. II. Open loop emergency control,* Power Systems, IEEE Transactions on, 2003, Vol. 18, p. 1454-1460

[11] Yi-qun, L., Lin, T., Wang-shun, L., Jian-fei, L. *The study on real-time transient stability emergency control in power system*, IEEE Canadian Conference on Electrical and Computer Engineering, 2002

[12] Glavic, M., Ernst, D., Ruiz-Vega, D., Wehenkel, L., Pavella, M. *E-SIME - A method for transient stability closed-loop emergency control: achievements and prospects*, Bulk Power System Dynamics and Control - VII, 2007

[13] Huan, X., Bao-Hui, Z., Hao, T.Z.G., Wang, C.G., Peng, L., Cheng, L.Y., You, M., Bo, Z.Q., Klimek, A. *Study on closed-loop transient stability emergency control based on Wide Area Measurement*, IEEE/PES Transmission and Distribution Conference and Exposition: Latin America, 2008

[14] Reliability Test System Task Force, *The IEEE reliability test system - 1996,* IEEE Transactions on Power Systems, Vol. 14, No.3, 1999

[15] Johansson, E., Uhlen, K., Kjølle, G., Toftevaag, T. *Reliability evaluation of wide area monitoring applications and extreme contingencies*, 17th Power Systems Computation Conference, 2011, Stockholm, Sweden

[16] Chenine, M., Karam, E., Nordström, L. *Modeling and simulation of wide area monitoring and control systems in IP-based networks*, IEEE/PES General Meeting, 2009

Paper VI:

***The change of power system response after successive** faults*

Lamponen, J., Hillberg, E., Haarla, L., Hirvonen, R.

VI

Proceedings of the 18th Power Systems Computation Conference, 2014, Wroclaw, Poland
PSCC 2014
ISBN 978-83-935801-2-5

The Change of Power System Response after Successive Faults

Jarno Lamponen
Aalto University
Helsinki, Finland
jarno.lamponen@aalto.fi

Emil Hillberg
NTNU
Trondheim, Norway
emil.hilberg@ntnu.no

Liisa Haarla
Aalto University
Helsinki, Finland

Ritva Hirvonen
Fingrid Oyj
Helsinki, Finland

***Abstract*— This paper illustrates the usefulness of visualizing the secure operating domains and the value of dynamic analyses when considering the vulnerability of a power system. The paper includes studies of the secure power transfer limits and vulnerabilities of the IEEE Reliability Test System (RTS). The limits and vulnerabilities are determined by simulating the dynamic response of single and multiple faults. The results are presented by visualizing the secure transfer domains as a function of the power flow on critical transfer corridors. The paper also provides an estimate for the frequency of blackouts related to the different operating domains. The results show how the vulnerability of the power system increases in steps as the amount of power transfer over a corridor increases.**

Keywords—Vulnerability, security, stability, multiple contingencies

I. INTRODUCTION

Ensuring secure operation of a power system by identifying and mitigating vulnerabilities has been the topic for many rigorous studies. Several studies concentrate on a specific phenomenon that may jeopardize the security, such as cascading failures [1]–[4] or protective device failures [5]–[8]. Focusing on a specific phenomenon reveals vulnerabilities connected to the studied phenomenon but does not necessarily discover or value the vulnerabilities of other phenomena. Visualizing techniques such as nomograms have been used to describe $N-1$ security of a system [9], [10]. $N-1$ nomograms can give essential information to the system operator on the operating boundaries of normal operation. In general, multiple contingencies are not considered, thus failing to reveal the vulnerabilities beyond the normal operation conditions.

In [15] and [16], blackout phenomenon are described as a process with separate phases. In [15], these phases are suggested to be separated by distinctive transitions and are defined as: a *thermally governed phase* and an *unstable phase*. The work in [15] underlines the importance of analyzing multiple contingencies when assessing a power systems vulnerability to large disturbances. This paper continues the work presented in [15], where large European blackouts are analyzed and the importance of assessing the vulnerabilities related to dynamic instability is highlighted.

This paper presents a systematic analysis of the IEEE Three Area Reliability Test System 1996 (RTS) and quantifies vulnerabilities related to dynamic instability. The paper identifies the secure operating domains and critical vulnerabilities of the RTS by simulating the dynamical response of the system to faults. Phenomena defining the secure power transfer are described for different operating scenarios.

Two-dimensional nomograms of multilevel contingencies are used together with deterministic and probabilistic quantifications in order to illustrate the difference in vulnerability for various operational scenarios. Further development of the use of nomograms is presented in this paper, where vulnerability domains are identified based on the calculation of the system collapse frequency.

The paper is organized as follows: A short presentation of the RTS is included in Part II. Part III presents and visualizes the secure operating domains of the RTS. Part IV describes the vulnerability of the RTS deterministically and probabilistically. Part V describes the possibilities of mitigating blackouts. Part VI includes the discussion and conclusions.

II. IEEE RELIABILITY TEST SYSTEM 1996 (RTS)

To obtain a more realistic dynamic response of the RTS model than the original described in [11], detailed dynamic models are used to represent the synchronous generators, turbine-governors, and excitation system, as proposed by [12].

Further improvements on the RTS dynamic response have been made after the studies presented in this paper. These improvements may be found in [17], and are focusing on the voltage stability impact from load response and excitation system limiters.

A single-line diagram of the RTS is presented in Fig. 1. The optional HVDC connection as well as the control of the phase-shifting transformer, both connected between areas A and C, have been neglected in this study. Using HVDC or a phase-

Paper submitted to Power Systems Computation Conference, August 18-22, 2014, Wroclaw, Poland, organized by Power Systems Computation Conference and Wroclaw University of Technology.

shifter control could significantly improve the reliability of the system, as the power flows in the system could be better controlled in case of disturbances.

In several previous studies, the RTS has been used for analyzing the reliability limited to the (post-fault) adequacy rather than dynamic security of the power system. In this study, the added dynamic models have enabled the analysis of dynamic phenomena related to faults, i.e. the security. The dynamic analyses reveal the vulnerabilities that have remained hidden in the studies based merely on steady state power flow analyses.

III. THE SECURE OPERATING DOMAIN

The first part of this section describes a dynamic $N-1$ contingency analysis of the RTS, with a secure operating domain identified and visualized from these results. The second part describes the $N-k$ security of the RTS, and visualizes an $N-2$ secure operating domain of the system. These studies are based on analyses on approximately 50 different operating scenarios. It should be noted that an infinite number of operating scenarios are possible, thus this study only covers a part of the total operational space and can only identify the vulnerabilities of the studied scenarios.

A. N − 1 security assessment

A dynamic $N-1$ contingency analysis with generator trips and line faults was performed on the RTS. The studied line faults were three-phase faults with 100 ms duration, followed by a permanent trip of the faulted line. Line fault locations were near the line ends. The total number of studied contingencies was approximately 300. The list of contingencies together with the selected operating scenarios results in an $N-1$ contingency analysis based on around 15000 dynamic simulations. Based on this $N-1$ contingency analysis, the stability of the transition from the pre-fault state to the post-fault state, as well as the adequacy (line loading and voltage levels) of the post-fault steady state were assessed.

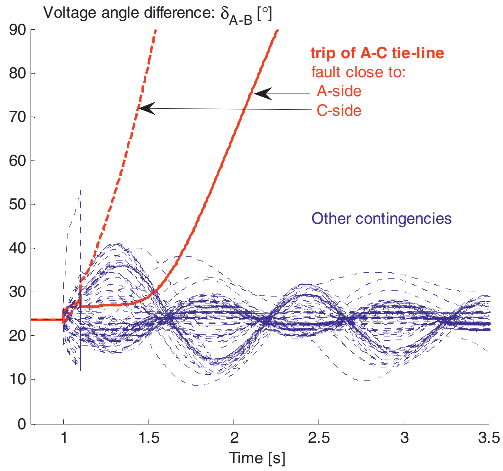

Fig. 2. Angle difference over the line connecting areas B and C for all single line faults (with subsequent line tripping) of operating scenario X (see Table I and Fig. 3). Blue curves correspond to faults resulting in stable operation, while the fault and trip of the line connecting area A and area C result in an unstable system (red curves).

The angle differences over the line connecting area B and area C (the BLOCH–CLARK line) are presented in Fig. 2 for all studied line faults in operating scenario X. Details of this high transfer scenario are presented in Table I and in Fig. 3. The bold red curves in Fig. 2 show the instability of the studied system after the trip of the line from area A to area C (the ATTLEE–CURTISS line), when the fault occurred near either line end. This contingency is therefore considered as a critical contingency for scenario X.

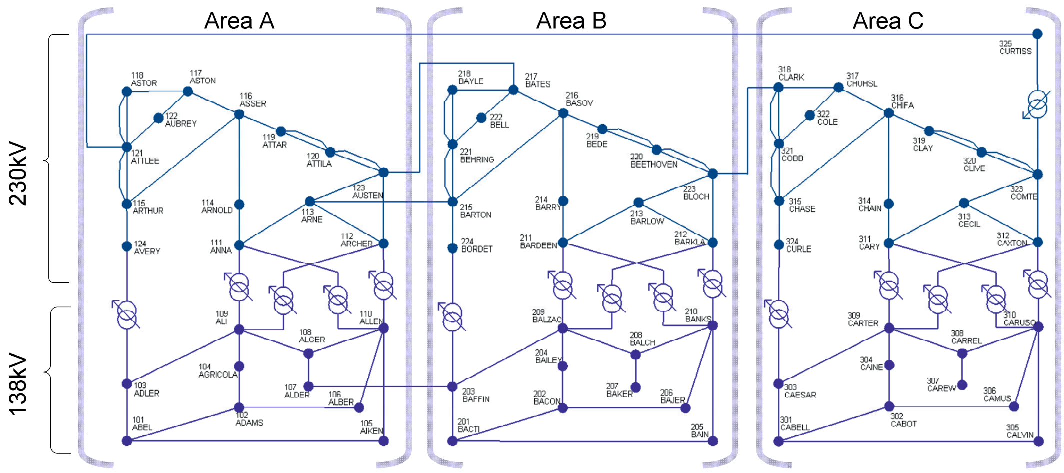

Fig. 1. Single-line diagram describing the IEEE Reliability Test System 1996 [11]. The dimensions do not reflect the line lengths.

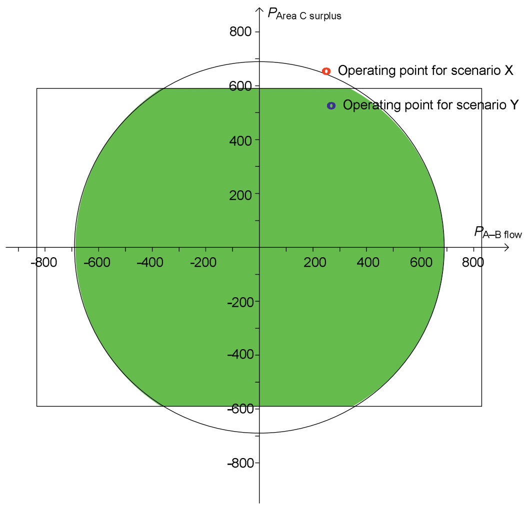

Fig. 3. $N-1$ secure operating domain for the RTS (green area). The rectangle domain represents the thermal rating of the lines while the circle domain represents angle stability limitations. The operating point of two of the studied scenarios, X and Y, are illustrated by a red and a blue ring, respectively.

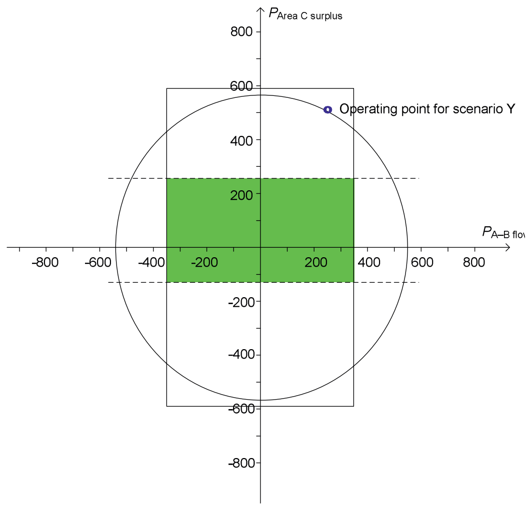

Fig. 4. $N-2$ secure operating domain (green area) for the RTS. The rectangle domain represents thermal long term emergency rating of the lines and the circle domain represents angle stability limitations. The dotted lines represent frequency stability limits, which ensure a successful islanding in the case of the two lines connecting area C are disconnected.

TABLE I
Inter-area power exchange of studied operating scenarios X and Y.

	Case X	Case Y
Power flow from area A to B(MW)	220	255
Power flow from area A to C (MW)	-240	-150
Power flow from area B to C (MW)	420	365
Area A Power export (MW)	15	-105
Area B Power export (MW)	-640	-620
Area C Power export (MW)	655	515

B. The N − 1 security operating domain

For the RTS, it is possible to identify critical transfer corridors directly from the system topology due to the weak connections between the three meshed areas. These transfer corridors can be used to visualize the secure operating domains of the system. In case of a multi-corridor system, such as the RTS, this would imply a multi-dimensional space. However, here we use more comprehensible two-dimensional illustrations for visualizing the secure operating domains. In this paper, two corridors connecting area C to the other areas are combined to form one dimension 'area C surplus' while the other dimension is the power flow on the corridor between areas A and B.

By using the two-dimensional space of 'power flow A–B' and 'area C surplus', the thermal limitations of the secure operating domain are presented as a rectangle in Fig. 3. Long term emergency ratings defined in [11] were used as thermal limits for the lines. The circle in Fig. 3 represents the limitations induced by transient stability and defined by the dynamic studies of line faults and generator trips in different power flow cases. Inside this circle, no transient instability cases were identified among the studied scenarios.

In Fig. 3, operating scenarios may be identified where a single fault leads to unstable operation even though the thermal limits are not exceeded in the post fault state (i.e. the domain inside the rectangle but outside the circle). Thus, $N-1$ secure operating domain for the RTS would not have been defined correctly without the stability assessments.

C. The N−k secure operating domain

The most critical contingencies identified in the $N-1$ contingency analysis are the faults and trips of lines in the transfer corridors between areas A, B, and C. These contingencies were selected as the first contingency in an $N-2$ contingency analysis. Thus, the $N-2$ contingency analysis comprise of approximately 15000 dynamic simulations.

Fig. 4 presents the $N-2$ secure transmission limits for two successive line faults. A line disconnection significantly reduces the thermal limits between areas A and B compared with the $N-1$ limits of the intact grid. The reason for this is that there are two 230 kV lines and one 138 kV connecting areas A and B. If one 230 kV line is disconnected, there is still one 230 kV line and one 138 kV line, and the thermal $N-1$ limit between the area A and B is roughly equal to the power that these lines can carry together (the alternative long path via area C does not carry significant amount of power). However, if two 230 kV lines are disconnected, there is only one 138 kV line between the areas in addition to the longer transfer path via area C. Now a relatively larger share of the power will flow via area C in the $N-2$ case compared with the $N-1$ case. The overall impact of this path on the transfer capacity between areas A and B is small due to the high impedance. Therefore, the difference between the thermal $N-1$ limit, shown in Fig. 3, and the $N-2$ limit, shown in Fig. 4, is roughly the thermal capacity of one 230 kV line connecting areas A and B.

The disconnection of any single line in the transfer corridors between areas A, B, and C has a smaller effect on transient angle stability limits than on thermal limits because the disconnection of any of these lines does not significantly affect the operating state of the generators (if the operating scenario is within the secure operating domain). However, line disconnections weaken the ability of the grid to absorb the kinetic energy from the generators, which explains the reduction from the transient angle $N-1$ limit to the $N-2$ limit.

When considering stable power transfers between areas A and B, the most critical combination of the successive $N-2$ line faults was the trip of both 230 kV lines connecting areas A and B. The same $N-2$ fault combination also dominates the reduction in the thermal limits.

The main difference between the thermal and stability limitations are that the thermal limits do not depend on the order of occurrence of the faults, whereas for stability, the order of the fault sequence and also the time interval between the faults are significant. The consequences can be completely different depending if the transient from the previous fault has stabilized or not when a second fault occurs. In this study, the system was assumed to have reached a steady state between subsequent faults. The most critical order of the faults was the following: first a fault and trip of ARNE–BARTON line (a 230 kV line from area A to area B) followed by a line fault near bus AUSTEN in area A and the trip of the other 230 kV line between area A and area B: AUSTEN–BATES line.

When considering the power surplus and deficit of area C, the most restricting set of successive $N-2$ line contingencies is the disconnection of both lines connecting area C to other areas. This will isolate area C, and successful islanding requires that the available reserve power cover the power deficit in each isolated area. Furthermore, island operation also requires suitable power and frequency controls.

Assuming that the frequency controlled instantly activated reserves equal 400 MW (the largest unit in the system) divided evenly between the areas (in each area the largest unit has the same size), results in 133 MW reserves in each area. Thus, the power deficit of area C in the initial operating scenario cannot exceed 133 MW to ensure successful islanding. Similarly, the power surplus of area C cannot exceed 266 MW to ensure that areas A and B have the required reserve power. In Fig. 4, the dotted lines represent these frequency stability limits. The rectangular thermal $N-1$ and $N-2$ limits, illustrated in Fig. 3 and Fig. 4 respectively, are equal in 'C surplus' dimension because if both lines connecting area C to other areas are tripped, there remain no lines that could be overloaded.

D. Change in system response

If the operating scenario is not within a secure operating domain, and a fault occurs, the consequences are significantly different if the thermal limits of the lines are exceeded or the stability of the system is jeopardized.

As described in the previous sections, when determining the secure power transfer limits, the limit is the one that is the lowest: either the thermal current carrying capacity of the lines

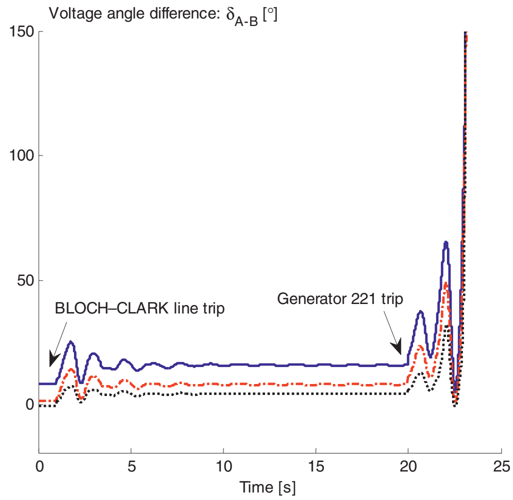

Fig. 5. Results from $N-2$ contingency analysis for scenario Y, showing voltage angles over the three tie-lines forming the corridor between areas A and B. The system reaches a stable state after the first contingency (a short circuit followed by the trip of line BLOCH–CLARK at $t = 1$ s) but is not able to regain stability after the trip of generator 221 at $t = 20$ s.

after a fault, the ability of the generators to maintain the synchronism, or stable voltages during and after a fault transient.

In the case with thermal limitations, overloading may eventually lead to protective actions that disconnect the overloaded component. Depending on the protection scheme and the level of overload, the protection may act in a few seconds or after several minutes. This protective action may lead to the increased loading of parallel components, leading to further protective actions in a (often rather slow) cascade. This part of a blackout process may be referred to a *thermally governed phase* [15]. If the cascade continues, at some stage it will lead to instability.

If stability limitations are exceeded, the system enters an unstable and uncontrollable state, referred to as the *unstable phase* of the blackout process [15]. This phase is characterized by one or several of the following dynamic phenomena: oscillations of voltage, power, or frequency, or the decay (or rise) in voltage or frequency. Such phenomena often lead to the triggering of several component protections, where the affected area of the power system is difficult to anticipate.

The consequences after exceeding stability limitations are usually faster and more wide-spread and therefore more severe than the consequences of exceeding thermal limits. Therefore, it is crucial to know not only of the actual security limits of the system, but the response of the system and the phenomenon that is limiting the system at different operating scenarios. For a system, originally limited by the thermal capacity of the lines, the loss of stability after it has faced several contingencies, corresponds to a change of the system response.

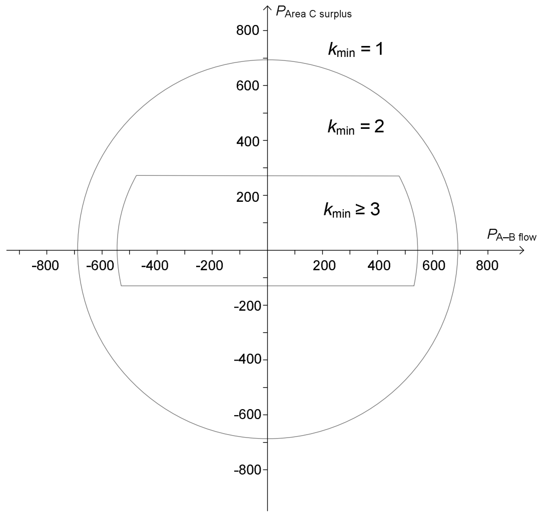

Fig. 6. Quantification of system vulnerability using the $k_{\min}$ indicator. which describes the minimal number of contingencies after which the instability occurs.

Scenario Y in Fig. 3 and Fig. 4 exemplifies the change in the system response. This operating scenario is $N-1$ secure as shown in Fig. 3, but not $N-2$ secure as shown in Fig. 4. For scenario Y, the $N-1$ secure power transfer between area C and the rest of the system is thermally limited. Considering multiple contingencies however, the system can become instable after only two subsequent faults. Two successive faults can cause instability for scenario Y, for example the trip of the largest generator in area B (connected to bus 221, BEHRING) and the fault and trip of BLOCH–CLARK line (the only line between areas B and C). Regardless of the order of the contingencies, the system cannot maintain a stable operation after the second contingency, as Fig. 5 shows. This example describes the value of performing dynamic $N-k$ contingency analyses, and not limiting to $N-1$ analyses.

IV. SYSTEM VULNERABILITY

This section describes different aspects of system vulnerability. The first two parts examine the vulnerability of the RTS using a deterministic and probabilistic method while the last part discusses the consequences of protection system failures.

A. Deterministic indication of vulnerability

The vulnerability of a given operating scenario can be assessed deterministically by studying the combinations of contingencies that cause system wide consequences. The vulnerability of the system can thus be assessed using the indicator, $k_{\min}$, defined in [15] as:

$$k_{\min} = \min\,(s_1, s_2, \dots, s_n), \tag{1}$$

where s_i is a set of contingencies leading to an unstable state at the specific operating scenario. The indicator describes the minimal number of contingencies after which instability occurs. Fig. 6 illustrates the vulnerability level quantified by the $k_{\min}$ indicator for the RTS, where $k_{\min} \geq 3$ indicates that the stability of the system is not threatened by any of the studied double contingencies.

In the studied $N-1$ and $N-2$ contingencies, the fault sequences leading to system collapse consist of faults on the lines on the transfer corridors between areas A, B, and C as well as generator trips.

B. System collapse frequency as probabilistic indication of vulnerability

The frequency of a system collapse can be assessed by identifying the specific chains of events leading to the collapse. For a given operating scenario o_i the frequency of a system collapse F^{o_i} that takes into account $N-1$, $N-2$ and $N-3$ contingency sets can be calculated as follows

$$F^{o_i} = \textstyle\sum_{N-1} f_l^{o_i} + \sum_{N-2} f_m^{o_i} p_n^{o_i} + \sum_{N-3} f_r^{o_i} p_s^{o_i} p_t^{o_i}, \tag{2}$$

where $f_{l,m,r}^{o_i}$ is the frequency of the occurrence of a fault in contingency set $N-k$. $p_{n,s,t}^{o_i}$ is the conditional probability that an additional fault occurs before mitigating actions have been performed. The term with a minimum number of faults that lead to a collapse dominates in (2) and thus gives an estimation of the system collapse frequency. Therefore, the $N-2$ and other higher-order events, which consist of a two or more successive independent contingencies, have less effect on the system collapse frequency than the lower order events.

For the RTS, different domains of vulnerability caused by consecutive line faults are presented in Fig. 7. An estimation of the system collapse frequency is determined for every vulnerability domain (1–8 in Fig. 7) by summing the frequencies of the critical events. The critical events are chains of events that may consist of faults that cause instantaneous instability but also faults that lead to instability by causing overloading and a fault of another line. Table II presents the estimated system collapse frequencies.

When estimating the system collapse frequency, it is assumed that mitigating actions to reduce power transfer in time, in case of line overloads, fail with the probability of 1 %, which causes a new line fault. The outage data of [11] is used for estimating the frequency of $N-2$ contingencies.

The first fault has the frequency of 'permanent outage' in [11] and the frequency of the second fault is the sum of permanent and transient outages in [11]. In the dynamic simulations, all the line faults were three-phase faults.

TABLE II
The estimation of the RTS system collapse frequency caused by consecutive line faults. The descriptions for the domains are presented in Fig. 7.

Domain	Restricting fault (set) and phenomenon		Estimation of system collapse frequency [1/year]
	Line faults that cause instability	Line faults that cause thermal overloading	
1	113–215 or 123–217 or 121–325 or 223–318		>1
2	121–325 and 223-318	121–325 or 223-318	1.38E-2
3	113–215 and 123–217 or 121–325 and 223–318		5.03E-3
4	121–325 and 223–318	113–215 and 123–217	2.99E-3
5	121–325 and 223–318		2.97E-3
6	113–215 and 123–217		2.06E-3
7		113–215 and 123–217	2.06E-5
8			<2.06E-5

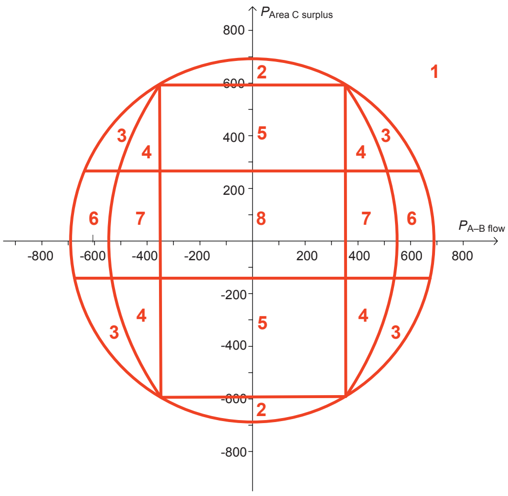

Fig. 7. Vulnerability domains of the RTS caused by consecutive line faults.

1. Outside of $N-1$ stability limits
2. $N-1$ stable, outside of $N-2$ frequency stability limits and $N-1$ thermal long term emergency ratings
3. $N-1$ secure, outside of $N-2$ stability limits (and $N-2$ thermal long term emergency ratings)
4. $N-1$ secure, outside of $N-2$ frequency stability limits and $N-2$ thermal long term emergency ratings
5. $N-1$ secure, outside of $N-2$ frequency stability limits
6. $N-1$ secure, outside of $N-2$ angle stability limits (and $N-2$ thermal long term emergency ratings)
7. $N-2$ stable and $N-1$ secure, outside of $N-2$ thermal long term emergency ratings
8. $N-2$ secure

The system collapse frequency as a function of power surplus in area C when power transfer from area A to area B is 0 MW is presented in Fig. 8. Thus, the system collapse frequency illustrated in Fig. 8 corresponds to a move along the Y-axis in Fig. 7 from the $N-2$ secure domain to the unsecure domain. In Fig. 8, the vulnerability increases in steps when the power flow exceeds certain limits. The steps are caused by the

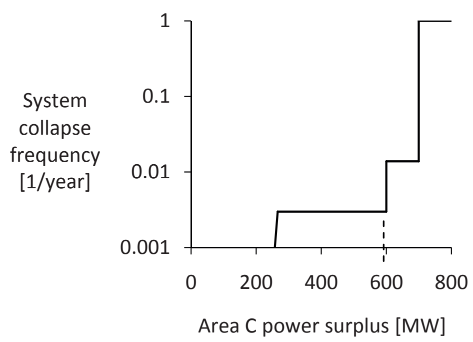

Fig. 8. The estimation of the RTS system collapse frequency [1/year] as a function of the area C power surplus. The power transfer from area A to B is 0 MW. The dotted line represents the $N-1$ secure transfer limit.

drastic increase in the number of single and multiple faults leading to undesired system consequences, which occur when the power flow exceeds the identified limits. The steps correspond to the border lines between the vulnerability domains in Fig. 7.

The faults and fault combinations occur with a certain probability on a given time period and are independent of the power flow. The increment of the system collapse frequency is especially significant when the power flow exceeds the $N-1$ secure level.

C. Impact of protection system and circuit breaker failures

Failures of protection systems have been identified to have significant impact on events leading to a system collapse [6]. Protective device misoperations may aggravate the consequences of disturbances by leading to further disconnections or even transform the system directly to an unstable operating state. The failure of the circuit breakers or main protective relays to separate the faulty component of the system leads to further disconnections by the back-up protection or by the breaker failure relay. More importantly, it always extends the fault duration, which may lead to generators falling out-of-step and thus initiate a process leading to system

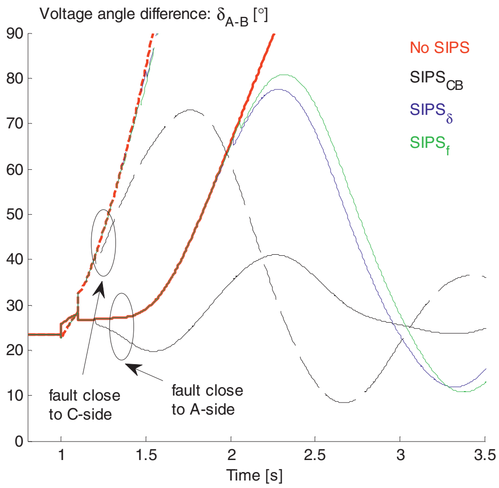

Fig. 9. Results from the SIPS study of operating scenario X, showing the angle difference over the corridor between areas B and C. The results describe the effect of different SIPS solutions for the critical fault, i.e. a short circuit located close to either side of the ATTLEE–CURTISS line followed by the trip of the line.

collapse. As the protection system and circuit breaker failures often lead to severe consequences, characterized by a significant dynamical response of the system, it is necessary to analyze this response to identify the vulnerabilities related to protection system or circuit breaker failures.

Since a stuck circuit breaker during a line fault should also be regarded as an $N-2$ fault, additional simulations have been performed to analyse the system impact of such failures. Here, bus fault simulations were made for every bus in the RTS. The fault duration was selected to 250 ms, reflecting a fault sequence with a line fault, having a stuck circuit breaker at one line end and the clearing of the fault by the breaker failure protection. Simulations were done for all previously studied operational scenarios, resulting in an additional 3500 dynamic simulations. In contrast to the successive line faults, which resulted in instability for some operating scenarios, a 250 ms fault at buses located near large generators resulted in transient instability of all the studied operating scenarios. Therefore, for the RTS, a stuck circuit breaker during a line fault can be regarded as the most critical $N-2$ fault.

V. MITIGATION OF LARGE DISTURBANCES

It is possible to implement remedial actions to prevent wide spread consequences caused by critical contingencies. To ensure that the system remains at a secure operating point, the TSO can use several preventive actions such as change the power flows of AC lines by controlling HVDC links, using phase-shifting transformers, or re-dispatching of power generation. If a critical contingency occurs when the system is not in a secure state, mitigating actions can be used to prevent a blackout. To prevent transient instability, the response of such actions might be required within fractions of a second after the undesired event has occurred; hence, only automatic actions are possible to prevent instability.

One solution to mitigate blackouts is the implementation of system integrity protection schemes (SIPS), which are, in contrast to common component protection, designed to preserve the power system integrity during abnormal conditions. A possible classification of SIPS is on the type of activation signal, which can be either event-based (detecting of predefined events, such as breaker tripping signals) or response-based (measuring electrical parameters, e.g. frequency or voltage).

Three SIPS solutions have been studied with the RTS, utilizing different activation signals:

- $SIPS_{CB}$: activated by status signals from circuit breakers
- $SIPS_{\delta}$: activated by voltage angle measurements
- $SIPS_{f}$: activated by frequency measurements

The results for the critical contingency of operating scenario X, shown in Fig. 9, illustrate the possibilities to prevent the system from becoming unstable. Here, an internal arming of the response-based SIPS is used together with a time delay to prevent unwanted action during switching events. Based on a dynamic contingency analysis described in [13], arming and activation signal magnitudes have been selected as:

$\Delta\delta_{BC}$ - arming: 40° for 200ms, activation: 50°.
Δf_{BC} - arming: 0.2Hz for 200ms, activation: 0.25Hz.

The total delay between measurement and the implementation of mitigating action is assumed to be no longer than 100 ms.

Depending on the fault location, the transient behavior of the system sets different requirements on the response time of the SIPS solution. Such is also the case with different fault types and fault durations, meaning that the SIPS may not prevent instability in all scenarios.

The response-based solutions, $SIPS_{\delta}$ and $SIPS_{f}$, are not as fast as the event-based, $SIPS_{CB}$. The event-base SIPS will efficiently and fast provide the actions foreseen as sufficient to prevent the transient instability. However, since the trigger signal of the $SIPS_{CB}$ is based on the triggering of specific protections, the system is not protected against unforeseen events. The response-based SIPS will be able to provide increased protection against multiple or unforeseen contingencies, but might need longer response time depending on how the SIPS are designed.

VI. DISCUSSION AND CONCLUSIONS

When performing a comprehensive vulnerability analysis, also post fault dynamics should be included. Studies based on steady state analyses can erroneously indicate “secure” operation outside the $N-1$ stable domain, as the domain outside the circle but inside the rectangle in Fig. 3 clearly illustrates. It should also be noted that, when stability is an issue, an *outage* is not the only concept that should be analyzed since it is the *fault* that accelerates the generators.

Furthermore, a line trip may weaken the system and lead to cascading disconnections due to instability. Thus, studies where dynamics are ignored may provide too optimistic results since they do not reveal vulnerabilities connected to instability. In our case study, the instability occurred inside the steady state (thermal) limits, a result that cannot be reached with steady state analyses only. In some cases, it may be possible to provide angle stability limits using simplified models as [14] shows.

A proper identification of power system vulnerabilities requires knowledge of the dynamic behavior of the system in disturbed conditions and awareness of a possible change in the system response after several faults. Therefore, dynamic $N-2$ or even higher-order contingency analyses should be used in power system vulnerability assessments. As the vulnerabilities are identified, mitigating actions can be planned and implemented.

It is shown in this paper that the vulnerability of the power system may increase in distinct steps as the amount of power transfer is increased over the critical corridors. Thus, increasing power transfer above certain limits may drastically increase the number of faults or fault combinations with undesired consequences.

For the system operator, the identification of the secure operating conditions is essential, and nomograms may support identification of vulnerabilities of the system at different operating conditions. Nomograms can provide information of the existing restrictions on the secure transfer capacity as well as the margin to the security limits in an illustrative manner. In this paper two-dimensional illustrations are favored over multidimensional when visualizing the secure operating domain, this is done since two-dimensional illustrations are usually more comprehensible to the observer. The illustrations in this paper are based on the power transfer over critical corridors of the RTS system. For other systems, it may be more feasible to select other parameters, e.g. the demand in certain areas, as limiting factors. The presented visualizations of operating domains for the RTS are symmetrical in relation to power transfer, due to the symmetrical topology of the RTS.

If the circuit breakers or main protective relays fail to disconnect the faulted component from the grid, the fault duration extends and several components are tripped by the breaker failure relays or by the back-up protection. This type of faults should be considered as multiple contingencies and must be included when assessing the risk of system collapse. Simulations made on the RTS system underlines the importance of considering this type of faults since the extended fault duration near critical generators significantly increases the risk of large disturbances, even in operating scenarios with a lightly loaded grid.

Simulation results presented in this paper highlight the value of dynamic analyses, and illustrate that analyses based on steady-state studies (load flow) may overestimate the security of the system as they cannot reveal the vulnerabilities related to the dynamic response of the system. Therefore, dynamic analyses should be considered imperative in security and vulnerability assessment studies.

REFERENCES

[1] H. Ren, I. Dobson, and B. A. Carreras, “Long-term effect of the n-1 criterion on cascading line outages in an evolving power transmission grid,” IEEE Trans. Power Systems, vol. 23, no. 3, pp. 1217–1225. August 2008.

[2] J. Chena, J. S. Thorp, I. Dobson, “Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model,” International Journal of Electrical Power & Energy Systems, Volume 27, Issue 4, May 2005, Pages 318–326.

[3] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, V. E. Lynch, “Criticality in a cascading failure blackout model,” International Journal of Electrical Power & Energy Systems, Volume 28, Issue 9, November 2006, Pages 627–633.

[4] L. Chang, Z. Wub, “Performance and reliability of electrical power grids under cascading failures,” International Journal of Electrical Power & Energy Systems, Volume 33, Issue 8, October 2011, Pages 1410–1419

[5] X. Yu, C. Singh, “A practical approach for integrated power system vulnerability analysis with protection failures,” IEEE Trans. Power Systems, vol. 19, no. 4, pp. 1811–1820. November 2004.

[6] S. Tamronglak, S. E Horowitz, A. G. Phadke, J. S. Thorp, “Anatomy of power system blackouts: preventive relaying strategies,” IEEE Trans. Power Delivery, vol. 11, no. 2, pp. 708–714. August 1996.

[7] J.S. Thorp, A.G. Phadke, S.H. Horowitz, S. Tamronglak, “Anatomy of power system disturbances: importance sampling,” International Journal of Electrical Power & Energy Systems Volume 20, Issue 2, February 1998, Pages 147–152

[8] D. S. Kirschen, D. P. Nedic, “Consideration of hidden failures in security analysis,” in Proc. 14th Power Systems Computation Conference (PSCC’02), 2002

[9] K. Morison, L. Wang, P. Kundur, “Power system security assessment,” Power and Energy Magazine, IEEE, Issue Date: Sept.-Oct. 2004 Volume 2, Issue 5, Pages 30 - 39.

[10] H. Sarmiento, G. Pampin, R. Barajas, R. Castellanos, G. Villa, M. Mirabal, “Nomograms for assistance in voltage security visualization,” Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES. Pages 1–6.

[11] C. Grigg, P.Wong, P. Albrecht, R. Allan, M. Bhavaraju, R Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour. C. Singh, “The IEEE Reliability Test System-1996. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee,” IEEE Trans. Power Systems, vol. 14, no. 3, pp. 1010–1020. August 1999.

[12] E. Johansson, K. Uhlen, G. Kjølle, T. Toftevaag, “Reliability evaluation of wide area monitoring applications and extreme contingencies“, in Proc. 17th Power Systems Computation Conference (PSCC'11), 2011

[13] E. Hillberg, F. Trengereid, Ø. Breidablik, K. Uhlen, G. Kjølle, S. Løvlund, J.O. Gjerde, “System Integrity Protection Schemes – Increasing operational security and system capacity”, in Proc. 44th CIGRE Session, 2012

[14] I. Hübl, R Robert Schmaranz, H. Renner, “Active power instability in a 110 kV network”, (In German:Wirkleistungsinstabilität in einem 110-kV-Netz). A Tutorial in protection and automation systems. March 20–21 2007, Dortmund, Germany organised by Energietechnische gesellschaft im VDE.

[15] E. Hillberg, J. Lamponen, L. Haarla, R. Hirvonen, “Revealing stability limitations in power system vulnerability analysis”, in Proc. 8th Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, 2012

[16] P. Henneaux, F. Faghihi, P-E. Labeau, J-C. Maun, L. Haarla, “Two-level blackout probabilistic risk analysis: application to a test system”, in Proc. 22nd European Safety and Reliability (ESREL 2013), 2013

[17] V. Storvann, E. Hillberg, K. Uhlen, “Indicating and Mitigating Voltage Collapse”, in Proc. IEEE/PES Innovative Smart Grid Technologies, 2012

Johansson, E., Uhlen, K., Nybø, A., Kjølle, G., Gjerde, O.
Extraordinary events: understanding sequence, causes, and remedies
European Safety & Reliability Conference, 2010, Rhodes, Greece

I

Johansson, E., Uhlen, K., Kjølle, G., Toftevaag, T.
Reliability evaluation of wide area monitoring applications and extreme contingencies
17th Power Systems Computation Conference, 2011, Stockholm, Sweden

II

Hillberg, E., Trengereid, F., Breidablik, Ø., Uhlen, K., Kjølle, G., Løvlund, S., Gjerde, J.O.
System integrity protection schemes – increasing operational security and system capacity
44th CIGRE Session, 2012, Paris, France

III

Hillberg, E., Lamponen, J., Haarla, L., Hirvonen, R.
Revealing stability limitations in power system vulnerability analysis
8th Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, 2012, Cagliari, Italy

IV

Hillberg, E., Toftevaag, T.
Equal area criterion applied on power transfer corridors
5th IASTED Asian Conference on Power and Energy Systems, 2012, Phuket, Thailand

V

Lamponen, J., Hillberg, E., Haarla, L., Hirvonen, R.
The change of power system response after successive faults
18th Power Systems Computation Conference, 2014, Wroclaw, Poland

VI

Perception, Prediction and Prevention of Extraordinary Events in the Power System

Emil Hillberg