Portuguese Transmission Grid Incidents Risk Assessment

By

Susana Alexandra Barros de Almeida
M.Sc. in Power Systems

A thesis submitted to the
University of Porto
Faculdade de Engenharia
For the degree of
Doctor of Philosophy

February 2010

Thesis under the scientific orientation of
Professor Doutor Fernando Maciel Barbosa

To Roald
To my mother

"Imagination is more important than knowledge"
Albert Einstein (1879 – 1955)

ACKNOWLEDGMENTS

Now, that I have reached the end of this research work, I want to express my gratitude to everyone that was by my side and have contributed to it.

First, I would like to thank to my supervision team. To Professor Doutor Maciel Barbosa, my eternal gratitude for the friendship, the understanding, the wise advices and guidance, the total availability to help, the encouragement and the trust in me. To Rui Pestana, who willingly discussed all my doubts, thanks for the active contributions, the supervision on REN's side and for believing in this project from the beginning to the end.

I would like to thank my friend, Nélio Machado, for the support, the technical brainstorming, the many hours invested in this project by my side, helping me with the automation of online forest fires information and with the implementation of contingency and cascading analysis. I wish I can do the same for you very soon.

I am very grateful to Albertino Meneses and Albino Marques for their support, their confidence in me, their suggestions and many advices. They have contributed significantly to this work with their vast knowledge and experience, improving it a lot. Thanks to both for your friendship and special thanks to Albertino Meneses for the language revision.

I would like to express my gratitude to Christiaan Engelbrecht for his precious guidance and support, helping me with the method for the prediction of faults caused by lightning. Thanks for being part of this work, it became a lot better.

I am grateful to my colleagues that helped me in an enthusiastic way with the big challenge of collecting data. To Nuno Ribeiro, thanks for the patience and for the effort in providing me the data that I so desperately needed. I want to thank the collaboration of the two persons in Line Maintenance department that helped me most, namely José Figueiredo and João Guincho. I would extend my gratitude to João Emanuel Afonso and to António Marques, for their constructive comments and statistical data on the protection system's domain. I also thank José Amarante dos Santos for his support and Ricardo Vasco Fernandes for the help organizing some of the information. In addition, I would like to express my appreciation to Medeiros Pinto for his friendship and support. Thanks to the rest of the colleagues that in some way gave their contribution.

I would like to thank José Penedos and Henrique Gomes for the first step of this work, making it possible inside the Portuguese TSO. This was a great opportunity for applying scientific knowledge in practice.

Finally, warm thanks to Roald, my love, for his unconditional support in every moment, helping me in finding my way back when I was feeling lost and, of course, with MatLab.

ABSTRACT

The increasing competitiveness of the power systems' environment has created new challenges to the power system security assessment, demanding the development of new methodologies. The unbundling of generation, transmission and distribution, caused by regulatory changes, the increased environmental concerns, making it more difficult to build new assets, and the strong incentives to the generation from renewable energy sources have created more vulnerable networks and a more complex security assessment in operations environment. The electricity market also presents more unpredictable and less stable power flows and a market-driven generation pattern more unpredictable and less controllable as well. Therefore, control room operators are frequently faced with difficult situations caused by stressed system operating conditions while their permanent goal is to keep the system secure, fulfilling all the established security criteria.

The use of methodologies that take advantage of the actual real-time conditions in combination with past knowledge, using probabilistic methods, is extremely interesting in the system operation environment, because it gives a more accurate overview to the control room operators. This thesis proposes a risk assessment methodology with a probabilistic analysis, considering different probabilities related to different contingencies. The developed methodology provides control room operators with risk indices for the next period, which take into account probability and severity, allowing them to react in advance and to be aware of inherent risks, preventing harmful situations. Single and common cause double contingencies were considered in the risk analysis.

The methodology developed in this thesis takes into account the effect of frequency of faults, local conditions, such as physical network, environmental, geographical and geological characteristics, and current conditions, such as adverse weather, e.g. lightning occurrence, and risk of or active forest fires, or their forecasts. It considers the fault historical data from 2001 until the end of 2009. A concept of short-term failure rate was implemented. Statistical analysis for the estimation of the probability of events and mathematical modelling for the inclusion of all influencing factors that introduce realism in the methodology were made. The areas that are more exposed to risk were identified per type of risk.

To evaluate severity, a steady-state analysis was performed. The severity evaluation is composed of several functions, aiming to reflect the consequences of each contingency in terms of thermal overload, voltage limit violations, voltage instability, loss of load, loss of generation and cascading sequences. The severity functions per type of impact are defined in such a way that their outcome is a normalized value, which is used in the calculation of a global severity index.

Information organization has represented a big challenge and an extremely time-consuming task in this research, but it was essential for its development and to obtain good results. The need of field input data makes this methodology easier to implement within a TSO structure, where the asset owner and the system operator are the same entity, and joins together, in a unique way, two different realities: systems operation and field information, increasing veracity in the results.

The methodology was applied to the Portuguese transmission System in the second half of 2009 and results per hour were obtained.

Keywords: Electrical Transmission Systems, Faults, Online System Operation, Portuguese Transmission Grid, Failure rate, Security assessment, Probability and Risk analysis.

RESUMO

A actual evolução dos Sistemas Eléctricos de Energia impõe o desenvolvimento de novas metodologias para analisar a segurança do sistema. Num ambiente competitivo, as empresas de produção, transporte e distribuição são entidades distintas, o que acrescenta complexidade à avaliação da segurança do sistema. Adicionalmente ao exposto, as restrições ambientais, que limitam a construção de novas linhas e o aparecimento de novos centros produtores, o forte incentivo à produção a partir de fontes de energia renovável e a imprevisibilidade de trânsitos de potência criada pelo mercado de electricidade, contribuem significativamente para uma operação do sistema mais complexa e mais próxima dos seus limites de segurança. Por sua vez, o operador do sistema tem como objectivo a permanente manutenção dos critérios de segurança definidos, mantendo o sistema seguro e fazendo face a todas as situações que possam surgir, independentemente da sua dificuldade.

A utilização de metodologias, baseadas em métodos probabilísticos, que tiram partido da informação em tempo real combinada com o conhecimento adquirido através de dados históricos, é extremamente interessante para a avaliação da segurança do sistema no ambiente actual, pois proporciona ao operador uma visão mais precisa e realista do estado do sistema. Esta tese propõe uma metodologia de avaliação de risco, que considera diferentes probabilidades de ocorrência para as diferentes contingências, consoante o período em análise e as condições actuais. A metodologia desenvolvida fornece aos operadores da sala de comando índices de risco, para o período em análise, que são calculados com base na probabilidade e na severidade de cada contingência. O conhecimento do risco irá permitir uma consciencialização do estado do sistema e uma reacção, por parte dos operadores, executando as medidas de controlo necessárias com o objectivo de minimizar eventuais consequências, face aos eventos analisados. Para o efeito, foram consideradas para a análise contingências simples e duplas com causa comum. No desenvolvimento da metodologia de avaliação do risco foi incluído o efeito das taxas históricas de defeitos na rede, a rede física instalada no terreno, características ambientais, geológicas e geográficas, dos locais onde a rede está instalada, e as condições em tempo real, nomeadamente as condições meteorológicas, como por exemplo previsão e ocorrência de descargas atmosféricas, o risco e a ocorrência de incêndios em território nacional. Foram considerados dados históricos desde 2001 até ao final de 2009. Foi implementado o conceito de taxa de falha a curto prazo, válida para o próximo período em análise. A análise estatística para o cálculo da probabilidade dos eventos e a modelização matemática para a inclusão de todos os factores considerados foram efectuadas, introduzindo realismo nos resultados da metodologia. Adicionalmente, a identificação das áreas da rede mais expostas ao risco foi realizada por tipo de risco.

Na avaliação da severidade foi efectuada uma análise em regime permanente. Esta avaliação é composta por várias funções, que têm por objectivo traduzir as consequências de cada contingência, em termos de sobrecarga térmica, violação de limites de tensão, instabilidade de tensão, perda de carga e de geração e possibilidade de acontecimentos em cascata. As funções de severidade são definidas por tipo de impacto, tendo como resultado um valor normalizado compatível com a sua integração num índice de severidade global.

A recolha e organização de informação representaram um desafio e uma parte onerosa em termos de tempo, mas foi essencial para o desenvolvimento do método e para a obtenção de bons resultados. A necessidade de dados do terreno faz com que esta metodologia seja mais facilmente executável dentro duma estrutura *TSO*, onde o proprietário (ou detentor da concessão) da rede e o operador do sistema sejam a mesma entidade. O trabalho desenvolvido reúne de forma única duas realidades distintas: operação do sistema e a realidade do terreno, aproveitando esta simbiose para aumentar a veracidade dos resultados. A metodologia desenvolvida foi aplicada à rede nacional de transporte, obtendo-se índices de risco por hora para a segunda metade de 2009.

Palavras-Chave: Avaliação da segurança, Operação em tempo real, Probabilidade, Rede Nacional de Transporte, Risco e Taxas de falha.

RESUMÉ

L'évolution actuelle des Systèmes d'Energie Electrique impose le développement de nouvelles méthodologies pour analyser la sécurité du système. Dans un environnement de plus en plus compétitif, les compagnies de production, transport et distribution sont des entités séparées, ce qui rend plus complexe l'évaluation de la sécurité du système. D'ailleurs, les restrictions environnementales, qui limitent la construction de nouvelles lignes et l'implantation de nouvelles centrales, le fort encouragement à la production dérivée de sources renouvelables d'énergie et l'imprévisibilité des fluxes de puissance en résultat du marché d'électricité, contribuent d'une façon significative pour que l'opération du système soit plus complexe et plus proche des limites de sécurité. A son tour, l'opérateur du système a pour but de maintenir de façon permanente les critères de sécurité définis pour le réseau et faire face à toute situation qui puisse arriver, indépendamment de sa difficulté.

L'utilisation de méthodologies basées en probabilité, qui profitent de l'information en temps réel combiné avec la connaissance acquise à partir de données historiques, s'avère très intéressante pour évaluer la sécurité du système dans un environnement d'opération, car elle donne à l'opérateur une vision plus précise et réaliste de l'état du système. Cette thèse propose une méthodologie d'évaluation de risque qui considère différentes probabilités d'échéance pour les différentes contingences, selon la période analysée et les conditions actuelles. La méthodologie développée donne aux opérateurs de la salle de contrôle des indices de risque, pour la période analysée, dont le calcul est basé sur la probabilité et sévérité de chaque contingence. La connaissance du risque permettra une prise de conscience de l'état du système et une réaction de la part des opérateurs, prenant les mesures de contrôle nécessaires pour minimiser les éventuelles conséquences des évènements analysés. À cet effet, l'analyse a considéré des contingences simples et doubles à cause commune.

Le développement de la méthodologie d'évaluation du risque a pris en compte l'effet des taux historiques d'incidents dans le réseau, les conditions locales, en particulier les caractéristiques physiques, environnementales, géologiques et géographiques du réseau, et les conditions en temps réel, notamment les conditions météorologiques, comme prévision / existence d'orages et prévision / existence d'incendies. Les données historiques depuis 2001 jusqu'à 2009 ont été considérées. Le concept de taux de défaillance à court terme, valable pour la période analysée suivante, a été implémenté. L'analyse statistique pour le calcul de la probabilité des évènements et la modélisation mathématique ont été mises en place pour l'inclusion de tous les facteurs considérés et qui rendent plus réalistes les résultats de la méthodologie. En plus, l'identification des zones du réseau plus exposées au risque a été faite par type de risque.

Pour évaluer la sévérité on a effectué une analyse en régime permanent. Cette évaluation est composée de différentes fonctions, ayant pour but de traduire les conséquences de chaque contingence, en termes de surcharge thermique, violation des limites de tension, instabilité de la tension, perte de charge ou de génération et possibilité d'évènements en cascade. Les fonctions de sévérité sont définies par type d'impact et de façon que leur résultat est une valeur normalisée compatible avec l'intégration dans un indice de sévérité global.

Le rapatriement et l'organisation de l'information ont été à la fois un défi et une tâche temporellement lourde, mais essentielle pour le développement de la méthode et pour obtenir de bons résultats. La nécessité de données du terrain rend cette méthodologie plus facile à mettre en place dans le cadre d'une structure TSO, où le propriétaire (ou concessionnaire) du réseau et le gestionnaire du système sont une même entité. Le travail peut alors rassembler deux réalités : opération du système et réalité du terrain, augmentant la véracité des résultats. La méthodologie développée a été appliquée au réseau national de transport du Portugal et on a obtenu des indices horaires de risque pour le second semestre de 2009.

Mots-Clés: Évaluation de la sécurité, Opération du système en temps réel, Probabilité, Réseau National de Transport, Risque et Taux de défaillance.

TABLE OF CONTENTS

Chapter 1. Introduction 1

1.1. Research motivation 1
1.1.1. Deterministic and probabilistic approach 2
1.1.2. Risk assessment 3
1.1.3. Online risk evaluation 4
1.2. Aim of research 5
1.3. Research questions 6
1.4. Research approach 6
1.4.1. Characterization of events 6
1.4.2. Data preparation 7
1.4.3. Probabilistic method 8
1.4.4. Severity calculation 8
1.4.5. Risk evaluation 9
1.5. Outline of the thesis 9

Chapter 2. Recent Major Disturbances 11

2.1. International blackouts 11
2.1.1. The North-Eastern United States and South-Eastern Canada in 2003 11
2.1.2. Denmark and Sweden in 2003 12
2.1.3. Italy in 2003 13
2.1.4. Greece in 2004 15
2.1.5. Greece in 2007 16
2.1.6. Brazil in 2009 17
2.1.7. Other blackouts 18
2.2. European emergency situations 19
2.2.1. French blackout and Iberian islanding in 1999 19
2.2.2. Poland in 2006 20
2.2.3. UCTE network in 4th November 2006 21
2.2.4. Island operation in Jutland- Funen in 2007 26
2.3. Recent Portuguese disturbances 27
2.3.1. 9th of May 2000 27
2.3.2. 6th of September 2001 29
2.3.3. 2nd of August 2003 31
2.3.4. 23rd of December 2009 32
2.4. Discussion 33
2.5. Conclusion 35

Chapter 3. State of the Art 37

3.1. Introduction 37
3.1.1. Power system operating states 37
3.1.2. Reliability concepts in power system analysis 39
3.2. Contingencies 40
3.2.1. Main causes of contingencies 41
3.2.2. Contingencies selection methods 41
3.2.3. High-order transmission contingencies 42
3.2.4. Contingency probability 43
3.3. Power system security 44
3.3.1. Deterministic security assessment 47
3.3.2. Probabilistic security assessment 48
3.3.3. Comparison between approaches 49
3.4. Protection systems 50
3.4.1. Protection systems hidden failures 51
3.5. Probabilistic risk assessment 53
3.5.1. Concept of risk 54
3.5.2. Risk-based security assessment 55

3.5.3. Online risk-based security assessment 58
3.5.4. Risk index for protection systems hidden failures 60
3.5.5. List of software found in the literature 60
3.6. Conclusion 63

Chapter 4. The Portuguese Transmission System 65

4.1. Introduction 65
4.2. Network characteristics 67
4.3. The generation mix 68
4.3.1. Impact of wind generation 69
4.3.2. The main power plants 72
4.4. Typical substation layout 73
4.5. System operation 74
4.5.1. Energy management system 75
4.5.2. Security analysis in the control room 76
4.5.3. Thermal dynamic rating 83
4.5.4. Remedial actions 85
4.6. Real-time system monitoring 87
4.7. Interconnected system 87
4.7.1. Interconnection capacity 88
4.8. Electrical power system control 89
4.8.1. Primary control 90
4.8.2. Secondary control 91
4.8.3. Tertiary control 92
4.8.4. Types of generation reserve 93
4.8.5. Under-frequency load shedding 93
4.8.6. Voltage stability 95
4.8.7. Pumped storage 96
4.9. Operator training and qualification 98
4.9.1. Portuguese experience 99
4.9.2. Joint training between TSOs 99
4.10. Conclusion 101

Chapter 5. Portuguese Transmission System Incidents 105

5.1. Introduction 105
5.2. Concept of incident 105
5.3. Main causes of PTS incidents 109
5.3.1. Storks 110
5.3.2. Forest fires 114
5.3.3. Fog in combination with pollution 118
5.3.4. Lightning 121
5.3.5. Other causes 124
5.4. Number of OHL faults per length 130
5.5. Busbar faults 131
5.6. Incidents involving the loss of an EHV level 132
5.7. Contingencies general statistics 132
5.7.1. Independent and dependent contingencies 133
5.8. Quality of service 134
5.9. Conclusion 136

Chapter 6. Information Gathering and Organization 141

6.1. Introduction 141
6.2. Information gathering 141
6.2.1. Network data 143
6.2.2. Geographical data 143
6.2.3. Geological data 145
6.2.4. Weather data 145
6.2.5. Forest fires 151
6.2.6. Environmental data 153
6.2.7. Incident data 153
6.2.8. Operational information 156

6.3. Data preparation algorithms 156
6.3.1. Number of towers per OHL per municipality 156
6.3.2. Lightning density calculation 156
6.3.3. Soil resistivity per tower 157
6.3.4. Statistics of online lightning observation 157
6.4. Input information update scheme 158
6.5. Conclusion 159

Chapter 7. Probabilistic Method 161

7.1. Introduction 161
7.2. The probability of fault 161
7.3. Correlations 162
7.3.1. Temperature 162
7.3.2. Number of forest fires 162
7.3.3. Number of lightning flashes 162
7.3.4. Working hours 163
7.4. Influence of different causes in the system 163
7.5. Grid elements for probability calculation 164
7.5.1. The overhead line 164
7.5.2. The transformer 165
7.5.3. The busbar 165
7.6. Probabilistic method for OHL circuit-part 165
7.6.1. Failure rates 166
7.6.2. Length at risk calculation 167
7.6.3. Lightning backflash rate 170
7.6.4. Common cause faults in overhead lines 183
7.7. Probabilistic method for transformers 188
7.7.1. Failure rates 188
7.8. Probabilistic method for busbars and circuit-ends 189
7.8.1. Circuit-ends 190
7.8.2. Busbars 190
7.9. Final fault probability 190
7.10. Multiple independent contingencies 191
7.11. Interface for manual calculation 191
7.12. Final probability results 192
7.13. New grid elements 201
7.14. Conclusion 201

Chapter 8. Risk Assessment for Operations 205

8.1. Introduction 205
8.2. Risk evaluation time frames 205
8.3. Risk assessment 206
8.4. Severity evaluation 208
8.4.1. Analysed contingencies 209
8.4.2. Thermal overload 209
8.4.3. Voltage limit violations 210
8.4.4. Non-convergence index 210
8.4.5. Loss of load 210
8.4.6. Loss of generation 211
8.4.7. Islanding criterion 211
8.4.8. Cascading analysis 211
8.4.9. Global severity 213
8.5. Risk indices 214
8.6. Severity results 214
8.7. Risk results 217
8.8. Computational time 221
8.9. Contingency costs 221
8.10. Wind generation facing disturbances 222
8.11. Restoration time 225
8.12. The methodology in the control room 227

8.13. Conclusion 227
Chapter 9. Final Conclusions 229
9.1. Synthesis of the work 229
9.2. Future work 235
REFERENCE LIST 239
LIST OF PUBLICATIONS 247
GLOSSARY 249

APPENDICES

Appendix A Network map A-1
Appendix B Overhead line corridors B-1
Appendix C Summer temperature C-1
Appendix D Overview of faults in PTS D-1
Appendix E Stork nests density E-1
Appendix F Pollution F-1
Appendix G Lightning density G-1
Appendix H Faults caused by fog and pollution and composite insulators H-1
Appendix I Backflash rates overhead lines I-1
Appendix J Contingency probability results J-1
J.1 Overhead lines J-1
J.2 Busbars J-22
J.3 Transformers J-39
J.4 Overhead lines N-2 ..... J-40
J.5 Overhead lines contingency probability results: maximum, minimum and average J-43

LIST OF FIGURES

Fig. 2.1 – Simulated Satellite Picture 14/08/2003 11
Fig. 2.2 – Sequence of events [24] 12
Fig. 2.3 – Sequence of events in Italy [27] 14
Fig. 2.4 – Affected Area [28] 15
Fig. 2.5 – Conditions before and after the disturbance in Greece [29] 16
Fig. 2.6 – Conditions before and after the disturbance in Brazil [30] 17
Fig. 2.7 – Damage from the storms in France [32] 19
Fig. 2.8 – Storm effects on the French System [32] 19
Fig. 2.9 – The Iberian frequency evolution 20
Fig. 2.10 – Generation overview in the Polish system at 12:00 [33] 20
Fig. 2.11 – UCTE system split into three areas [2] 22
Fig. 2.12 – Load and pumps shedding by TSOs [2] 22
Fig. 2.13 – E.ON network in Germany [34] 23
Fig. 2.14 – Time sequence of the cascading tripping in Germany [2] 24
Fig. 2.15 – Frequency and Load Evolution on 4th November 2006 25
Fig. 2.16 – Stork nests located in the affected overhead line 27
Fig. 2.17 – Short-circuit origin location and Electrocuted Stork 27
Fig. 2.18 – Incident tripping scheme 28
Fig. 2.19 – Incident's Location in the network 28
Fig. 2.20 – North-South power transfer 29
Fig. 2.21 – Cleaning under voltage 30
Fig. 2.22 – Separated network scheme in 6/09/2001 30
Fig. 2.23 – Forest Fires under overhead lines 31
Fig. 2.24 – Illustration of the destroyed pylons in the PTS on the 23rd December 2009 32
Fig. 2.25 – Wind speed measurements at the time of the incident 33
Fig. 3.1 – The process of Power System Operation [12] 38
Fig. 3.2 – Decision Drivers of Power System Security [62] 46
Fig. 3.3 – Time scales in emergency – types of control 46
Fig. 3.4 – Time scales in emergency control actions [45], [62] 46
Fig. 3.5 – Illustration of a two dimensional risk graph 55
Fig. 3.6 – Illustration of OL-RBSA process [17] 59
Fig. 3.7 – Overview organization of PRA used in Korea Power System [15] 61
Fig. 3.8 – POM and PRA flowchart [82] 62
Fig. 4.1 – Yearly evolution of the consumption in the Portuguese System [89] 66
Fig. 4.2 – Wind generation evolution in the Portuguese System [91] 68
Fig. 4.3 – The contribution of each energy source in the consumption supply [89] 69
Fig. 4.4 – Voltage dip characteristics to be withstood by wind generating units 70
Fig. 4.5 – ACE of the 220 kV OHL short-circuit on 15th November 2009 at 11:14 71
Fig. 4.6 – Wind Farms behaviour on 15th November 2009 71
Fig. 4.7 – Geographical distribution of power plants 72
Fig. 4.8 – Classical substation topology 73
Fig. 4.9 – Breaker-and-a-half substation topology 73
Fig. 4.10 – SCADA MIMIC 74
Fig. 4.11 – REN's system operations control rooms 74
Fig. 4.12 – Display of the Day-ahead schedule technical verification results[93] 80
Fig. 4.13 – SCADA display – Contingency Analysis Results 83
Fig. 4.14 – Kuipers-Brown model equation [94] 83
Fig. 4.15 – Weather conditions for off-line studies [95] 84
Fig. 4.16 – Off-line study example [95] 84
Fig. 4.17 – Representation of the type of remedial action in the power system states diagram 86
Fig. 4.18 – Principle frequency deviation and subsequent activation reserves [6] 90
Fig. 4.19 – Automatic Generation Control Scheme [99] 92
Fig. 4.20 – ACE recovery facing Generation Outages (> 300 MW) in 2009 92
Fig. 4.21 – Single diagram of the TSO and the DSO networks' border [101] 94
Fig. 4.22 – Examples of Wind generation daily pattern (from December 2009) [102] 97
Fig. 4.23 – Wind generation daily distribution [103] 97

Fig. 4.24 – Geographical Regions included in the Restoration Process 100
Fig. 4.25 – Portuguese Group during Iberian training..... 101
Fig. 5.1 – Incident Structure [19]..... 105
Fig. 5.2 – Incident Example [19]..... 106
Fig. 5.3 – Number of incidents in the EHV network per day..... 107
Fig. 5.4 – Number of incidents 24h period distribution in the EHV network 108
Fig. 5.5 – Number of incidents 24h period distribution average in percentage for the EHV network..... 108
Fig. 5.6 – Number of faults in OHLs caused by the main causes 109
Fig. 5.7 – Percentage of fault causes..... 109
Fig. 5.8 – Quantification of faults caused by Internal Origin..... 110
Fig. 5.9 – Stork nests in an OHL tower & Devices to prevent faults caused by storks 111
Fig. 5.10 – Number of actions/devices taken to avoid incidents caused by storks 111
Fig. 5.11 – Installed Devices in an OHL tower 112
Fig. 5.12 – Comparison between the number of stork nests and the number of faults caused by storks 112
Fig. 5.13 – Percentage and number of faults caused by storks per voltage level..... 113
Fig. 5.14 – Faults caused by storks' distribution per month, period and voltage level 113
Fig. 5.15 – Total number of faults caused by storks' distribution per month per period 113
Fig. 5.16 – Forest Fires in Portugal..... 114
Fig. 5.17 – Right-of-way maintained under an OHL 114
Fig. 5.18 – Yearly amount in the period from 2001 until 15-10-2009 115
Fig. 5.19 – Month distribution in the period from 2001 until 15-10-2009..... 116
Fig. 5.20 – Percentage and number of faults caused by forest fires per voltage level..... 116
Fig. 5.21 – Faults caused by forest fires distribution per month, period and voltage level..... 117
Fig. 5.22 – Total number of faults caused by forest fires distribution per month per period..... 117
Fig. 5.23 – OHLs in a foggy environment..... 118
Fig. 5.24 – Percentage and number of faults caused by fog+pollution per voltage level..... 118
Fig. 5.25 – Faults caused by fog+pollution distribution per month, period and voltage level..... 119
Fig. 5.26 – Total number of faults caused by fog+pollution distribution per month per period 119
Fig. 5.27 – Overview of the taken measures in OHL 120
Fig. 5.28 – Preventive measure taken in OHL to avoid faults caused by Fog+pollution..... 121
Fig. 5.29 – Cloud-to-ground lightning [112] 121
Fig. 5.30 – Percentage and number of faults caused by lightning per voltage level..... 122
Fig. 5.31 – Number of lightning flashes and of faults caused by lightning from 2003 to 2009 123
Fig. 5.32 – Faults caused by lightning distribution per month, period and voltage level..... 123
Fig. 5.33 – Total number of faults caused by lightning distribution per month per period..... 124
Fig. 5.34 – Percentage of incidents caused by Human Errors in the PTS..... 124
Fig. 5.35 – Faults caused by Human Errors distribution per month, period and voltage level 125
Fig. 5.36 – Total number of faults caused by Human Errors distribution per month per period 125
Fig. 5.37 – Origin and affected elements disconnected by protection system's incorrect operation..... 126
Fig. 5.38 – Protection System's performance..... 127
Fig. 5.39 – Hour distribution of faults caused by Protection System Incorrect Operation 127
Fig. 5.40 – Protection systems operating average time per voltage level 128
Fig. 5.41 – Protection System's performance..... 128
Fig. 5.42 – Damage in Germany [118]..... 129
Fig. 5.43 – Destroyed pylons on the 23rd December 2009 130
Fig. 5.44 – Number of faults in OHL per 100km (including all the causes)..... 130
Fig. 5.45 – N-k characterization for the PTS incidents 133
Fig. 5.46 – Indicators Organization [64] 135
Fig. 5.47 – Energy not supplied in the Portuguese Transmission System 135
Fig. 5.48 – Average interruption time in the Portuguese Transmission System 136
Fig. 5.49 – OHL total length evolution versus the number of OHL faults 137
Fig. 6.1 – Information type scheme..... 143
Fig. 6.2 – Tower information sources flowchart..... 144
Fig. 6.3 – Part of REN Transmission System visualised in Google Earth 144
Fig. 6.4 – 4 meters deep soil resistivity map [128] 145
Fig. 6.5 – Temperatures result file (December 2008) 146
Fig. 6.6 – Maps of the average maximum daily temperature in January and July 2009 [126]..... 147
Fig. 6.7 – Lightning monitoring system detection network..... 148
Fig. 6.8 – Lightning monitoring system user interface..... 149
Fig. 6.9 – Lightning detection data file 149

Fig. 6.10 – Risk of forest fire for 3-09-2009 [126] 151
Fig. 6.11 – Evolution of the number of forest fires and the DSR for 2005, 2006 and 2007 [141] 152
Fig. 6.12 – Main Incident's Register Display 155
Fig. 6.13 – Incident analysis organization [64] 155
Fig. 6.14 – Lightning density per municipality and 4km^2 mesh (2003-2009) 157
Fig. 6.15 – Division of Portugal in north and south for online lightning observation 158
Fig. 7.1 – Correlation coefficient of fault causes with temperature 162
Fig. 7.2 – Geographical influence of the four main causes 163
Fig. 7.3 – Overhead line scheme for probability calculation 164
Fig. 7.4 – Transformer scheme for probability calculation 165
Fig. 7.5 – Busbar scheme for probability calculation 165
Fig. 7.6 – Relation of stork nests and towers with nests with the number of towers per municipality 167
Fig. 7.7 – Analysis of the installation of composite insulators in the PTS from 2001 to 2009 168
Fig. 7.8 – Risk level of the municipalities where forest fires caused faults (2007-October 2009) 169
Fig. 7.9 – CIGRE reference cumulative distribution 171
Fig. 7.10 – Typical rod 172
Fig. 7.11 – Tower footing resistance measure versus soil resistivity values 172
Fig. 7.12 – Tower footing resistance approximation curve 173
Fig. 7.13 – OHL contour exemplification near a substation 174
Fig. 7.14 – Conductors' scheme 175
Fig. 7.15 – Surge Voltage at the tower and across the insulation 176
Fig. 7.16 – Expected number of faults versus actual number of faults for 150 kV network 178
Fig. 7.17 – Expected number of faults versus actual number of faults for 220 kV network 178
Fig. 7.18 – Expected number of faults versus actual number of faults for 400 kV network 179
Fig. 7.19 – The two methods results versus actual number of faults for the 150kV OHLs 181
Fig. 7.20 – The two methods results versus actual number of faults for the 220kV OHLs 181
Fig. 7.21 – The two methods results versus actual number of faults for the 400kV OHLs 181
Fig. 7.22 – Model for common cause forced outages [21] 184
Fig. 7.23 – Reliability block diagram for CCF events 184
Fig. 7.24 – Example of two OHL sharing part of the right-of-way 185
Fig. 7.25 – OHL corridors geographical representation with the higher number of faults per km 186
Fig. 7.26 – Reliability scheme for transformers and OHLs 190
Fig. 7.27 – Interface for manual probability calculation 191
Fig. 7.28 – Very short 400kV OHL that connects a substation to a power plant 192
Fig. 7.29 – Probability of fault occurrence for a 150kV OHL 193
Fig. 7.30 – Probability of fault occurrence for a 220kV OHL 193
Fig. 7.31 – Probability of fault occurrence for a 400kV OHL 194
Fig. 7.32 – Probability of fault occurrence for a 150kV OHL 194
Fig. 7.33 – Probability of fault occurrence for a 220kV OHL 195
Fig. 7.34 – Probability of fault occurrence for a 400kV OHL 196
Fig. 7.35 – Probability of fault occurrence for a 220 kV Busbar affected by fog combined with pollution 198
Fig. 7.36 – Probability of fault occurrence for a 150 kV Busbar 198
Fig. 7.37 – Probability of fault occurrence for 400/150 kV autotransformers 199
Fig. 7.38 – Probability of fault occurrence for 220/60 kV transformers in the North 200
Fig. 7.39 – N-2 contingency composed by two 220 kV OHLs 200
Fig. 7.40 – N-2 contingency composed by two 150 kV OHLs 201
Fig. 8.1 – Risk assessment methodology flowchart 207
Fig. 8.2 – Risk analysis inputs (*currently used in the deterministic analysis) 207
Fig. 8.3 – Relative importance of each severity type 214
Fig. 8.4 – Severity evaluation flowchart 215
Fig. 8.5 – Cascading algorithm flowchart 216
Fig. 8.6 – N-2 severity results for the 23rd of December 2009 216
Fig. 8.7 – Specific busbars severity results for the 23rd of August 2009 217
Fig. 8.8 – System's total risk per hour 218
Fig. 8.9 – Probability vs. severity graph of the period under analysis 218
Fig. 8.10 – Zoomed probability vs. severity graph for the period under analysis 218
Fig. 8.11 – Probability vs. severity graph of four different contingencies in the period under analysis 219
Fig. 8.12 – Total risk per hour of the LRMAM contingency 219
Fig. 8.13 – Total risk per hour of the LSNOQ1+LSNOQ2 contingency 220
Fig. 8.14 – Total risk per hour of the B1 150 kV SSN contingency 220

Fig. 8.15 – Total risk per hour of the B2 220 kV SRR contingency 220
Fig. 8.16 – Interruption time histogram 221
Fig. 8.17 – Voltage pattern in pu and wind farms location [152] 223
Fig. 8.18 – Characteristic of the 15th November 2009 short-circuit [152] 224
Fig. 8.19 – Voltage measurements recorded in three different substations at the moment of the fault .. 224
Fig. 8.20 – Voltage dips recorded in 2008 225
Fig. 8.21 – Total number of incidents and incidents wind generation loss 225
Fig. 8.22 – Cumulative frequency of the restoration time for OHLs and transformers 226

LIST OF TABLES

Table 4.1 – Total Line length per voltage level in the PTS 67
Table 4.2 – Number of autotransformers and installed power in the PTS 67
Table 4.3 – Number of transformers and installed power in the PTS 67
Table 4.4 – Installed power of shunt capacitors in the PTS 68
Table 4.5 – Characterization of PTS substations 68
Table 4.6 – Hydro and thermal power plants active power (2009) 72
Table 4.7 – Wind farms installed active power (2009) 72
Table 4.8 – Security criteria used in the PTS elements 79
Table 4.9 – Considered temperature for security analysis 79
Table 4.10 – Load shedding scheme in the Portuguese system 94
Table 4.11 – Plan for Load Shedding Scheme in the Portuguese System after Policy 5 95
Table 5.1 – Total amount of Origin Elements 106
Table 5.2 – Total amount of Origin and Affected Elements 106
Table 5.3 – Overview of fault causes in the system 110
Table 5.4 – Overview of forest fires and faults [109] 115
Table 5.5 – Number of towers that were washed per year 120
Table 5.6 – Number of installed composite insulators 120
Table 5.7 – Number of lightning flashes in Portugal 123
Table 5.8 – Probability of operating time less than 150ms 128
Table 5.9 – Average number of faults per 100km per voltage level 131
Table 5.10 – Number of busbar incidents in the PTS 131
Table 5.11 – Number of incidents with total loss of an EHV level in the PTS 132
Table 5.12 – Number of contingencies in each N-k group 133
Table 5.13 – Faults in the PTS per type of contingency 133
Table 5.14 – Dependent contingencies in the PTS 134
Table 5.15 – Hidden Failures in the PTS 134
Table 5.16 – Faults Characterization per cause 138
Table 6.1 – Update frequency for input information 158
Table 7.1 – Surge impedances for one and two ground wires 176
Table 7.2 - Correlation between the expected number of faults and the actual number of faults 179
Table 7.3 – Mean absolute error between the expected and the actual number of faults 179
Table 7.4 – Root mean square error between the expected and the actual number of faults (6 years) 180
Table 7.5 – Correlation between the expected and the actual number of faults 180
Table 7.6 – Multiplier for North and South 182
Table 7.7 – Number and Types of faults caused by lightning 183
Table 7.8 – CCF Rate Results per year for per N-2 events caused by lightning (2003 to 2008) 186
Table 7.9 – OHL pairs and β for N-2 contingencies caused by the same forest fire (2003 to 2008) 187
Table 7.10 – OHL groups disconnected non-simultaneously by the same forest fire 187
Table 7.11 – Data for probability calculation for LSNPO2 195
Table 7.12 – Probability calculation summary for LSNPO2 195
Table 7.13 – Data for probability calculation for LCVRTJ 196
Table 7.14 – Probability calculation summary for LCVRTJ 196
Table 7.15 – Data for probability calculation for LRARR2 197
Table 7.16 – Probability calculation summary for LRRRA2 197
Table 7.17 – Maximum and minimum probability of fault per period per type of transformer 199
Table 8.1 – Average errors per type of forecast 206
Table 8.2 – Severity weighting factors 213

LIST OF ABBREVIATIONS, SYMBOLS AND ACRONYMS

AAC	Already Allocated Capacity
ACE	Area Control Error
AGC	Automatic Generation Control
AT	Autotransformer
ATC	Available Transfer Capacity
AVR	Automatic Voltage Regulation
BFR	Backflash Rate
CA	Contingency Analysis
CCF	Common Cause Failure
CFO	Critical Flashover Voltage
CHP	Combined heat and power plant
CIGRE	International Council on Large Electric Systems
DACF	Day Ahead Congestion Forecasts
DG	Distributed Generation
DSR	Daily Severity Rating
DTS	Dispatch Training Simulator
EHV	Extra-High Voltage (including 150kV, 220 kV and 400kV)
EMS	Energy Management System
ENS	Energy Not Supplied
ENTSO-E	European Network of Transmission System Operators for Electricity
EENS	Expected Energy Not Supplied
EPRI	Electric Power Research Institute
FWI	Fire Weather Index (calculated by the Portuguese Meteorological Institute)
GAI	Incident Analysis Group
GestInc	Incidents Data Base
GIS	Geographic Information System
IEEE	Institute of Electrical and Electronics Engineers
IM	Portuguese Meteorological Institute
IT	Information Technology
LFC	Load Frequency Control
LMS	Lightning Monitoring System
LOLP	Loss of Load Probability
MAE	Mean Absolute Error
MIBEL	Iberian Electricity Market
NASA	National Aeronautics and Space Administration
NERC	North American Reliability Council
NGCC	Natural Gas Combined Cycle
NTC	Net Transfer Capacity
OH	UCTE Operation Handbook
OHL	Overhead Line
OL-RBSA	Online Risk Based Security Assessment
PRA	Probabilistic Risk Assessment

PTS	Portuguese Transmission System
QRS	Quality of Service Report
RBSA	Risk Based Security Assessment
REN	Rede Eléctrica Nacional
RMSE	Root Mean Square Error
SCADA	Supervisory Control and Data Acquisition
SE	State Estimator
SPS	Special Protection Scheme
TF	Task Force
TR	Transformer
TSO	Transmission System Operator
TRM	Transmission Reliability Margin
TTC	Total Transfer Capacity
UC	Underground Cables
UCTE	Union for the Coordination of Transmission of Electricity
VPN	Virtual Private Network
WG	Working Group

LIST OF UNITS

GW	gigawatt (10^9 W)
h	hour
Hz	hertz (1/s)
kA	kiloampere (10^3 A)
km	kilometre (10^3 m)
kV	kilovolt (10^3 V)
m	meter
mHz	miliHertz (10^{-3} Hz)
min	minute
ms	milisecond (10^{-3} s)
MVA	megavolt-ampere (10^6 VA)
Mvar	megavars (10^6 var)
MW	megawatt (10^6 W)
MWh	megawatt-hour (10^6 Wh)
s, sec	second
V	volt
W	Watt
Ω	Ohm
€	Euro

Chapter 1.

Introduction

1.1. Research motivation

The changes of the conditions in which power systems must be operated have created new challenges regarding security assessment, demanding the development of new methodologies. In many countries today, the introduction of a market-driven competitive environment in the power system industry and the regulatory changes causing the unbundling of generation, transmission and distribution, have resulted in more stressed operating conditions and more vulnerable networks. Apart from this economic context, the increased environmental concerns, which limit the construction of new transmission lines and generation capacity, contribute as well to increase the stress on operating conditions and, consequently, place the systems closer to their security limits.

In addition to the latter, regarding environment and the reduction of CO_2 emissions, the generation through renewable energy sources is strongly incentivised. Strategically, Portugal aims to supply 45% of the national electricity demand from renewable energy sources until 2010 [1], which has strongly encouraged the appearance of wind farms connected to the network. While the energy from large hydro and thermal power plants is traded in the electricity market, other renewables, such as wind farms and solar power plants, are paid with a favourable feed-in tariff and all their generation is completely absorbed by the grid, independent of market conditions. Additionally, wind generation is increasing the uncertainty in system operation environment, because of its intermittent characteristic and behaviour when facing a disturbance, e.g. as in the large European disturbance in 2006 [2].

Finally, the interconnected network is no longer just for mutual support; nowadays it has become the base platform for trading electricity allowing the shifting of increasing volumes of power across the system. Despite the doubtless many benefits, from the operations perspective the electricity market also presents more unpredictable and less stable power flows and a less controllable market-dependent generation pattern. Concerning the tie-lines between neighbouring systems, violent overloads may cause network separation (islanding) and a low voltage level may reveal voltage instability, warning for a deficit of reactive power injection. Therefore, the daily routine of transmission system operators has become more complex and control room operators are frequently faced with difficult situations caused by stressed system operating conditions. As a consequence, there is an increasing need to identify the operational security level of a transmission system [3].

System operation is an essential and complex task that has the goal to ensure the well being of the electrical power system. Control room operators are often called upon to take decisions and prompt actions, which require a trade-off analysis between security and economy. Operators are required to perform a close monitoring of the system in order to maintain a good performance and to achieve all the essential tasks for which it was designed. Therefore, the continuous improvement of the control room performance must be a permanent goal. To guarantee this, there is an increasing need to provide control room operators with useful information, adequate decision-making tools for adequacy and security assessment, and frequent training, among other things. Operator training using simulators is one of the best ways to provide control room operators with the skills to deal with consequences of unforeseen disturbances that place the system in an emergency situation. When facing an incident, the operators' reaction is decisive to minimize consequences. Competence, education and training are of paramount importance. This is applicable not only to control room operators, but also to operation, planning and maintenance staff. Human quality will surely reduce the risk of system failures [4]. Reference [5] is just an example of the Portuguese TSO continuous purpose to provide decision support tools for operators,

allowing them to better understand events and to take suitable control measures for the secure operation of the network.

All the described factors that introduce uncertainty and stress on the operation conditions influence the severity (consequences) when facing a disturbance. International data confirm that the frequency of large blackouts has increased in the recent past, and also that simple initiating faults can have very severe consequences, meaning that their risk cannot be neglected.

In the transmission system, disturbances happen quite often, but they are distinct in probability and impact. Online control is a continuous (just in time) decision-making task for the operator, and despite all the efforts being done regarding supervisory practices, operation strategies, protection systems and control systems improvements, it is technically and economically impossible to eradicate major disturbances and blackouts. They will be a permanent threat to the electrical power system. Chapter 2 presents a few examples of severe disturbances, which occurred in the recent past. Hence, the need to continuously increase efficiency in system operation makes incident analysis a crucial activity.

Nowadays, utilities are facing stricter requirements regarding quality of service, therefore there is an increasing awareness that in a power system severe contingencies can happen, in an unpredictable way, which far exceed the reasonable and widely used deterministic security principles used for planning and system operation. These incidents can be caused by several reasons, mentioned in the development of this thesis, and they play an important role in power systems analysis and operation, although they have not been included in the existing security analysis, because they are considered not likely to happen.

The probabilistic assessment has become an important topic for researchers and engineers. It is possible to evaluate the risk of contingencies by combining severity and probability. It is known that probabilistic methods constitute powerful tools for use in many kinds of decision-making problems and in order to manage this increased exposure to risk, the use of such techniques becomes essential.

The use of methodologies that take advantage of the actual real-time conditions in combination with past knowledge, using probabilistic methods, is extremely interesting in the system operation's environment, because it gives a more accurate overview to the control room operators. It has become essential for the decision-making process to have security indices that allow the operator to react in advance and to be aware of inherent risks, preventing harmful situations.

1.1.1. Deterministic and probabilistic approach

The deterministic security assessment has been widely used by Transmission System Operators (TSOs) to guarantee a high level of security in system operations. It is known as N-1 criterion [6], and constitutes a basis for determining trade-offs between security and economy. It tends to provide a conservative security zone for protecting the system against severe disturbances. This method has provided high reliability levels and is easy to implement because of its simplicity, but it has some weaknesses.

The deterministic approach only addresses the severity of contingencies, in terms of thermal loading, voltage violations and loss of load, considering that events are equally likely to occur and therefore it cannot address increased or decreased uncertainty in the operating conditions.

Facing an adverse weather situation, such as lightning occurrence or a high risk of forest fires, the likelihood of contingencies in the deterministic approach is still the same, although there are TSOs that also include specific N-k events, with $k>1$ (normally $k=2$), in their "must-run" contingency list. The risk of multiple contingencies cannot be neglected and the analysis needs to include local conditions, such as environmental, geographical and geological data, e.g. the presence of pollution or storks' population, but also current conditions, such as adverse weather or risk of forest fires.

The deterministic security assessment does not consider the current conditions (such as lightning occurrence), or the effect of longer overhead lines (OHLs), which are more exposed to the action of external factors due to their dispersion over a wide area than the shorter ones; neither the inherent characteristics of the geographical area where they are deployed nor the actual presence of the fault's cause, which increases significantly its probability of fault. Probabilistic assessment gives the opportunity to include, through historical failures rates, the seasonality, geographical influence and even current conditions in the probability calculation. The probabilistic assessment versus deterministic assessment is a broadly discussed topic, which appears in several references, such as [7-9].

The security principles used for operation and planning in the Portuguese transmission system determine that, in general terms, after an incident which involves the breakdown of any grid element (N-1) or, in specific cases, the simultaneous failure of a double-circuit overhead line (N-2) or the failure of the largest generator in service, supply interruptions (excluding single-feeding points without alternative), permanent overloads and voltage violations shall never take place. Sometimes, because of the unpredictable nature of the incidents and the coincidence of several events, incidents that were not foreseen may occur. If the power system withstands the specified criteria then it is considered secure, if not, it is considered insecure. The security is checked by a deterministic contingency analysis, taking into account the set of contingencies considered most probable to happen, but in the moment that they are selected to be part of the lists, their probability becomes the same. To perform this analysis, a tool, embedded in the Energy Management System (EMS) software, is used. The EMS software, which many transmission system operators (TSOs) use as a complement of SCADA, allows the operator to check the security principles applied for system operation. Contingency Analysis Applications (as part of EMS) are designed with simplified algorithms in order to carry out the calculation of dozens of contingencies in just a few seconds. Most of the time, this criterion is appropriate to prevent major disturbances, at least cascading events caused by overloaded elements, although it may not be economically efficient because it does not consider the probability of events and consequently their risk.

Probabilistic assessment asks for the definition of an acceptable level of risk and consequently enables a more efficient use of the transmission capacity according to the current or expected conditions. This approach is especially efficient for short-term analysis, as close as possible to the period under evaluation, because of forecasts' accuracy.

1.1.2. Risk assessment

Reliability and risk assessment tools have been broadly used for several applications, for example in nuclear power plants and in the aerospace industry (e.g. at NASA) with probabilistic risk assessment (PRA) procedures [10]. The use of probabilistic risk is mentioned in the literature as the natural evolution for power system security assessment [8], because it quantifies probability and consequence of occurrences, hence risk. Risk assessment has been considered in system planning for many years, but it has not yet been used in power system operations, although there is an increasing need for security level decision-making support tools, and probabilistic methods show potential in this matter. The risk evaluation of power system operation has to consider the likelihood of failure events and the severity of their consequences. Zero risk is beyond reach, because random and unexpected failures are not controllable.

Power system risk assessment is complex, and it is associated with the system operating state, i.e. system topology (planned, programmed and forced outages), generation pattern (market-driven) and load profile that result in a specific power flow result, and it is affected by unexpected disturbances (contingencies) and quickly applicable remedial actions.

It is important to be aware, and it is mentioned in a considerable part of the existing literature, that as every new development, also probabilistic security assessment has to be embraced in a prudent and careful way. All innovations need a sustainable approach while being introduced in the daily and regular

procedures, because they have to be understood and accepted by everyone, and its implementation needs to pass the infancy stage.

It is the final customer that pays the cost of the system and this is one issue that cannot be forgotten, because deterioration in the security level will directly oppose the benefits of decreased energy costs brought on by competition and energy markets.

Internationally, risk assessment is presently an important topic for research and utilities. In the new Policy 3 – Operational Security of the UCTE Operation Handbook [6], risk analysis appears as a requirement to be fulfilled by all ENTSO-E partners. It is stated that the definition of N-1 is mainly based on the risk assessment considered by each TSO, the contingencies and their consequences for the system to be considered in the security calculations, the observed area by each TSO, the accepted operating limits with the minimum risks for the system, the adequate and possible remedial actions and the coordination between TSOs. In appendix 3 of Policy 3, system reliability is defined as the ability to ensure normal system operation, limit the number of incidents, avoid major disturbances and limit their consequences whenever they do occur. This definition implies a combination of efforts from many areas within a TSO, as not only system operation can influence system reliability. As will be shown in chapter 5, many measures can be applied in the field in order to limit the number of incidents. The planning stage can also influence the system's reliability as options at that stage can significantly impact the consequences of disturbances.

The quote *"Reliability, but not at any price"* [6] expresses the need to define acceptable and unacceptable risks, to identify significant initiating events and to analyse measures to limit the risks.

CIGRE reports from Task Force 38.03.12 [3], [11] recommended further study of probabilistic security assessment methods, and a later CIGRE Task Force, 38.02.21 [12], was tasked with implementing this recommendation [3]. Recently, CIGRE Task Force 38.02.24 [13], presented Risk Assessment in its chapter 8. The Electric Power Research Institute (EPRI) was also involved in efforts to develop probabilistic risk assessment tools for security assessment [14], [15].

CIGRE's TF 38.02.24 report has as its main purpose to make recommendations on operational defence plans against extreme contingencies. The report presents the definition of a defence plan, an overview of existing ones, answers to questions like "how to design it and to implement it" and, more related with this work, it points out risk assessment as one of the future directions in power system defence strategies [13]. It describes risk assessment as an important task for the protection of critical infrastructures.

One of the biggest challenges for the utilities is to make risk assessment in power system operations a reality, which gives the motivation for this research work.

1.1.3. Online risk evaluation

For online risk evaluation, short-term failure rates are crucial when the security for the next hour is assessed, considering actual conditions, identifying which are the areas more exposed to risk, as well as historical fault data, including network characteristics, geographical, geological, and environmental and weather data in the calculation. Reference [7] gives a good insight on the operational risk assessment and discusses the external influencing factors and the concept of short-term failure rate, which is developed in this thesis. The use of only average failure rates in operational risk assessment would overestimate the risk during periods of normal weather and underestimate the risk in periods of adverse weather. Therefore, it is crucial to identify which risks are present in each moment and where, in order to incorporate them in the probability calculation for the next period under analysis.

Reference [16] deals with contingency probability estimation for use in operational decision-making, including temperature and wind speed in the algorithm. These two parameters were not used in this work because of the lack of available historical data in case of wind speed and a low correlation in case of

temperature. Statistical methods employed in the estimator include maximum likelihood and linear regression. The lack of data and the importance of weather conditions in operational decisions are also mentioned in this thesis. It states that operational decisions are mostly influenced by failures (forced outages) and therefore the repair times are of little interest when evaluating online security, which is an important aspect also for this research work. Finally, the Poisson model is used in this work, because it is effective in representing the next failure, and the failure rates are expressed as a continuous function of temperature and wind speed.

The operators' decision-making process requires real-time updated information, which means also updated probabilities computed with the most recent information. In a control room, the operators have always available the weather information and a prediction for the next hours with a high degree of certainty. Beyond that, in the Portuguese TSO, the control room has installed an application that monitors lightning strokes in real time, enabling the control room operator to follow the lightning evolution in the territory. It is important to calculate the contingencies probability at a particular time and date, as the calculation results are going to change depending on the actual operating conditions.

A methodology for online risk-based security assessment is presented in [17]. This approach introduces risk as an expectation of severity. It gives more emphasis to the forecasted operating conditions in terms of load and generation than to the probability of the contingency and is presented further in section 3.5.3.

1.2. Aim of research

The aim of this work is to develop an integral risk assessment methodology to perform power system operation security analysis, and to evaluate the probability of contingencies and their severity, in terms of violations of operating limits, loss of load, necessary generation reserves and their economical impact. It will provide control room operators with risk-based security indices for the next period (such as one hour). The quantification of risk associated with contingencies is going to be very useful to operators and operations planning engineers when evaluating network security for the decision–making process.

In any electricity transmission system, a stable condition must be assured, but as already mentioned, power systems are currently more complex and heavily loaded, which means that the consequences of each contingency become more severe, and consequently the risk increases. Hence, it is essential when making decisions to have risk-based security indices that allow the operator to be aware of current risks and to react in advance, if possible, preventing or mitigating harmful situations.

The effects of weather conditions, environmental factors, generation pattern, network and field characteristics, among others, were introduced in the analysis, aiming to assess short-term risk in a realistic way. Incident data is normally confidential information, but because this work aims to quantify the risk to the Portuguese TSO, all the research was made with full access to the existing data, allowing the accomplishment our purpose. A TSO structure, i.e. where the system operator and the asset owner are part of the same organisational entity, facilitates the process of information gathering.

The developed methodology is composed of two parts: probability of occurrence and severity for all contingencies under analysis, mainly N-1 and N-2 events. This work aims to create a strong link between theory and practice, applying the developed knowledge directly to the security analysis process of the Portuguese transmission system operation, making it more efficient. The expectations are that, with this methodology, security and economic benefits will be achieved when maximizing the efficiency of the power system inside an acceptable risk level. For this it is necessary to determine the acceptable risk level, which is a management decision, and therefore goes beyond the scope of this research.

The final goal of this work is to demonstrate that the risk methodology is adequate for online and short-term evaluation, presenting the current risk level and its trend within a defined time frame. The nature of the work performed in a control room has to be taken into account, thus being focused on the operators.

It is also important to make the methodology flexible and easily updated to be valid for now and for the future. i.e. the relevant variables should be added, changed or removed from the probability of occurrence when needed and according to the evolution of the physical network, terrain and meteorological conditions and system's security requirements.

The biggest challenge of this study is to build up something useful, to succeed with a practical, rather than an only theoretical approach and finally to create a method that works with a complete real system and real data, whereas many of the published research work limits itself to reduced network test models.

1.3. Research questions

In order to achieve the purpose of this research work, the following questions were raised and need to be answered:

1. How to calculate the probability of occurrence of contingencies in order to obtain realistic and accurate results for the period under analysis, including all the relevant and available parameters in the calculation? How to estimate short-term failure rates? Which are the significant inputs for the probability calculation? What are the selection criteria?

2. How to evaluate the relevant set of contingencies for analysis? Which are the events that have to be considered regarding simultaneous outages in the context of operations?

3. What is relevant to include when evaluating severity? How many overloads or voltage violations are there and how severe are they? Is cascading possible? How to address cascading events from an operating perspective? How to estimate an overall severity? Which operational costs have to be included in the analysis?

4. How to make risk an effective measure in system operation environment? How to present risk-based indices to control room operators?

1.4. Research approach

The research approach consists of the following five main steps:

1. Characterization of events
2. Data preparation
3. Development of the probabilistic method
4. Calculation of severity
5. Risk evaluation

These steps are further elaborated in the following paragraphs.

1.4.1. Characterization of events

As every transmission system, regarding contingencies occurrence, the Portuguese system also has its own intrinsic characteristics, which directly influence events' probability, hence the definition of credible contingency can be different for other utilities. In order to calculate the probability of fault occurrence, the faults, between 2001 and 2009, were evaluated and the variables that influence the probability value were defined. As relevant variables, the following have been identified:

- Weather conditions

- Lightning data
- Environmental data (such as: the stork population area and polluted areas)
- Forest fire data (risk per region and online location of active fires)
- Geographical and geological characteristics
- Network data (topology, physical characteristics, equipment technology, etc.)

Through event characterization, it was possible to identify the characteristics of each cause (such as time, season and location), their failure rate per length depending on the time and the impact of all the improvements being made in the network. The improvement actions show that the future will not be equal to the past. Therefore, the data for the risk assessment methodology has to be constantly updated to be able to provide credible indices. Near future information must also be integrated in the model, such as lightning data (the Portuguese TSO has a real-time monitoring system that provides geographical and amplitude information), forest fires' daily risk and meteorological information. It is important to point out that each country or region has its own intrinsic characteristics and it is important to include them in the probability calculation. For example, in Portugal the presence of stork nests in OHL towers causes every year tens of faults, which is why this parameter is included in the methodology.

In order to assess the importance of some available variables, aiming their integration in the methodology that is being developed, several correlation calculations were performed.

To complete this analysis, recent blackouts and emergency situations were studied (see chapter 2) to identify common causes and characteristics. The lessons learned from past events were used in the development of this research work.

1.4.2. Data preparation

Information organization represents a big challenge and an extremely time-consuming task for a TSO, but it allows an accurate analysis of the system and the development of methodologies. In practice, perfect information does not exist, therefore expectations had to be adapted and the work had to proceed with what was available, reliable enough and possible to update regularly.

To obtain accurate results, data collection and organization is crucial for the development and maintenance of the risk assessment methodology. This forces the TSO to maintain an updated asset database with all the required information. This research joins together two different realities: system operation and field information, which increases realism in the results. The data is organized made by geographical location, aiming to influence the length of OHLs and substations exposed to risks.

After gathering the raw data, the data was processed and several different software packs were used in order to achieve the final stage to be used in the probability calculation. For data preparation and analysis the following software was mainly used:

- *MsExcel*: to organize the available data, to prepare the input matrices and to perform the statistics; Together with MsExcel, several macros were built in VBA for applications in order to automate updates and processes.
- *Matlab*: to process lightning data, geographical data (municipalities and OHL towers) and to produce figures in an efficient way.
- *Jobs from Meteorage*: to monitor lightning and to access the lightning data base, running since June 2002.
- *Transcoord from Instituto Geográfico Português* [18]: for coordinates conversion (from DATUM LISBOA (PRT-SCE) system used by the Portuguese TSO to WGS84 (GPS) system and vice-versa).
- *KMLCSV converter*: Open source software to convert CSV files into KML files and vice-versa.
- *Google Earth*: for geographical visualization.

1.4.3. Probabilistic method

To pursue an accurate risk assessment, it is necessary to determine for each contingency under analysis the associated probability of occurrence, independently of the event's dimension. The distinction between independent and dependent failure events is important, being aware that dependent failure events generally produce much more severe consequences than single independent ones and are much more likely than multiple independent ones. Examples of dependent failure are:

- Simultaneous failure of two overhead lines sharing the same tower due to lightning.
- Busbar fault (fault on terminal equipment at a substation) normally causes multiple circuit outages.
- Several lines tripping due to the same forest fire, simultaneously or not. This concerns the overhead line corridor concept introduced in [19], [20].
- Adverse weather conditions increase the failure probability of all components that are exposed to it.

Contingency probability was calculated by fitting an existing probability model to the incidents' historical data. Specifically, the probability of fault occurrence on a component was modelled using the Poisson distribution with a constant fault rate [21]. To calculate the probability of fault occurrence per component (OHL, transformer or busbar) combining all possible causes, probability concepts were applied. The applied concepts can be found in [10], [22].

The failure rates were calculated per cause for each grid element, considering all the relevant factors. Additionally and because we are developing work for system operations environment, current conditions are also included, aiming to assess short-term risk in a realistic way. Here the concept of short-term failure rates is implemented, valuing the current risks that are actually present in each evaluation.

1.4.4. Severity calculation

After calculating the probability of an event, it is important to study its consequence, in order words, the severity. The severity evaluation has to consider the results of power flow simulations. For each contingency, the severity calculation has to assess thermal overloads, voltage limit violations, voltage instability, loss of load, loss of generation and the danger of cascading. Several severity function are defined, one per each type. These functions are defined in such a way that their outcome is a normalized value, which will be used in the calculation of a global severity index. The global severity index is based on a weighting concept.

To calculate severity for the next hour, current State Estimator snapshots that contain all the information needed, regarding topology information, load pattern and generation profile, were used. The expected changes in actual conditions such as programmed outages, wind generation forecast, load forecast and expected market-driven generation pattern are included in the analysis.

The steady state simulations were made using the Power Flow Module of PSS/E software from Siemens PTI, using State Estimator snapshots that represent pictures of the real system, with the necessary adjustment to reflect current conditions. This software has proved suitable, robust and efficient when executing this task. The chosen steady state simulation method to be used by the software was the "Full Newton-Raphson Method".

Other issues, such as the costs of contingencies, the wind generation behaviour when facing faults and the restoration time are also addressed, constituting additional information to the severity functions results, which may influence the consequences of contingencies.

1.4.5. Risk evaluation

In general, risk analysis is based on the definition of risk, according to the standard ISO 14121-1:2007 [23], which defines the risk related to an event as the product of probability of occurrence and extent damage. For system operations, risk is assessed by the product of event probability and severity of its consequences. Given an acceptable level of risk, the higher the probability of a contingency, the lower is the accepted severity.

To evaluate risk, individual indices are calculated per type of severity and additionally combined in to a global index. These indices aim to provide an insight to control room operators of the network state and of the probability and severity of each contingency. For successful implementation and acceptance of the new methodology, the results have to be simple and linked to the deterministic ones. Both methods, deterministic and probabilistic, should run in parallel until the outcomes are fully understood and accepted by operators. After gaining experience with the practical meaning of the numerical value, this risk index can for example be made visible to the operator using a colour coding, as in a traffic light.

During the development of a methodology that has to be effective enough to manage the risk of contingencies in the system operations environment, assumptions are necessary, but have to be taken carefully. To decide how to select the contingency set, available statistics based on historical data are of great interest, because they allow the evaluation of the event probability.

In order to validate the methodology and to evaluate the meaning of the results, both in terms of probability and severity, the complete process, i.e., the probability of occurrence was performed from the beginning of June until the end of December 2009 and the severity from July until December 2009. The list of contingencies to be evaluated is composed by single and double common cause contingencies.

1.5. Outline of the thesis

Chapter 2 presents some examples of severe disturbances, which occurred in the recent past.

Chapter 3 presents the previous work that was considered relevant for the development of this research work. It introduces topics such as transmission system security, types of contingencies, protection systems and the concepts of reliability and risk.

Chapter 4 presents the Portuguese transmission system, its characteristics and how the system is operated, including security evaluation issues. It also summarizes the various concepts of power system control that ensure a good performance of the system, including automatic load shedding. In the final part, it emphasizes the importance of operators' training and it describes the Portuguese TSO experience.

Chapter 5 introduces the concept of incident, characterizes the system faults due to the most relevant causes in the Portuguese transmission system and presents all the related statistics. The analysis of the fault occurrence with the intrinsic characteristics of the Portuguese territory is also performed, including geographical and meteorological data. The characterization of faults is crucial for the success of this methodology.

Chapter 6 describes the work of collecting and organizing all the relevant data. It also presents all the developed algorithms that process the data to make it available and usable. In order to incorporate the intrinsic characteristics of Portugal that influence the occurrence of faults and the actual risk, information gathering, knowledge and organization are crucial.

Chapter 7 presents the probabilistic method to calculate the probability of fault occurrence for all grid elements and explains all the steps for each of the fault causes in a detailed way. The method uses the relevant influencing factors, such as the presence of lightning and forest fires, as inputs and introduces

the current conditions in the calculation. Hence, the concept of short-term failure rates is implemented, valuing the current risks that are present in every evaluation. The probability of common cause double contingencies is also addressed. Probability results are presented for the period from June until December 2009.

Chapter 8 joins the results from chapter 7 and the severity evaluation, giving shape to the integral risk assessment methodology, which was implemented for the Portuguese TSO. This chapter presents the severity function per type of impact and the possible risk indices. Additional issues, such as wind generation behaviour during faults, the restoration time, the cost of contingencies and the methodology in the control room are also addressed. Severity and risk results are presented from the period from July until December 2009.

Final conclusions, including a synthesis of the research work, and perspectives for future work are presented in chapter 9.

Chapter 2.

Recent Major Disturbances

2.1. International blackouts

A short description of some the most important blackouts world-wide since 2003 is presented.

2.1.1. The North-Eastern United States and South-Eastern Canada in 2003

In the afternoon of 14th August 2003, a major blackout has affected eight states in the Midwest and the Northeast of the United States and the Canadian province of Ontario [24]. Over 50 million people were without power supply and approximately 61.8GW of load was lost, causing a huge economic cost.

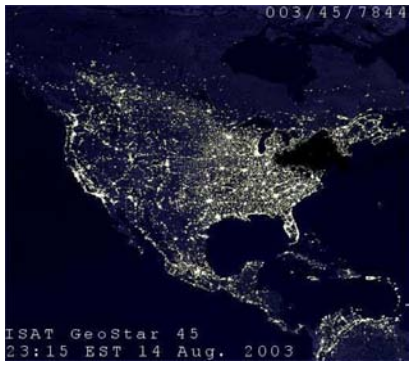


Fig. 2.1 – Simulated Satellite Picture 14/08/2003

Before the blackout, between 12:15 and 16:04, the state estimator and real time contingency analysis tool of the Midwest Independent System Operator (MISO) was out of service and, obviously, without these tools it was not possible to perform security analysis on the relevant control area.

At 13:31, First Energy's (FE) Eastlake generation unit 5 tripped, which is a critical source of active and reactive power for the Cleveland-Akron area, but FE operators did not perform a contingency analysis to determine whether the loss of further transmission lines or generating capacity would put its system at risk. At 14:02, the Stuart – Atlanta 345 kV line trips due to an overgrown tree.

At 14:14, FirstEnergy began losing its SCADA system alarms, but operators were not aware of the failure. FE's alarm system was only restored just before the blackout. Sometime after, FE's EMS server fails, thus operators did not know their system was loosing lines and voltage until perhaps 15:46. After 15:05, FE lost three 345 kV lines in the Cleveland-Akron area under normal load due to contact with trees, causing heavy loading on other lines in the system. Consequently, between 15:39 and 16:08, 16 138 kV lines were lost, in the Cleveland-Akron area, due to overloads and ground faults. At 15:57:05 EDT, the Sammis-Star 345 kV line also tripped due to overload. This event started a cascading blackout and, in less than 10 minutes, more than 508 units at 265 power plants were lost. The northern part of the whole eastern interconnection was split into five islands. The sequence of events is displayed in figure 2.2.

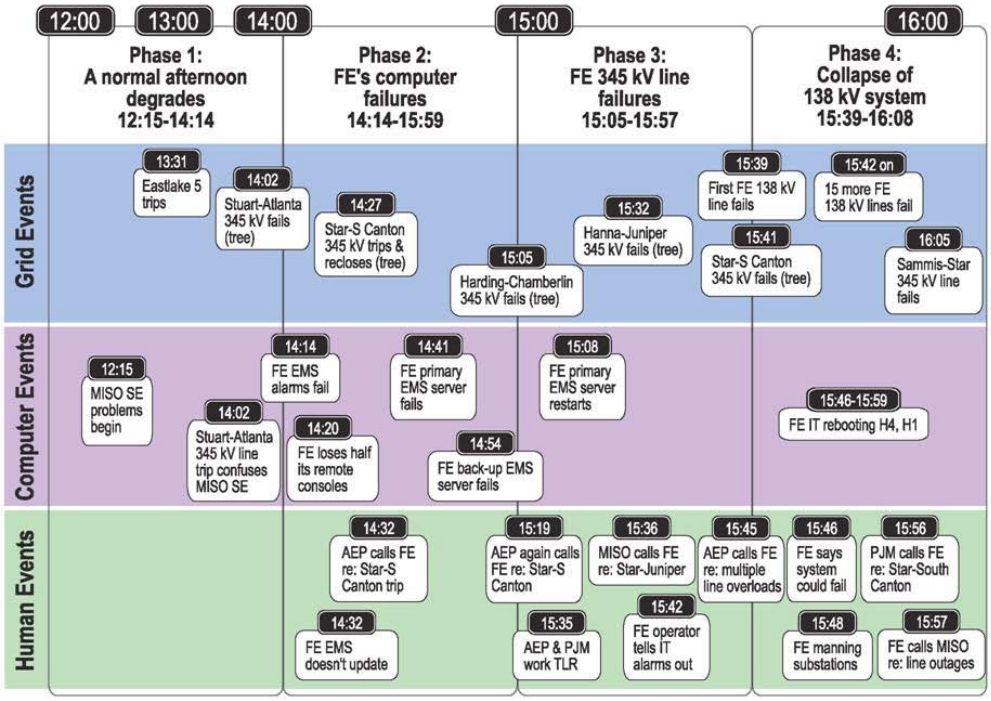


Fig. 2.2 – Sequence of events [24]

Most services were restored in the United States within two days, with all services fully restored within four days. Restoration was greatly assisted by the ability to energize transmission from neighbouring systems and by some relatively large islands that survived the disturbance.

Like every major event, also the August 14th blackout had multiple causes and recommendations associated with the event. The final report of the Task Force identified four groups of causes, namely:

- Inadequate System Understanding
- Inadequate Situational Awareness
- Inadequate Tree Trimming
- Inadequate Diagnostic Support from Reliability Coordinators

Summing up, the key issues raised in the recommendations included the need to improve governance, regulation and enforcement, to improve system operator training, particularly in relation to managing emergency events and avoiding future emergency events through more effective management of near emergency conditions, to ensure that system operation is supported by effective diagnostic and management tools and information, which facilitates real-time contingency analysis, system monitoring and operational management, to clarify standards and operating practises relating to vegetation management, and to improve coordination, communication and data exchange between system operators and reliability coordinators at a local and regional level.

2.1.2. Denmark and Sweden in 2003

At 12:37 on Tuesday, 23rd of September 2003, the southern part of Sweden and the eastern part of Denmark, including its capital city of Copenhagen, were blacked-out [25]. A combination of severe faults, which were beyond the acceptable security criteria in operations, occurred in between 12:30 and 12:35. Prior to the disturbance, several grid elements were out of service due to planned maintenance and works (two 400 kV lines, four nuclear units and three HVDC links from Germany and Poland), but operating conditions were stable within the acceptable security criteria.

At 12:30, unit 3 in Oskarshamn Nuclear Power Plant shut down due to mechanical problems, thus about 1200 MW of generation was lost (this contingency is standard according to security criteria applied within the Nordic Interconnected Grid). At 12:35, a double busbar fault occurred in a 400 kV substation on the western coast of Sweden, representing a serious failure, where four 400 kV lines were disconnected, and leading to the loss of two 900 MW nuclear units. This triggered power oscillations, low voltages and a drop of the system frequency, initiating automatic under-frequency load shedding. The grid was then heavily overloaded on the remaining south-east and south-central parts.

During 90 seconds the oscillations faded out and the system seemed to stabilize, but when the demand started to recover, further stress was placed in the remaining 400 kV lines, lowering the voltage down to critical levels. At 12:37, the situation developed into a voltage collapse in Southern Sweden and Eastern Denmark. The restoration process began immediately, using the hydro power in Norway, northern Sweden and Finland, which was fully available to pick up the recovery of the demand. Complete restoration was achieved in a few hours. Around 6350 MW of load was lost, around 4500 MW in Sweden and 1850 MW in eastern Denmark, which affected 4 million people.

This blackout was caused by the sequence of events, which led the system to conditions that were beyond operating limits and prepared remedial actions. It is important to mention that the probability of such a coincidence is extremely low. The investigations recommended the review of security standards applied in the Nordic grid, grid reinforcements, the restructuring of some critical substations, the review of the methodology and procedures of the out-sourced maintenance, the inspection and replacement of critical components, operator training, the ability for house-load operation and black-start of large generation units and communication procedures to inform the public, authorities and institutions [26].

2.1.3. Italy in 2003

On Sunday, 28th of September 2003, the sequence of events was triggered by a trip of the Swiss 380 kV line Mettlen-Lavorgo at 03:01 caused by tree flashover [27]. Several attempts to automatically reclose the line were made by ETRANS (Swiss TSO) without success. A manual attempt at 03:08 also failed, because of the high power flows into Italy, which had created a too high phase angle difference in voltages between line ends. The load of the tripped line was taken over by others, causing an overload in the Swiss 380 kV line Sils-Soazza. According to the UCTE operational standards, an overload with the magnitude of this one (110%) is acceptable for a short period during emergency situations.

At 03:11, a phone conversation took place between the Swiss coordination centre of ETRANS in Laufenburg and the GRTN (Italian transmission system operator) control centre in Rome. ETRANS asked GRNT to take countermeasures within the Italian System, in order to relieve the overloads in Switzerland and return the system to a secure state. In essence, the request was to reduce Italian imports by 300 MW, because Italy imported at this time up to 300 MW more than the agreed schedule, which amounted to 6400 MW on the northern border. This reduction took effect 10 minutes after the phone call. This import reduction, together with some internal countermeasures taken within the Swiss system, was insufficient to relieve the overloads. At 03:25, the line Sils-Soazza also tripped after a tree flashover, which was likely caused by the sag in the line, due to overheating of the conductors. After losing two important lines, the additional power flow in the remaining lines created unacceptable overloads on the remaining lines in the area. Almost immediately, the line Mettlen-Airolo tripped because of high overload. In sequence the remaining interconnection lines towards Italy tripped, isolating the Italian system from the European network, taking about 12 seconds after the loss of the line Sils-Soazza. During these 12 seconds of very high overloads, instability phenomena had started in the affected area of the system. The result was a very low voltage level in northern Italy and consequently, the trip of several generation plants in Italy. Figure 2.3 shows the sequence of events in the Italian blackout.

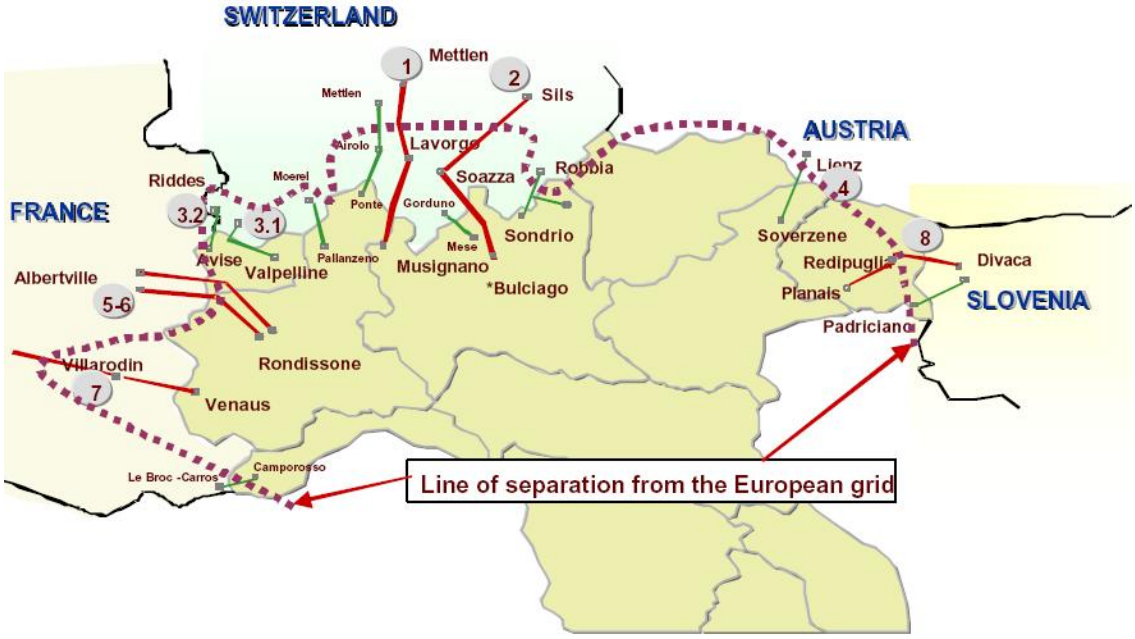


Fig. 2.3 – Sequence of events in Italy [27]

Separation of the UCTE network created a large generation deficit of nearly 6650 MW, which also caused a fast frequency drop throughout the Italian system. After separation from the European network, the fast frequency drop in Italy was temporarily stopped at approximately 49 Hz, by the primary frequency control and the automatic shedding of the pumped storage power plants and part of the load. Subsequently, additional generating units tripped. Despite the shedding of about 10000 MW of load in the Italian System, the frequency continued to decrease and the system collapsed in 2.5 minutes after the islanding, when the frequency reached the threshold of 47.5 Hz. The analysis of the UCTE system outside Italy after the splitting of the network shows that the primary frequency control performed well, limiting the positive frequency deviation. The early trip of some generation units by over frequency has also been observed, consisting of either large centralised plants units or smaller decentralised units embedded in the distribution system.

In Italy, the restoration process started immediately after the blackout. The northern part of Italy was energised before 08:00, the central part around 12:00 and the remaining parts of mainland Italy at 17:00. Sicily was fully energised at 21:40. A total of 27.7 GW of load was lost and about 57 million people were affected. The Italian system is strongly dependent of external generation to feed the supply, which leads to system's weakness through insufficient interconnection capacity. As main causes of the Italian Blackout, UCTE identified the following:

- Unsuccessful re-closing of the Lukmanier (Mettlen–Lavorgo) line because of a phase angle difference that was too high
- Lacking a sense of urgency regarding the San Bernardino (Sils-Soazza) line overload and call for inadequate countermeasures in Italy
- Angle instability and voltage collapse in Italy
- Right-of-way maintenance practices

The recommendations of the Italian blackout identified the need to perform joint operator training programs, to improve inter-TSO operational coordination and communication, to clarify and harmonize the application of the N-1 criterion, to improve day ahead congestion forecast (DACF) data, increasing the number of areas involved and the frequency of calculations in order to assess the performance of the forecasts, to extend the real time data exchange with the neighbouring TSOs, to determine on a UCTE level a set of minimum requirements for generation equipment, defence and restoration plans, and consequently improve the regulation and national grid codes, to improve load shedding control strategies, to accelerate the ongoing Wide Area Measurement System installation program, to block the tap changers

of distribution transformers in case of a severe voltage drop and, finally, to evaluate and improve vegetation management.

2.1.4. Greece in 2004

On the 12th of July 2004, at 12:39, the south part of the Greek Interconnected transmission system collapsed, after being separated from the rest of the system, losing about 4500 MW of load [28]. In the last decade, the peak of the Hellenic system has migrated from winter to summer and the system became prone to voltage instability due to the maximum power transfer from the generating areas in the North and West to Athens metropolitan area, which means a big electrical distance between generation and load. In addition, the combination, on July 12th, of the yearly peak load with the delay in planned new upgrades and some outages due to failures and maintenance, were key factors to the blackout. The voltage values in the Athens grid area were unusually low.

On the 11th of July, at 16:30, a generating unit (125 MW) in Peloponnese was out of service, causing further stress in the Athens grid area. On the 12th of July at 7:08, unit 2 (300 MW) of the Lavrio power station in the Athens area was lost due to auxiliary UPS failure. The failure was repaired, but due to further problems during start-up, the unit was only synchronized at 12:01. As the load was growing, reaching 9160 MW, the voltages in Athens area were decreasing, reaching 90% of its nominal value. At 12:12 Lavrio unit 2, still in the process of achieving its technical minimum and on manual control, was lost again due to high water level in the steam drum. This event brought the system to an emergency state, because the other generating stations in Athens and Central Greece had trouble in keeping up with the reactive power demand.

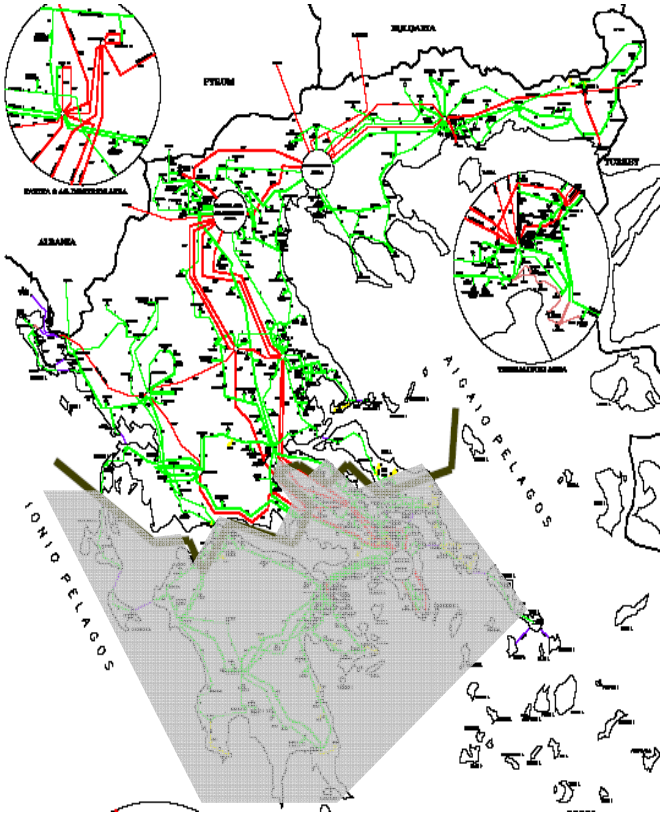


Fig. 2.4 – Affected Area [28]

At 12:22, a load shedding of 100 MW was requested by the Hellenic Transmission System Operator (HTSO). The 80 MW shed manually were insufficient to stop the voltage decline, so an additional request was made to shed 200 MW more. At this moment, the total load had reached 9320 MW. Figure 2.4 shows the affected area of the Greek transmission system.

Before the second load shedding command was executed, at 12:37 unit 3 of Aliveri power station in the weak area of Central Greece tripped automatically. At 12:38 the remaining unit 4 in Aliveri (same size) was manually disconnected. At 12:39, the system was split by the protection system of the North-South 400 kV lines and voltage collapse was now unavoidable.

The North and Western parts of the Hellenic system remained interconnected, but the excess of generation changed the flow at the north interconnections from import of 900 MW to export 1100 MW and the frequency of the UCTE interconnected system increased to 50.75Hz, creating disturbances in the neighbouring systems. The restoration of the south system started at 12:45 and it was relatively fast, with the support of the generating units of the North and West. After half an hour, all the main substations of the south were under voltage. At 14:00, 1900 MW of load had been supplied. Because of generation

unavailability, there were restrictions in supplying the whole load due to voltage constraints, but at 15:05 the first two units (Aliveri) were synchronized. The consumers were totally supplied at 17:30.

As main causes of the Southern Greece Blackout, HTSO identified the following:

- Deterioration of voltage levels
- Delay in system reinforcement during the period 2003-2004
- Network operating conditions on the event's day (outages and failures)
- Inefficient and slow load shedding procedures
- Generation units behaviour

The main conclusions and recommendations of the blackout were the installation of new generation in the south, the reinforcement of the transmission system including excess reactive compensation also in the south, the development of an automatic system for load shedding and new load management methods, and the development of the ability to monitor the stability limits of the system.

2.1.5. Greece in 2007

On the 27th of June 2007, a big forest fire in Parnitha Mountain near Athens caused a major disturbance in the Hellenic Transmission System [29]. Before the incident, the total load of the system was 9630 MW, the load in Attiki area was 3400 MW and in Peloponnisos area 940 MW. The total generation in the affected area was 1425 MW divided between hydro plants (185 MW) and thermal plants (1240 MW). The Greek System was importing 490 MW through the north border.

The forest fire was close to some OHLs that supply power to Athens and it was the cause for the one 150 kV line and one 400 kV line from Distomo – Koumoundourou trip, at 17:57 and 18:26, respectively. The tripped lines remained open due to the forest fire. At 18:32, the second 400 kV line Distomo – Koumoundourou tripped due to the fire and, simultaneously, the other double 400 kV line Acharnes – Koumoundourou also tripped due to incorrect operation of the protection system at Acharnes substation (which recognized the fault in the first protection zone instead of the second protection zone). Thus, the affected area was connected with the rest of the system with three 150 kV lines and, within seconds, the remaining lines tripped due to overload, isolating the affected area from the rest of the system.

Immediately after the disturbance, there was a loss of 1975 MW of consumption and 350 MW of generation from the Ag. Georgios thermal plant that tripped. The frequency in the isolated area reached 51.5 Hz, but the rest of the power plants in the isolated area reduced power in order to bring the frequency down to 50 Hz. In the north, the Greek Transmission System was exporting 830 MW. This resulted in loss of power in part of Athens area and part of Peloponnisos, with the rest of Peloponnisos operating in island mode, as shown in figure 2.5.

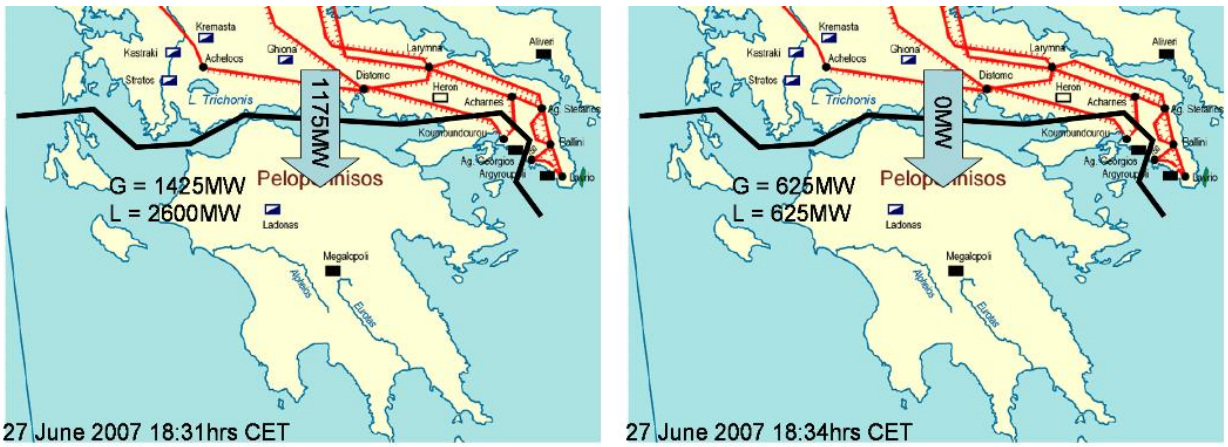


Fig. 2.5 – Conditions before and after the disturbance in Greece [29]

The restoration process was initiated right away, following the loss of supply. At 18:35, the electrical island was connected with the rest of the system, closing one of the 400 kV lines from Acharnes to Koumoundourou. All consumers were supplied through the distribution system at 19:30. Most of the power units in the affected area did not trip which aided the quick restoration of power to the consumers.

As main causes of the 2007 Greek disturbance, HTSO identified the big forest fire near Athens and the protection relay incorrect operation. As a recommendation, it was identified the need to upgrade the version of all the protection relays identical to the one with the incorrect operation.

2.1.6. Brazil in 2009

On the 10th of November 2009, at 22:13, due to extreme weather conditions with strong wind and high lightning activity, a sequence of events caused a major blackout in the Brazilian Interconnected Transmission System, also affecting Paraguay and Formosa Province in Argentina [30]. Before the blackout, the Brazilian system was being operated with N-2 security criteria; therefore they were prepared to cope with the loss of two circuits.

Figure 2.6 represents the Brazilian System divided in regions and the power flows between those regions. It is possible to observe that Itaipu Binacional, which is a hydro power plant that belongs to both Brazil (50% of the units working at 60 Hz) and Paraguay (50% of the units working at 50 Hz), was injecting about 11 GW in the Brazilian system. The 60Hz level of Itaipu power plant is connected to Foz do Iguaçu substation. Three short-circuits caused the almost simultaneous disconnection of the three 765 kV circuits between Ivaiporã (which is connected to Foz do Iguaçu) and Itaberá substations, cutting the flow in this transmission corridor that was connecting Itaipu and "Sul" area to the "Sudeste/Centro-Oeste" area (see figure 2.6). Due to the steep decrease in the voltage, first the 500 kV interconnections between Ibiúna and Bateias substations and then 4 units of Itaipu 60 Hz were disconnected, causing the voltage collapse of 3 Brazilian states. Afterwards, the HVDC links that connect the 50 Hz part of Itaipu to the Brazilian system were also disconnected, followed by the 9 units of Itaipu 50Hz, causing a blackout in Paraguay and Formosa Province in Argentina. The cascading sequence continued, disconnecting several extra-high voltage (EHV) lines and power plants in the "Sudeste/Centro-Oeste" area. The operation of several islanding protection schemes and the controlled opening of 230 kV and 500 kV OHLs prevented the spread of the disturbance to several regions that in the end were only partially or not at all affected, such as the "Sul" area. Several states in Brazil were without energy supply, the load interruption totalized 24436 MW and the average restoration time was 222 minutes.

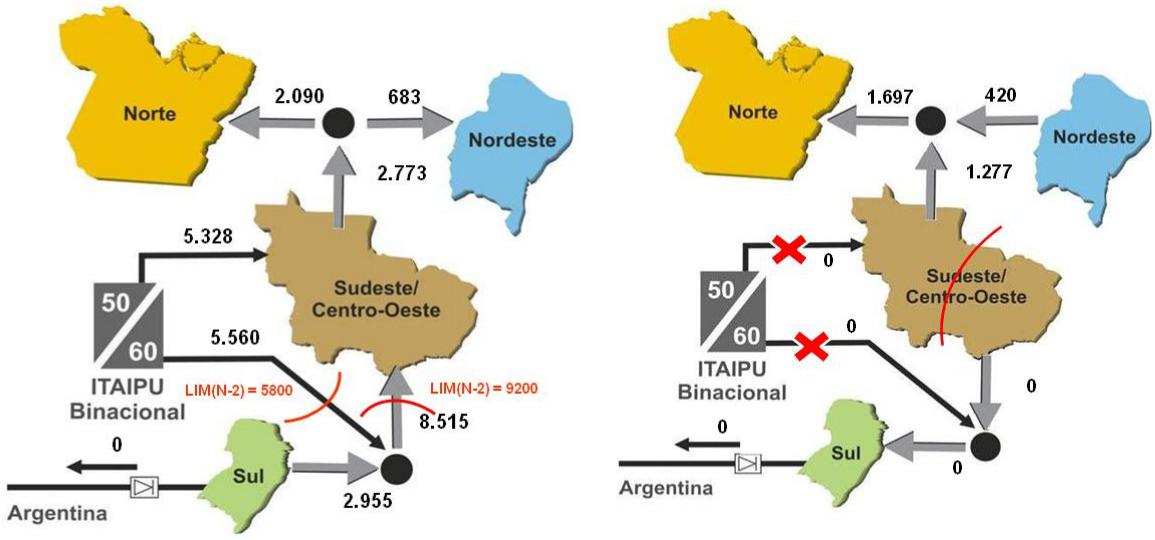


Fig. 2.6 – Conditions before and after the disturbance in Brazil [30]

At the time of the Brazilian system disturbance, Paraguay was importing around 1000 MW from Brazil and 400 MW from Argentina. The Paraguay system was supplying 45 MW to a northern part of Argentina called Formosa Province which normally has a radial connection to Paraguay, being isolated from Argentina's system due to voltage constraints. The disconnection of the 50Hz part of Itaipu power plant caused the blackout of 1000 MW in part of Paraguay and Formosa. The other part of the Paraguay system kept on importing 400 MW from Argentina, but 2 minutes later there was a failure on the interconnection circuit, not related to the previous event. As a result, Paraguay was now fully blacked out. Due to the prompt restoration of some Itaipu units and the reconnection of the interconnection with the Argentinean system, Paraguay and Formosa Province were restored in less than 1 hour.

2.1.7. Other blackouts

There are many other blackouts that are worth mentioning since 2003 in addition to the ones described in this work up to now. The previous selection includes the most representative and important ones, although it is worth to make a short description of some of the smaller blackouts, which also had impact internationally.

2.1.7.1. London 2003

On 28th of August 2003, at 18:20, a combination of events led to an electricity power supply failure in south London. On this day, scheduled maintenance was underway on one circuit from Wimbledon to New Cross and one from Littlebrook to Hurst. At 18:11, operators in the Electricity National Control Centre received a Buchholz alarm indicating that a transformer, or its associated shunt reactor, at Hurst substation, could fail, potentially with significant safety and environmental impacts. Under National Grid operating procedures, a Buchholz alarm is serious enough to warrant the isolation of equipment and reduced security is acceptable for "switching time". The switching sequence began at 18:20, disconnecting the transformer in a safe way, but leaving Hurst supplied by only one feeder (Wimbledon via New Cross). Unexpectedly, a few seconds after the switching, the automatic protection equipment on the number two circuit from Wimbledon to New Cross operated, when interpreting the change of power flows, due to the switching, as a fault, which revealed an incorrect setting on the backup protection relay. This disconnected New Cross, Hurst and part of Wimbledon from the transmission system, causing the loss of supply of 724 MW, which represents 20% of London consumption, 410.000 customers and the interruption of parts of the underground and NetworkRail system. Restoration began at 18:26 and power supplies from National Grid were fully restored at 18:57. After the blackout many actions were pursued by National Grid, among them an urgent survey of all installations as a further check on the integrity of the automatic protection equipment and the examination of all aspects of the management of the protection systems, so as to eliminate, as far as possible, the risk of incorrect installation or operation of automatic protection equipment, which was the main cause of this incident [31].

2.1.7.2. Barcelona 2007

On 23rd of July 2007, a major disturbance affected the city of Barcelona in Spain and affected 350.000 consumers. The chronology of events is the following:

1. At 10:53, a 110 kV cable of Jardi-Collblanch line fell over the 220 kV busbar 1 in Collblanch substation, causing a busbar fault. The busbar protection system acted immediately, opening all circuit-breakers connected to busbar 1.
2. Immediately afterwards, the cable touched the 220 kV busbar 2 in the same substation, again with the busbar protection system operation, tripping all the grid elements connected to busbar 2 and causing a blackout to Collblanch substation.
3. Three seconds later, the 110 kV cable of Jardi-Collblanch touched the 220 kV Collblanch – Urgell line, tripping the other circuit-end that was still connected.

4. Almost instantaneously, the 220 kV Badalona – Margall also trips, producing a blackout also in Margall and Urgell 220 kV substations.

2.2. European emergency situations

2.2.1. French blackout and Iberian islanding in 1999

The storms of December 1999 in France caused major blackouts and devastating damage from the French perspective, but from the Iberian perspective it was an emergency situation, because Iberia was separated from the rest of the UCTE interconnected for 1 hour, 51 minutes and 17 seconds. Hence, from the author's point of view, this disturbance can be described as an emergency situation.

Fig. 2.7 – Damage from the storms in France [32]

The French TSO (RTE) in reference [32] mentions a storm of unprecedented violence with devastating effects. The wind hit with incredible strength, reaching maximum speeds between 150 and 165 km/h, and in some places (coast, Orly, Vatry), the speed exceeded 180 km/h.

About 8% of the transmission network was out of service after the storm, but only 0.4% of the total length of the network was destroyed. Also 0.4% of all the towers of the transmission network were partially or totally destroyed. On the evening of 27th December, 3.9% of the substations supplying power to distributors and industrial customers were disconnected.

Fig. 2.8 – Storm effects on the French System [32]

Several tens of thousands of persons were mobilised, not to mention emergency services and help provided by volunteers, to put the overall French power system back into operation as quickly as possible and 91% of the 184 customer HV/MV substations were restored until 31st of December. The remaining substations were connected on 5th of January 2000, except 4 substations whose customers were restored through MV network. This short description helps us to imagine the extent of the damage in the French

electrical power system. Additional details about the final repairs and reinforcements of the grid can be found in reference [32].

At the moment of the Iberian separation, the frequency dropped, as shown in figure 2.9. Before, Spain was importing power from France and suddenly Iberia was supplying a part of southern France. Due to the limited transmission capacity between Spain and France, representing an important bottleneck to the Iberian system, the islanding can happen easily during an emergency situation. The Iberian Power System was synchronized with the UCTE Interconnected System at 21:44:09.

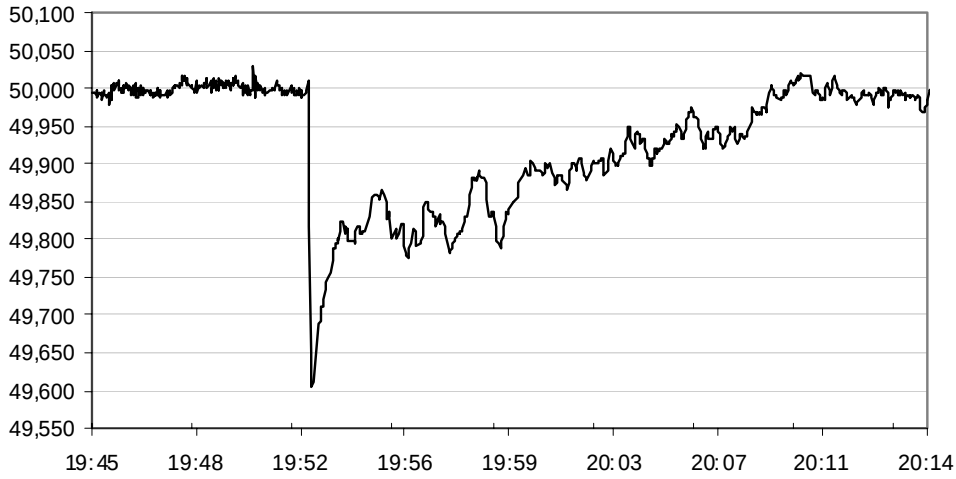


Fig. 2.9 – The Iberian frequency evolution

2.2.2. Poland in 2006

On the 26th of June 2006, a voltage instability incident occurred in the Polish Transmission System [33]. According to the day-ahead operational planning, the security criteria were fulfilled, concerning the load forecast, the programmed outages for maintenance and the generation capacity reduction. However, forced outages and an actual load higher than expected, due to unusual hot weather, created the necessary conditions for voltage instability with the risk of collapse. Through interconnection links, the Polish System had planned to export 1300 MW to central Europe and to import 300 MW from Sweden.

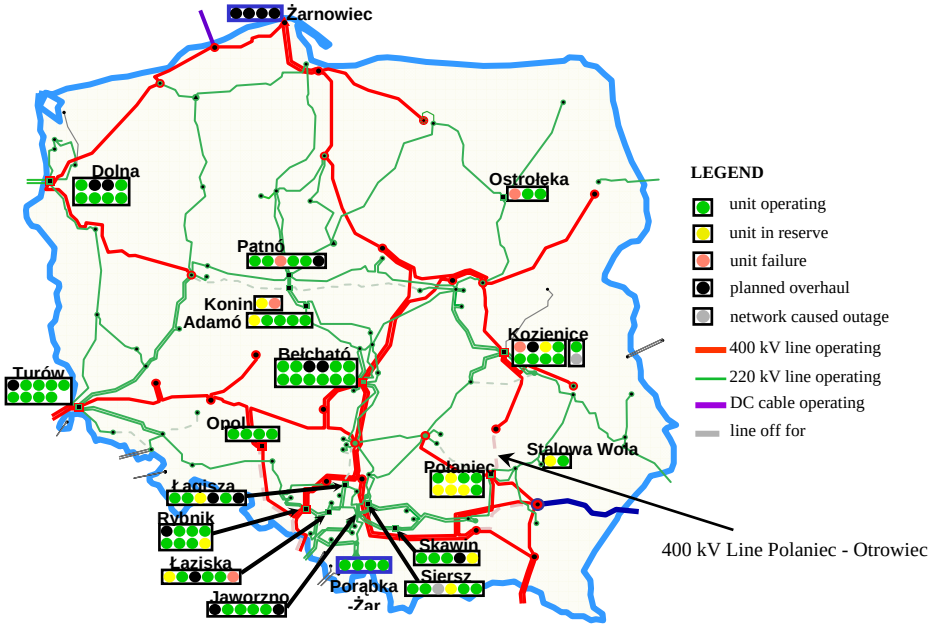


Fig. 2.10 – Generation overview in the Polish system at 12:00 [33]

Before 12:00, voltage values in 220 kV and 400 KV busbars were inside the acceptable range, although close to the lower limit. Within one hour, the load increased due to extremely hot weather and the increased active and reactive power demand caused a voltage decline and the exhaustion of the reactive power reserves in power plants. The peak load occurred at 13:00, reaching 18722 MW (ca. 600 MW above the forecast). During this period, voltage values at 220 kV and 400 kV busbars were below the acceptable limits, although lower voltages were within normal limits due to the on-load tap changing action. After 13:00, the voltage continued to drop, despite the fact that all the available generation was producing as much as possible in terms of active and reactive power, creating an emergency situation.

Around 13:08, unit 3 in Ostroleka power plant tripped due to inter-generators oscillations protection. Two minutes later, unit 2 in Ostroleka also tripped, because of low water level in the drum due to inter-generators oscillations, rendering the whole power plant unavailable. Afterwards, at 13:09, unit 7 in Konzienice power plant and 2 units in CHP Bialystok tripped, due to internal protection and low voltage in the 110 kV, respectively. At 13:12, 3 units in CHP Starachowice also tripped due to low voltage in the 110 kV. At 13:13, the outage of the DC link to Sweden (importing 300 MW) occurred due to low auxiliary voltage. The described events resulted in deficit of active power (1000 MW) and reactive power (600 Mvar) within the Polish System, further voltage decrease and increased power flows from South to North of Poland, causing overloads.

The remedial actions taken by the Polish TSO to bring the system back to a secure state were:

- Starting-up of a hydro unit in Zydowo, in order to recover the auxiliary voltage in Slupsk HVDC substation. Thus, it was possible to import from Sweden, starting with 200 MW at 14:31 and increasing gradually up to 600 MW at 15:43.
- Load shedding of 110 MW between 13:58 and 16:04 and switching off the 220 kV Ostroleka-Elk line, in order to recover the needed auxiliary voltage to start up the units in Ostroleka power plant. The synchronisation of unit 3 was made at 15:27 and unit 2 was also connected at 17:37.
- The TSO gave instructions to local power plants, which were not centrally dispatched, to increase generation in order to improve the reactive power balance.

Around 16:00, the Polish system was operating in a normal state again. The main causes of this emergency situation were the exceptional high demand, the forced outages of important generation units, the large amount of forced reduction of generation capacity during the morning, lack of reactive power injection, incapacity of generation units to operate under low network voltage and too late recognition of the emergency state by control room operators (consequently, not taking remedial actions on time).

While analysing this event, the Polish TSO understood that in case of significantly high demand the Polish power system has a too small margin for secure operation and there is a risk of voltage collapse. The need to install local reactive power sources, to monitor voltages and reactive power margin and to perform the supervision of the 110 kV level was identified, aiming to take the necessary remedial actions.

2.2.3. UCTE network in 4th November 2006

The description of this incident is presented in detail on the references [2], [34-36]. The consequences of this rare disturbance spread all over the UCTE interconnected system (now Continental Europe Regional Group of ENTSO-E) and have involved many countries and many international entities in the analysis.

2.2.3.1. Basic description

On the evening of 4th November 2006, at around 22:10 (21:10, in Portuguese Time), the UCTE interconnected system was affected by a serious incident, which had its origin in the North German

transmission grid and led to the splitting of the UCTE synchronously interconnected network into three areas (West, North East and South East).

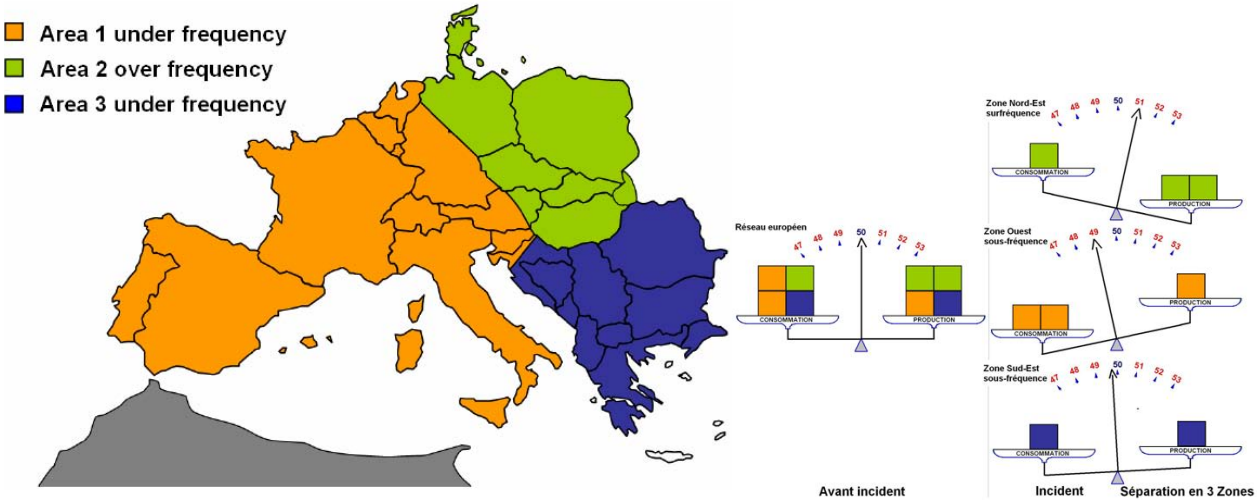


Fig. 2.11 – UCTE system split into three areas [2]

As shown in figure 2.11, Area 1 and Area 3 had a generation deficit, while Area 2 had an excess of generation. In Area 1, where the Portuguese system was included, the load shedding plan was activated by all Transmission System Operators, taking immediate action to prevent a Europe-wide blackout, according to the UCTE security standards. With the load shedding, it was possible to mitigate quickly and effectively the imbalance between supply and demand. The amount of load and pumps shedding can be observed in figure 2.12.

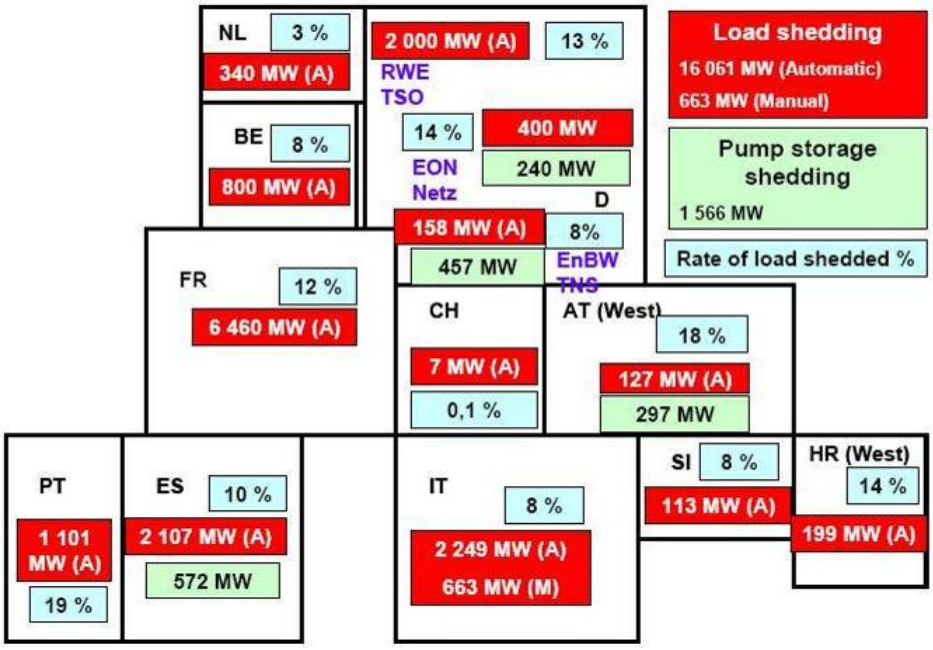


Fig. 2.12 – Load and pumps shedding by TSOs [2]

Immediately after the frequency drop, some generation units tripped, thus increasing the imbalance between demand and supply in the area. The most significant part of the generation which tripped were small power units, but they are numerous and not directly controlled by TSOs. About 40% of the total power which tripped during the incident was generated by wind power units. Moreover, 60 % of the wind generation connected to the grid at 22:09 tripped just after the frequency drop. Similarly, 30% of combined-heat-and-power in operation just before the event, tripped during the frequency drop. In the Western area, a total of about 10.900 MW of generation tripped.

In the origin of this incident was the manual disconnection of the double-circuit 380 kV Conneforde-Diele line (E.ON Netz), at 21:38, to allow the crossing of the ship “Norwegian Pearl” under the overhead lines. Before, at 21:29, according to E.ON Netz, a load flow calculation made by E.ON Netz did not indicate any violation of limit values. Based on an empirical evaluation of the grid situation, E.ON Netz staff assumed, without numerical computation, that after switching of the Conneforde-Diele line the N-1 criterion would be met in the system. Around 21:30, TenneT and RWE TSO confirmed to E.ON Netz that the flows between Germany and The Netherlands were high, however since TenneT and RWE TSO grid would be secure, TenneT and RWE TSO gave its agreement to the switching operation of the Conneforde-Diele lines.

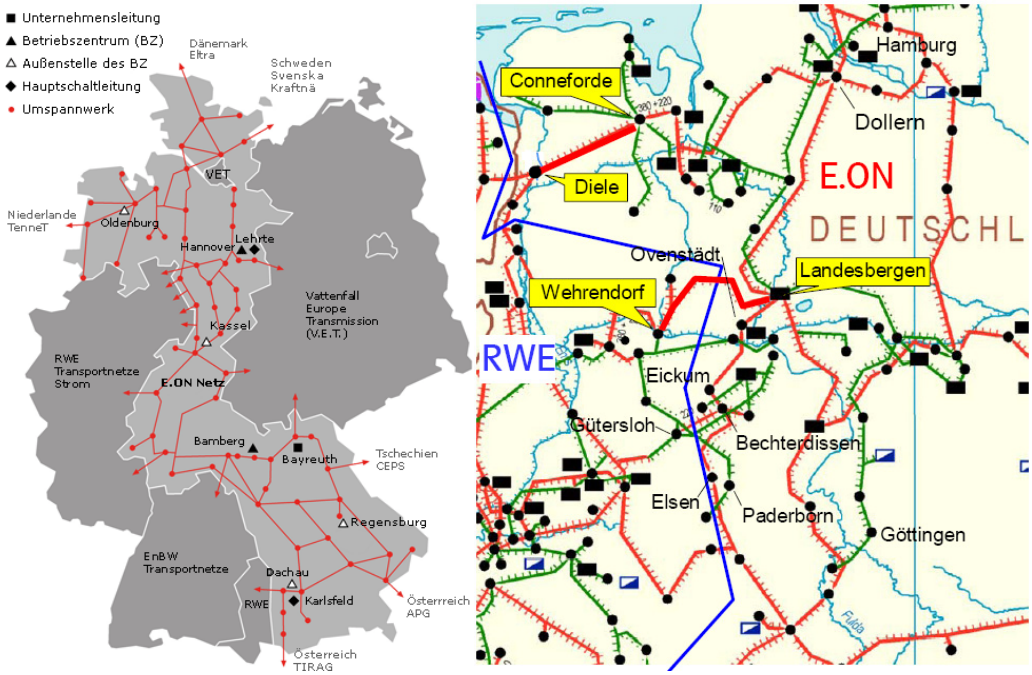


Fig. 2.13 – E.ON network in Germany [34]

At 21:41, RWE TSO informed E.ON Netz about the safety limit value of 1795 A on the line Landesbergen-Wehrendorf (an interconnection line between E.ON Netz and RWE TSO). However, at this point of time the current on this line was still under the given limit, and the N-1 criterion was still met in the internal RWE TSO network.

Between 22:05 and 22:07, the load on the 380 kV line Landesbergen-Wehrendorf increased by 100 MW exceeding the warning value of 1795 A for RWE TSO. At this point, it is important to mention that, according to E.ON Netz, dispatchers were not aware of the settings in the protection system in Wehrendorf (RWE TSO substation) and therefore the dispatchers did not take into account the correct values for their evaluation of the situation. This triggered an immediate reaction of RWE TSO that called E.ON Netz at 22:08 with the request for urgent intervention to restore safe grid operation. E.ON Netz made an empirical assessment of corrective switching measures without any load flow calculations for checking the N and N-1 criterion. E.ON Netz expected that coupling of the busbars in the substation of Landesbergen would result in a reduction of the current by about 80 A. This manoeuvre was done at 22:10 without any further coordination with RWE TSO due to necessary rush, and it had the opposite consequence.

At 21:10, following the tripping of the interconnection lines between E.ON Netz – RWE TSO Wehrendorf – Landesbergen and Bechterdissen – Elsen, a cascading sequence happened (see details in figure 2.14).

Nr.	Zeit	kV	Leitung
1	22:10:13	380	Wehrendorf-Landesbergen
2	22:10:15	220	Bielefeld/Ost-Spexard
3	22:10:19	380	Bechterdissen-Elsen
4	22:10:22	220	Paderborn/Süd-Bechterdissen/Gütersloh
5	22:10:22	380	Dipperz-Großkrotzenburg 1
6	22:10:25	380	Großkrotzenburg-Dipperz 2
7	22:10:27	380	Oberhaid-Grafenrheinfeld
8	22:10:27	380	Redwitz-Raitersaich
9	22:10:27	380	Redwitz-Oberhaid
10	22:10:27	380	Redwitz-Etzenricht
11	22:10:27	220	Würgau-Redwitz
12	22:10:27	380	Etzenricht-Schwandorf
13	22:10:27	220	Mechlenreuth-Schwandorf
14	22:10:27	380	Schwandorf-Pleinting

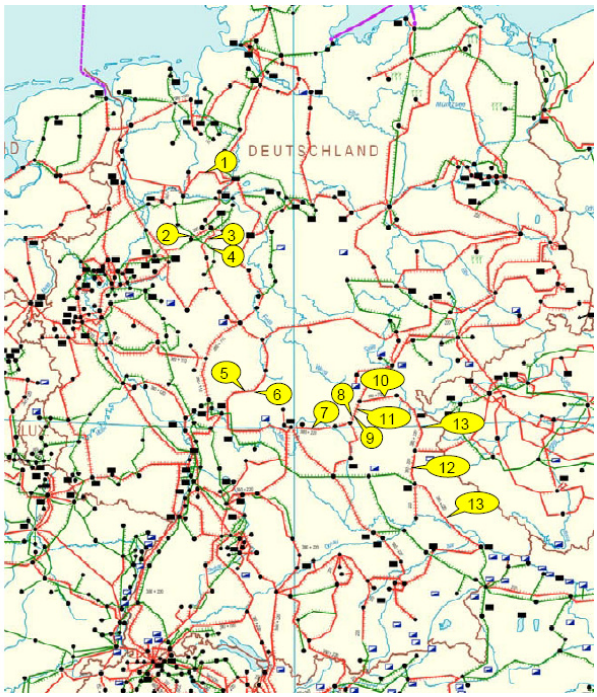


Fig. 2.14 – Time sequence of the cascading tripping in Germany [2]

The preparations to reconnect tripped lines started immediately after 22:10, but due to the huge differences in frequency values, successful switching on the lines required extraordinary measures. There were several unsuccessful attempts to re-close the open lines. Finally, at 22:47, successful resynchronization took place first on the 380 kV line Bechterdissen-Elsen. Further lines were switched-on very quickly and after 6 minutes (at 22:53) already nine 380 kV and four 220 kV lines on the border between area 1 and area 2 were in operation in Germany and in Austria. The restoration sequence was finally finished in Germany, at 23:24, with 17 transmission elements re-closed. The resynchronization sequence was finished, at 23:57, when the last 400 kV line between Croatia and Hungary was switched on.

The very rapid splitting of the interconnected system could not be stopped once the cascade tripping of the lines had started. Due to the good performance of countermeasures activated at UCTE level in the individual control areas, a Europe-wide blackout has been avoided.

2.2.3.2. Main causes

The three identified main causes for this incident were:

- Non fulfilment of the N-1 criterion - after manual disconnection of the double-circuit 380 kV Conneforde-Diele line (E.ON Netz), the N-1 criterion was not fulfilled in the E.ON Netz grid and on some of its tie-lines to the neighbouring TSOs.
- Insufficient inter-TSO co-ordination – the initial planning for switching-off the double-circuit 380 kV Conneforde-Diele line scheduled for 5 November from 01:00 to 5:00 was duly prepared by the directly involved TSOs (E.ON Netz, RWE TSO and TenneT). However, the change of the time for this switching manoeuvre was communicated by E.ON Netz to the other directly involved TSOs at a very late moment; it was also not sufficiently prepared and checked in order to ensure the secure operation of the system in this area after the switching-off. No specific attention was given by E.ON Netz to the fact that the protection devices have different settings on both sides of the Landesbergen-Wehrendorf line although this information was critical due to the very high flow on this line.

– Non performance of a study - when E.ON Netz was coupling the busbars in the substation of Landesbergen, expecting a reduction of the current by about 80 A. Current that actually increased with the manoeuvre.

Summing up, the critical factors identified in the UCTE report were the generation behaviour (significant amount of generation units tripped due to the frequency drop), the lack of control of the embedded generation, the uncontrolled reconnection of generation, the limited range of action available to dispatchers for handling grid congestions, the TSO/DSO coordination in the context of defence and restoration plans, the coordination of the resynchronization process (several unsuccessful attempts to put tie-lines back into operation and to resynchronize the three different areas with only a partial view of the status of the whole grid) and the training of dispatchers (joint simulation training with neighbouring TSOs has to become a common practice).

Additionally, the ERGEG recommendations are summarized in the need for an improved legal and regulatory framework to minimize the risk of future interruptions and in the implementation of measures by TSOs in order to assure secure and effective coordination and cooperation among each other.

With this European-wide incident, UCTE has the responsibility of assuming an even more preponderant role in the operation rules, in order to prevent incidents like this one. The supply of more than 15 million European households was interrupted by this disturbance.

2.2.3.3. Portuguese perspective

The Portuguese system was part of Area 1, where the frequency dropped abruptly, reaching 49Hz, because of the generation deficit. Figure 2.15 presents the relationship between the frequency (in Area1) and the load shed/connected.

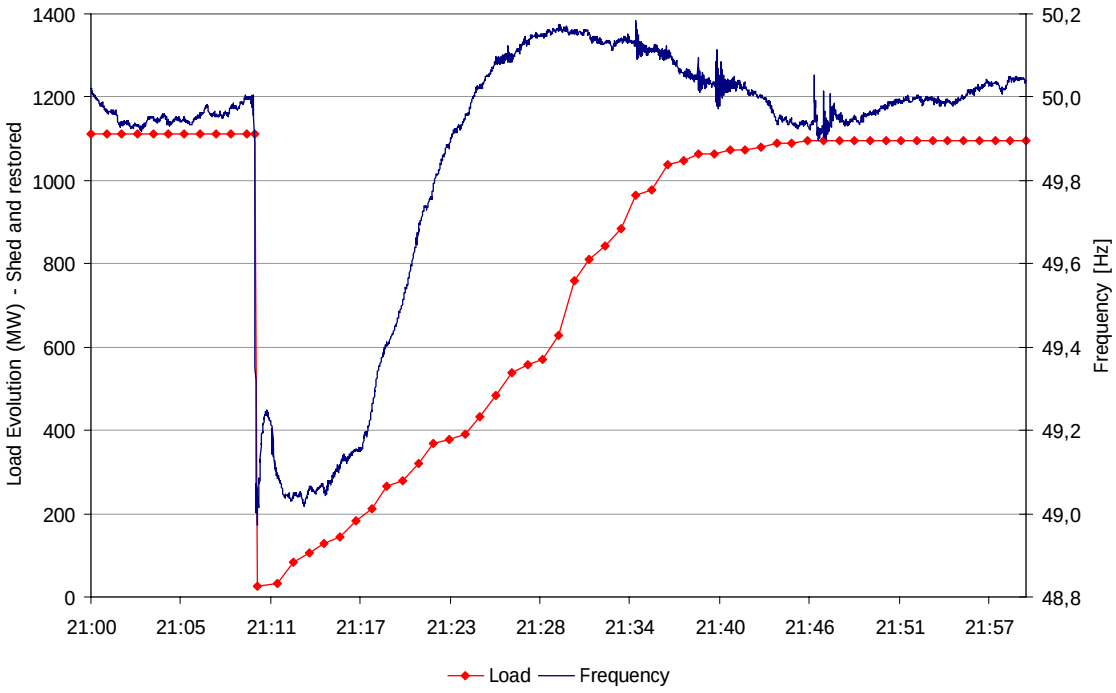


Fig. 2.15 – Frequency and Load Evolution on 4th November 2006

In figure 2.15 it is possible to observe the frequency's sharp drop until 49Hz, followed by a quick recovery of more than 0.2Hz, which is explained by the load shedding and the primary reserve contributing to frequency support. Then again a mild decrease caused by generation trip and non-coordinated load restoration and finally a marked recovery with the secondary and tertiary reserves.

2.2.4. Island operation in Jutland- Funen in 2007

On 29th of May 2007, at 09:49, a current transformer exploded in the Wilster 380 kV substation in Germany [37]. The protection system saw this event as a fault in the two substation's busbars and therefore tripped all circuit breakers connected in the substation. Consequently, the 380 kV lines to Audorf were disconnected in one of the circuit-ends.

At this time, around 1100 MW was being exported from Denmark to Germany and the 380 kV/110 kV transformer in Audorf tripped due to overload (there are no more 400 kV links between Western Denmark and Germany). Consequently, also the 220 kV connections between Denmark and Germany tripped due to overload. This was the beginning of a cascading sequence of events, involving the tripping of the 220/110 kV transformer in Flensburg, the 220/150 kV transformer in Ensted, the 220 kV lines between Ensted and Flensburg and between Kassø and Flensburg and finally the 220 kV lines between Audorf and Flensburg. As a result, at 09:50, Western Denmark and Flensburg were in islanding operation mode with an increase of the frequency value, which stabilized at 50.3 Hz after a couple minutes. The frequency in the UCTE interconnected system decreased to 49.95 Hz, due to the loss of the imported power through the disconnected tie-lines and loss of generation.

The synchronization of the Western Danish System with the rest of UCTE was accomplished by E.ON Netz when connecting the 380 kV lines between Audorf and Wilster. The frequency deviation between the two systems was approximately 300 mHz before Western Denmark and Flensburg again were synchronous with the rest of the UCTE. According to E.ON Netz, the 220 kV grids could not be connected until about 20 minutes after the fault occurred due to a relatively large phase difference. The UCTE system was fully re-established at about 11:00.

2.3. Recent Portuguese disturbances

The Portuguese blackouts description is based mainly on the internal reports, such as [38-40]. The 9th of May 2000 incident was presented at CIGRE Workshop on Large Disturbances [41].

2.3.1. 9th of May 2000

"A simple incident with serious consequences", this was the definition of this incident cited in REN's internal publication.

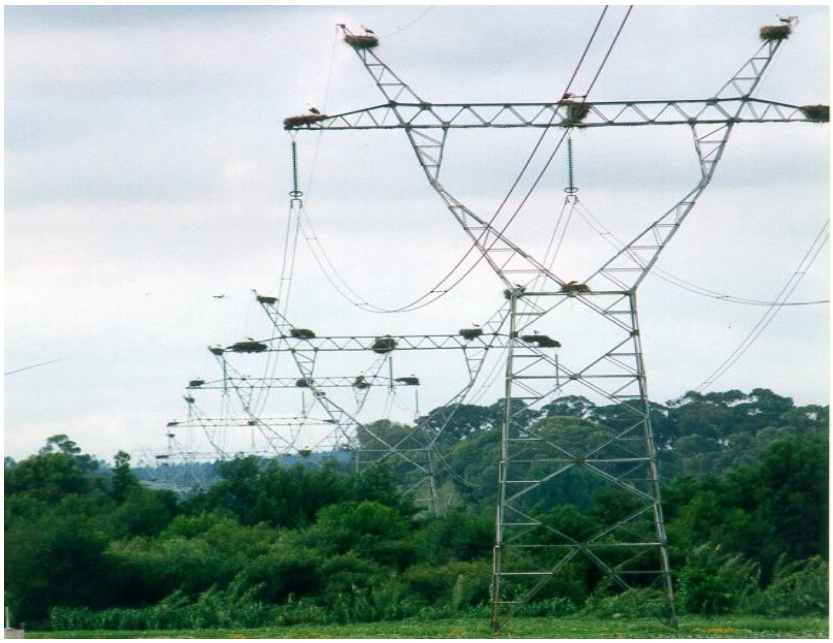


Fig. 2.16 – Stork nests located in the affected overhead line

On the 9th of May 2000, at 22:17, a short-circuit occurred in one of the two 400 kV overhead lines which establish the connection between Recarei and Rio Maior substations. The short-circuit was single-phase to earth and tower number 327 was identified as the origin spot. The incident's initial cause was a stork whose nest was located over the affected phase. Figure 2.17 shows the stork's nest and the electrocuted stork on the ground near the tower.

Fig. 2.17 – Short-circuit origin location and Electrocuted Stork

The clearance of this short-circuit should have been made by the tripping and consequent opening of the appropriate circuit-breakers, which are located at each circuit-end of the faulty overhead line, but the lack of operation of Rio Maior circuit-breaker occurred, caused by a bad indication of the line disconnector.

In spite of the opening of Recarei circuit-breaker, the short-circuit remained fed by Rio Maior.

The protection system at *Rio Maior* had operated correctly, but the described fault in the circuit-breaker, has provoked the operation of the breaker failure protection. The breaker failure protection issued trip orders to all the circuit-breakers connected to the busbar where the fault was located, but the 400 kV busbar coupler did not open because of wrong cabling. The other circuit-breakers did not open because the current caused by the fault did not reach the set limit for tripping.

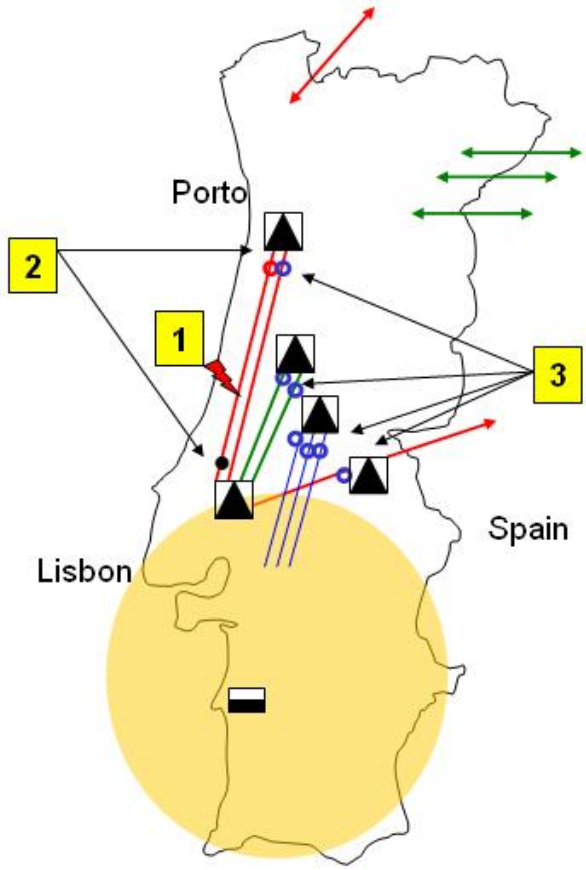


Fig. 2.18 – Incident tripping scheme

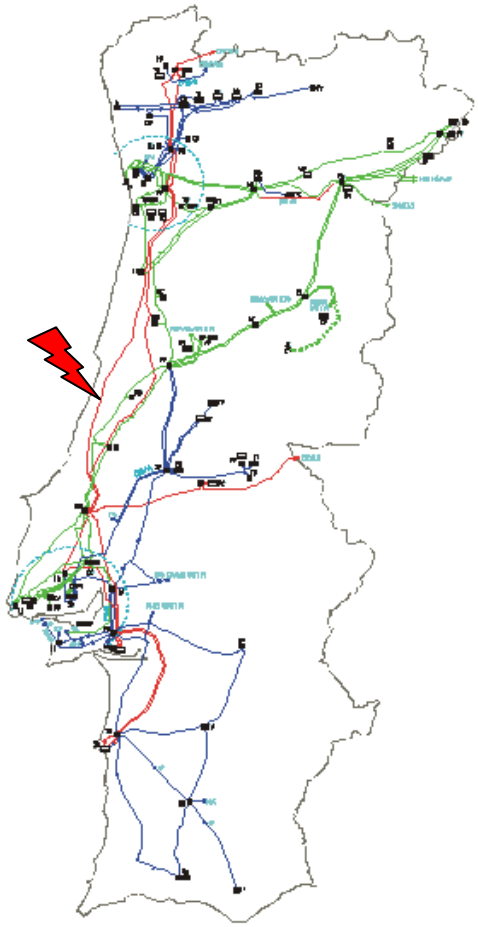


Fig. 2.19 – Incident's Location in the network

Thus, the short-circuit remained fed by all the overhead lines connected to Rio Maior substation (4 400 kV overhead lines and, through the 2 autotransformers, 6 220 kV overhead lines), that consequently tripped at the opposite circuit-ends (as shown in figure 2.18).

The opening of the overhead lines connected to Rio Maior provoked a zero voltage situation at the substation and the interruption of the North –South corridors of 400 kV and 220 kV.

The remaining 150 kV overhead lines of the North–South corridor tripped almost immediately, after the 400 kV and 220 kV lines, due to overload, ending the cascading phenomena and creating an isolated south island (represented by the yellow circle in figure 2.18).

At the moment of the incident, the production in the southern area was mainly ensured by the power plant *Central de* Sines (CSN) with approximately 900 MW of production. The total load in the south was about 1700 MW, which implies the existence of a strong transit from North to South (800 MW) before the incident, due to favourable Hydroelectric conditions, as shown in figure 2.20. In the North part of Portugal the production was 3600 MW in total.

The favourable hydroelectric conditions due to the presence of an abnormal amount of rain in the previous weeks caused an asymmetry in the generation pattern.

The generation deficit in the South island, created by the cascading trips, originated a collapse (frequency and voltage), causing the South power plants to trip.

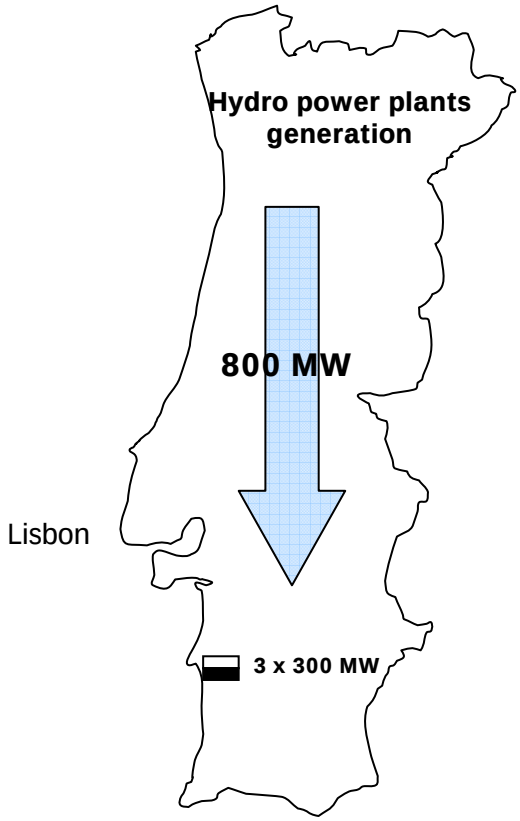


Fig. 2.20 – North-South power transfer

With all the substations located in the south of Rio Maior without power, the service restoration was initiated 3 minutes after the beginning of the incident by an automatic device in one of the affected substations. About 20 minutes later, most of the EHV overhead lines that feed directly consumption delivery points were connected. The restoration process was completed after 1 hour and 10 minutes, with the exception of one substation, where the restoration process took 2 hours and 21 minutes due to telecontrol problems. In the meantime, the suitable remedial actions were performed by control room operators in order to ensure the system balance and to maintain the voltage within the acceptable range.

In this incident, 1900 MW of consumption was lost and approximately 5 million people were affected. This incident has emphasized the importance of maintenance and commissioning procedures, operator training, network reinforcements and the need of the new interconnection line with Spain, located further south than the existing ones, which was put into service at the end of 2004. The new interconnection line would have prevented this major event, because it would have been able to compensate the unbalance between generation and consumption in the south of Portugal.

In chapter 5, it is possible to observe through incident's statistics that every year storks cause tens of incidents in the Portuguese transmission system, which normally goes unnoticed.

2.3.2. 6th of September 2001

On the 6th of September 2001, at 15:42, a major disturbance in the Portuguese transmission system occurred and interrupted the energy supply to the South of Portugal. The incident started with the trip of *Palmela – Sines 2* 400k kV overhead line, because of a single-phase to earth short-circuit caused by the insulators' cleaning process in Palmela substation, as it is possible to observe in figure 2.21.

The overhead line was being operated in a special exploitation regime justified by the live line work, thus it didn't have the automatic recloser active and both circuit-end breakers remained open.

Simultaneously with the opening of Palmela – Sines 2 overhead line, the opening of Palmela – Sines 3 overhead line only in Palmela substation occurred, caused by the incorrect operation of the circuit-end protection system. This overhead line was also operated in a special exploitation regime justified by the same reasons as the previous line. The cleaning action of insulators in several towers was being performed. The simultaneous loss of both 400 kV overhead lines, which connect Palmela and Sines substations, provoked a change in the power flows. The flows that were being carried by those lines to the North (around 1200 MW) caused serious overloads in the 150 kV overhead lines and, consequently, they tripped. With the 400 kV and the 150 kV overhead lines disconnected, the Portuguese transmission system was separated in two parts:

Fig. 2.21 – Cleaning under voltage

- North of Sines substation, which was interconnected to Spain.
- South of Sines substation, which was an isolated island.

In the isolated island, shown in figure 2.22, the generated power (1262 MW) exceeded the consumption (486 MW), creating an imbalance in the affected area.

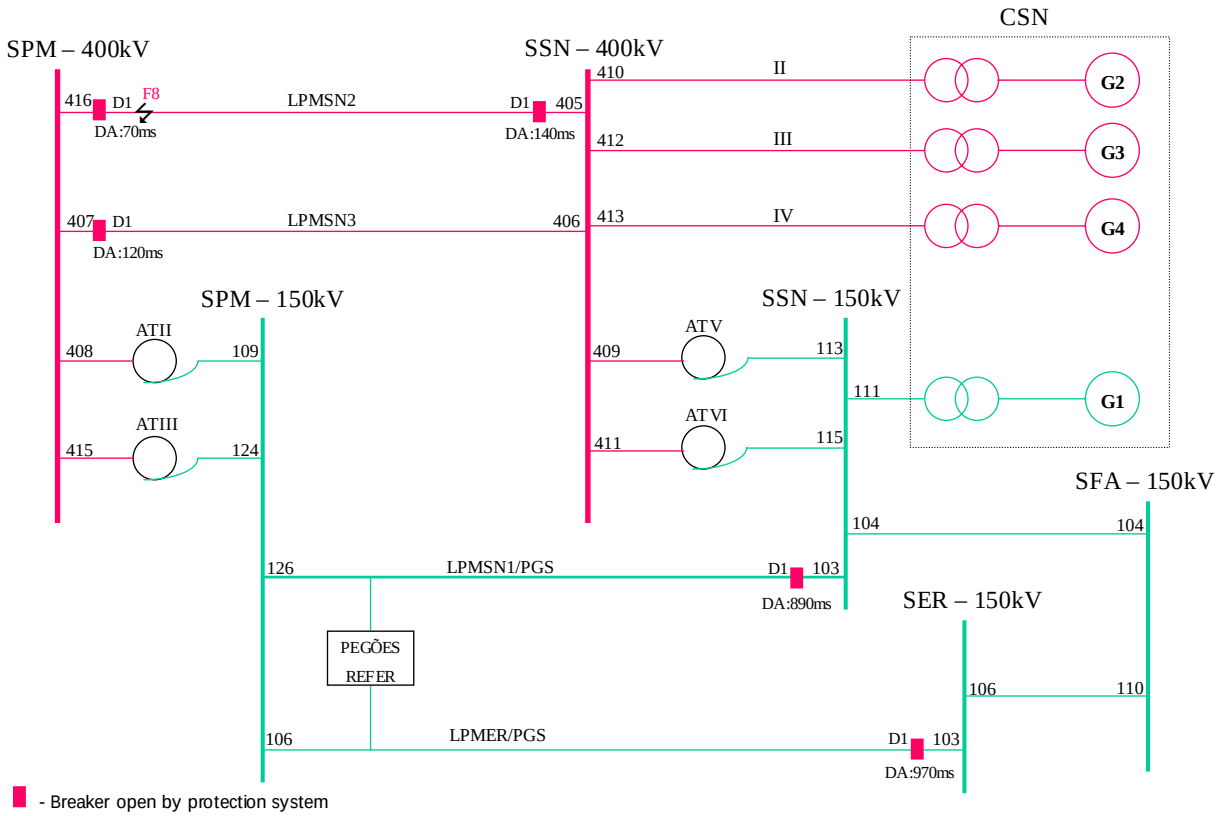


Fig. 2.22 – Separated network scheme in 6/09/2001

The Southern area was isolated for 4 minutes and a half, but a stability loss of the thermal power plant in this area made the collapse inevitable. The entire network in the South of Sines substation was without energy supply. The control room operators followed all the phases of the occurrence. The interconnection flow between Portugal and Spain suffered a deviation of 760 MW to compensate the lack of generation in

the North area, but this deviation was corrected in just about 11 minutes, according with UCTE requirements.

The restoration process in this incident started immediately after the blackout and all substations were connected after 35 minutes. As every major disturbance also this event was accurately analysed and recommendations were made in order to improve the power system performance and to reduce risk of operation, such as the special exploitation regime (used for live line work) cannot be implemented simultaneously in two overhead lines that have a circuit-end connected to the same substation. Once again, the importance of maintenance and commissioning procedures was emphasized. The need of the new interconnection line with Spain, which was put into service at the end of 2004, was again obvious in this incident.

2.3.3. 2nd of August 2003

On the 2nd of August 2003, at 14:17, another major disturbance in the Portuguese transmission system occurred caused by several forest fires in the southern part of Portugal.

Fig. 2.23 – Forest Fires under overhead lines

First, the 400 kV overhead line Palmela – Sines 3 tripped and, after one minute, the trip of the second 400 kV overhead line Palmela – Sines 2 occurred. Both disconnections were caused by forest fires. Obviously, the simultaneous outage of the 400 kV lines provoked the change of the flows in that network area. The excess of generation in relation to the consumption in the southern area was 700 MW and it was transferred to the northern area through the 150 kV overhead lines. The power flow on the 150 kV overhead lines caused serious overloads and, consequently, immediate tripping, creating two independent areas in the Portuguese transmission system, namely:

- North of Sines substation, which was interconnected to Spain.
- South of Sines substation, which was an isolated island.

The instability of the isolated island caused by the lack of balance between generation and consumption has led to the trip of all the power units of Central de Sines (generation in the southern area), causing the collapse and blackout of the entire southern area.

Central de Sines is a slow thermal coal power plant and it took some time before being able to generate again, which meant that without the possibility of connecting the 400 kV *Palmela – Sines* overhead lines, the consumption connected in the south area was limited to the capacity of the 150 kV corridors that connect the northern to the southern area.

The restoration process in this incident started immediately after the blackout and it was completed at 15:12. Unfortunately, the forest fires that originated the first blackout were still active, causing many trips in the vicinity overhead lines.

At 15:39, both 400 kV overhead lines between Palmela and Sines tripped, causing a 350 MW generation deficit instead of an excess. This deficit was the difference between the generation of Central de Tunes (fast power plant in the south) and the consumption already connected. Thus, to mitigate the mentioned deficit and the existing overload in the 150 kV overhead lines, it was necessary to perform load shedding at the Distribution level, following REN instructions, in order to prevent the repetition of their disconnection.

The load shedding process took into account the consumption evolution, continuously controlling the power flow on the 150 kV overhead lines. At 18:51, the first unit of Central de Sines was connected, but the 400 kV overhead lines remained out of service. At this point, a very slow connection of consumption was initiated. Approximately at 19:45, the second unit of Central de Sines and both 400 kV overhead lines between Palmela and Sines were also connected. From this point on, the entire load was promptly supplied. This incident was classified with a force majeure cause.

2.3.4. 23rd of December 2009

On December 23rd at dawn, Portugal faced extremely severe wind conditions, affecting two localized areas [42], namely the regions of Centre-West and Algarve. This meteorological phenomenon is called explosive cyclogenesis.

In spite of the 27 damaged pylons, placing 6 circuits out of service, including two double and two single OHLs, plus one circuit under construction, there was no supply interruption caused by the transmission grid, which is extremely meshed. Only on the distribution network level, there was energy not supplied due to further damage in the distribution network.

This is an exceptional phenomenon that occurs rarely and there is no memory of anything similar in the last 60 years in the Portuguese transmission system. However, there was a similar phenomenon, more than one decade ago, that caused less damage affecting only a few towers of a double circuit that was also affected by this disturbance. Figure 2.24 shows the destruction caused by the strong winds.

Fig. 2.24 – Illustration of the destroyed pylons in the PTS on the 23rd December 2009

In the Centre-West region, the 4 circuits that were out of service have affected the connection between the north and the south of the country, creating the need for a different generation pattern than the one being used, in order to operate the transmission system, fulfilling security criteria. At that moment, the

generation pattern was mainly composed by hydro power plants in the north and their output was reduced in response to the disturbance, starting more units in the south. In the Algarve, it was necessary to start local gas units during peak load periods.

Figure 2.25 shows wind measurements at the moment when this phenomenon occurred. The Meteorological Institute estimated wind gusts of 220 km/h.

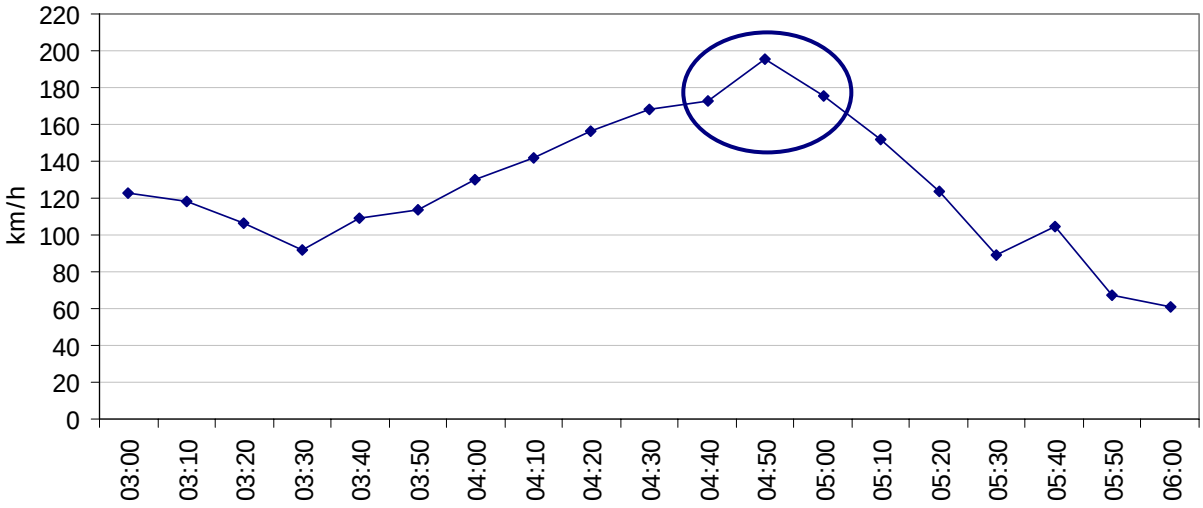


Fig. 2.25 – Wind speed measurements at the time of the incident

Six weeks after the disturbance, the first damaged OHL was returned to service.

2.4. Discussion

First, it is important to mention that many blackouts have as their initial cause force majeure events, such as forest fires, lightning, storms and hurricanes, which are unavoidable, although their consequences can be mitigated. Hence, blackouts cannot be completely avoided, but we can be better prepared to face them.

Recently, disturbances have become more frequent and the need to evaluate their risk more urgent. Whenever an incident occurs, after an accurate analysis, it is crucial to be able to learn, to identify the improvement points and to perform the changes that are needed. So, many fundamental lessons are learned from it, which helps to avoid repeating the same mistakes.

After a major disturbance, most of the TSOs normally gather a task force to issue recommendations and actions that should be quickly implemented, aiming to improve the power system performance in terms of reliability and quality of service, which is a continuous goal. Finally, this can be seen as a risk avoidance procedure.

After analysing the presented blackouts, it is possible to identify many similarities in the initial causes and in the recommendations that are presented by the investigation committees. At this point, it is relevant to point out the following question: What lessons should we have learned by now with all these blackouts?

For instance, according to North American Reliability Council (NERC), the August 14th 2003 blackout in the USA and Canada had many similarities with previous large-scale USA blackouts, including the 1965 Northeast blackout that was the basis for forming NERC in 1968, and the July 1996 outages in West USA. The common identified factors included: conductor contacts with trees, inability of system operators to

visualize events on the system, failure to operate within known secure limits, ineffective operational communications and coordination, inadequate training of operators to recognize and respond to system emergencies, and inadequate reactive power resources.

Also in the blackout of September 28th 2003 in Italy, vegetation management was pointed out as an issue to be handled in order to prevent cascading events. Asset management is required for a reliable performance and this includes equipment maintenance practices, adequate commissioning procedures and environmental related actions, e.g. stork nests (as is the case in Portugal) and vegetation management.

Forests fires are also a very serious problem, which affects especially the Southern European countries. In the described incidents, it is possible to find two, where the initial cause was forest fires (2nd of August 2003 in Portugal and 27th of June 2007 in Greece). These kind of natural disasters go beyond the TSO responsibility, so a national plan is needed to avoid or mitigate their consequences.

The Brazilian blackout in 2009 is an example of how extreme weather conditions can cause severe disturbances, so that even when systems are operated to withstand an N-2 loss of components it may not be enough, because an N-3 event can always occur. This disturbance also illustrates how it can spread to neighbouring systems and how special protection schemes that force the system separation (islanding) can help prevent even worse consequences in such large interconnected systems.

The 4th of November 2006 disturbance, which is the most significant disturbance in the UCTE synchronous interconnected system, can be considered a case of success, despite many improvements that were identified as necessary. The consequences of cascading were limited, because prompt and automatic actions were taken by all affected TSOs, according to the ENTSO-E Operation Handbook policies [6]. Although the whole European system was facing an emergency situation, in the restoration process, each TSO acted according to its own internal rules without any special coordination or knowledge of the other control areas within the split system. Hence, some attempts of resynchronization failed.

Improved coordination, communication and data exchange between TSOs is a crucial point, which has appeared in the recommendations for three of the described blackouts (14th of August 2003 in USA, 28th of September 2003 in Italy, 4th of November 2006 in UCTE and in 10th November 2009 in Brazil). Coordination among TSOs in large and interconnected transmission systems is essential in every operating state. Although there is still a need for better coordination and communication, it is worth to mention that several mechanisms have been developed to improve day-ahead information exchange, such as DACF[1] in the ENTSO-E Continental Europe interconnected system, where System Operators make available a snapshot of their system's forecasted operating conditions for the next 24 hours.

Everyone agrees that effective coordination and communication are vital for a successful and secure system operation and, therefore, reduce risk exposure. Mutual understanding and coordination facilitates real-time operation and response to emergency situations in one or more control areas of the interconnected system. The interaction and cooperation among neighbouring TSOs has to go beyond day-ahead information exchange, so coordinated real time security assessment and operation is required. And it will provide an important platform, helping operators to be aware of the overall system security beyond their borders. For example, between the Portuguese and Spanish TSOs, real-time information is exchanged within SCADA, allowing operators to monitor and assess, in terms of security, the relevant part of each grid from the neighbour's point of view.

Again in the 14th of August in USA 2003, 28th of September 2003 in Italy and 4th of November 2006 in UCTE, it is possible to identify as common denominators the inappropriate estimation and understanding of the situation in the interconnected system and bad operator decisions when dealing with an emergency situation, which further increases the disturbance development.

[1] DACF data sets are AC load flow calculation input data sets given in the UCTE format and corresponding to the forecast state of the transmission grid (topology, loads and generation pattern) at a determined time stamp of the day-ahead.

Automatic load shedding has proven to be crucial every time that load and generation are imbalanced, especially on the 4th of November 2006 disturbance, where it played a preponderant role to avoid a total blackout in one of the areas. The improvement of load shedding strategies has appeared as a recommendation in the 28th of September 2003 Italian blackout and in the 12th of July 2004 Greek blackout, because of the need to balance load and generation after an islanding situation. After the 4th of November 2006, this recommendation became crucial not only at national but also at international level, because it has to be part of the European defence plan, which is another step to avoid risk.

In the same line of thought goes the review of operational standards and security procedures, which again appear as a recommendation in several of the described blackouts, because this is an issue which must be clarified and harmonized through the UCTE Operation Handbook [6].

Every time some equipment fails and causes an incident, one of the actions resulting from the incident analysis is to check that equipment in particular as well as all the others of the same model that are installed in the system. In this way, it is possible to avoid the repetition of the same failure in the grid. It is also important to have accurate commissioning and testing procedures that will help to minimize the risk of misoperation.

One of the most frequent recommendations deals with operator training. Operator training using simulators is one of the best ways to provide control room operators with the skills to deal with consequences of unforeseen disturbances that put the system in an emergency situation. In most cases, the impact of a blackout's damage can be reduced by operators taking the right decisions and actions at the right time. The Portuguese TSO has a Dispatcher Training Simulator since 2001 and it was after the 9th of May 2000 incident that the need and benefits of operator training became more clear and urgent. More attention was also focused on emergency training since the 2003 international blackouts. This topic will be further developed in this thesis in section 4.9.

Finally, the need to improve real-time information and the development of new support tools, mentioned also in many of the blackouts, is one of the biggest motivations for this research work. Having the experience of working at the back office of a control room for the last nine years, the author knows that operators appreciate every tool, no matter how simple, that can support their work. Furthermore, having a security indicator and being aware of the system's security margin is extremely useful to them, as in the example presented in reference [5]. This appreciation and usefulness gives meaning to the development of an online risk assessment tool to be used in the control rooms of the Portuguese TSO.

Following the analyses and discussions presented in this chapter, it is probably easier to understand that blackouts are normally the result of a combination of events with different causes. Of course, there is always an initial cause, but in most cases that cause is followed by other unforeseen events. The performance of a power system is dependent on a diverse set of features, beyond the unavoidable natural causes already mentioned. Among those that can play a crucial role in the power system's performance, it is possible to identify the control room operators, the SCADA and EMS system, the hidden failures and protection system malfunctions, the asset management policies and strategies, the additional existing support tools, the national grid code and operating procedures. All these topics are going to be further developed in this thesis.

2.5. Conclusion

In this chapter several disturbances that happened throughout the world are described. They have increased the awareness of TSOs for these major events. Following their analysis, many improvement and corrective actions were taken by several TSOs; new procedures were also developed and implemented. The presence of adverse conditions increases the risk of major disturbances and the security analysis should take them into account because of the increased probability of multiple events.

Chapter 3.

State of the Art

3.1. Introduction

The application of Power System Risk Assessment (PRA) has gained increased interest in the electrical utility industry, particularly since massive power outage events happened across the world in recent years. In essence, power systems contingencies occur stochastically and system risk cannot be fully avoided [21]. Probabilistic results are important risk-based measures which accounts for the stochastic nature of system contingencies.

Risk management and quantified risk assessment have become increasingly important since the power industry entered the deregulation era. The competition environment forces utilities to plan and operate their system closer to their reliability limit. The stressed operating conditions can lead to the deterioration of the power system performance and this deterioration could have severe social and economical consequences. The system is under increasing stress because of load growth, renewable energy sources located far from the load centres and the level of power exchange between interconnected networks. The factor that makes stress decrease is investment, e.g. network reinforcement, innovative technologies and operational concepts. Also, in this environment, uncertainty is a characterizing feature of current system operation and transmission loading patterns are differing from those which were initially planned by network design, adding more complexity to this whole process.

Deterministic methods are widely used in TSOs for power system security analysis. The deterministic approach is blamed for being too conservative and resulting in an expensive operation of the power system. In reference [12], it is described as tending to be quite restrictive to be on the safe side. It is also mentioned that, in practice, this means that planners propose strong systems and operators operate with large security margins. Without incentives to become more efficient, not knowing or evaluating which is the actual risk, the deterministic approach will prevail. This can only be sustainable when investments and operational costs are relatively high. Obviously, the use of deterministic methods has resulted in a high level of reliability in power systems and there is also expected inertia to the change of approach.

To ensure a more cost-effective and still secure operation of the power system, the daily use of new security assessment methods is imperative. Since the power system has already been planned to meet the single contingency criterion, it means that is also important to also study multiple credible contingencies. Hence, in order to perform risk analysis, probabilistic methods become essential. The developments in communications systems, computer science and power system engineering make possible to perform more accurate analysis, reducing the impact of contingencies on society.

3.1.1. Power system operating states

In power systems operation domain, it is necessary to consider the system states classification that is proposed in IEEE, EPRI and CIGRE publications. Figure 3.1 presents the scheme of the process power system operation and the interconnections between states [12].

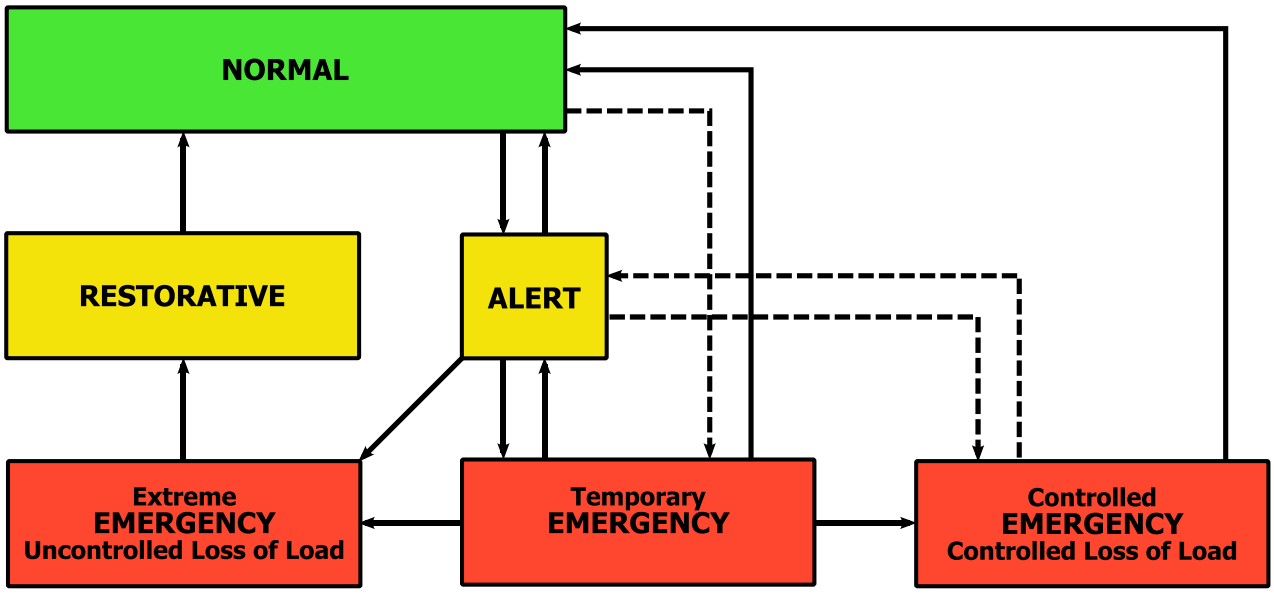


Fig. 3.1 – The process of Power System Operation [12]

Based on [12], [43-45], the major four system states are described as follows. In the Normal state, no credible contingency can result in a system problem (temporary or permanent system failure). Load flows, voltages and frequency are respecting operational limits and here the security criterion is fulfilled. Thus, this corresponds to a secure state, i.e., normal state. A contingency can place the system again in another normal state or transfer it to an alert state. The system should have the ability to withstand the contingencies performed in the deterministic assessment (N-1 criterion). The Alert state happens normally after the occurrence of a credible contingency, but quick control actions are needed to replace the security criteria, although the system is still considered adequate. If another contingency happens while the system is in the alert state, it may result in loss of load, stresses of system components beyond their acceptable limits, bus voltage and system frequency outside the acceptable range, cascading, instability and islanding (system split). At this point, the system is placed in the Emergency state and immediate remedial actions have to be taken to bring the system back to an acceptable state. The Normal and Alert states are both considered adequate, although the latter doesn't have reserves available for more disturbances. The Emergency state is considered inadequate. Figure 3.1 divides the Emergency state in three different ones.

In a temporary emergency condition operator action can relieve unacceptable line stresses or bus voltages violations and return the system to an alert or even a normal state. In many cases, however, remedial action is possible only if load is shed, placing the system in a controlled emergency state. A controlled emergency state can also be reached from an alert state if a contingency can directly cause supply interruption, without operator action, while system stability and integrity of interconnected operation remain unaffected. Other contingencies in an alert state could force the system into an extreme emergency condition where the stability and/or integrity of the system are threatened [43]. The Restorative state describes the period where the system is brought back to a Normal state.

After describing the possible system states, it is pertinent to introduce the definition of operation. According to the International Electrotechnical Vocabulary [46], "operation" is the combination of all technical and administrative actions intended to enable an item to perform a required function, recognizing necessary adaptation to changes in external conditions.

The operation of a transmission system is a complex process with continuous changes in the state of the system, which is influenced by disturbances, planned or unplanned outages, change of loading conditions and change of generation pattern (which is in our days driven by market and by the wind conditions). Every time that a change occurs in the power system, a new operating state may be introduced. It is

crucial to be prepared for emergencies in order to limit their consequences and quickly restore the system to its normal state.

3.1.2. Reliability concepts in power system analysis

Reliability of a power system is a general term that refers to the probability of its satisfactory operation in the long term. According to NERC, as quoted by [47], the reliability of 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. The degree of reliability may be measured by the frequency, duration and magnitude of adverse effects on consumer service*. Reliability of power systems is divided into two different aspects: security and adequacy.

It is not possible to accomplish 100% reliability of an electrical power system. That is technically and economically not achievable due to unexpected power system faults. However, with investments in the network, in system operation and in maintenance, the reliability level can improve. It is important to have a sustained investment level, because over investment can lead to excessive system costs and under investment can lead to unreliable load supply.

Security is considered one important aspect of reliability and many definitions can be found in literature. According to [47], power system security *is the ability of the power system to withstand sudden disturbances such as electric short-circuits or unanticipated loss of system elements. Security refers to the degree of risk in its ability to survive imminent disturbances (contingencies) without interruption of customer service.* Thus, it relates to robustness of the system in a context of imminent disturbances and depends on the power system operating condition before the disturbance and the contingent probability of disturbances. Security is a dynamic issue and it implies both the transition to the new operating point and the state of this new operating point. Security requires that both steady-state adequacy and stability performance criteria are respected. Security limits constitute the first line of defence of a power system against the many unforeseen events which can disturb or threaten its operation.

Power system adequacy is defined by [47] *as the ability of the system to supply the aggregate electrical demand and energy requirements of the customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.* Adequacy is therefore a steady state issue and deals both with generation and transmission capacity.

The adequacy indices are given in terms of frequencies and durations of system problems such as overload on transmission circuits, violation of bus voltage limits, voltage depression, isolation of individual buses or network islanding and indices expressing loss of load caused by interruptions of supply.

The definition of adequacy, presented earlier, must be modified for transmission systems operating in competitive environment. A possible definition is the following: "*the ability of a transmission system to supply the aggregate electric power and energy requirements at its load buses, fed from either internal or external sources, and to accommodate through-flows arising from contractual obligations within component ratings and voltage limits, taking into account planned and unplanned component outages. In a market- and competition-based operating environment the composite of generation, transmission and distribution can no longer be evaluated for adequacy. The installation and location of new generation will be governed almost entirely by market considerations which may or may not be influenced by generation reserve requirements. Transmission system adequacy studies will require major and innovative changes to accommodate the effect of through-flows and other additional flows dictated by contractual obligations"* [43].

Nowadays, system adequacy is determined by a deterministic analysis (so-called N-1 analysis), which is developed further in section 3.3.1.

CIGRE TF 38.03.12 [12] also explains the distinction between security and adequacy. The implication behind this subdivision (security and adequacy) is that the two are different in concept and in evaluation which can lead to misunderstanding of the reasoning behind this subdivision. Part of the reason for the subdivision is that adequacy, as defined, is far easier to calculate and therefore worthwhile to evaluate and apply, leaving the problem of "security" for further development and research. Although the distinction between adequacy and security in a reliability sense is generally understood by those developing the analytical techniques, the distinction has become less obvious to those involved in the practical applications of reliability assessment to real systems. Therefore, according to the latter, the security analysis is more related with the possibility of instability, despite the fact that it has led to much misunderstanding because it is used in different senses by different people [12]. The intention is to ensure that reliability indices are calculated in a simple structure and in a logical way.

3.2. Contingencies

In Policy 3 of the UCTE Operation Handbook [6], a contingency is defined as the trip of one single or several network elements that cannot be predicted in advance. The number of possible contingencies in a power system is enormous, so it is not feasible to analyse them all, and depending on its dimension, the disturbance can cause significant harm to the system. Hence, it is important to prioritize the contingencies and, additionally to the ones already included in the N-1 criterion, to select a range of severe contingencies (beyond the deterministic security principles used) that are crucial for system online security analysis, for which the simulation is important. Severe contingencies that actually may harm the system are unexpected and uncontrolled, presenting a stochastic nature; the ones that are anticipated have already been accounted for in power systems planning and operation, thus no harm is expected. To compute the consequences of events of stochastic nature, a probabilistic assessment is required.

Contingencies can be divided in single and multiple unexpected outages and the multiple contingencies can even be divided in:

- Independent contingencies – contingencies resulting from different causes and which are not related to each other; they can be single (the most common case), double or multiple.
- Dependent contingencies – faults triggered by the same event, such as common cause contingencies (normally OHL sharing the same towers and path), different cause contingencies (such as hidden failures in protection systems in adjacent grid elements) or even when the functional state of one component is affected by the functional state of another (such as a transformer being single fed by one overhead line or cascading failure caused by over-current after an initiating fault).

Dependence can be classified as intrinsic or extrinsic. Intrinsic dependencies occur where the functional state of one component is affected by the functional state of another. Extrinsic dependencies refer to external common cause, such as lightning flash causing a simultaneous fault in two OHLs that share the same towers [10].

A common cause failure is an event defined as the failure of more than one component due to a shared cause during the system mission [10]. Common cause outages are not consequences of each other.

During periods of adverse weather or forest fires multiple contingencies have a high likelihood of occurrence. Therefore, the assumption that only single contingencies should be considered (or that the fixed contingency set used in the deterministic analysis is suitable) is for sure doubtful, because the rate at which outages occur increases so much with adverse conditions that the probability of simultaneous or quasi-simultaneous, outages is no longer negligible. This matter will be developed further in section 7.6.4.

In the Portuguese TSO, contingencies that actually have happened are named incidents. An incident is an event that leads to the unplanned disconnection of one or more grid elements, called incident elements,

which may lead to energy not supplied [19]. It is also relevant to mention that incidents do not necessarily have the presence of a short-circuit current, e.g. in case of human errors, the short-circuit current might not exist, although an unplanned outage will occur.

Finally, incidents in overhead lines are much more likely than in underground cables, transformers or busbar, as can be further observed in chapters 5 and 7.

3.2.1. Main causes of contingencies

A power system can become more vulnerable for several reasons, including component failures, communication-system failures, human errors, weather conditions and environmental conditions, among others. In the Portuguese transmission system, it is possible to identify as main causes the following:

- **Atmospheric** - lightning that affects several grid elements simultaneously; fog in combination with pollution in a specific region; or (less common) rain, floods, snow, hail or strong wind.
- **Environmental** – regions populated with storks; localized pollution areas; forest fires of huge proportions that affect several grid elements (such as overhead line corridors or the confluence of several elements in the neighbourhood of a substation).
- **Human Errors** – e.g. during switching operations, refurbishment activities, assembling and commissioning/testing, or operation decision error.
- **Equipment fault** - incorrect operation or failure of the protection and control systems; breakdown of EHV equipments (e.g. explosion of current transformers, protection fails to trip, breaker fails to open or an inadvertent tripping of a protection system).

3.2.2. Contingencies selection methods

In literature, two types of contingency selection methods can be found. First, the enumeration method defines a list of contingencies, providing an enumeration for each level of contingencies. Second, Monte Carlo simulation is used to generate random contingencies. Both methods can be used to rank contingencies according to their impact on system operation. Depending on the purpose of the analysis, different contingencies can be selected.

Nowadays, enumeration is the selection method used by the TSOs to perform security analysis and the contingencies included in the list are considered credible events, i.e., recognized as sufficiently likely for the electric power system to be designed and operated to withstand them [46]. The definition of credible contingency can be different for each utility, because it is related to the intrinsic characteristics of each system. The online security analysis uses a “must run” contingency list (see section 4.5.2.1), which includes the most credible and significant events for the system and is normally associated with the N-1 criterion.

Beyond the “must run” list and the busbar list, the Portuguese TSO has created several new contingency lists, which are available in the Energy Management System (EMS), namely loss of OHL corridors (beyond N-2 criteria), distribution network border failures (considering closed rings and transformers), loss of an entire EHV voltage level in a substation (considering all the facilities with at least 2 different voltage levels) and extreme disturbances (that have actually happened). All these lists are complementary to the existing ones that fulfil the ENTSO-E security requirements and they were created in order to improve and to complete the security analyses that are currently made by operation planning.

The other method for contingency selection that is often used is Monte Carlo simulation, which generates random contingencies in order to model uncertainties. This method is used by D. Kirschen and his co-workers for computing the Value of Security, e.g., in [48-51] and it is also mentioned in Wenyuan Li

research work, e.g., in [21], [52], [53]. Monte Carlo simulation for contingency selection is not suitable for online analysis, because of the high computational requirements even with today's powerful computers.

3.2.3. High-order transmission contingencies

First, it is important to define high-order contingency. Reference [54] defines it as the loss of multiple elements during a short time period in power systems. Looking back to the past 7 years, these disturbances considered rare events have happened several times throughout the world in the recent past. Obviously, the probability of high-order events is much lower when compared with N-1 events and this is also the reason why they are not considered in the usual deterministic approach for security assessment. Due to low probability of N-k (for k>1), they are not currently considered in the operations' security analysis. Reference [55] mentions that it is very hard for system operators to take remedial actions *a priori* to prevent them, because it is not cost effective.

Following recent blackouts, presented in chapter 2, high-order contingencies in power systems are of great interest, because they may cause huge losses. This is the reason that motivates many TSOs and entities like NERC, former UCTE (now ENTSO-E), IEEE and CIGRE to pay closer attention to severe multiple contingencies, associating to them a high level of risk. Adding this interest to advances in computing technology, it is possible to develop a decision-making support tools for operations that consider also contingencies of a higher order than the one used today.

In reference [19], a set of higher order contingencies were analysed, mainly on the 400 kV. After the summer of 2003, when forest fires created catastrophic scenery in Portugal, the occurrence of many multiple contingencies has motivated the analysis of a set of multiple contingencies considered credible and severe. This analysis included overhead line corridors and the loss of a voltage level in an electrical facility which contains this voltage level, by circuit breaker fault or a busbar fault when the whole service is connected to a single busbar. The applied corridor definition was developed by the Portuguese TSO and establishes that such a corridor is less than 200 meters wide, the number of circuits is greater than or equal to 2 (including common tower cases), and the lines' parallel pathway is greater than 1000 meters. The busbar fault simulation is justified by maintenance works, which leave all the grid elements connected to a single busbar, during short periods of the year. Obviously, these outages for maintenance are well planned in advance and they are placed in the more favourable periods, diminishing in this way the possible impact of an incident.

High-order events can be simultaneous or cascading. From these, double contingencies and (higher order ones) are distinguished. In section 3.2.1, the main causes of transmission system faults are presented, but from the general set it is possible to identify the ones that normally cause a higher order contingencies, namely forest fires, lightning, protection misoperation, hidden failures, breaker failure, busbar faults and extreme severe weather phenomena located in a place with a high density of overhead lines. These examples fit in the definition of independent and dependent events presented in section 3.2. Finally, cascading trips caused by overloads due to a stressed operating condition or a previous high-order event.

Cascading events, heavy load, reactive power deficit, a more weakened system due to outages, a specific generation profile and, as a result, unfavourable network power flow patterns, can be identified as favourable conditions for severe and extensive consequences of a given contingency.

Concerning cascading events, it is worth to mention that they may lead the system into a separation or a collapse situation, starting from small initiating contingencies. Normally, if these first disturbances are not handled in time, they tend to spread throughout the system, transferring it from an alert state into an emergency state, and this process can last from minutes until a few hours.

As mentioned by Dobson in [56], there are many ways in which failures can influence further failures, including overloads, hidden failures of protection systems, software, control or operator error, flawed or inapplicable operating procedures, and a variety of dynamic and stability phenomena including transients, oscillations, transient stability and voltage collapse. Cascading failure is influenced by operational policies, software and human errors, upgrade and the responses to previous blackouts, in addition to the varied and complicated ways in which failures interact via physical laws on the power grid. It is recognized that the probability of occurrence of successive events increases following the occurrence of a contingency. The time interval between an initiating event and successive events can vary greatly. The time interval may be long enough for an operator to initiate actions to mitigate the undesirable trend [55]. Once again, the operator plays an essential role in preventing and mitigating the consequences of a potential cascading event that is beginning to spread out.

However, the literature on systematic selection of high-order contingencies, called N−k contingencies with $k \geq 2$, is limited. The difficulty of N−k contingency selection lies in the combinatorial nature of their number: the total number of distinct non-ordered (simultaneous) N−k contingencies is $N!/[k!(N-k)]$ [55], [57]. Obviously, it is unfeasible to analyse the total number of contingencies in an electrical transmission system, thus it is sensible to make some assumptions to select the most suitable and worthwhile set of contingencies to be analysed, decreasing the number of contingencies in the analysis. In [55], the probability order two (p^2) is used as a criterion for cut-off; this means that it is assumed only one breaker could suffer a stuck failure, and only one neighbouring component could suffer inadvertent tripping.

Contingency set identification is an essential step in monitoring the power system security level. Currently, most literature on contingency selection emphasizes the screening method to select contingencies from a presumed N−1 contingency set plus a limited number of high-order contingencies, ranking them by using an appropriate severity index [55].

Reference [55] presents an algorithm to identify the influence of topological actions in high-order contingencies and it uses topology processor information, which is part of the EMS software, that complements SCADA. In [55], dynamic system simulation is performed, assuming that the failed component is immediately removed from service, and three types of contingencies are addressed, namely: inclusion of all the forced outages (contingency) due to primary protection tripping caused by whatever reason (normally it is an N-1 event, but can be a multiple one as defined previously, e.g., overhead line corridors), a stuck breaker tripping following a contingency; and protection inadvertent tripping following a contingency. According to the author of [55], these contingency categories capture the majority of high-order contingencies that can be systematically identified by topology processing. A dynamic event tree (DET) is used to enable identification and implementation of actions following the initiating contingency. This approach includes decision nodes where it is effective and possible to take actions that avoid or mitigate event consequences [55]. The DET aims to provide support to control room operator as an operational defence plan, allowing a quick response to the high risk N-k contingencies.

3.2.4. Contingency probability

Literature presents three ways to estimate the contingency probabilities of power systems. The first is to fit an existing probability model to historical data; the second is to use physical attributes of each individual event; the third is to use Monte Carlo simulation with variance reduction.

Reference [55] presents three possible probability models to estimate probability of rare events, namely Poisson, cluster, and power law. The power law model appears associated with probability of cascading events and it is also proposed [58]-[59]. This model is in accordance with the existing large power outage statistics in the sense that it predicts that large events happen with a much greater probability than commonly expected. According to [58], a power system does not always exhibit power law until it is heavily loaded, which limits its application to other power system conditions. Clustering of contingencies is expected from a large power system network. When the power system is heavily loaded, other

contingencies tend to develop. Reference [55] states that cluster model is more suitable to high-order contingencies than power law, which overestimates its probabilities. The Poisson distribution assumes that events are independent, i.e. the failure of one component does not affect the failure probability of another component.

Accurate contingency probabilities are essential when applying probabilistic methods to system operation security assessment and consequent decision-making process. For risk-based security assessment, it is important to have the probability associated with each contingency, which is going to be simulated.

Reference [16] presents a contingency probability estimator to be used in operational decision-making constrained by contingencies violations, as already described in section 1.1.3. They include two inputs in the estimation: temperature and wind speed. This paper shows concern about two operational issues: first the lack of data and second the influence of weather conditions in operational decisions. They mention another relevant aspect of real time operation analysis, which is the correlation between outages and the examined factors, using information to identify where risks are higher in the network. The Poisson is used because it is considered adequate to model the next failure of a component.

Operational decision, in a control room, is not only influenced by weather conditions and forecast but also by other factors, such as risk of forest fires. When calculating contingencies probability, the significant factors must be considered. The operators' decision-making process requires real-time updated information, which means also updated probabilities computed with the most recent information, namely: lightning information, forest fires information per region, weather information and forecast, among others. In this research work, the objective is to determine the failure rates that are going to be used to calculate the contingency probability for the next period under analysis (such as 1 hour), taking into account the influencing variables already described in section 1.4.1.

3.3. Power system security

Facing a major disturbance, protection systems and control actions will operate in a way to stop the power system degradation, preventing the disturbance from spreading and avoiding worst consequences. All the actions will have the purpose to lead the system to a secure operation state. Depending on how fast the disturbance evolves, automatic control actions can be slower than it is needed to control the situation. The main objective when reacting to this kind of occurrences is to minimize their consequences to the electrical system, restoring and returning the transmission system, as quickly as possible, to secure operating conditions. The operator is the one having the overall vision of the system through SCADA, relying on the information that reaches him to perform the analysis and having to deal with extreme complex situations.

"Human reasoning presents an oscillation of two main intellectual movements: comprehension and analysis, being the former the inaugural glint to the admirable manifestations of beings and the latter the methodological effort of understanding phenomena: by comprehension, we see it as the way things that seem to be apart become together; by analysis, things that are together seem to become apart. Thus, whenever one is trying to analyse a specific topic of a protection system, a broader sense of holism is brought to our mind — such is also the nature of Protection System Co-ordination", by João Emanuel Afonso in [60]. Although this paragraph is applied to Protection System Coordination as the main concern of protection engineers, it can also be applied to power system secure operation as the main concern of control room operators.

There is an increasing need to provide system operators with accurate, simple and user-friendly online information, regarding system security levels at critical points, allowing them to apply promptly the most suitable control measures. System operations engineers are extremely conscious that their systems are permanently exposed to risk, in relation to the consequences of unexpected contingencies. The goal in operation is to achieve the best trade-off between security and economy.

As already mentioned in section 3.2, contingency set identification is an essential step in monitoring the power system security level, however the number of possible contingencies is huge, which means that they are impossible to predict and it is not cost effective to perform expensive preventive actions in advance, or to install special protection schemes for all the severe disturbances. Therefore, a very effective approach is to allow the control room operator to make decisions and to perform quick remedial actions whenever it is necessary and feasible. These solutions don't require either actions or cost to the system, unless and until it is really needed.

Power systems always reside in one of four states: normal, alert, emergency or restorative, where emergency state could be extreme, temporary or controlled, as shown in figure 3.1. These states were adopted in system operation procedures and requirements manual [44] from the Portuguese TSO, which includes all operating requirements, rules and guidelines, because they provide a decision-making basis for security issues. The aim of security assessment is to take decisions so as to reach an appropriate compromise between operating costs and robustness with respect to possible disturbances.

In operations, the decision-maker is the operator, the decision is how to constrain the economic operation of the power system in order to maintain the normal state, and the basis for the decision are operating rules. Even in the normal state, unpredictable events may have severe consequences to the system, which means that the system is always potentially insecure and it is important to quantify how much [61]. The level of risk will be different, depending on the operating condition and also on the disturbance that may occur.

To operate the power system closer to the traditional security limits, more sophisticated methods for security assessment are needed that take into account the probabilistic nature of uncertain variables in the decision-making environment. This is something that has been appearing throughout time. In reference [61] the following quotation was made:

"Operators, in making decisions about what corrective actions are going to be taken, need to know the probability of occurrence, and then determine whether or not we want to take some steps that may be very undesirable… If we agree, in the coming hour, to make a certain transaction that we know is going to increase the loading on certain facilities, is that going to have a significant effect on the security of the system? This is something we are thinking about. This is in my way of thinking a system parameter: a transmission system, a cross-state transfer, a loading or something like that, that if we go that next hundred megawatts, is that going to make a significant difference in the system security? If so, it's not worth the economics. If on the other hand, for a relatively small increase in the probability that the security is going to increase, then it may be worth it. And we're into dollars and cents. 'What is the value of taking that next step'?' and then 'What is the cost of having a major disturbance occur?"

These words are described as being said in 1988 by an experienced and respected operating engineer.

Figure 3.2 presents the different types of security problems that can be caused by a disturbance. Thus, these are considered the three main areas of security assessment, as stated in reference [62].

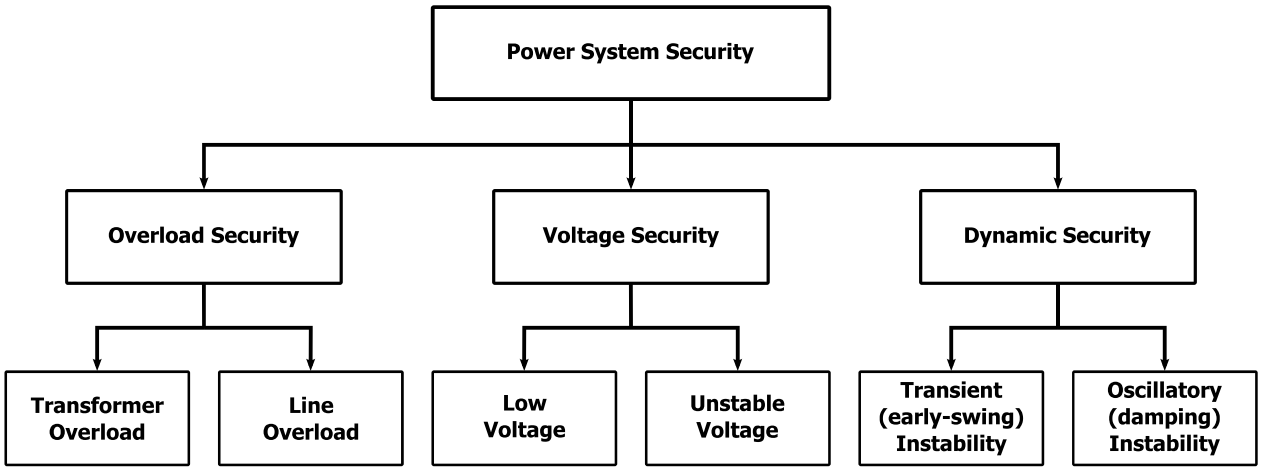


Fig. 3.2 – Decision Drivers of Power System Security [62]

The time to perform the remedial control actions in order to prevent and to mitigate security problems will depend on the type of problem. Figures 3.3 and 3.4 suggest the time available to take corrective actions for each type of impact.

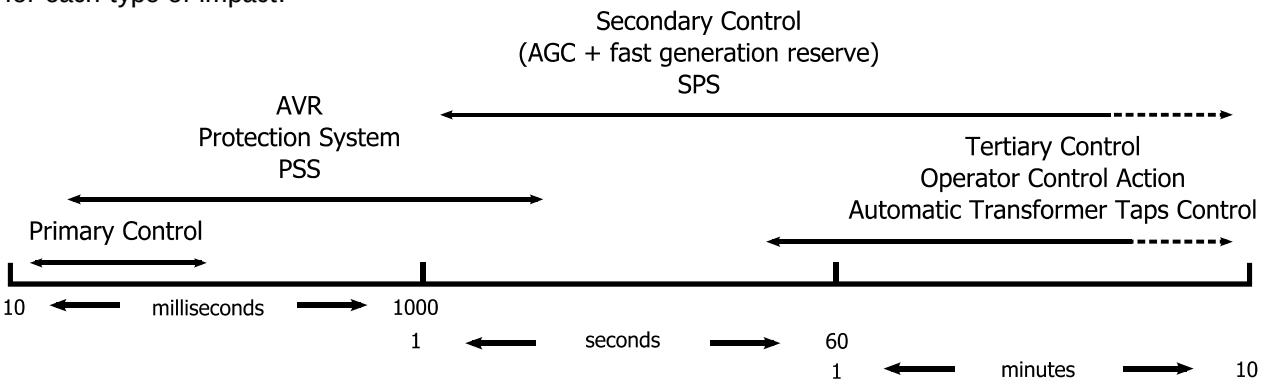


Fig. 3.3 – Time scales in emergency – types of control

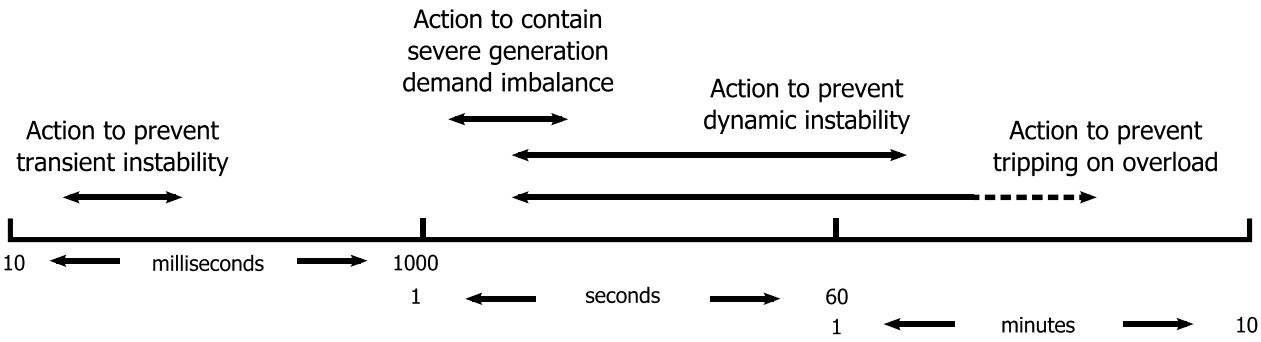


Fig. 3.4 – Time scales in emergency control actions [45], [62]

In system operations, the achievement of security is the main goal: from the operator's point of view, if the system is secure at all times, regarding to operating rules, reliability is achieved. In system planning, due to the practical difficulties associated with identifying secure and insecure states, reliability assessment has historically been based on the concept of adequacy [12].

The two security assessment approaches identified in the literature are deterministic and probabilistic. The deterministic approach provides a simple process for decision-making. It defines a conservative security region for protecting the system against severe contingencies. This can only be sustainable when investments and operational costs are relatively high and obviously this results in a high level of reliability in power systems [12].

As described in [12], now the pressure is to operate the system closer to its limits (meaning lower security margins), due to economic imperatives, resulting from the competitive environment, the organizational separation between generation, transmission and distribution, and to practical difficulties such as obtaining authorizations from regulatory bodies and permits from local government bodies to build new transmission lines and power plants, which makes the grid more vulnerable to disturbances. In order to operate the system with the current conditions, more refined methods for power system security assessment are needed, which take into account the probabilistic nature of many variables in the decision-making environment. Probabilistic methods are widely accepted as powerful tools.

Making a more general analysis, we have realised that almost everything in TSO environment influences directly or indirectly system security, for example, generation pattern, planned outages schedule, operator's training, operating procedures, incident analysis, reliability of system components, communication systems and SCADA.

Energy Management System (EMS) enables security assessment through SCADA, state estimation and deterministic contingency analysis. However, the use of these tools in the decision making process requires a significant amount of subjective assessment regarding questions like: How many overloads or voltage violations are there and how severe are they? How close to voltage instability is the system? Is cascading possible? What is the likelihood of occurrence for each contingency? [17]

At this juncture, in Portugal, all the possible measures are taken in order to avoid risk, independently of its probability, no matter what is the cost. Is this approach sustainable and reasonable?

3.3.1. Deterministic security assessment

Nowadays, security assessment in operations is performed in two stages. Operational planning engineers study expected future conditions off-line to identify operating rules. Operators then apply these rules, together with EMS security assessment software, to assess system security levels and make decisions regarding preventive and corrective actions [3].

In the deterministic approach, only the contingencies that are included in the pre-defined list are considered to be sufficiently credible to deserve consideration, and in the end they are treated like they have exactly the same probability of occurrence. Single contingencies are indeed much more likely than multiple contingencies (simultaneous or not), if the outages are independent events. The decision is founded on the requirement that each outage event results in system performance that satisfies the chosen performance evaluation criteria. These assessments, typically involving large numbers of computer simulations, are defined by selecting a set of network configurations, a range of system operating conditions, a list of outage events, and the performance evaluation criteria. Study definition requires careful thought and insight because the number of possible network configurations, the range of operating conditions, and the number of conceivable outage events are each very large and an exhaustive study of all combinations is not reasonable. Consequently, an approach has evolved within the electric power industry to minimize study effort and to provide useful results, called the deterministic approach. This approach depends on the application of two criteria during study development [3], [8], [61], [63]:

- Credibility: The network configuration, outage event, and operating conditions should be reasonably likely to occur.
- Severity: The extent to which failure criteria are violated.

The outage event, network configuration and operating condition on which the decision is based, should result in the most severe system performance, i.e., there should be no other credible combination of outage event, network configuration, and operating condition which results in more severe system performance [3], [61]. When performing the assessment, all contingencies included in the credible contingencies list are considered to have the same probability of occurrence, which is not accurate.

Deterministic Security Assessment tends to provide a conservative security zone for protecting the system against severe contingencies. The main weakness of the deterministic criteria is that it does not account for the stochastic nature of power system behaviour. Both adequacy and security are tested by a series of systematic simulations. In the case of adequacy, the so-called N-1 criterion is applied: a list of contingencies is the base to remove each component, one-by-one, and the system must be so designed that no adequacy violations occur in the resulting system configurations. The line loads and bus voltages are computed through a power flow analysis. The adequacy is judged by the utility's accepted operating criteria, which include thermal limits and acceptable voltage range. Security limits are determined so that the system is stable, loses no load due to such contingencies, and system quantities remain within emergency operating values regardless to system topology [12].

Operators classify an operating condition as secure or insecure, according to whether each and every contingency that is analysed satisfies the specified network security criteria. If one or more contingencies are in violation, remedial actions have to be taken to move the security level into the secure state. If no disturbances are in violation, then no action need be taken, or actions can be taken to enhance the economic efficiency of the energy delivered to the end-users.

Section 4.5.2 describes the security analysis performed in the Portuguese transmission system using the deterministic approach.

3.3.2. Probabilistic security assessment

Probabilistic methods for the evaluation of system security have received some attention by system operators [12], although security assessment in system operation is currently performed by deterministic methods. In the Portuguese TSO, it is combined with a probabilistic tool (called Zanzibar), mainly used in the planning environment. As already mentioned, the change in power systems environment from regulated into a competitive one has created new challenges to the power system security assessment. According to [12], the major challenges in implementing this approach are practical ones. Indeed the first challenge concerns the data collection problem, in other words, how to develop sufficiently adequate probabilistic models of the power system?

Nowadays, system operation and supervision centralization, combined with the capacity to import from local event records, speeded up the data gathering process and the incident analysis activity, allowing a prompt data base population. The development of information technologies and the present-day automation level of substations offer a large set of data to analyse, allowing a strict treatment, integration and data collection. Regarding the data collection process, the Portuguese TSO has an incidents data base, called GestInc [64], with all the information since the beginning of 2001. Before that, there is an MsAccess data base with incident data since 1991, although the confidence in the quality of those data decreases significantly. Thus, the gathering and processing of statistical information about disturbances is going to be possible using the data collected since 2001.

Utilities are collecting large amounts of real-time data in a systematic way with automatic processes. Concerning power system states and models, this involves the gathering and processing of statistical information and the engineering knowledge and judgment to fill in missing information, as stated in [12].

The second challenge is the definition of a severity function, which has to include the technical constraints, the loss of load and the economic evaluation of the consequences of a disturbance. In the future, to correctly assess the risks of large disturbances, it may become necessary to develop more detailed and more global simulation models than those used today in security assessment [12].

The third challenge is related to computational aspects, according with [12]. How to estimate the expected risk with sufficient accuracy in online environment? How to identify decisions leading to a better

economic trade-off between risk and operating costs? How to define boundaries between acceptable and unacceptable risks?

In literature, e.g., [12], [13], [21], [48], [49], [51], the probabilistic approach is associated with Monte Carlo simulation and uneven prior probabilities of possible causes which could lead to extreme conditions are taken into account. The economic impact of their consequences is also evaluated, and various uncertainties about less well known system components are integrated in the decision-making process [13]. Probabilistic approach aims to enhance the decision-making process, making better use of the available information in order to reach an appropriate compromise between operating (and investment) costs and robustness with respect to possible disturbances [12], which explains the growing interest in this approach by many utilities. This approach brings new insight into the understanding of the system behaviour by associating probabilities with system impacts [65].

3.3.3. Comparison between approaches

The deterministic approach has served the industry well; it has provided high reliability levels without requiring excessive study effort, because it is a simple process [61]. It is this simplicity that has made the deterministic method so attractive, and so useful, in the past, but there is a growing recognition that this simplicity also carries with it significant subjectivity, and this can result in constraints that are not uniform with respect to the security level [63]. Yet there has been a real and tangible price to pay for using this approach: solutions tend to be overly conservative, due to the emphasis of the most severe, credible event. Consequently, existing facilities are not fully utilized, from an operating perspective, and the system becomes overbuilt, from a planning perspective [61].

Nowadays the Portuguese transmission grid has a regulation that favours investment in infrastructures, but as soon as the investment policy together with the current regulation rules change, the need to operate the system closer to its stability limits will appear and, consequently, the need to have tools that support the decision-making process, considering both security and economical issues. The Portuguese situation will be further developed in chapter 4.

With frequently stressed system operation, the weaknesses of the deterministic approach become noticeable. One weakness that is immediately recognizable in the deterministic approach is the fact that it does not consider the inherent nature of power system behaviour, mainly, contingencies. The Portuguese transmission system does not know yet such a situation, because the investment level in the network is very high and at the moment the network is not being operated near its security limits. Nevertheless, the search for lower costs and greater efficiency in system operation is a continuous aim.

Other identifiable weaknesses from the deterministic approach are [3], [7], [9], [61], [62]:

- The analysis considers limit violations (current and voltage) and severe stability problems normally detected when the power flow does not converge, judging the security level, but it does not account for event occurrence probability. Thus, it is accepted the implicit assumption that all events in the contingency set occur with equal probability (frequency). However, even if the contingency set includes only N-1 events, significant variation in occurrence frequency may exist. There may be some situations where a deterministic violation contributes to a very low risk because the outage probability is extremely low. There may be other situations where a deterministic violation contributes to a very high risk because of a high outage probability.
- It only analyses a defined set of contingencies and the selected set normally does not include multiple contingencies, such as cascading events and hidden failures.
- Only consequences are evaluated and it does not quantify the economical impact of the violations. All violations are considered unacceptable without distinction and without judging their real consequences to the power system quality of service; this implies that all violations are equally severe. For instance, if a conductor exceeds its emergency overload rating by few per cent for 30 minutes this is deemed unacceptable, but it has almost zero economic impact. An out of

step condition at a plant is equally unacceptable, yet the cost of replacing the energy source is high. The occurrence of energy not supplied in a delivery point is also extremely serious and cannot be compared with a low percentage of overload.

- Decisions are made addressing only the effects of contingencies that are constraining the system, limiting the contingency set to N-1 contingencies, and using simple, conservative performance requirements based on "worst-case" analysis used by the industry to handle uncertainty in security assessment.
- It cannot address uncertainty in operating conditions. This limitation inhibits a rigorous analysis of near future operating conditions since the future is inherently uncertain.
- During adverse weather conditions, the failure rate of overhead lines increases significantly, which is not taken into account because the probability is considered the same as in normal weather conditions. The probability of multiple contingencies is no longer negligible.

On the other hand, the probabilistic approach [3], [12]:

- Considers the probability of contingencies occurrence; the probability of occurrence may vary with equipment type, location and configuration as well as with meteorological conditions.
- Captures the increased risk caused by multiple constraints as it sums risk associated with all contingencies and failure conditions, i.e., the probabilistic approach is capable of composing risk from multiple events and multiple failure conditions and it reflects the total composite risk and not simply the one resulting from the single most restrictive contingency.
- Treats uncertainty in operating conditions very well and it is consequently appropriate for assessing future conditions.

Probabilistic approaches reduce these weaknesses. It is well known that probabilistic methods constitute powerful tools for use in many kinds of decision-making processes, but their usefulness is compromised in two areas where the methodology is not yet fully mature. One is the accuracy of the probabilistic models employed and the other is the precision of the solution methods [12] and for that accurate data collection is necessary. Reference [12] has demonstrated that a probabilistic approach to security analysis provides a promising framework for obtaining more flexible limits and for better assisting in operating decisions. Given the high frequency of stressed conditions observed in many control centres today, it is clear that online control is a continuous decision-making problem for the operator [63]. Although the introduction of probabilistic methods has many recognized advantages, changes always have opposing strengths in the beginning and operators are comfortable with the current methodology, therefore the probabilistic approach has to enter progressively into the system operation daily routine. Another disadvantage is that it is not a priori clear how to interpret the risk results, since acceptable risk level can only be defined after having gained sufficient experience with their numerical values.

3.4. Protection systems

An electrical power system must be provided with a suitable protection system for the grid that promptly and effectively disconnects any faulty element in a selective manner. The protection system has to permanently monitor system's behaviour and, when facing a disturbance, act on the breakers in order to isolate selectively the faulted element as quickly as possible, minimizing consequences and damage for the power system. The high short-circuit currents, which may occur during a fault, can damage the grid equipment, cause fire and, in the worst scenario, lead to a system collapse. Thus, if the fault is not correctly cleared, the following might occur:

- Loss of generator units;
- Equipment damage;
- Non-selective actions, which can lead to system's partial or total loss;
- Industrial processes loss and damage of power system clients.

A protection system is required not to act under normal operating conditions, but it has to immediately take action when a fault occurs.

Lack of dependability may lead to the failure in isolating faulty components, although in the Portuguese transmission system protection systems are usually redundant and diverse, i.e., each grid element is protected by two independent protection systems competing with each other, which means that the probability of a non-operation for a fault in its protective zone is very low. With damage and outage cost as a concern, the design of protection systems tends to privilege dependability over security to minimize damage in system components such as transformers, generators, OHL and other equipments. Unnecessary trips (without fault or non-selective trips) can occur due to protection system equipment failures or setting errors. This may lead to cascading events, which spread the disturbance to more grid elements than needed. Hence, it is obvious that a compromise between dependability and security is usually inevitable.

When the power system is operating closer to its limits, the good performance of protection systems becomes even more crucial, because a protection system misoperation may lead to more severe consequences. The protection system performance can be classified as correct or incorrect operation. It is possible to identify the main causes for incorrect operations, namely: inappropriate design or installation of the protection system, wrong settings facing a specific operating condition and protection system component failure. At the basis of the first two reasons may be human errors, which are also a direct cause of protection systems misoperation during maintenance or commissioning activities.

In the 6th September 2001 blackout, presented in section 2.3.2, the trip of the Palmela – Sines 3 overhead line, occurred only at the Palmela line-end, caused by a hidden failure and the initiating fault was a short-circuit in the parallel line Palmela – Sines 2. Hidden failures are further developed in section 3.4.1.

The majority of faults in the Portuguese transmission system occur in OHLs, so they take a preponderant role concerning multi-function protection system applications. Since 2005, the Portuguese TSO is installing on OHLs, as one of the main functions in the protection system, the phase current differential protection, with distance functions within the same protection system. The distance function is operational in parallel with the differential one, but also works as backup for the case of communication failure, together with an independent and redundant protection system based on step and teleprotection aided distance protection schemes.

Busbar faults normally have a big impact on system security. Therefore another very important protection is the busbar protection, usually based on the selective phase current differential biased principle. In the classical substation layout scheme (see section 4.4), the busbar protection operates disconnecting only the grid elements connected to the faulty busbar, including the bus coupler. Thus, it maintains connected all the grid elements in the healthy busbar. Without the busbar protection, all grid elements connected to the two coupled busbars would trip by distance backup zones (usually zone 2) at the opposite circuit-end, with much higher clearing times and causing a more severe disturbance. For maintenance reasons or with special topological schemes, the substation service can be connected to only one busbar or unevenly divided through the existing busbars, creating a lack of efficiency in the busbar protection operating benefits. Therefore, these periods must be minimized.

The statistics of protection system performance in the EHV network are presented in section 5.3.5.2.

3.4.1. Protection systems hidden failures

Hidden failures can be defined as “a permanent defect that will cause a relay or a relay system to incorrectly and inappropriately remove a circuit element(s) as a direct consequence of another switching event” [66], e.g., it removes incorrectly an additional grid element from service, acting simultaneously as

the correct protection system when clearing a fault on an electrically near grid element. It is relevant to mention that failure to operate is not considered a hidden failure and in this case other protection will take out the faulted equipment, working as a backup.

In recent research [67], [68], protection system hidden failures are considered as one of the main contributing causes of disturbance propagation, i.e., cascading events. Hidden failures in protection occur as a result of the following two phenomena [69], [70]:

- A protection element functionality defect. This type of defect may be a result of hardware failures, outdated settings, or human error.
- The second contributing factor is the logical arrangement of devices with the protection element functionality defect. The logic will determine if the failure will or will not remain hidden within the protection scheme until another event uncovers it.

By performing blackout analysis, it is possible to conclude that the cascading may be caused by unwanted operation of some protection system, whether combined or not with a stressed power system or another cause for high order contingencies.

Hidden failures remain normally unrevealed until the protection system is exposed to abnormal conditions and they can remove incorrectly more grid elements than the ones strictly needed for fault clearance. Misoperation is more likely to occur in protection systems located in the vicinity of the short-circuit current, i.e., protecting the electrically near grid elements inside a vulnerability region. When a fault occurs, for instance in an OHL, the line protection systems send tripping signals to the corresponding circuit breakers. Before the faulted line opens, some relays in the vicinity may also detect the fault and operate incorrectly, opening a healthy grid element (commonly another OHL).

The grid elements in the vicinity of the faulted one are more vulnerable to hidden failures than all the other elements. The vulnerability region is determined through an analysis of the installed protection relays. The subset of elements that can be disconnected because of hidden failures can be identified after defining this region for an initiating fault in any grid element. Hence, the N-2 events caused by an initiating fault plus hidden failures can also be determined and evaluated. These contingencies are dependent faults and much more likely than N-2 independent faults and therefore they should be included in the system's security analysis. Obviously, the severity of each hidden failure depends on which grid elements are disconnected and on the system's operating state, although there are hidden failures clearly more severe than others in the network. Some stay an N-2 contingency; some can trigger a thermal overload cascading event or a voltage collapse.

Reference [67] states that confirmed field experience is probably the only practical way to determine appropriate values for the probability of hidden failures. This probability depends on the likelihood of operating incorrectly when facing an initiating fault on another grid element and therefore the conditional probability concept has to be applied.

The probability of A (hidden failure in the i^{th} grid element) if B (initiating fault in the j^{th} grid element) occurs is $P(A|B)=\frac{n_{AB}}{n_B}$ where n_{AB} is the number of times that both occurred and n_B the number of initiating faults. The conditional probability of A given that B has occurred is given by equation (3.1).

$$P(A|B)=\frac{P(AB)}{P(B)}, \qquad P(B)\neq 0 \tag{3.1}$$

To calculate the probability of occurrence of the double contingency, $P(AB)$, composed of an initial fault and of a hidden failure, equation (3.1) can be used.

Reference [68] presents a hidden failure monitoring and control system. To estimate the probability of hidden failures after grouping the relays per classes, the following is proposed:

"Consider a given relay class, say the ith *class. Let* n_i *denote the total number of relays of that class involved in all the events of the sample S. Let* m_i *denote the total number of these relays whose hidden failures have been exposed. Then, an estimate of the probability of hidden failures of the* ith *relay class is defined as* $p_i = \frac{m_i}{n_i}$ *."*

It also presents a system failure probability based on a dynamic event tree, which considers the trigger (initial) event, the breaker status and the system failure. Particularly, in the system failure level, hidden failures and overloads are considered.

Reference [67] argues that the possibility of hidden failures should be included in the security analysis. It presents a technique to identify the most dangerous double contingencies caused by an initial fault and a hidden failure revealed by this fault. The definition of vulnerability region is also discussed and used to determine the N-2 contingencies that need to be evaluated for each transmission line.

The risk indices for power system hidden failures are discussed in section 3.5.4.

3.5. Probabilistic risk assessment

Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance. NASA intends to use PRA in all of its programs and projects to support optimal management decisions for the improvement of safety and program performance [10].

In the meantime, the nuclear industry picked up PRA to assess safety. This analytical method was gradually improved and expanded by experts in the field and has gained momentum and credibility over the past two decades, not only in the nuclear industry, but also in other industries like petrochemical, offshore platforms and defence. Because of its logical, systematic, and comprehensive approach, PRA has repeatedly proven capable of uncovering design and operation weaknesses that had escaped even some of the best deterministic safety and engineering experts. This methodology showed that it was very important to examine not only low-probability and high-consequence individual mishap events, but also high-consequence scenarios which can emerge as a result of occurrence of multiple high-probability and nearly benign events.

In many of the analysed literature, it was possible to find references to PRA method. In reference [71], this method is presented as being a more suitable approach not only because its calculation includes the worst case consequence, but also for its capability in accounting for the probability of occurrence and impacts, because an index can be developed to quantitatively capture the factors that determine security level: the likelihood and severity of the events. Two power system applications examples of PRA are presented. First, facing a large number of possible severe contingency cases, it would be difficult to determine which cases to be included in the Special Protection Schemes (SPS) that are most effective in enhancing the system security, thus PRA was used in this decision-making process. Second, it shows the application of a PRA method for determining the power transfer limit in a longitudinal electric power system [71].

One of the most common methods to implement PRA is the Event Tree methodology, which can be found in many references, such as, [10], [55], [68], [72].

3.5.1. Concept of risk

The concept of risk includes both the probability of occurrence (or frequency) and severity (or undesirable consequences) of disturbances. A very common definition of Risk is that of a set of triplets [73]. To determine risk in general the following questions need to be answered [10]:

1. What can go wrong? What can happen?
2. How likely is it?
3. What are the consequences (if it happens)?

To answer these questions, it is necessary to make a list of scenarios and for each scenario a set of triplets can be defined, as in equation (3.2) [10]:

$$(s_i, p_i, x_i) \tag{3.2}$$

Where:
s_i – scenario description;
p_i – probability of i^{th} scenario
x_i – consequence of i^{th} scenario

Particularly, in this case, the answer to the first question is a set of contingencies. The second question requires the evaluation of the probabilities of these contingencies, which are being analysed and the third calculates their consequences to the system. For this research work, these will be addressed in chapters 7 and 8.

Risk has been used for many years, at least qualitatively, in establishing the philosophy by which the industry has judged reliability levels; quantitative use of risk in operational decision-making can therefore be viewed as a change in method, but not in principle. In power system operation, the difficulty with deterministic approach is that, in terms of risk, it may result in inconsistent decision-making. Low-risk cases may be included in studies and high-risk cases omitted from studies, and these dangers may remain hidden because deterministic studies do not quantify risk [3]. The risk index computed in PRA measures the economic consequence of an uncertainty weighted by its probability of occurrence. This property provides a direct bridge between power system economics and security [61].

As already mentioned in section 1.1.2, the new Policy 3 – Operational Security of the UCTE Operation Handbook [6] – introduces the concept of Risk and it has also introduced a definition for the power system reliability as the “ability to ensure normal system operation, limit the number of incidents and avoid major incidents and limit the consequences of major incidents whenever they do occur”. It is intended to define the unacceptable consequences of incidents, identify the initiating events and define mitigation measures limiting the risks. IEEE also defines risk as the “product of probability and consequence”.

The operation of a power system from the point of view of risk management implies the definition of a risk level that should be respected for any kind of events. This risk level is assessed by a reference value of the product “Event probability x Expected loss”. The greater the probability of an event, the lower is the accepted loss. The loss may be defined either by a financial loss or more commonly for a power system in terms of a potential power cut or energy loss. By defining an acceptable risk level, a new paradigm is being introduced in power system operation: *Reliability, but not at any price* [6]. Although, this definition of “probability times consequence” can be misleading, because it can place a low-probability with high-consequences occurrence in the same level of risk as a high-probability with low-consequences occurrence. This needs to be forewarned in the development of this research work.

Normally, risk is represented with two dimensions (frequency of occurrence and consequences); hence it is illustrative to show it in a two-dimensional graph, as in figure 3.5, where the transition lines represent the same value of risk.

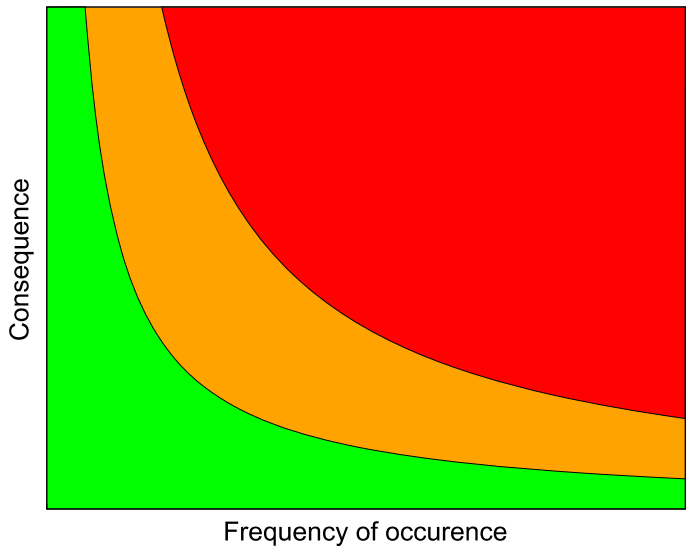


Fig. 3.5 – Illustration of a two dimensional risk graph

The quantified risk is evaluated according to specified acceptance criteria. The criteria are typically divided in low, medium, and high risk, which can be easily represented by colours, such as green, yellow and red. It is important to mention that the decision of what is an acceptable risk is a political and strategic question. The acceptable risk is something that has to be completely embraced. The probabilities of extreme incidents are low and difficult to assess accurately, because of lack of statistical data. Their consequences are usually severe, their costs equally difficult to assess, and in case of extended and prolonged outages, they are considered unacceptable.

The risk of power system failures depends on the frequency of the combination of faults and disturbances that lead to a system collapse and on the consequence of the interruption in terms of power and energy not supplied, duration of the outage, and other factors such as serious damage or injuries. This is closely related to the way the system is designed and the operating security criteria that are applied [4]. By quantifying risk we believe that is possible to turn the decision-making process more accurate. As mentioned in [21], risk management includes at least the following three tasks:

- Performing quantitative risk evaluation
- Determining measures to reduce risk
- Justifying an acceptable risk level

3.5.2. Risk-based security assessment

Over the last few years, several research groups have developed security assessment techniques that are explicitly based on the concept of risk. In a comprehensive series of papers [3], [17], [57], [61], [74-76], McCalley and co-workers have developed risk-based measures for various types of security assessment and various components of the power system. These measures of risk consider only a predefined set of contingencies, taking into account the probability of these events as well as the uncertainty affecting the future load and other system variables. The impact is measured in terms of the violations of the operating constraints that these contingencies would cause [48].

Reference [48] points to the fact that the results presented in the papers [17], [74-76] stand for an indirect quantification of the level of risk faced by users of the network, because line overloads and

voltage violations don't cause direct harm or adverse consequences for the system users. Depending on the operating conditions and on the set of simulated contingencies, the worst post-contingency constraint may not necessarily lead to cascade tripping or to a blackout situation.

Furthermore, violations of the acceptable limits do indeed weaken the transmission system and, this will obviously influence the risk level, having an indirect cost associated. This indirect cost is associated to the remedial actions that are necessary to return the system to a secure operation state. If only no cost measures are applied, the associated cost is zero.

Risk-based security assessment (RBSA) was first proposed in [76] by J. McCalley and his co-workers. One contribution of this work is the development of an index that quantitatively captures the factors that determine security level: likelihood and severity of events. However, other indices have been used in the past, and among these, deterministic methods have employed performance measures such as line current, voltage magnitudes, and stability margins. Yet these measures reflect severity but not likelihood. A well known probabilistic index, mainly used in planning, is loss of load probability (LOLP), but it reflects likelihood and not severity. Other probabilistic indices, the expected energy not supplied (EENS) and the interruption duration in minutes (so called system minutes), do capture likelihood and severity, but the measure of severity reflects only load interruption and not costs associated with equipment damage or lost opportunities from equipment unavailability [61]. Most previously presented probabilistic indices used rather crude rules based on fixed bus voltage and line current limits to identify when load interruption occurs.

The RBSA risk index proposed in [61] is a measure of the system's exposure to failure, which takes into account both likelihood and severity and uses a severity model that captures the consequences in terms of load interruption, equipment damage, and opportunity costs due to equipment outage. The mathematical expression for calculating risk is given by equation (3.3).

$$Risk(Im \mid X_t) = E(Im(X_{t+1}) \mid X_t) = \int_{X_{t+1}} \int_{E_i} Pr(E_i, X_{t+1} \mid X_t) \times Risk(Im \mid E_i, X_{t+1})\, dE_i\, dX_{t+1} \qquad (3.3)$$

Where I_m denotes the impact or cost-consequences associated with load interruption, equipment damage, or opportunity cost due to equipment unavailability. Here the risk associated with the pre-contingency operating condition X_t (e.g. loading, dispatch, voltage profile) is given by the expected values of the monetary impact of the operating condition in the next time period X_{t+1} (the next hour) given the current operating condition, i.e., $E(Im(X_{t+1}) \mid X_t)$. This expectation is the integral of the product of probability of the uncertain event, defined by E_i (the contingency state) and X_{t+1} (operating condition in the next time step) times its corresponding impact over the set of all possible events [61].

A distinctive feature of RBSA is that the impact of a specified contingency state E_i for a specified operating condition X_{t+1} is considered to be uncertain, therefore we denote it as $Risk(Im \mid E_i, X_{t+1})$ [61]. This analysis was illustrated on a modified IEEE Reliability Test System.

The uncertainty associated with each impact depends on the nature of the impact. For line overload, the uncertainty is in the ambient temperature, wind speed and direction, and solar radiation [77]. For transformer overload, the uncertainty is in the ambient temperature and the transformers' loading cycle [78]. For voltage security, it is in the interruption voltage level of the loads at each bus [75]. For dynamic (angle) security, it is in the fault type and fault location of the out of service circuit corresponding to contingency state E_i [76], [79].

Reference [61] presents several benefits of using RBSA for power system security assessment. First, it claims to provide a direct bridge between power system economics and security, which allows the operator to perform a security versus economy trade-off in the decision-making process. Second, it

presents the risk index as a leading indicator, using available information to take preventive actions preparing the system for the next time period (in operations planning environment). Third, the results of RBSA illustrate the functional dependence of risk on pre-contingency operating conditions that operators are able to monitor, understand and control. Fourth, since risk is computed for each security problem, for each contingency, and each component, it is easy to identify which components or operating conditions are causing it. Fifth, it provides a measure of the overall security level per region, because risk computation reflects for a local operating region or an entire system, the composite effect of all contingencies and all resulting security problems, including those associated with overload, voltage and dynamic (angle) security. Sixth, risk can be calculated for each operating condition and the summation over all time instances provides a cumulative risk assessment over the specified time period. Finally, RBSA provides the capability to manage security based on the decision maker(s) preference regarding risk exposure.

Referring other authors that have developed research in risk-based security assessment, in order to present different approaches, it is important also to point out D. Kirschen and his associates work. With references [48-51] and [67], [80], it is possible to get a global vision of their work. A steady-state security assessment is performed and the contingencies are generated randomly instead of using a predefined list through Monte Carlo simulation. The possibility of hidden failures in the protection system is considered, because it may cause sympathetic tripping of intact components in the vicinity of the fault and, in fact, many severe contingencies have hidden failures associated and leading to cascade. They also analyse the consequences of these contingencies to determine whether additional branches, generators and loads might be disconnected because of overload, load/generation imbalances and voltage or transient stability [48]. The latter introduces the concept of corrective actions taken by the operators to restore a secure operating state and with this approach it is possible to evaluate the impact of random contingencies, concerning to energy not supplied (ENS). As explained in [48], using a model of the restoration process, this is translated into ENS. In turn, the ENS can be multiplied by the estimated value of lost load to obtain an estimate of the cost of an outage. Integrating this calculation in a Monte Carlo simulation ensures that the probabilities of various events are properly taken into account and yields an estimate of the actual risk faced by users of the transmission system under the considered conditions. The drawback of this approach is that it relies on a Monte Carlo simulation, thus a considerable amount of computing resources is required and therefore is not compatible with online analysis.

Reference [71] presents two application examples of probabilistic risk assessment (PRA) in power system operations. In the first example, a risk based method is proposed to take the uncertainty of contingency occurrence and impacts into account to provide an essential set of contingency cases for a transient stability special protection system (SPS) implementation. In the second example, an approach for determining the power transfer limit of a longitudinal electric power system is presented. In these examples, the PRA method retains the numerical tools and procedure of the traditional deterministic approach, but also includes the computing of operation risks which account for contingency occurrence probability and impacts in terms of load shedding and generation rejections to avoid system transient instability.

3.5.2.1. Voltage security assessment

In any electricity transmission system, a stable condition must be assured, but power systems are currently more complex and heavily loaded, which means that voltage collapse is becoming an increasingly serious problem. It is possible that, under specific conditions, the system can be placed on a state in which it may not be possible to maintain the voltage levels within secure limits in one or more of the network busbars. Economic and environmental concerns limit the construction of new transmission lines and generation capacity, thus increasing the stress on the operating conditions and consequently placing the system closer to its stability limits. Voltage collapse can be defined as instability of heavily loaded electric power systems that lead to declining voltages and blackout, which has severe security repercussions and jeopardizes the essential service to final customers. System instability can occur if one or more grid elements disconnect by tripping (contingency), the load increases suddenly or the

geographical profile of the generation dispatch is abnormal [5]. Or even if the system is subjected to reactive power shortages [75].

Reference [75] presents a method to calculate the risk of voltage insecurity for a given short term operating condition, which provides a quantitative justification of reliability in terms of system economics. There are two distinct outcomes for the future performance of system voltages, collapse or no collapse. In case of a system operating without suffering a voltage collapse, the voltage may go below the tolerance of loads, resulting in load interruption, which will lead the voltage back to the acceptable range. On the other hand, under some conditions, the system may approach a voltage collapse although all voltages are close to their nominal values. Considering these two situations, risk expression is given by equation (3.4).

$$R(X_0) = P(Collapse|X_0) \times E[I(Collapse)] + [1 - P(Collapse|X_0)] \times E[I(NoCollapse)] \qquad (3.4)$$

where, X_0 stands for the current operating condition. $R(X_0)$ depends on the probability of voltage collapse $P(Collapse|X_0)$ under X_0, the expected impact of collapse $E[I(Collapse)]$ and the expected impact of no collapse $E[I(NoCollapse)]$. All items are calculated as described in [75].

3.5.3. Online risk-based security assessment

Online risk-based security assessment (OL-RBSA) evaluates the risks of the power system operating in real time. The time frame for this kind of assessment is usually short (such as within one hour). It computes the risks for the power system for the next several minutes up to the next hour.

The use of online risk indices in a control room provides additional information to operators, leading to a better understanding of the system state and of potential network problems, such as overload, cascading overload, voltage limit violations and voltage instability. Therefore, it is possible to achieve an improved decision making process, regarding security assessment.

The Task Force on Probabilistic Aspects of Reliability Criteria of the IEEE PES Reliability, Risk, and Probability Applications Subcommittee has presented in 2004 reference [3]. The probabilistic index presented in [3] was shaped by the recognition that an important objective of security assessment is to analyse the future. In the traditional deterministic assessment, the online analysis uses the most recent state estimation, whose results are descriptive of the conditions sometime in the past. In the Portuguese transmission system, the state estimation results are updated at least every 5 minutes, which is adequate for online analysis.

The state estimation results can be used to extend the assessment into the future so that decisions can be made on expected future conditions. However, such an extension requires not only a forecast of future operating conditions but also appropriate models of forecast uncertainty [3]. Reference [3] aims to perform security assessment of a power system for the purpose of making a decision that will be effective for some time in the near future. The presented method to evaluate risk was tested in an IEEE test system.

An online risk-based security assessment (OL-RBSA) is presented in [17], aiming to provide rapid online quantification of the security level associated with an existing or forecasted operating condition. This approach condenses contingency likelihood and severity into indices that reflect probabilistic risk, using the forecasted near future operating conditions. The traditional online security assessment uses the last state-estimation snapshot to perform analysis, which means the assessment is done with a recent past condition. This OL-RBSA method includes overload security (flow violations and cascading overloads) and voltage security (voltage magnitude violations and voltage instability).

The risk index is the product of the outcome probability with its severity. In figure 3.6, assigning probabilities to each branch, the probability of each terminal state is the product of the probabilities assigned to the branches that connect the initial state to the terminal state [17].

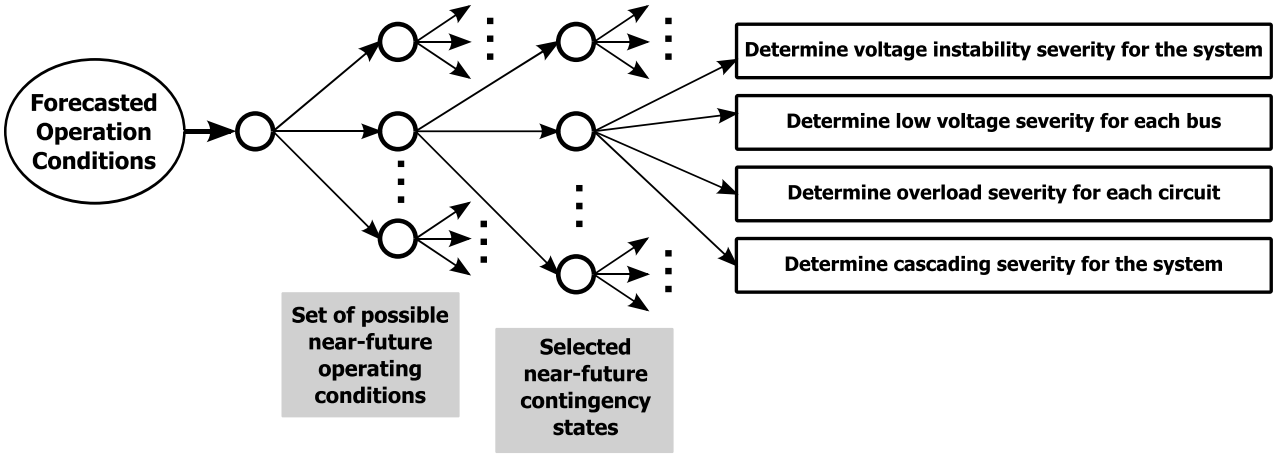


Fig. 3.6 – Illustration of OL-RBSA process [17]

Assigning severity values to each terminal state, the risk can be computed as the sum over all terminal states of their product of probability and severity, as shown in equation (3.5) [17].

$$Risk\left(X_{t,f}\right)=\sum_{i} P_r\left(E_i\right)\cdot\left(\sum_{j} P_r\left(X_{t,j}\middle|X_{t,f}\right)\times Sev\left(E_i,X_{t,j}\right)\right) \qquad (3.5)$$

Where, $X_{t,f}$ is the forecasted condition at time t; $X_{t,j}$ is the jth possible loading condition; $P_r\left(X_{t,j}\middle|X_{t,f}\right)$ is the probability of load forecasted uncertainty; E_i is the ith contingency and $P_r\left(E_i\right)$ is its probability; $Sev\left(E_i,X_{t,j}\right)$ quantifies the severity of the ith contingency occurring under the jth possible operating condition. It represents the severity for overload, low voltage, voltage instability and cascading overload.

The severity function has to measure the consequences of a contingency and it needs to be fully understandable by control room operators, because they need to react according to the extent of the violations in the network parameters. Reference [17] presents several options for severity functions, namely:

- Severity function for low voltage in each node (busbar); this severity function can be discrete (one if the voltage magnitude is lower than the low voltage rating, and zero otherwise). It can also be a percentage of violation severity function (which measures the voltage magnitude with respect to the lower voltage level and estimates a percentage of violation) or it can be a continuous severity function (the severity increases linearly with the decrease in voltage magnitude).
- Severity function for overload defined to each circuit (line or transformer); the power flow as percentage of rating of each circuit determines the overload severity of that circuit. It can also be defined as a discrete, continuous or percentage of violation severity functions.
- Severity function for voltage instability; this is a system severity function rather than a component severity function. It uses the loadability corresponding to the system bifurcation point to determine the voltage instability severity.
- Severity function for cascading overloads; Risk of cascading overload is calculated through an iterative algorithm with three assumptions, namely: cascading is a sequential succession of dependent events (which can vary greatly), a circuit will be removed from service if its MVA flow exceeds K times its emergency overload rating and no control action is applied by the control room operator.

3.5.4. Risk index for protection systems hidden failures

Reference [68], [70] explains the technique of hidden failure analysis of protection systems and presents how to determine their severity as well as the risk posed by these occurrences. As already mentioned, for a hidden failure to cause a false trip, it is necessary that a fault occurs in its vicinity. The index of severity ranks the protection schemes according to the overall effect of consequential tripping of two power system elements. The index considers the dynamics of the protection schemes and is calculated based upon the extent of the region of vulnerability, the loss of load, the loss of generation and the ability of the system to reach a post-disturbance steady state after the contingency. This severity index also provides a prioritized list of places on the power system where countermeasures against hidden failures must be implemented in order to have the greatest impact on the power system's ability to resist cascading failures. It is clear that this chain of contingencies are dependent upon each other due to the protection system interactions, either directly or indirectly via the changes in the distribution of power through the network, and due to the possible multiple impacts of a triggering event. Consequently, the probability of occurrence of cascading failures is much higher than the probability of a random (i.e. independent) tripping of any two components of the system.

The approach is based on a dynamic event tree to describe power system cascading failures. Once the probability of system failures has been evaluated, it is important to assess the system failure significance (i.e. risk index) that accounts for both the probability and severity of a system failure, which is defined as in equation (3.6).

$$R_i = P_i \times S_i \times w_i \tag{3.6}$$

where:

R_i - Risk index for i^{th} trigger event.

P_i - Probability of system failure due to i^{th} trigger event.

S_i - Severity index for system failure due to i^{th} trigger event.

w_i - Weighting factor, this is used to account for the importance of loss of load, loss of key substations, or system instability.

Reference [67] presents a risk index associated with the outage of lines k and j that is calculated as in equation (3.7).

$$R_{kj} = P_{kj} \times Severity_{kj} \tag{3.7}$$

P_{kj} is the system state probability following the double contingency of lines k and j given that the outage of line j is due to a hidden failure revealed by the fault in line k. $Severity_{kj}$ is assessed for two situations:

1. Power flow convergence is achieved after load shedding, when necessary
2. When power flow converges normally, an indicator is calculated to evaluate the level of stress in the system, which is prone to system collapse.

3.5.5. List of software found in the literature

Several software tools were found in literature to perform risk assessment of an electrical power system.

3.5.5.1. Probabilistic reliability assessment

The Probabilistic Reliability Assessment (PRA) software pack is described in [15] with the following features:

- It offers energy companies a more accurate tool for assessing grid reliability under restructured market conditions.
- It calculates a measure of the probability of undesirable events and a measure of the severity or impact of the events.
- It provides the means to identify the most critical potential grid failures, identify bottlenecks in the grid, evaluate their adverse impacts and recommend effective mitigation alternatives.
- It allows the assessment of trade-offs between the probability of a contingency and the cost of operational changes to avoid those contingencies.

As described in [15], [81], [82], PRA consists of two commercial software packages:

1. Physical and Operational Margins (POM), which is a fast contingency analysis tool, licensed by V&R Energy Systems Research, Inc. (V&R) to EPRI and qualified EPRI members.
2. Probabilistic Reliability Indices (PRI) is a software pack, developed by EPRI, to compute and display reliability indices, which uses the contingency analysis results and equipment outage information as inputs.

The reliability is measured by the PRI, which is defined as product of an impact by a probability. The impacts and the reliability indices are of four distinct types: APRI (amperage or thermal overload), VPRI (voltage violation), VSPRI (voltage instability) and LLPRI (load loss). These indices are described in [65].

A practical method of probabilistic reliability evaluation was implemented in the Korea Power system, as described in [81], using PRA and POM. This case study computes the Probabilistic Reliability Indices (PRI) of Korea Power system from 2007 to 2012. It takes a large number of contingencies in load flow simulations and combines them with a practical method of characterizing the effect of the availabilities of generators, lines and transformers. Figure 3.7 presents an overview of the organization of PRA.

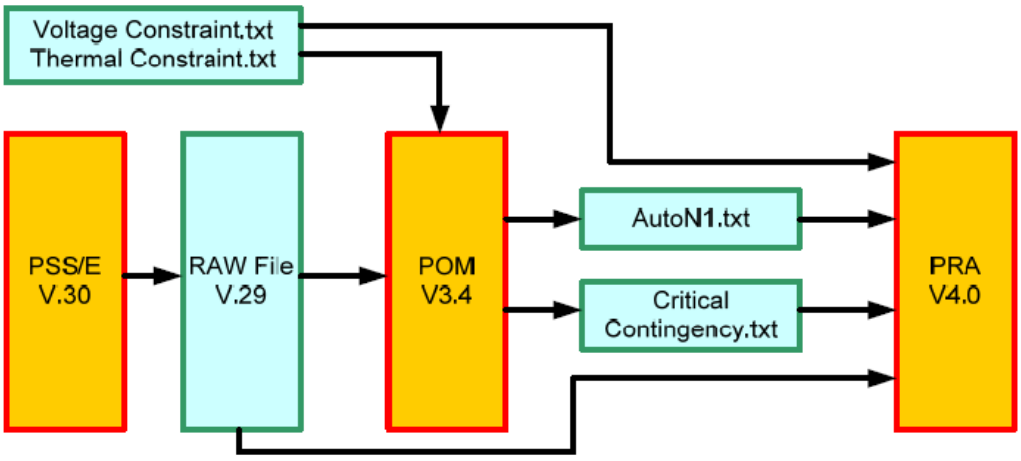


Fig. 3.7 – Overview organization of PRA used in Korea Power System [15]

In spite of this case study being a planning analysis, because it presents a probabilistic reliability evaluation for the system for the next 5 years, it has an interesting organization also for operations environment.

Figure 3.8 shows the POM and PRA flowcharts.

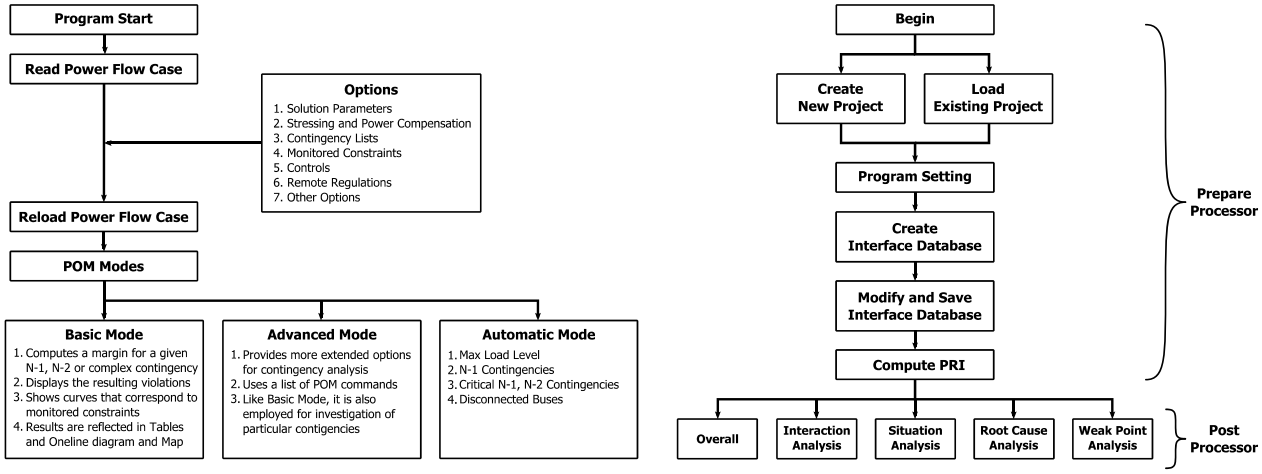


Fig. 3.8 – POM and PRA flowchart [82]

The methodology presented in reference [65] has been implemented in the described PRA software packages. It was applied on the US Eastern interconnection and has been applied by several utilities belonging to the EPRI PRA user group. It simulates contingencies selected by enumeration and draws a quantitative and probability-weighted evaluation of the system behaviour, concerning changes in system configurations that lead to a violation of operation limits (branch thermal ratings, bus voltage limits, and voltage instability). The flows and voltages resulting from the simulations provide the data to calculate impacts, which are also the ones described previously. These violations may be mitigated by remedial actions in an extended methodology. This paper shows an application of the method in a planning environment, because the results are used to provide insights on root causes, weak points and regional causes and effects and for developing effective remedial actions or investment options. It has also been mentioned that the reliability indices could be used for measuring or monitoring bottlenecks, if an online computation of these indices is implemented. Hence, the PRA methodology could be adapted to an operation environment by keeping and modelling the time dependence nature of that situation probability [65].

It makes sense to translate all the calculated impacts (APRI, VPRI, VSPRI and LLPRI) into costs and in reference [65] a single reliability cost is presented, which sums up the cost components derived by multiplying the PRI components by appropriate cost coefficients. In order to do that, it will be necessary to have data relating the cost attributable to these unacceptable impacts.

3.5.5.2. Other software packs

Reference [72] has used RiskSpectrum software to build the substation reliability model. Thus, the event and fault trees were created and analysed by its use. This software package calculates the probabilities of the different events and it also analyses several importance measures. The software includes advanced tools for fault tree and event tree analysis, documentation, risk monitoring and failure mode and effect analysis.

To perform transmission reliability evaluation for large scale systems, references [83-86] refer reliability software, called TRELSS, which was used to calculate indices, such as: probability of load curtailments, expected duration of load curtailments, expected energy not supplied, loss of load probability, energy index of reliability and expected interruption cost. This software is mainly used in planning studies and it uses a probabilistic value-based approach that enables system planners and operators to maintain transmission networks that balance cost and reliability. TRELSS ranks contingencies according to system failure and systematically lists failures according to their probability of occurrence. The system failure criteria include circuit overload, high and low voltages, bus voltage deviation, islanding, capacity

deficiency and divergence of load flow. TRELSS also solves load flow and applies remedial actions (Linear Programming based) when necessary. Reliability indices are computed at the system and bus level [14].

3.6. Conclusion

From the bibliography research, most of the work presented is focused on the planning field. Only lately because of the competitive environment, the attention is being turned into power system operations. There is a limited number of publications that analyse power systems security with a risk-based approach in an operations environment and an even more limited set for online assessment. Many of the references applied to planning environment calculate annual risk or reliability indices and most of them are not applicable to real system due to its dimension, being only tested in smaller IEEE test systems.

Reliability of power systems is divided into two different aspects: security and adequacy. Reliability criteria are rules by which the performance of an electric power system due to component failures, in different loading conditions, can be judged acceptable or unacceptable. Unreliability by definition is linked with energy not supplied, which has a high cost to system operation. It is difficult to judge security price when supply interruptions are uncommon and when they happen they are normally solved very quickly. If the major disturbances were much more frequent, the price of security that consumers would be willing to pay would probably be much higher.

Risk includes both the probability of occurrence (or frequency) and severity (or undesirable consequences) of contingencies and, in real life, it is neither possible to eradicate contingencies nor reduce risk to zero, but it is possible to choose an acceptable risk level and avoid certain risks. Many different kinds of risk can be discussed, such as security risk, social risk, economic risk, investment risk, safety risk, political risk, etc [73]. Hence, the risk definition has to be adapted according to the specific problem, which is being analysed. In most of the analysed publications, risk is measured through constraint violations, but it is important to be aware that overload will not necessarily result in a cascading sequence of events and neither a low voltage (below the acceptable limits) will necessarily result in a voltage collapse, although the constraints weaken the electrical power system and they should be considered and evaluated.

It is necessary to prevent that when applying the definition of risk such as probability times impact, as a single measure, the result will be misleading, i.e., placing in the same level of risk both low-probability with high-consequences and high-probability with low-consequences occurrences. A contingency with extremely severe consequences may have low probability of occurrence and a “normal” contingency (such as N-1 contingency) may have high probability of occurrence and low impact. These two situations cannot be placed at the same level of risk, because the social and financial losses are completely different. Therefore, risk as a single measure of the security level alone might not be enough and the control room operator plays an essential role, distinguishing what is more important. Another possibility is to evaluate the cost of each contingency and provide operators with this additional information. Obviously, for a power system, the most important measures after a disturbance are the amount of energy not supplied and the interruption time.

Contingencies can be classified as independent and dependent and divided as single or multiple. The number of possible contingencies in a transmission system is huge and it is not feasible to analyse them all, therefore it is essential to select a range of contingencies that is crucial for system online security analysis. In literature, contingency selection is made either by enumeration methods or by sampling methods. Enumeration is the most suitable method for online evaluation. In the latter, contingency selection is normally based on: what has been used in the deterministic approach; the most severe known contingencies; and the likelihood of events based on the historical incidents data base.

The probability of events based only on the historical data does not include in its calculation neither current conditions nor system characteristics. Especially for online assessment, the inclusion of current

conditions and of all the characteristics that influence directly the value of the probability of contingency is of paramount importance. Therefore, inputs such as the ones mentioned in section 1.4.1 (e.g., weather conditions and environmental conditions, among others) must be included in the calculation and continuously updated when concerning current conditions. This was something which was not very deeply studied yet in system operation security assessment.

Probabilistic tools are complex for power system operators to work with due to their interpretation of system security [62]. Deterministic assessment versus probabilistic assessment is extensively discussed in this research work and it is also a broadly discussed topic in literature, where the weaknesses and strengths of deterministic when compared with the probabilistic approach are pointed out. Traditional security assessment does not consider: the likelihood of contingencies, the uncertainty in the operating conditions neither the effect of longer overhead lines. It only addresses the severity of contingencies, in terms of thermal loading, voltage violations and loss of load. Therefore, it includes in the analysis neither the possibility of cascading tripping of lines nor the possibility of protection system hidden failures, which can cause major blackouts and can have severe financial and social impacts. If the power system withstands the specified criteria then it is considered secure, if not, it is considered insecure. The security is checked by a deterministic contingency analysis, taking into account the set of contingencies considered most probable to happen, although for the analysis all events are considered equally likely. Contingencies can only be analysed rigorously using probabilistic techniques, because they are random in nature. The probabilistic assessment gives the opportunity to include in the probability calculation the geographical influence, the seasonality and hourly distribution through historical failures rates, and also current conditions.

To perform the severity evaluation a network model is needed and for that the best way to achieve it is to use the State Estimator snapshots that contain the information needed, regarding topology information, load pattern and generation profile. It is important to be aware that it is not only contingencies that are unexpected in the operation environment, load and wind generation pattern also have uncertainty associated. To perform a rigorous security assessment, load and wind generation forecast and also market-driven generation patterns must be considered for the period under analysis. Other information to be considered is the expected outages in the system.

In the control room, decisions have to be taken timely and as accurately as possible, which means that the operator needs to make a rigorous analysis of the system in a very short period of time, finding the best trade-off between security and economy. A risk assessment methodology with a probabilistic analysis can provide control room operators with indices for the next period, supporting them in the decision making process.

Chapter 4.

The Portuguese Transmission System

4.1. Introduction

This chapter aims to give insight into the Portuguese Transmission System (PTS) in order to present its most important characteristics and how the system is operated. To develop a methodology to evaluate risk, it is essential to be able to evaluate the severity of the analysed contingencies and the following information will be crucial to support future analysis and decision. The Portuguese transmission system is a medium size system, which has interconnections only with Spain, through 7 overhead lines. The transmission system operates at 400kV, 220kV and 150kV. The border with the distribution system lies at the circuit-ends of the 60 kV lines, which means that REN also owns EHV/HV transformers, HV (60 kV) busbar and 60kV bays installed in their substations.

Power system characteristics and the manner in which it is operated depend on several factors, such as:

- System size
- Topological structure (e.g., highly meshed network) and voltage level
- Generation mix and pattern distribution
- Load type and its distribution
- Market rules
- The interconnection with other countries
- Operating criteria, including security and reliability requirements
- Types of controls available and special protection schemes implemented
- Exposure to disturbances due to weather, environment and other internal and specific factors

REN, as the Portuguese Transmission System Operator (TSO), is responsible for the system planning, design, construction, operation and maintenance of its infrastructures. It is responsible for permanently maintaining the balance between generation and load by monitoring the system security, supervising all the equipment and adjusting the cross-border power flows with the Spanish grid. This is the task of the national control centre located in the vicinity of Lisbon. On the other hand, the grid operations control centre, located near Oporto, is responsible for monitoring and supervising the status of the Portuguese transmission system, for coordinating works in the system, ensuring the safety conditions, and for its remote operations and switching, e.g., system restoration. These two control rooms receive all the system's information in parallel (power plant information, power flow in the interconnections, the part of Spanish grid which is monitored and all the Portuguese grid nodes and lines) through a redundant and extremely reliable communications network, being connected with each other through two high speed links. Although each control room has a specific task, in case of an emergency both are equipped to perform each other's tasks next to their own [87].

The Portuguese system is diverse in terms of primary energy sources for generation, including hydro, natural gas combined cycle, wind, photovoltaic (solar panels), biomass, combined heat and power (CHP), fuel-fired and coal-fired power plants. Nowadays, the Portuguese government provides significant incentives for the use of renewable sources, because these power plants help to reduce CO_2 emissions in the electricity generation mix and the dependency on imported primary energy sources, such as coal, oil and gas. The goal is to produce 39% of the national electricity consumption through renewable energy sources until 2010, fulfilling European Community directive 2001/77/CE [88], and this is the reason for the appearance of wind farms with an increasing growth rate, connected to the EHV network. In 2007, the

39% target was revised by the Portuguese Government and a new goal of producing 45% of the national electricity consumption through renewable energy sources until 2010 was announced. This new goal is part of the National Energy Strategy published by the Ministry of Economy and Innovation [1].

Electricity consumption totalled 49.9 TWh in 2009, with a downward trend of 1.8% below on the previous year. Figure 4.1 presents the yearly evolution of the electricity consumption in the Portuguese System from 2000 to 2009. In 2009, the peak load in the system occurred on January 12 and it was about 9 GW.

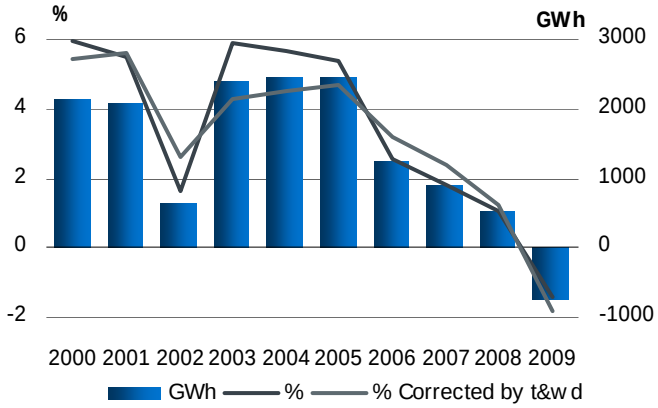


Fig. 4.1 – Yearly evolution of the consumption in the Portuguese System [89]

In 2000, the TSO function was unbundled from the vertically integrated structure and therefore REN became an independent company, defining a new investment approach [90]. Due to the level of investment in the Portuguese network, in the construction of new infrastructures and improvements to the existing ones (such as substation refurbishment and OHL uprating programs), it is possible to achieve the main goals of the electricity grid that are defined by law and regulations in force. Reference [87] describes the most important goals as follows:

1. Guaranteeing supply
2. Connecting new and large generation centres
3. Creating adequate conditions for the integration of renewable energy sources and for the reception of their generation
4. Creating conditions for the operation of the Iberian electricity market
5. Finding solutions to feed directly the EHV customers connected to the transmission grid
6. Prioritizing and coordinating plans for refurbishing or replacing equipments or systems at the end of their useful life
7. Increasing the interconnection capacity, in order to avoid market splitting

Especially for the first four items, it is essential to increase the transmission capacity, to reduce the constraints and to expand the transmission system throughout the national territory. As mentioned in reference [87], the construction of new infrastructures and improvements to existing ones have an impact on the socio-economic development of the region in which they are located.

Until the end of 2009, the OHL uprating actions have already covered approximately 40% of the OHL total length, aiming to increase the transmission system capacity. The uprating consists mainly in tower elevation but also includes insulator replacement, double earth cable (one OPGW) and, in few cases, new conductors [90].

The level of investment creates an extremely dynamic system in terms of assets: the OHL length and the number of substations (i.e. the number of grid elements) are increasing at a high rate and because of that the grid configuration and the OHL designation change very quickly, creating an additional issue to be addressed in the development of this work. Due to this fast development, it will not be possible to assess risk for each particular grid element, but it will only be possible to assess risk for each type of

element or for each type of path (especially in the case of OHLs, including its characteristics). The final results will consider the grid elements in service at the moment of the analysis. This approach will make the results independent of the existing grid.

The map of the Portuguese network is presented in appendix A.

4.2. Network characteristics

In the scope of this work, the analysis will be limited to the 150 kV, 220 kV and 400 kV network, excluding both the 132 kV (which represents only one OHL, normally disconnected, with a length of 9 km and a very limited transmission capacity), and the 60 kV equipment that belongs to REN. The analysis period of this work begins in 2001 and ends in 2009, thus this section describes the Portuguese transmission network characteristics for that period. Table 4.1 presents the line length evolution in the PTS, where approximately 16 km are underground cables:

	2001	2002	2003	2004	2005	2006	2007	2008	2009
132kV	9	9	9	9	9	9	9	9	9
150 kV	2352	2412	2429	2189	2274	2422	2652	2658	2662
220 kV	2599	2717	2704	2838	2875	3080	3177	3257	3289
400 kV	1235	1301	1403	1454	1500	1507	1588	1589	1609
Total	**6195**	**6438**	**6544**	**6489**	**6657**	**7018**	**7426**	**7513**	**7569**

Table 4.1 – Total Line length per voltage level in the PTS

The different EHV voltage levels are interconnected by autotransformers (AT). Table 4.2 presents the installed autotransformers in the PTS facilities in the period under analysis:

	2001	2002	2003	2004	2005	2006	2007	2008	2009
AT 400/220 kV	6	6	7	7	7	7	8	9	9
AT 400/150 kV	7	8	9	9	9	9	9	9	10
AT 220/150 kV	7	6	7	7	7	7	8	8	7
AT 150/132 kV	1	1	1	1	1	1	1	1	1
ATD 400/150 kV						1	1	3	4
Total number of AT	21	21	24	24	24	25	27	30	31
Total installed power (MVA)	6271	6401	7421	7421	7421	7871	8571	9921	10701

Table 4.2 – Number of autotransformers and installed power in the PTS

The interconnection between the EHV voltage levels and the 60 kV level is done by transformers (TR), which are still considered EHV grid elements in terms of statistics and therefore they are included in the analysis. Table 4.3 presents the installed transformers in the PTS facilities in the analysis period:

	2001	2002	2003	2004	2005	2006	2007	2008	2009
TR 400/60 kV	4	5	7	7	7	9	10	12	13
TR 220/60 kV	53	55	55	56	57	60	63	68	74
TR 150/60 kV	44	43	41	41	43	43	45	48	49
TR 150/130 kV									1
TR 150/30 kV	4	4	4	4	4	3	3	2	2
Total number of TR	105	107	107	108	111	115	121	130	139
Total installed power (MVA)	10781	11266	11744	11977	12547	13264	14526	16273	17534

Table 4.3 – Number of transformers and installed power in the PTS

The static reactive power compensation is made through shunt capacitors installed in the 60 kV level. Table 4.4 presents the number of shunt capacitors installed in the PTS facilities in the period under analysis:

	2001	2002	2003	2004	2005	2006	2007	2008	2009
Total installed power (Mvar)	1170	1230	1250	1370	1420	1770	1910	2000	2050

Table 4.4 – Installed power of shunt capacitors in the PTS

Table 4.5 shows the characterization of the PTS facilities during the analysis period

Facilities	2001	2002	2003	2004	2005	2006	2007	2008	2009
Nº of substations	48	54	55	56	56	59	63	67	70
Nº of 400 kV busbars	22	24	24	26	26	30	32	32	34
Nº of 220 kV busbars	44	46	48	48	48	52	56	62	66
Nº of 150 kV busbars	45	45	45	45	45	47	53	55	57
Total number of bays	463	462	500	511	522	557	615	668	725
Nº of 400 kV bays	69	60	84	91	95	113	127	143	164
Nº of 220 kV bays	216	219	228	240	244	253	275	291	316
Nº of 150 kV bays	178	183	188	180	183	191	213	234	245

Table 4.5 – Characterization of PTS substations

To populate table 4.5, only the busbars that are most of the time effectively in service are considered.

4.3. The generation mix

As it was already mentioned, the Portuguese system has a very diverse set of primary energy sources for generation. It includes hydro, natural gas combined cycle, wind, photovoltaic (solar panels), biomass, CHP, fuel-fired and coal-fired power plants. Strategically, Portugal aims to supply 45% of the national electricity demand from renewable energy sources, which has strongly encouraged the appearance of wind farms connected to the network. Figure 4.2 presents the wind generation evolution from 2000 to 2009.

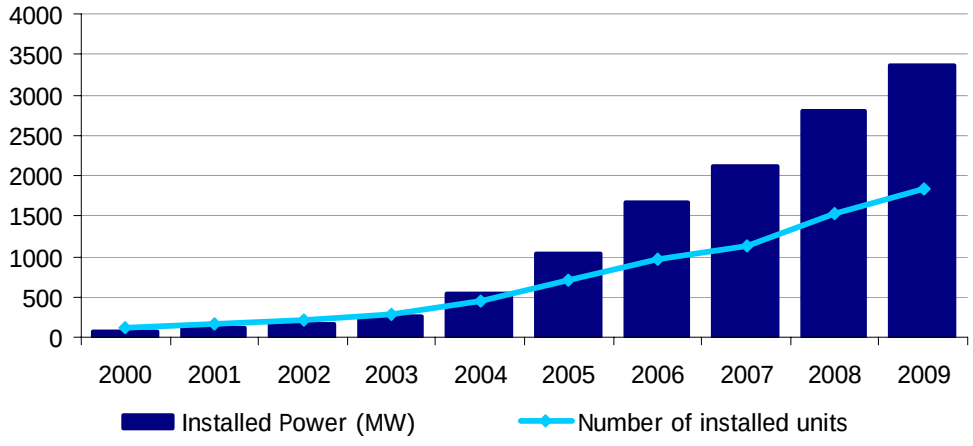


Fig. 4.2 – Wind generation evolution in the Portuguese System [91]

The big hydro and thermal power plants are in the electricity market (MIBEL), but the wind farms, and other that are considered by law as special regime generation (which includes small hydro, biomass, CHP, photovoltaic) are paid with a favourable feed-in tariff and all the generated power is absorbed by the grid independent of market conditions. The wind characteristics and the obligation to absorb their production represent a major challenge in maintaining the balance between generation and demand in system operation, namely to allocate generation reserve in order to perform the necessary adjustments. One of the efficient solutions that can be used is to combine wind generation with pumped-storage plants,

especially in off-peak hours when the wind generation exceeds the system needs, in order to fulfil the established security criteria.

In Portugal, at the moment, the installed hydro generation capacity represents about 50% and the installed wind capacity 36% of the national peak demand, turning wind into a meaningful component of the generation mix. The contribution of each energy source in the consumption supply is presented in figure 4.3.

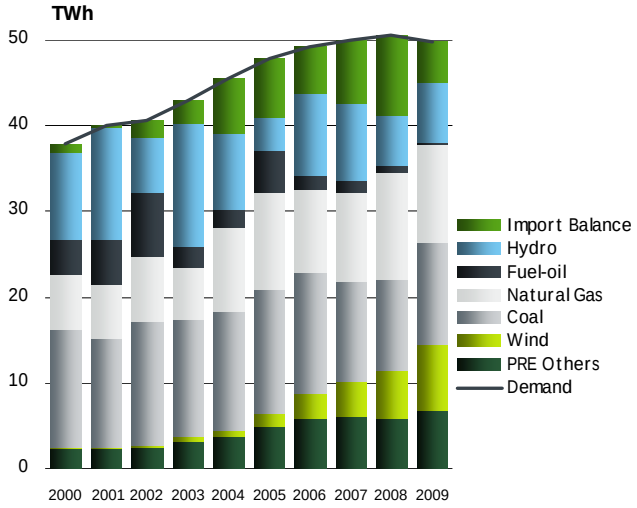


Fig. 4.3 – The contribution of each energy source in the consumption supply [89]

Despite its intermittent characteristic, wind generation guarantees on average more than 2000 working hours per year, whilst hydro generation presents a great variability depending on the yearly rainfall, from around 1000 hours in dry years to around 3000 hours in wet years. The number of hours per year is calculated dividing the annual produced energy by the installed power, which is equal to the utilisation factor [46] multiplied by the number of hours per year. Wind is dependent on weather conditions, and to cope with the intermittency of wind generation, research and development partnerships have been set up between REN, universities, producers and public institutions, to develop new methodologies for wind power forecast and control, decision support to system operation and maximization of the wind farms potential in the country.

4.3.1. Impact of wind generation

The reason to emphasize wind generation in this research work is because it represents an additional risk factor to the system when facing a disturbance. With the increase of wind generation connected to the grid, it is important to be aware of its impact on the bulk transmission system operation (including transmission and generation systems), namely:

- The trip of wind farms facing short-circuits, causing an instantaneous deficit of generation in the system which is automatically compensated by the tie-lines. Fault ride through capability is required to prevent the loss of wind generation (see figure 4.4).
- The additional need for generation reserve, in order to cope with wind fluctuations and the behaviour of wind farms in case of disturbance.
- Off-peak generation surplus caused by wind energy, needing compensation to maintain the system's security criteria.
- Lack of capacity to perform voltage regulation and primary reserve, creating additional problems in real time operation; however, in the future, wind generation could contribute to primary control in the direction of reducing active power with frequency increase.
- The lack of information about the distributed generation embedded in the distribution network, which causes difficulties in controlling an emergency situation.

In the scope of this research work, only the behaviour of wind power plants when facing incidents is relevant for the analysis, because it surely influences the severity of contingencies. This behaviour is described in some of the incidents treated in chapter 2, for instance the 4th November 2006 emergency situation. Short-circuits provoke voltage dips in the power system with the duration of the fault clearing time, consequently causing some wind farms (those not equipped with "Fault Ride-through capability") to trip.

On average, 86 % of the faults are cleared in less than 150 ms (see section 5.3.5.2) and there are records where the maximum loss of wind generation caused by a disturbance already reached or exceeded the power value of the biggest unit in the system (400 MW), thus possibly demanding more generation reserve. To prevent disconnection of wind turbines during short-circuits in the system, units must stay connected for voltage dips having the characteristic presented in figure 4.4, which is taken from the new regulation. It is also beneficial to the system if wind generating units inject reactive power during a short-circuit, because it mitigates the voltage dip.

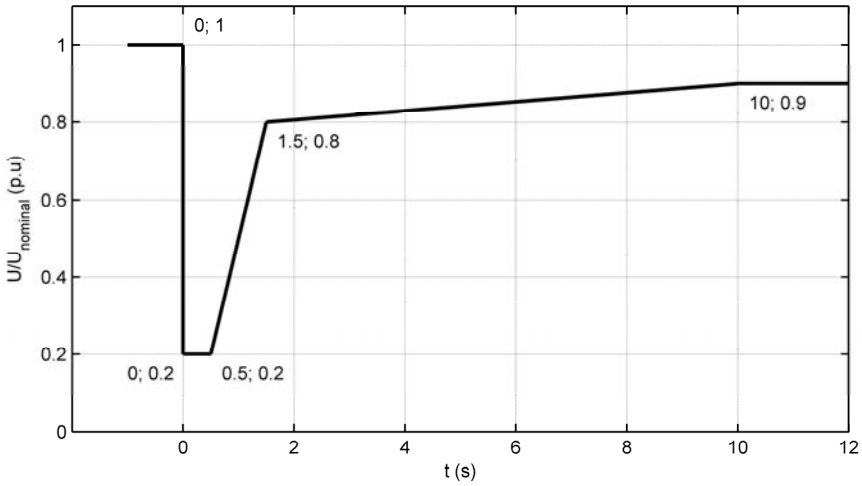


Fig. 4.4 – Voltage dip characteristics to be withstood by wind generating units

Due to the large amount of wind farms connected to the same grid node, the Portuguese TSO has installed phase-shifter autotransformers in two substations in order to control the active power flows coming from wind farms and directing them into the 400kV network, which has a bigger transmission capacity and lower losses. The wind farms connected to the PTS are on the 150 kV and 220 kV voltage levels, although the majority of wind farms in Portugal is connected to lower voltage levels on the distribution network.

In incidents analysis, the loss of wind generation is now also considered, in order to understand the risk level for each wind farm when facing a disturbance. On 15th November 2009, at 11:14 and at 14:35, simultaneously with a short-circuit in a 220kV OHL in the interior north of Portugal, about 1300MW of wind generation was lost, because of a voltage dip of 40% of amplitude that lasted only 80 milliseconds. According to figure 4.4, this voltage dip should be withstood by fault-ride-through capability. Both faults were phase-to-phase faults and strong wind was the most plausible cause for the faults. It is relevant to note that the span, where both short-circuits occurred, has a length of around 1500 meter. After the analysis, it was possible to identify which wind farms were with and without active fault-ride-through capability and to conclude that approximately 15 minutes after the disturbance about 60% of the wind generation was again reconnected in the system.

Figure 4.5 shows the area control error (ACE) of the Portuguese system when facing the first short-circuit. The deviation in the interconnections was recovered in 8 minutes, placing the ACE within the acceptable range. The fast recovery was due to the reconnection of the lost wind generation and the start of fast reserve (2 hydro power plants plus changing the operation mode of the units that were functioning as pumps to reactive power compensation). Through a short-circuit simulation, it was possible to conclude that the wind farms that lost all their units were in the area where the voltage was below 0.8 $U_{N.}$

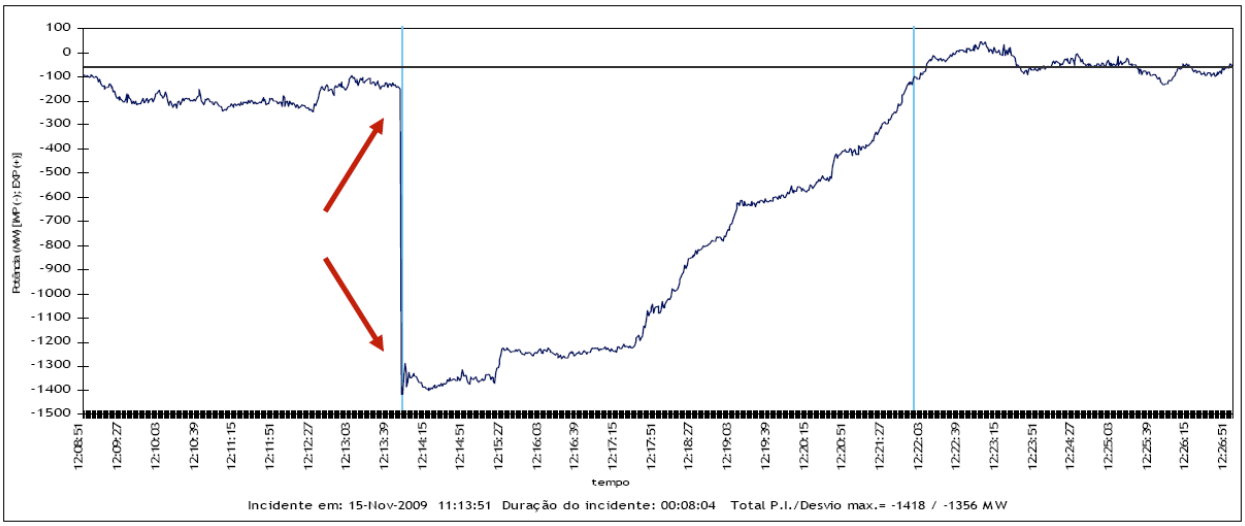


Fig. 4.5 – ACE of the 220 kV OHL short-circuit on 15th November 2009 at 11:14

Figure 4.6 shows the geographical distribution of the wind farms and their response to both short-circuits that occurred in a 220 kV OHL on 15th November 2009.

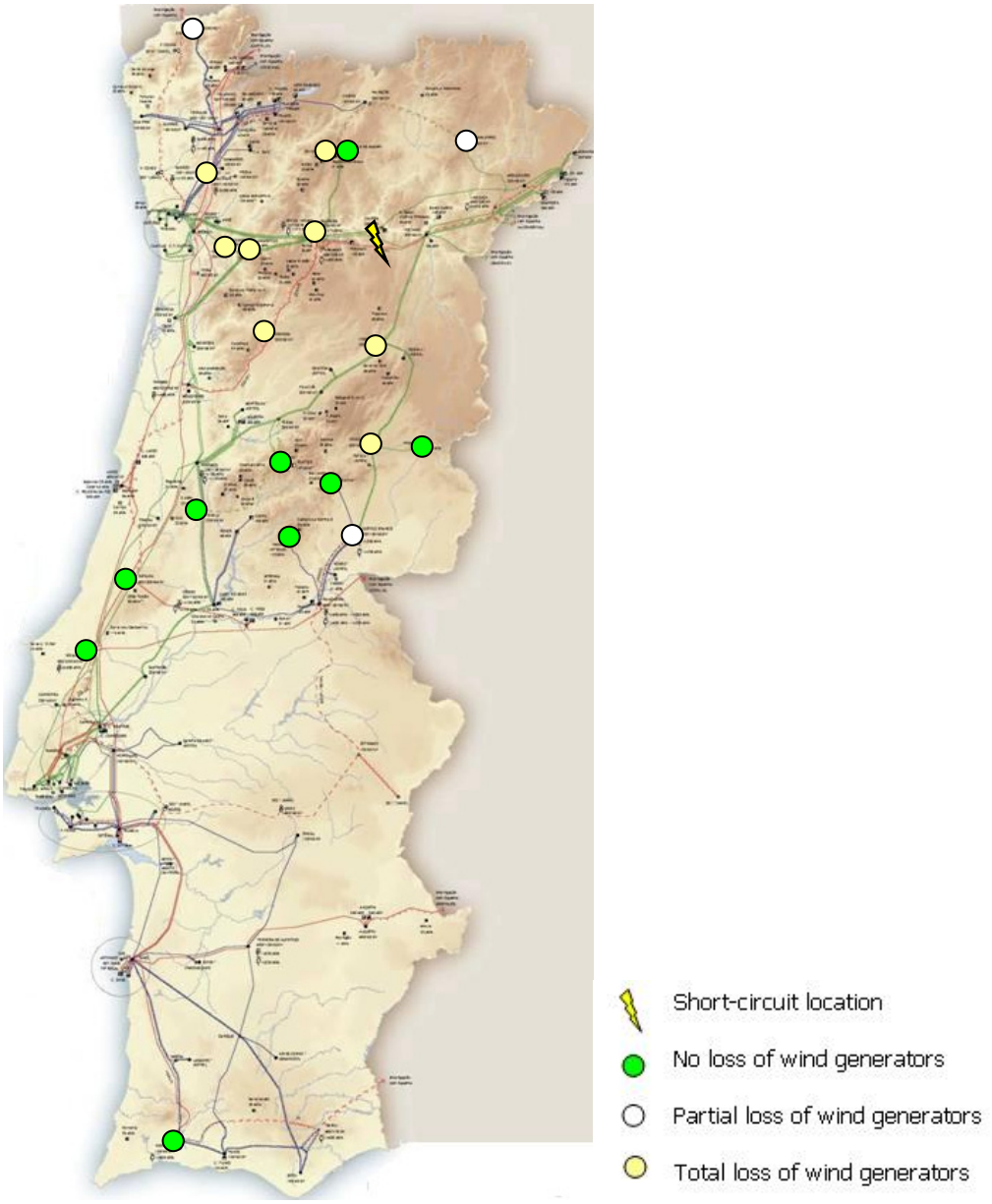


Fig. 4.6 – Wind Farms behaviour on 15th November 2009

4.3.2. The main power plants

Only the power plants connected to the EHV are presented on this section:

Hydro Power Plants:	Total (MW)	400kV (MW)	220kV (MW)	150kV (MW)
Lima/Cávado/Rabagão	1072	630		442
International Douro	804		804	
Nacional Douro	1005		947	58
Zêzere	443		159	284
Mondego	270		270	
Alqueva	230	230		
Thermal Power Plants :	Total (MW)	400kV (MW)	220kV (MW)	150kV (MW)
Turbogás (Oporto)	990		990	
Pego	584	584		
Carregado	710		710	
Lares	800	800		
Ribatejo	1200	800	400	
Setúbal	946.4	946.4		
Sines	1192	894		298
Tunes	82.5			82.5

Table 4.6 – Hydro and thermal power plants active power (2009)

Wind Power Plants :	220kV (MW)	150kV (MW)
Pampilhosa da Serra	114	
Toutiço	102	
Terras Altas de Fafe		106
Pinhal Interior		144
Gardunha		106
Alto Minho I		240

Table 4.7 – Wind farms installed active power (2009)

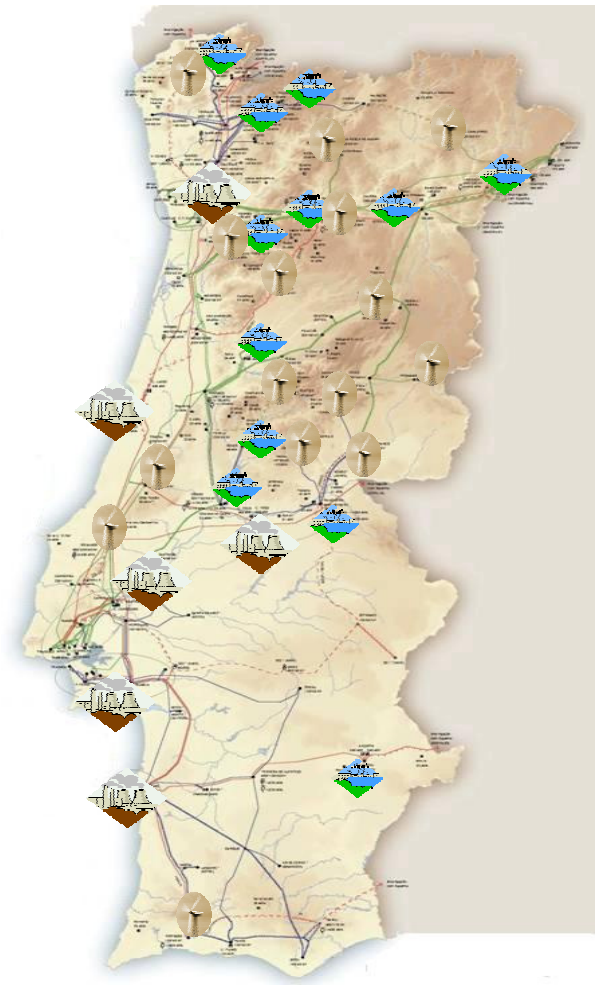


Fig. 4.7 – Geographical distribution of power plants

4.4. Typical substation layout

Two main layout schemes are used for substations in the PTS: the classical one (double busbar either with elevated by-pass or with transfer bus as in figure 4.8) and the breaker-and-a-half one (as in figure 4.9). The classical scheme has two main busbars with the option of each grid element connected to any of the busbars, allowing the distribution of lines and transformers. The bus coupler is normally closed and connects the main busbars. In this topology each grid element has one circuit breaker. The bus coupler can also be used to replace the circuit breaker of any grid element, by-passing the bay of that element.

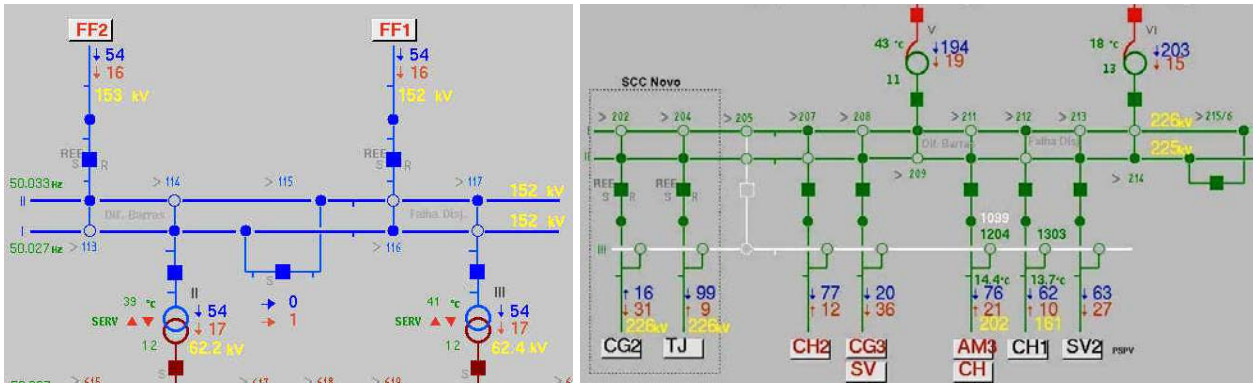


Fig. 4.8 – Classical substation topology

In the breaker-and-a-half scheme, all grid elements have two circuit breakers, sharing one of them (the "middle" breaker). The reliability of this scheme when facing busbar faults increases significantly, assuming that there is always a busbar differential protection. To clear a busbar fault in the classical scheme all the bays connected to the faulty busbar will trip, together with the bus coupler. In the breaker and a half scheme, only the busbar is removed from service without affecting the grid elements that are connected through the "middle" circuit breaker. Additionally, this scheme allows:

- More flexibility for maintenance works in the substation circuit breakers, because it avoids the outage of the grid element.
- Economy of space, when building new substations and OHLs which is extremely hard, although an additional circuit breaker increases costs.

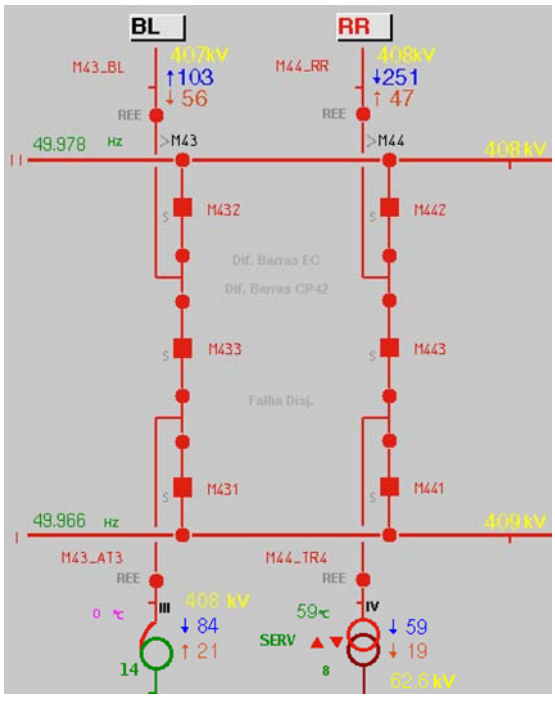


Fig. 4.9 – Breaker-and-a-half substation topology

4.5. System operation

The main purpose of the Transmission System Operator (TSO) is to maintain the balance between generation and demand, ensuring the real time management and coordination of the power system, without jeopardizing the security of supply. A secure interconnected network is the goal of the system operation.

In the current environment, after unbundling, system operators shall only interfere with the market if system security is at risk. In the interconnected system operation, each TSO is responsible for its own network, although the inter-TSO coordination takes more and more a preponderant role in the daily operation at regional level. Thus, each TSO must exchange information with its neighbours (mainly at the borders of their control areas). To monitor and control the power flow in the interconnections, i.e. the cross-border flows, and to facilitate the access to the transmission network is a duty of the TSO.

The parameters that allow the TSO to monitor and supervise the network operating state are the frequency (global stability parameter), voltage, power flows and temperature. It cannot be forgotten that an Electrical Power System is a dynamic system, that changes continuously, and real-time control, operation and supervision are crucial to guarantee its security. To fulfil this aim, a SCADA system (Supervision Control and Data Acquisition) is used, which allows receiving the information from grid nodes and elements (switching devices and measurements) and sending switching commands. This functionality permits the global management of the power system, whereas the responsibility of each TSO is to monitor its own control area and relevant information from the neighbouring ones, giving to the control room operators a wider and centralized vision of the network.

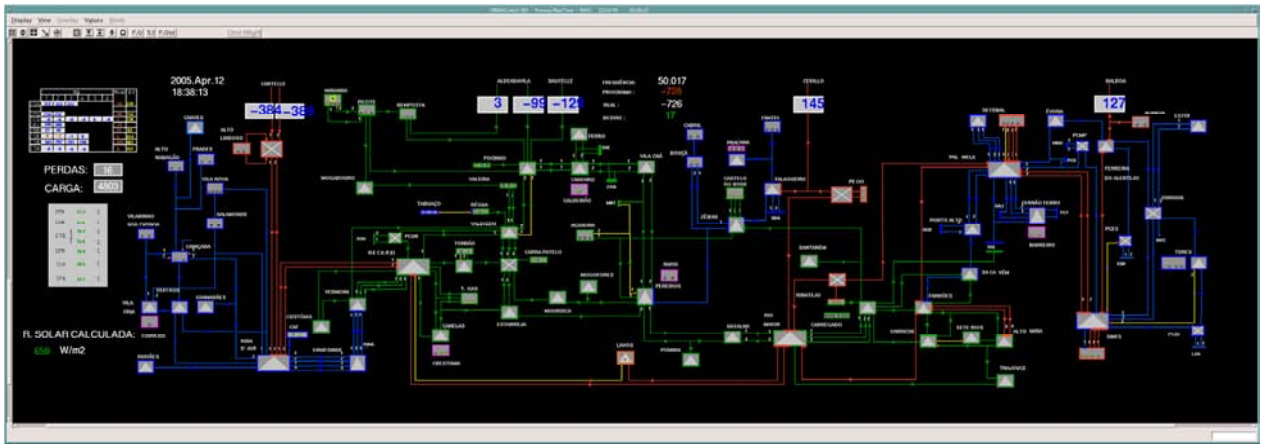


Fig. 4.10 – SCADA MIMIC

SCADA uses a reliable and redundant telecommunication system that ensures in real time the communication with each and every grid node (substation), performing the signal acquisition and processing. The signal processing includes, in addition to switching actions, the signal classification and alarm generation, providing accurate information to the control room operators.

Fig. 4.11 – REN's system operations control rooms

4.5.1. Energy management system

The Energy Management System (EMS) is one of the main functions supported by SCADA software. EMS includes several applications whose main purpose is to provide monitoring, assessment and decision-making support to the control room operators, in order to achieve the best secure and economical conditions in system's management; those applications are:

- **State Estimator (SE)** – runs automatically or at the operator's request and provides an estimated image from the grid (including estimated measures, parameters and switching devices status) based on the received data input, which enables the validation of the received information and the estimation of the missing one (caused by communication failure or circuit breaker status non-coherency). The state estimator is a computer algorithm that operates on real-time inputs and calculates voltage magnitudes and phase angles of the system buses, as well as transformer tap positions for pre-selected transformers which best fit the actual state of the network. Although SE results are similar to those available from a power flow simulation, the input data and the calculation algorithm are fairly different. It uses statistical information about the errors from each measurement, identifying in this way its quality (if it represents "good or bad data", where bad data are grossly erroneous analogue values which deteriorate estimation accuracy unless eliminated from the solution process). The statistical estimation method applied in SE is of the "Weighted-Least-Squares-Estimation" type. Generally, the SE filters the information which arrives to SCADA through the remote terminal units, executing some simple tests, in order to validate the quality of SCADA measurements, improving the network monitoring accuracy. In case of doubtful quality of a measure, the SE detects and identifies the existence of "discrepancy" or "bad data". After the mentioned filtering process, the SE converges with a valid solution, making it available online and in the EMS applications. The snapshots used for security analysis are also created by the SE.
- **Contingency Analysis (CA)** – checks if the N-1 criterion is fulfilled, i.e. in practical terms performs the security check running the "must run" contingency list. It also allows the evaluation of the impact of changes in network topology, after adjusting the power flow distribution within the grid elements that will remain in service, and the network security level, using as a starting point a valid solution from the state estimator. Contingency Analysis performs a full AC power flow calculation.
- **Automatic Generation Control (AGC)** – allows the control of generating units with control regulation capability, through signals sent by the control room, automatically or manually, aiming to maintain the balance between actual power generation and load demand and the interchange scheduled flow, i.e. minimizing the ACE and keeping the frequency at the desired nominal value.
- **Reactive Power Management (RMVC)** – determines the necessary actions to be performed in the equipment that regulate reactive power in order to restore the voltage values within the acceptable range and to minimize system losses. Thus, the Voltage VAR Schedule tool optimizes voltage profiles.
- **Load forecast** – provides an estimation of the load for the following days, based on the recent history of similar days and on the weather forecast.
- **Short-circuit current calculation** – performs the calculation of short-circuit currents (three-phase and phase-to-ground) for every busbar in the system.
- **Dispatcher Training Simulator (DTS)** – it is a replica of SCADA and allows the time domain simulation of grid scenarios in order to train control room operators. The DTS is discussed in more detail in section 4.9.
- **Study Mode** – provides a study platform to analyse the viability of planned outages, special topology schemes and switching operations, and to perform the Net Transfer Capacity (NTC) calculation. The studies are performed with a snapshot from the current

system state, which is created by the SE, manually or automatically, with a given frequency. Voltage (amplitude and phase) calculation uses a Newton-Raphson algorithm with a small mismatch in order to guarantee acceptable results accuracy. In study mode, it is possible to run everything like in real time operation, such as the contingency security evaluation and reactive power management application.

- **Switching Security** – allows the control room operator to check the consequences of a circuit breaker change of status in terms of security limits violations, according to N and N-1 criteria. Due to security concerns, before every non-programmed breaker switching, a power flow calculation is performed and its results (with N and N-1 security criteria) are presented to the control room operator.

There are other tools that can be part of the EMS, namely: optimal power flow, transient stability analysis, mid- to long-term stability analysis and voltage collapse analysis (based on PV or QV methods). All these tools are available to run in real time, thus a trade-off between processing time and accuracy is inevitable. It is also worth mentioning that real-time security assessment and decision support tools do not include dynamic simulation.

4.5.2. Security analysis in the control room

Nowadays, security assessment performed in control rooms is strictly dependent on the EMS. This assessment generally evaluates branch overloads and voltage limit violations. In the Portuguese TSO, for voltage instability assessment, an independent algorithm was developed internally, using the Power Flow Module of PSS/E combined with Python, to evaluate the distance to voltage collapse in an identified critical point and to assess the effect of remedial actions. The latter is presented in [5].

The control room must perform all the necessary security studies in order to assess the contingencies that may cause violations in the acceptable and established operating limits. The N situation is the starting point for security assessment in the control room and it is defined in [6] as the status of the TSO responsibility area without contingencies, including all known outages (planned, programmed and forced). This state is determined by power flow calculation including forecasts and outages. The forecasts include the expected load, market generation schedule and wind generation forecast (in case of wind, the average production based on historical data may be used, which represents about 30% of the wind installed capacity).

The principle “no cascading with impact outside my borders” must always be ensured by the TSO security analysis, because of the increasing number of interconnections among TSOs, which makes the analysis more interdependent and forces the TSOs to consider a part of the neighbouring grid. In case of exceptional events that may affect neighbouring networks, communication between control rooms of the involved TSOs must be ensured.

The N-1 security criterion aims to prevent the considered most likely events and their propagation outside of the TSO control area, i.e. outside its borders, up to the extent of one event at a time. The “must run” contingency list (referred next in section 4.5.2.1) includes all the relevant contingencies for each TSO, in order to assess their consequences and detect constraints in the network. Contingencies and parts of the neighbouring network are also included to evaluate the influence of those contingencies and mutual actions in the system.

In the security assessment, the remedial actions to relieve constraints are also included, in order to mitigate the severity of contingencies in advance (preventive) or after an incident (corrective). In the Portuguese TSO, the remedial actions analysis is performed through off-line studies by the control room operators or in the operations planning environment. The results of the security assessment are used by control room operators to analyse the post-contingency performance for each event on the defined list in

terms of limit violations, using a SE snapshot with the expected operating conditions. If any simulated contingency shows limit violations (see table 4.8) in its results, the operator's decision-making process begins, applying the most adequate remedial actions.

When facing adverse weather conditions, for instance lightning, the Portuguese TSO takes all the possible measures to guarantee system security. In case of lightning, a close look is taken at N-2 contingencies, especially when two lines share the same towers (so called double line [6]) over a long distance (more than 35 km), because it increases the likelihood of common cause incidents. The permits to work in the OHLs of the affected area (programmed outages) are also cancelled, in order to strengthen the network to withstand contingencies caused by lightning.

4.5.2.1. Lists of contingencies

The recent past clearly shows that major disturbances actually happen, at national and international level. It is relevant to point out that the probability of occurrence for incidents affecting several grid elements simultaneously, increases with the electrical and geographical proximity. Therefore, the security criteria currently used in real time should be complemented with more severe studies or replaced by a risk assessment approach. A selective analysis of incidents' historical data was made in order to identify credible contingencies, because it is not reasonable to simulate every possible contingency in a transmission system. With the credible set of contingencies, the aim was to analyse and evaluate them off-line, in order to identify suitable preventive and corrective actions to mitigate their consequences. Currently, the following lists are used in the security analysis:

- List A – The "must run" online contingency list, which is defined in the Portuguese operating procedures, according to the security criteria approved by the Portuguese Regulator. It is associated with the N-1 criterion, including the loss of the lines and transformers of the transmission network, generators and some N-2 criteria, such as overhead lines sharing the same towers for more than 35 km, and some lines of the neighbouring network that affect the system security (because of interconnection transmission capacity). This list is also used in the planning environment for investment criteria.
- List B – Busbar faults.

As a result of the described analysis, the Portuguese System Operator has created additional lists in the EMS system, namely the following:

- List C – Loss of overhead line corridors (which were selected using a proximity specific criterion, due to the risk of all lines in the corridor being affected by a forest fire). The OHL corridor definition can be found in [19], [20] and the list of corridors is presented in appendix B.
- List D – Distribution failures (includes closed rings through the distribution 60 kV network and the EHV/60kV transformers, excluding single feeders).
- List E – Extreme situations, which do not belong to any of the other lists, such as loss of whole substations or power plants, which were identified as credible and likely enough to be analysed.
- List F – Failure of a voltage level (including only substations with more than one EHV voltage level during periods when the TSO assesses a higher risk, such as work being performed in one of the busbars and a busbar fault would cause the failure of the complete voltage level in the respective substation).

After presenting all the defined sets of contingencies, it is relevant to divide them in three different categories. The first is the "must run" list, automatically run in real-time for security assessment by the EMS. The second is composed by lists B, C and D that can be activated whenever needed (e.g., active forest fire situations) or are run regularly off-line in an operations planning environment, in order to complement the security assessment performed online. The third ("Extreme") contains E and F lists, which

represent less likely but more severe contingencies, also available for periodical analysis. The additional contingency lists analysis gives the operator better understanding of the consequences of more severe contingencies, allowing him to identify better strategies to mitigate their impact, to define procedures for emergency situations and to anticipate incidents. Furthermore, these scenarios can also be used for operator training (topic presented in section 4.9). The definition of the additional lists was done before starting this research work.

The Policy 3 - Operational Security - of UCTE OH [6] describes three different types of contingencies:

- Normal type, which includes single line, single generating unit, a single transformer or phase shift transformer, a large voltage compensation installation and a DC link.
- Exceptional type, which includes a double line which refers to two lines on the same tower over a long distance, a single busbar and the common mode failure with the loss of more than one generating unit, including large wind production.
- Out-of-range type, which is defined as a failure with very low probability, including at least the independent and simultaneous loss of two lines, the loss of a whole substation with more than one busbar, the total loss of a power plant with more than two generating units, the loss of a tower with more than 2 lines or severe power swinging or oscillations.

Any event of the contingency list, previously called “must run” must not endanger the security of the interconnected operation. The TSO must select the exceptional contingencies to include in the contingency list based on specific operating conditions and their risk identification. This contingency list is also used to calculate the NTC as well as the schedule technical verification.

4.5.2.2. Security Criteria

The security assessment results must fulfil the following requirements:

- The voltage and current must be inside the acceptable operating range of voltage and maximum load during normal state and considering the contingencies included in the “must run” list.
- In any case, during normal state and for the contingencies included in the “must run” list, load shedding and degradation of quality of service must not exist.
- The frequency is permanently inside the margins established by [6].
- For the N-2 contingencies considered in the “must run” list, remedial actions must be applied in case of violations.

There are two types of operational limits, the permanent admissible transmission loading and the temporary admissible transmission loading. The permanent admissible transmission loading is the loading that can be accepted by a network branch for an unlimited duration without any risk for the material, while the temporary one can be accepted by a branch but only for a certain limited duration [6].

In normal operation (N situation) and in N-1 security criterion, the grid elements must be operated below the admissible transmission loading limit. Every time that this limit is exceeded, remedial actions must be taken to bring the system back to a secure operating state.

Table 4.8 summarizes the acceptable limits and overload maximum duration for each contingency regime, which are used in the PTS security analysis. The voltage range loosens slightly into exceptional values for N-1 and N-2 situations [44].

Criteria	Temporary Admissible Transmission overloading		Voltage Range (kV)
	LINES	TRANSFORMERS	
Contingency	time < 15 minutes	time < 2 hours	
N	0%	0%	400kV: 380kV - 420kV
			220kV: 209kV - 245kV
			150kV: 142kV - 165kV
N - 1	15%	Winter: 20% Summer: 5%	400kV: 372kV - 420kV
			220kV: 205kV - 245kV
			150kV: 140kV - 165kV
N - 2 described in the "must run" List	15%	Winter: 30% Summer: 10%	400kV: 360kV - 420kV
			220kV: 198kV - 245kV
			150kV: 135kV - 165kV

Table 4.8 – Security criteria used in the PTS elements

The operating limits of the network change depending on the season and weather condition. To determine the transmission capacity, the thermal behaviour equations, the temperature's historical data and the maximum design temperature are considered. In the Portuguese transmission system operation, three periods are used: winter, summer and spring/autumn. For winter (December, January and February), the considered ambient temperature to calculate the transmission capacity for each element is 15º C and for summer (June, July, August and September) is 30 ºC, but recent past shows that 30º C of temperature is not a suitable value, regarding the average summer temperatures in the last years in the interior of Portugal, especially in the south region. Hence, the coast region considers 30º C of ambient temperature, but it rises up to 35º C in the direction of the interior south of the country.

Reference [92] presents a map of summer temperatures to consider when determining the transmission capacity of grid elements, which is shown in appendix C. This map was built after a re-evaluation of temperatures, especially during summer, considering the historical data since 1985. In spring/autumn, the operating limits are in between winter and summer limits and they are regularly changed according to weather conditions, specifically temperature, as presented in table 4.9.

Month	Temperature
JAN	15
FEB	15
MAR	20
APR	20
MAY	25
JUN	30*
JUL	30*
AUG	30*
SEP	30*
OCT	25
NOV	20
DEC	15

*- The lowest summer temperature – it will depend on the region according to appendix C

Table 4.9 – Considered temperature for security analysis

4.5.2.3. Day-ahead schedule technical verification

In order to guarantee a secure system operation and the suitable fulfilment of operating criteria, the Portuguese TSO validates, in the day before, the generation schedule for its network that result from the Iberian energy market. To perform this validation, it is also necessary to consider, for the period under analysis, the planned outages, the load forecast, the wind generation forecast and the "must run" contingency list. Through this information, which is available for every hour, the system operator verifies if the generation schedule is technically viable, ensuring always a secure system operation.

The Portuguese TSO has developed an application based on the Power Flow Module of PSS/E, computing automatically several routines through an application developed in Python, which performs calculations and generates the specified results.

After the analysis is performed and the final results for the generation schedule are obtained, the solution is made available in the TSO intranet and its user interface is shown in figure 4.12. The colour code, which is a very effective way to present data, provides the operator with an intuitive perception of the results. In case of a critical security situation, a red circle is presented, giving an efficient indication to the operator of the need to verify the security conditions in that specific period.

Figure 4.12 shows the detail of the contingency analysis results for the next day. This technical verification runs for the daily and each of the 6 intra-day market sessions every day after gate closure. Detailed information is available for every analysed period, as it is shown for the 12:31 result.

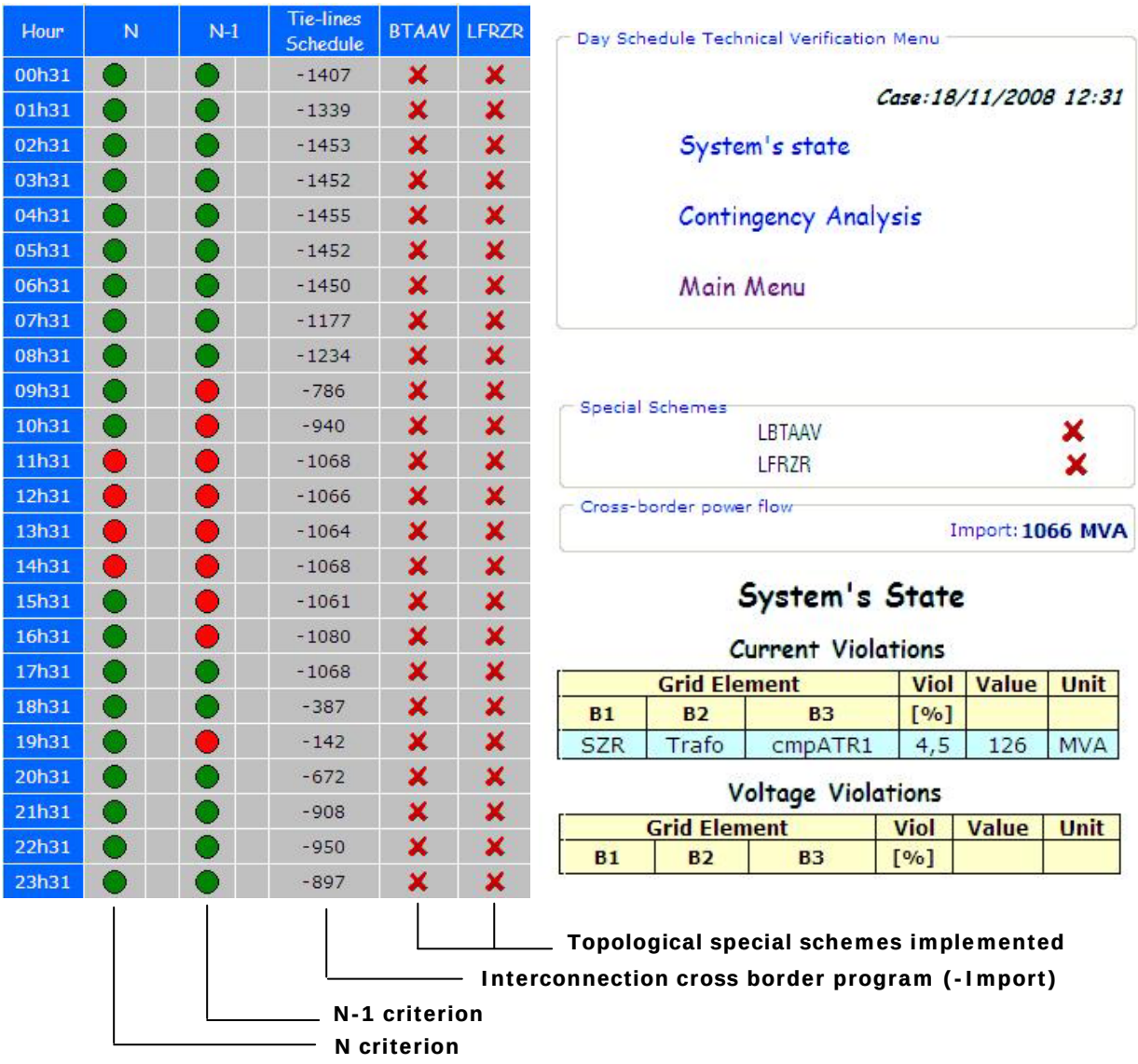


Fig. 4.12 – Display of the Day-ahead schedule technical verification results[93]

Whenever facing security limits violations in the N, N-1 or N-2 criterion, the operator will take the adequate remedial actions and a generation redispatch may be necessary to restore the security limits. In most situations the order of actions followed by the operator is the following:

- Topological special schemes.
- Load transfers to other substation through the distribution network.

- Conventional generation redispatch.
- Renewable generation redispatch.
- Load Shedding.

A more detailed approach to the remedial actions is presented further in section 4.5.4 of this chapter.

In this procedure, the part of the neighbouring network that is observable is considered with a static generation pattern, maintaining the same generation values, which were in SCADA at the exact moment that the snapshot was taken to be used in this analysis. State Estimator snapshots are network "pictures", which are created by the EMS system at a given moment in PSS/E "raw" format.

After gate closure of the market daily session, the Iberian Market Operator (OMEL) sends to both Iberian TSOs the provisional generation schedule for the next 24 hours, which needs to be validated by each TSO. The Portuguese TSO will consolidate a valid generation plan to be sent to OMEL, fulfilling all the security conditions, after introducing any necessary changes in the market results. This consolidated generation schedule for the forecasted network operating conditions for the next 24 hours will be then forwarded by OMEL to the energy market agents. Every four hours, this analysis is updated in order to validate the generation schedule for each of the 6 intra-day market sessions.

4.5.2.4. Day-ahead congestion forecast

The Day-ahead Congestion Forecast (DACF) procedure is described in the UCTE OH policy 4 [6], section C, and it consists of a set of AC load flow calculation input data, given in the UCTE format, and corresponding to the forecast state of the transmission grid (topology, loads and generation pattern) at a determined timestamp of the day-ahead.

The purpose of DACF is to organize this exchange of confidential data among TSOs in order to provide each TSO with a set of data to allow for a more reliable power flow forecast during the operational planning stage. Through DACF data analysis, possible congestions and the inter-influence on neighbouring networks may be identified, especially for contingency analysis. Hence, almost every TSOs of the Central Europe group within ENTSO-E makes available the snapshots with the corresponding forecasted conditions for the 24 hours of the following day.

The Portuguese TSO makes available the hourly snapshots of the Day Ahead Schedule Technical Verification for the following day, described in section 4.5.2.3., containing the verified operating program. It also uses the snapshots from the Spanish TSO to validate once more its own results. This additional validation completes the technical analysis, because it considers the whole neighbouring network and the generation schedule already checked and validated for the following day.

After joining the two networks for analysis, an algorithm equivalent to the Day Schedule Technical Verification is run, considering the complete Iberian system and providing to the control room operator the same kind of interface shown in figure 4.12.

In this way, the limitation of including only the nearest part of the neighbouring network in the EMS system is overtaken by integrating DACF data sets in the security analysis for the daily market, but it is mainly used for awareness of possible constraints, because the market schedule at this moment is already settled.

4.5.2.5. Off-line security analysis

Off-line studies are used to analyse real-time operational constraints and remedial action as well as the technical viability of programmed and forced outages, and they are performed in the following steps:

1. Prepare the base case for analysis, with the expected conditions for the chosen time period, by using snapshots corresponding to the week period (week day, weekend day) and different loading conditions (peak, partial peak, off peak). To adapt the base case, it is necessary:
    a. To adjust the system load, keeping the load's tan(φ) constant.
    b. To adjust the generation, considering the load and the interconnection program and regarding average marginal market prices and hydro power plants constraints; this adjustment must not create technical constraints in the base case.
    c. To perform voltage control, switching on/off shunt capacitors in the network depending on the load in analysis.
    d. To run a power flow simulation with transformer taps adjustment in the EHV/HV transformers, maintaining the voltage nominal value in the secondary side. In the autotransformers at the EHV levels, the tap adjustment is manual (so not automatically done in the power flow simulation).
    e. To verify the existence of technical constraints in the simulation results, such as overloads and voltage limit violations. If there are constraints, it is necessary to eliminate them before continuing.
2. Select the contingency list to use in the analysis. By default, "must run" list (List A as described in section 4.5.2.1) is considered.
3. Evaluate the range of operating conditions, concerning possible variations of load and generation, which are expected during the relevant time period. In case of actual variation in the operating conditions, this will later assist the results assessment, in the online analysis, in order to decide whether or not to perform a new security analysis study.
4. Validate the N security criterion for the operating conditions in the specified range. Identify the event or events that "first" violate the performance evaluation criteria; if there are no such violations within the study range, the region is not security-constrained (i.e., it does not have constraints).
5. Validate the N-1 security criterion for the operating conditions in the specified range. Identify the event or events that "first" violate the performance evaluation criteria; if there are no such violations within the study range, the region is not security-constrained.

4.5.2.6. Online security analysis

Online, the State Estimator is automatically and systematically run by the EMS every time a topological change occurs or at least every 5 minutes without changes in the topology. The Contingency Analysis (CA) is run every 10 minutes or under request, performing the "must run" contingency list. With a bigger time interval, every 15 and 30 minutes, the EMS runs the voltage VAR schedule and online short-circuit applications, respectively.

In the contingency analysis, the "must run" contingency list is analysed by default. However, the control room operator has the option to change the list that is run. The CA results are presented in a table as shown in figure 4.13.

In this interface table, the limit violations can be sorted by three parameters (current, voltage and reactive power); by default the results are sorted by percentage of current. The worst violations are displayed at the beginning of the page. Control room operators permanently check these results in order to act promptly, applying the necessary remedial actions.

Last Execution CS 26.01.07 15:54:28 | Comment RESTARTED | Page 1 of 18
Last Execution CA 13.11.08 16:19:54 | Comment ENDED WITH REPORTS

Calculated Contingency List List A
Displayed List Ordered Repl%
Ranked List Ordered Repl%

VPI = 99.9 * VPI_I + 0.0 * VPI_V + 0.0 * VPI_Q

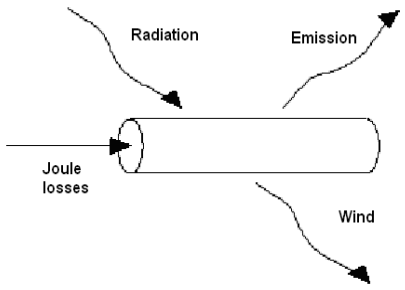
	No.	B1	B2	B3		RepV	Repl	RepQ	V%	I%	Q%	VPI CA	VPI CS	Rank CS
Del	3	TieLine	400	CTL-SAL	LimV	2	1	0	111	105	0	9.5		
Del	3	TieLine	400	CTL-SAL2										
Del	164	Line	150	SPM-SSB1	LimV	5	1	0	112	100	0	8.2		
Del	178	Line	150	SPO-STN2	LimV	5	0	0	112	0	0	8.1		
Del	179	Line	150	SPO-SSI	LimV	5	0	0	112	0	0	8.0		
Del	180	Line	150	SSI-SSN	LimV	5	0	0	112	0	0	8.0		
Del	181	Line	150	SOQ-STN	LimV	5	0	0	112	0	0	8.0		
Del	182	Line	150	SET-SOQ1	LimV	6	0	0	112	0	0	8.1		
Del	183	Line	150	SET-SOQ2	LimV	6	0	0	112	0	0	8.1		
Del	185	Line 3	150	VNRA-OR	LimV	5	0	0	112	0	0	8.1		
Del	185	Line 2	150	VNRA-OR										
Del	185	Line 1	150	VNRA-OR										
Del	186	Line 2	150	ARFD-CV	LimV	5	0	0	112	0	0	8.0		
Del	186	Line 3	150	ARFD-CV										
Del	187	Line 3	150	CDRA1-FD	LimV	5	0	0	112	0	0	8.1		
Del	187	Line 2	150	CDRA1-FD										
Del	188	Line 3	150	CDVI1-VF	LimV	5	0	0	112	0	0	8.1		
Del	188	Line 2	150	CDVI1-VF										

Fig. 4.13 – SCADA display – Contingency Analysis Results

4.5.3. Thermal dynamic rating

In order to maximize the transmission capacity, dynamic limits for overhead lines can be used instead of static ones, providing the control room operator with more accurate information of the actual loading of an OHL. The operating limit of electrical lines is determined by the maximum allowed temperature of the conductor of the line and not by the current flowing through it. Since the market price is lower during off-peak hours (normally during the night), the OHL capacity reserved for the thermal solar radiation input is released and the lower temperature during the night is also considered to maximize the transmission capacity available.

To achieve this goal, in Portugal, besides the investments in structural changes, dynamic rating systems are being applied in some of the most critical OHLs; this is done mainly through off-line analysis. To perform the calculation using Kuipers-Brown model [94], as in figure 4.14, some dynamic measures are needed, such as the actual current on the conductor, the solar radiation and the ambient temperature. The wind speed is considered constant. In the current state of technology, it would not be cost effective to measure them in every overhead line, due to the high cost of measuring devices and their integration in the SCADA real-time environment.



$$I^2Rt + A \cdot R \cdot d = 8{,}55(T_P - T_A)(W \cdot d)^{0{,}448} + \pi \cdot E \cdot C \cdot d \cdot \left(T_P^4 - T_A^4\right)$$

I – current [A]
R – Solar Radiation [W/m^2]
T_a – Ambient Temperature [K]
T_P – Design Temperature [K]
W – Wind speed [m/s]
d – conductor diameter [m]

R_t – Electrical resistance at temperature T of conductors [Ω]
A – Solar Absorptivity coefficient
E – Effective emissivity of the conductor
C – Stefan-Boltzmann constant (5,7x10^{-8} W/m^2.K^4)

Fig. 4.14 – Kuipers-Brown model equation [94]

Through this equation it is possible to obtain two different results: the maximum current using the design temperature or the conductor temperature using the actual current.

4.5.3.1. Off-line dynamic rating

In order to compute thermal off-line ratings for each overhead line, the algorithm computes 3 limits per day, as shown in figure 4.15, and the following information is needed:

- Ambient temperature – a reference temperature is used. After sunrise, the monthly reference temperature considered in SCADA is used and before sunrise, it is the same monthly reference temperature (see table 4.9) minus 5 ºC.
- Solar radiation – uses solar radiation equal to 1000W/m^2 from sunrise until sunset and during night time 0W/m^2.
- Wind speed – a constant value of 0.6 m/s is used.

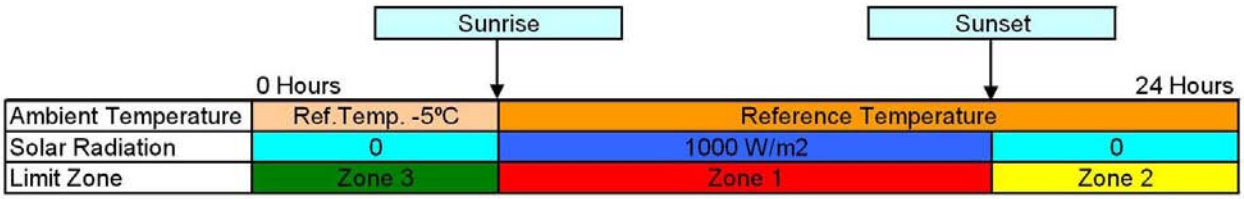


Fig. 4.15 – Weather conditions for off-line studies [95]

Figure 4.16 presents an example of the increase in the OHL transmission capacity considering the three zones for analysis.

Summer	Zone 3	Zone 1	Zone 2	
Radiation	0	1000	0	w/m2
Amb.Temp	25º	30º	30º	ºC
ZEBRA-50ºC	758	524	679	A
Gain	**145%**		**130%**	%

Winter	Zone 3	Zone 1	Zone 2	
Radiation	0	1000	0	w/m2
Amb.Temp	10º	15º	15º	ºC
ZEBRA-50ºC	951	780	892	A
Gain	**122%**		**114%**	%

Fig. 4.16 – Off-line study example [95]

4.5.3.2. Online dynamic ratings

The online dynamic rating algorithm runs every minute and includes every OHL that constrains the network operation, which is different than the off-line studies that include every OHL in the system. The information needed for the off-line studies is also used in the online analysis, however with some differences, namely:

- Ambient temperature – is obtained through SCADA that receives real-time temperature measurements located in several substations. This can be improved by using in the calculation real-time measurements acquired at the OHL.
- Solar radiation – Algorithm that computes it every minute with the assumption of clear blue sky in Lisbon, which is considered the worst case [96].
- Wind speed – a constant value of 0.6 m/s is used. This approach can be improved by online wind measurements (Nowadays transpower (former E.ON) is the only TSO in ENTSO-E Continental Europe Regional Group that uses online wind measurements). Although based on the wind forecast tool and the wind measurement given by the wind farms connected to the PTS, the Portuguese TSO can surely start to use wind dynamic measurements in a short time.
- Current – SCADA measures.

To validate the "default" values used for each situation with real time measures, the Portuguese TSO has installed, in 2004, a real-time monitoring equipment, in order to determine the thermal rating (actual mean temperature of the conductor), in one 220 kV overhead line near the Lisbon area, called CAT-1. CAT-1 was developed by "The Valley Group, Inc." and it measures the mechanical stress of the conductor. More recently, in January 2009, fibre optics temperature sensors, based on the Fibre Bragg Grating

technology, were installed in two pylons with double 220 kV circuits, in the North of Portugal, in order to monitor their temperature in real-time. This technology was developed and installed by Fibersensing [97].

According to the CIGRE Working Group (WG) 22.12 report on "Real time monitoring", it is possible to increase the thermal rating of an OHL at least 10 to 15% on average thanks to real time monitoring. With real time thermal rating, a TSO aims to:

- Calculate the rating considering the actual weather conditions.
- Provide real time information to control room operators, supporting them when making decisions and speeding up the decision-making process.
- Guarantee reliability when maximizing the line capacity (or usage), avoiding thermal fatigue of the conductor and increasing its life time.
- Minimize the need of remedial actions (such as redispatch), increasing cost efficiency.
- Maintain reliability when facing disturbances (contingencies), having a more accurate vision on the system's actual constraints.
- Keep historical data for analysis (for operations and investment decisions).

Whenever there is capacity to monitor the weather conditions in order to calculate online the thermal dynamic rating of a grid element, the result should be taken into account for security analysis. Using thermal dynamic rating, it is possible to increase the actual transfer capacity of OHLs, allowing a more efficient NTC management and therefore an increase of the cross-border trade with Spain. With online dynamic ratings and weather information, it is possible to incorporate the awareness of the real time conditions.

4.5.4. Remedial actions

A remedial action is any measure applied by a control room operator in order to restore security criteria in a transmission system and it is normally prepared in advance during operations planning, i.e. previously assessed by simulations to check its efficiency. In case of identified risk of cascading with impact on neighbouring TSOs, common remedial actions must be prepared in a coordinated way. The possible remedial actions are [6]:

- Tap change of phase-shifting autotransformers.
- Topology changes (e.g., creating special schemes to reduce the power flow of an OHL).
- Cancellation of maintenance works with restoration of the grid element in due time.
- Reactive power compensation (e.g., through shunt capacitors, on-load transformer taps and synchronous compensation by generating units, changing generators' excitation in order to achieve more reactive power injection).
- Transfer load to other delivery points through the distribution network (totally dependent on the distribution network availability).
- Generation re-dispatch.
- Change of the scheduled interchange cross-border power flow.
- Counter-trading with neighbouring control areas.
- Intervention in scheduling (freezing or reducing scheduled exchanges).
- Reduction of interconnection capacities.
- Start-up of tertiary reserve.
- Operation with wind generation.
- Pump tripping.
- Shedding of interruptible customers.
- Automatic load shedding. This is the last action to be applied.

The remedial actions that do not interfere with the level of consumption, generation pattern or interchange cross-border power flow are considered no-cost measures and they are the first ones to be implemented.

There are two types of remedial actions [6], as indicated in figure 4.17 with red and green arrows:

- Preventive remedial action – these are taken to anticipate a need that may occur. Normally, these actions are taken under special operating conditions (such as planned outages), when the possible consequence cannot be mitigated in due time after a specific contingency.
- Curative remedial actions – these are very common after more severe contingencies, in order to mitigate constraints and bring the system into normal state.

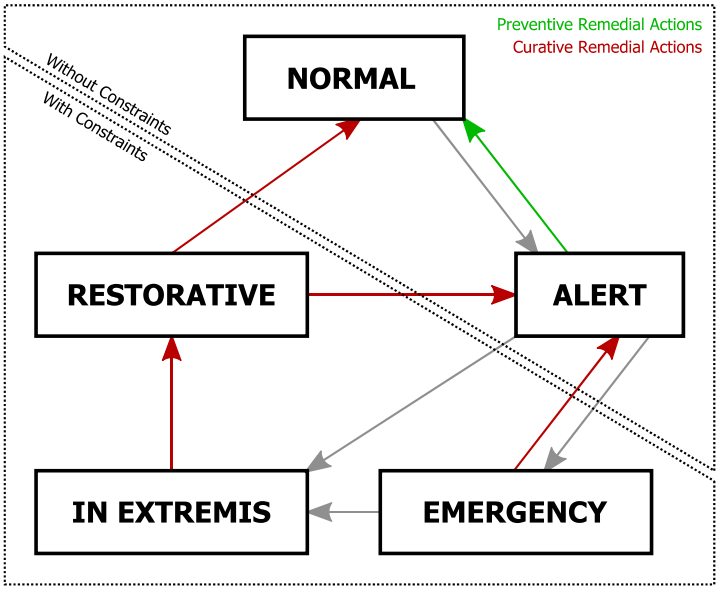


Fig. 4.17 – Representation of the type of remedial action in the power system states diagram

In this way, most of the applied remedial actions are corrective, although there are also remedial actions that are taken preventively in anticipation of likely events, depending on the system operating conditions, but it is relevant to mention that preventive actions cost money. Therefore, for rare major disturbances preventive actions are not reasonable, because their costs cannot be justified for events that are so unlikely [54].

Remedial actions are crucial reaction measures whenever a disturbance occurs and places the system in an insecure state. If the power system state is considered inadequate, this implies that security limits are violated or an interruption of supply has occurred, therefore curative remedial actions are required to bring back the system into a secure state (normal state), mitigating the disturbance impact and, if necessary, re-establishing the voltage levels, frequency and power flows within predetermined security limits. Even after one contingency (single event), remedial actions must be taken quickly to restore the N-1 security criterion again in the system, because the next contingency can happen at any time, and while the system is no longer N-1 compliant the risk level increases. Hence, remedial actions are crucial to minimize impact of a disturbance and not jeopardise the system safety or the security of supply.

Depending on the disturbance, different remedial actions are going to be needed and also their urgency will vary, but it is important to be aware that these actions require time to be performed and sometimes this time is not compatible with the system's response time, thus it might be too late to avoid a blackout. For instance, if the constraint violation is a thermal overload then the operators may have a reasonable time frame to solve it. If it is a voltage problem, it can be a high voltage decline or a sudden voltage collapse. In case of high voltage decline, operators may have a reasonable time frame to bring back the

voltage into acceptable levels [5]. If the disturbance causes transient instability, the timescale is seconds at most.

Regarding load transfer to other delivery points through the distribution network, this remedial action is suitable to solve local problems, because it does not change the total load level in the system but only changes the location of the load. It may be interesting when it decreases the risk in the area from where the load is transferred and this decrease is not equal to the increase of risk in the other area where the load is transferred to. Thus, sometimes it may reduce the operational risk in the transmission system. However, transferring load may increase the risk in the distribution network, because it is on this level that the transfer is actually done.

There are two types of load shedding that we can consider as remedial action. The automatic load shedding, which in the Portuguese transmission system only operates for under-frequency and will be described in section 4.8.5, and the manual load shedding, which is the ultimate remedial action taken by the control room operator.

4.6. Real-time system monitoring

In the supervision, control and operation of an Electrical Power System it is important to know:

- System's topology.
- Active and reactive power flow in every grid element.
- Power injections in the network.
- Loading conditions in every grid element.
- Voltage values in every grid busbar.
- Equipment in service and outages.
- System alarm messages, identifying exactly the location and the type of failure.
- Temperature.
- Frequency.
- On-load transformers tap-changing.

There are 4 essential points for an operator in a control room:

- Information: to receive, transmit, collect, process.
- Analysis: to perform the monitoring, supervision and analysis of the whole system in real time (security and economical issues), having the vision of the system as a whole, which makes the decision-making process easier to optimize. This can be improved with the use of suitable decision support tools.
- Balance and coordination: to maintain the balance between generation and consumption and to assure the fulfilment of the procedures in force.
- Actions: to carry out manoeuvres, remedial actions, service restoration and control of acceptable values (overloads in grid elements, voltage limits' violations).

4.7. Interconnected system

The ENTSO-E Continental Europe Regional Group, formerly called Union for the Coordination of Transmission of Electricity (UCTE), is composed of 29 TSOs, representing 24 countries. In general terms, an interconnected electrical power system has the following main benefits [98]:

- Mutual support for the interconnected systems in case of emergency, increasing security and reliability in system's operation and demand supply.

- More efficient frequency control, minimizing the impact of major disturbances.
- Improved voltage stability.
- Optimization of the installed capacity, coordinating the capacity of the TSOs.
- Reduced costs of power outages through the reliability improvements.
- Sharing reserve capacity and reducing the level of reserves required, achieving a better economic efficiency.
- Allows the development and the functioning of European Regional Markets.

Quoting a paragraph from the former UCTE webpage, which describes extremely well the reality of the interconnected system [98]: "*For more than 50 years, UCTE has been operating one of the largest synchronously interconnected systems in the world, securing reliable electricity delivery today to more than 500 million customers. The highly meshed system of 24 European countries consists of some 200.000 km of 400 and 220 kV lines, hundreds of generating capacities directly linked to the system, and hundreds of substations. Synchronous interconnection means that individual systems are connected and being run together, at the same frequency, assist each other if a disturbance occurs in a system. Vice-versa this also means that major disturbances might propagate throughout this whole interconnected system and endanger its stability. "*

The TSOs of the ENTSO-E Continental Europe Regional Group operate in a decentralized manner, where each TSO is responsible for its control area, but with respect to accurate and strict technical and organizational rules and standards by all members, which has proven to be effective in the last decades. The coordination between TSOs helps to enhance the importance of mutual support in the system's operation, which was the first goal of interconnecting neighbouring systems, preventing disturbances and mitigating their consequences, providing assistance to reduce the impact of a major disturbance, avoiding a total blackout (e.g., 4th November 2006 emergency situation described in section 2.2.3).

The interconnected network is no longer just a pool for mutual support; nowadays it has become the base platform for trading electricity, allowing the shifting of increasing volumes of power across the system. Obviously, despite all its many benefits, the free electricity market presents also many problems, which need analysis and research in order to achieve adequate solutions from the operations point of view. Therefore, new challenges come up that demand a closer and risk-based system operation by the ENTSO-E Continental Europe TSOs.

4.7.1. Interconnection capacity

According to reference [44], the interconnection capacity is defined as the maximum technical capacity of power flow in both directions of the neighbouring interconnected networks, ensuring the fulfilment of the established security criteria in both systems. The commercial usage of the interconnection capacity demands that the market players know in advance the maximum Available Transfer Capacity (ATC).

In case of the Iberian system, both TSOs perform on an annual, quarterly, monthly and weekly basis, the Available Transfer Capacity calculation. In Portugal, the method used to calculate ATC is regulated by law. In the real time operation, it may often happen that the consumption, the generation pattern and the programmed outages are actually different from the predicted in the weekly ahead calculation. Therefore, ATC value may be outdated and not suitable to guarantee a secure system operation, putting the system at risk. In this case, the weekly results will be updated on a daily basis, reducing if necessary the ATC value available for international cross-border transaction, and consequently the tie-lines power flow. In case of choosing to maintain the already established energy contracts, a generation re-dispatch is needed, in one or both systems, considering from the beginning that this choice represents an additional cost at least to one of the interconnected systems. On the other hand, the ATC value can be bigger than predicted in the week ahead, increasing immediately the available value for cross-border energy interchange.

In order to obtain an ATC value for each possible power flow direction (import/export) in each control area, it is necessary to adjust the generation in both areas, considering the units' marginal prices, beyond the required accurate verification of the specified security criteria (regarding to N, N-1 and N-2 events).

There are three main reasons that might impose limitations to the ATC, namely constraints in the tie-lines or in the internal grid elements or lack of generation to export inside a control area. In the situation of the Iberian transmission system, the constraints to the ATC were imposed in the beginning by tie-lines, which were solved after building new interconnection lines or upgrading the existing ones. Afterwards internal grid elements of both control areas were creating constraints, more than limitations in the tie-lines capacity. In order to reduce these constraints, significant investments were and are still being made (as already mentioned in section 4.1). Nowadays, the constraints to the ATC are frequently caused by lack of generation to export and this will remain until the new already foreseen power plants are built and come online. With the network development, one of the described reasons may cause constraints in different investment periods. These constraints are often worsened by programmed outages, causing the ATC value to decrease.

4.8. Electrical power system control

An Electrical Power System is a dynamic and complex system. Its demand is permanently changing and is being permanently supplied by the generation, which will vary in a continuous manner in order to balance them. The parameters that are constantly monitored and automatically controlled (inside an acceptable range) are the following:

- Frequency
- Voltage
- Current

The automatic control of these parameters is assured by:

- turbine speed governors of the generation units
- generators' excitation system
- On-load automatic tap changer of transformers and autotransformers
- Automatic Generation Control

Furthermore, the protection systems (mentioned in section 3.4) installed on transmission lines, generation units, transformers and busbars play an important role in power system control, when quickly clearing faults and avoiding damage to equipment. In the power system control, also the human action is extremely important, namely in the service restoration, in the coordination and implementation of security procedures for work execution and to perform all the necessary actions such as, fault detection on equipments through alarms, to monitor the acceptable range of all parameters, among others.

In an interconnected system such as the ENTSO-E Continental Europe Regional Group system, the steady-state frequency is the same in the whole synchronous network [6]. The system frequency is a measure of the rotation speed of the synchronized generators.

For the system to be balanced the constant equilibrium between generation and demand $\left(\sum generation = \sum demand + losses\right)$ has to be maintained, otherwise a system's frequency deviation $\left(\Delta f = f - f_0\right)$ occurs. In case of an incident with frequency deviation, i.e. disturbance in the balance, the speed governor of each generation unit will automatically act accordingly to its characteristic, changing the unit's power output.

It is easy to understand that a bigger rotating mass in the network will make the frequency variations smaller. The same thought can be applied to the interconnection capacity between two control areas, as the bigger the ATC between neighbouring systems, the more efficient will be the mutual support in case of disturbance, because it compensates automatically the frequency deviation through the interconnections' power flow. System's interconnection, on one hand and most of the time, improves security providing mutual support in case of emergency (for instance, energy deficit or the loss of a significant amount of generation or load), allowing to share reserve capacity and to reduce the level of reserves required, optimizing the installed capacity; but on the other hand, although rarely, it spreads major disturbances to the other control areas, affecting a wider area than the area where the disturbance started. If the imbalance cannot be compensated, as in the 4th November 2006 blackout, system separation and load shedding may occur and these emergency actions may save the system from a total blackout with much more severe consequences.

The primary, the secondary and the tertiary controls are vital to an adequate system operation. Power - frequency control is a key issue regarding system security, thus it is worth to mention that the generation reserve criteria aim to avoid consequences when the system faces unexpected outages of equipments, such as generator units and OHLs.

In case of an incident with a large frequency drop, the activation of primary control reserve (activated within seconds) is followed up by secondary control reserve (activated within minutes) and secondary control reserve is supported and followed up by tertiary control reserve [6], which can be faster (directly activated) or slower (schedule activated). Which generating units are going to be part of the operational reserve (namely: secondary and tertiary) is determined by the market, where the players can bid to provide it. The time frame of the activation of different generation reserves is presented in figure 4.18.

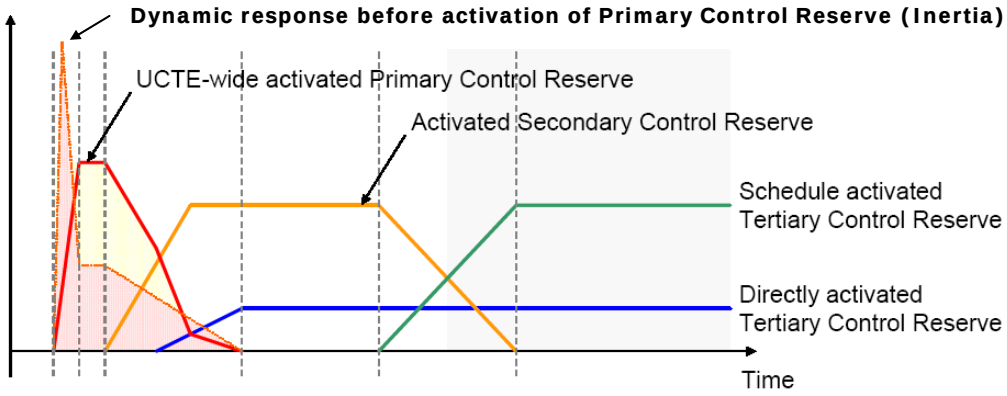


Fig. 4.18 – Principle frequency deviation and subsequent activation reserves [6]

The frequency in the ENTSO-E Continental Europe synchronous system is a global parameter and its control is a joint task of the TSOs. Another control action is Time Control, which monitors and corrects global time deviations of the synchronous time (UTC) in the long term as a joint action of all undertakings/ TSOs. It is applied during periods of uninterrupted interconnected operation, where the synchronous time is the same in all control areas. The requirements and guidelines for the primary, secondary, tertiary and time controls can be found in the UCTE Operation Handbook – Policy 1 Load-Frequency Control [6].

4.8.1. Primary control

The primary control maintains the balance between generation and demand in the network using turbine speed governors. It is an automatic decentralized function of the turbine governor to adjust the generator output as a consequence of a frequency deviation in the synchronous area [6]. Primary control is a mandatory non-paid ancillary service provided by the generation units and it ensures the operational reliability for the interconnected power. It consists of an automated device (installed locally on generation

equipment), which ensures a constant ratio between frequency changes and production (capacity) changes in no more than 30 seconds, which means that in few seconds secondary control needs to be activated as described in section 4.8.2. According to [6], the reference incident, defined as a sudden loss of 3000 MW of generation in the normal operating state for the entire synchronous area, must be compensated by primary control reserve without the need for load shedding (which starts at 49 Hz), following specific absolute frequency deviation (instantaneous: $\Delta f_{\max} < \pm 800 mHz$ and quasi-steady-state: $\Delta f_{\max} < \pm 200 mHz$) established in the Operation Handbook – Policy 1 Load-Frequency Control [6]. In case of a quasi-steady-state deviation of the system frequency, all available primary control reserves are expected to be fully activated.

When facing a sudden generation loss and during the necessary time to activate the control (time-frame of seconds), the frequency will drop, because of the imbalance between generation and demand in the network. This drop is minimized by the generating units' delivery of kinetic energy (stored in their rotating mass) to the grid and by the natural almost imperceptible reduction of the system consumption (load elasticity). The reduction in kinetic energy causes the turbine to decrease speed and, consequently, the synchronous generator frequency to fall. The change in speed will adjust the turbine input valve, changing the mechanical power output and bringing the system to a new steady-state. The primary reserve action allows the stabilisation of the system frequency at a new stationary value after a disturbance, balancing the system again.

The speed control consists mainly of maintaining the balance between the electric power of the generator and the mechanical power input of the turbine; the new speed is determined by the swing equation of the synchronous machine.

4.8.2. Secondary control

A proportional regulation like the primary control doesn't restore the frequency to its nominal value, it only stabilizes the system frequency at a new stationary value after the disturbance, which means the interconnection power flow will differ from the cross border program. In order to restore the frequency to the nominal value or/and to re-establish the agreed cross-border program, an integral control must be added to the control system. Due to the continuous change of the load in the system, to keep or restore continuously the frequency to the nominal value and to maintain constant the cross-border flows according to their schedule, a secondary control is needed to adjust the output of the generators and it will take over within 15-30 seconds. The Area Control Error is the instantaneous deviation between the nominal and the actual system's frequency combined with the deviation of the interchange power flow in a control area, having the following equation: if interconnected: $ACE_{system\,i} = \Delta P_{interconnection} + k \cdot \Delta f$; if islanded $ACE_{system\ i} = \Delta f$, where $\Delta P_{interconnection} = \sum_{i}^{n} \left(P_{measured}\right) - P_{programed}$; $n - Tie - lines$.

The Portuguese transmission system is one control area, which is operated in terms of system balance (including generation reserves) by one control room.

The secondary reserve is ensured by the Automatic Generation Control (AGC) in the time frame of seconds up to 15 minutes after system imbalance. AGC is a centralized and continuous system that automatically adjusts the selected generation set that is associated with it in order to maintain the cross-border interchange schedule between control areas and to perform its share of frequency regulation, which is determined[2] by k, as shown in equation 4.2. It must divide the load variations by the included generating units, having suitable monitoring, telemetering, processing and controlling functions to coordinate directly the speed governors of the generating units, in order to impose a specific output

[2] the k for a control area is part of secondary control to link frequency and power deviations in the secondary controller, given in Megawatts per Hertz (http://www.entsoe.eu/resources/publications/ce/oh/);

power. This function is commonly referred to as Load Frequency Control (LFC). This distribution of the required change in generation among units minimizes operating costs. Figure 4.19 presents the AGC scheme [99].

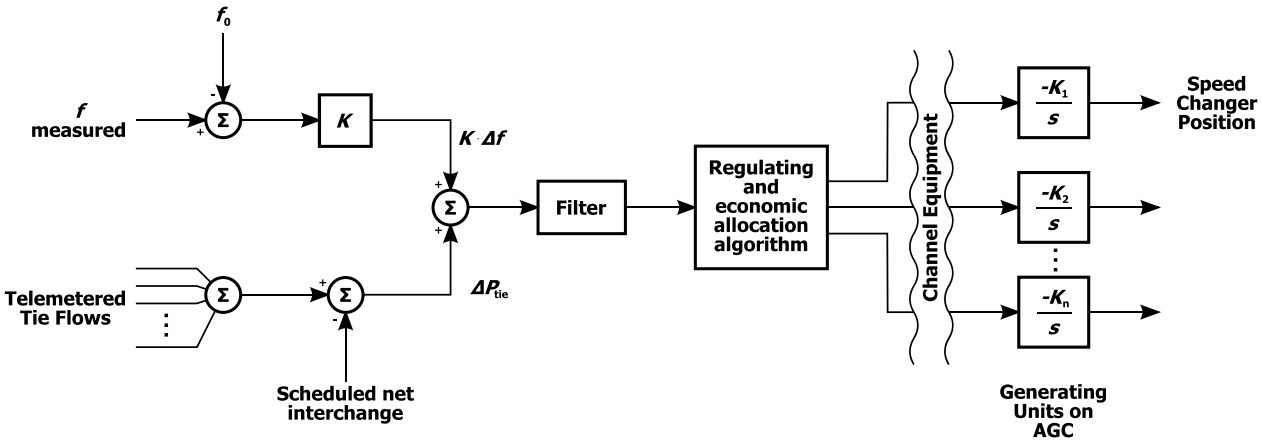


Fig. 4.19 – Automatic Generation Control Scheme [99]

The control room operator with the support of AGC must reduce the ACE to a value below a defined threshold (e.g. < 50 MW) within 15 minutes, restoring the interconnection schedule power flow. The proportional-integral control of AGC starts to respond in less than 30 seconds [44] and therefore, the secondary control takes action in the time-frame of seconds to typically the mentioned 15 minutes. The rules to establish the necessary amount of secondary reserve are defined in the UCTE Operation Handbook – Policy 1 Load-Frequency Control [6].

Figure 4.20 presents the secondary control action when facing a loss of generation bigger than 300MW. It is possible to observe that before the defined 15 minutes the ACE is inside the acceptable limit.

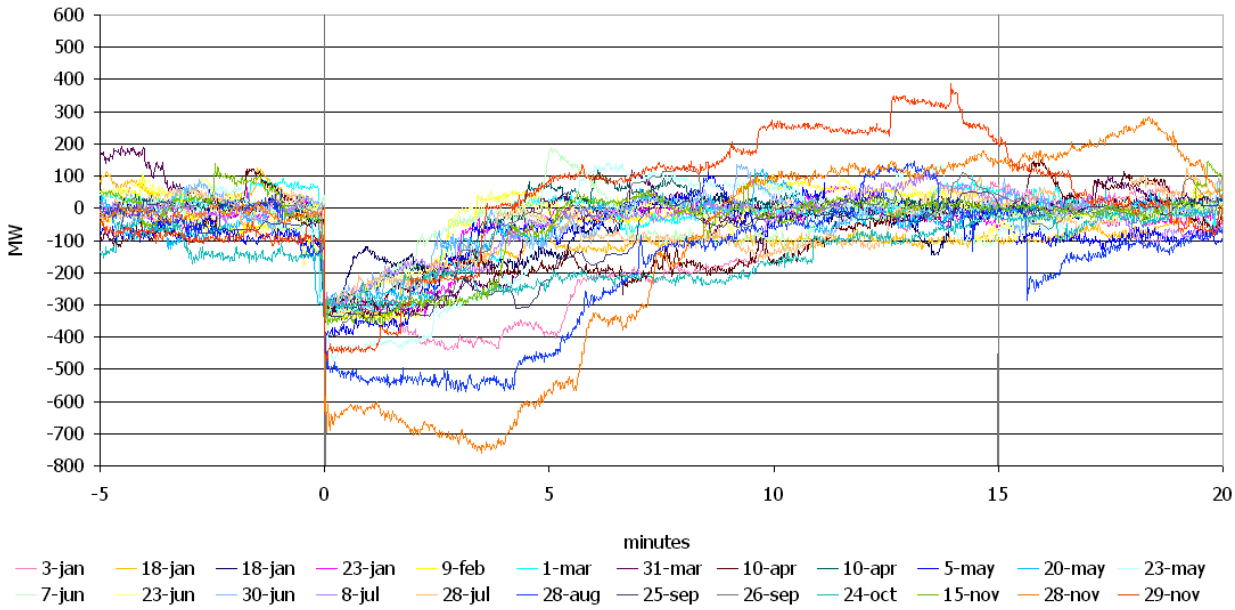


Fig. 4.20 – ACE recovery facing Generation Outages (> 300 MW) in 2009

4.8.3. Tertiary control

Tertiary control uses tertiary reserve that is usually activated manually by the TSOs in case of observed or expected sustained activation of secondary control. It is used to restore an adequate secondary control reserve in a balance situation at the right time, but it is also activated in addition to secondary reserve after disturbances in order to restore the system frequency and consequently release the system's wide

activated primary reserve [6], such as fast reserve (the units that are able to connect and to produce power in less than 5 minutes) and the power margin which is available in the units in service and not connected to AGC. The minimum tertiary reserve is defined by the system operator and in the Portuguese case it uses as reference the loss of the largest thermal generating unit caused by a single contingency (N-1) plus 2% of the predicted consumption in every programming period. This has to be performed within 15 minutes and must be able to stay for at least two hours.

4.8.4. Types of generation reserve

Generation reserve can thus be defined as the amount of generation capacity that can be used to produce active power over a given period of time and which has not yet been committed to the production of energy during this period [100]. In order to respond to different types of events, different types of reserve services are required over different time frames.

It is imperative that enough reserve of active and reactive power exists in the system, on both generation and transmission side, to guarantee a continuous consumption supply. The generation reserve can be divided in three different types:

- Spinning reserve: the unused capacity which can be activated on decision of the system operator and which is provided by generating units which are synchronized to the network and able to affect the active power [100]; Therefore, spinning reserve corresponds to the secondary and synchronized tertiary control reserves. The primary control reserve, which is not controlled by the TSO, is excluded from the spinning reserve.
- Fast reserve: ensured by the disconnected units, which are ready to be connected and come online in a few minutes. In the Portuguese System, in less than 5 minutes it is possible to start the gas turbines (Tunes) and some hydro power plants, namely: Alto Lindoso, Vilarinho das Furnas and Aguieira. The fast reserve is used to mobilize Tertiary Control Reserve within 5 minutes.
- Cold Reserve: ensured by the disconnected units, which take a longer time to start (Tertiary Control), e.g. other hydro power plants that take approximately 15-20 minutes and coal thermal power plants that take some hours to start generating.

4.8.5. Under-frequency load shedding

Facing a frequency drop below 49.8Hz in the European Interconnected System, caused by deficit of generation and after all LFC automatic actions have been exhausted, reference [6] recommends that all TSOs take the following manual actions in order to increase the frequency, at that specific moment: to stop or reduce the pumped-storage power plants, to increase the level of produced active power up to the maximum possible value and to mobilize the available generation reserves. If the described actions are not enough to control the imbalance and the frequency drops to a value equal or below 49.0Hz, in the Portuguese case, under-frequency load shedding is automatically activated. Therefore, the main purpose of this remedial action is to avoid the frequency drop into a value below the acceptable minimum.

The Operation Handbook (OH) establishes the standards and guidelines for all TSOs regarding emergency actions in Policy 5 [6]. According to the forthcoming Policy 5 - Emergency Operations, the total consumption of a control area has to be considered in the percentages to shed on the basis of evaluated scenarios. As guidelines, the triggers of load shedding are without delay, load shedding of customer consumption is allowed at 49.2Hz and mandatory at 49.0 Hz and a stepwise 50 % of the nominal load should be operated under load shedding relays in the range 49.0 to 48.0 Hz. In each step, UFLS disconnection shall not affect more than 10% of the load. At 49.0 Hz at least 5% of total consumption should be shed and, for each individual TSO, to this value should be added the expected generation loss at this stage induced by the frequency drop due to non compliance of units with grid requirements.

On a national level, in the evaluated scenarios, because of loss of generation or other individual requirements, higher values of load shedding may be justified. However, the disconnection of generating units may only start below 47.5 Hz and above 51.5 Hz.

Frequency relays should be preferably installed in the lower voltage levels, as close as possible to consumption, seeking a selective shedding process: to not shed critical loads and to avoid shedding distributed generation (DG).

As in every emergency situation, after a load shedding the control room operator must understand what has happened and act in a cautious way. Thus, reference [6] recommends to strictly forbid the automatic reconnection of shed load after automatic load shedding. The reconnection is performed by the DSO only after approval by the TSO.

4.8.5.1. Portuguese under-frequency load shedding plan

Currently (i.e. before implementation of the new OH Policy 5) the load shedding plan is designed with multi-steps in the first step, the pump-storage power plants are tripped at 49.5 Hz, and then two defined blocks of 25% of the total load are shed as described in table 4.10.

	Generation		***Distribution Network***		***Transmission Network (as backup)***	
Frequency [Hz]		**Time** [Seconds]	**Load**	**Time** [Seconds]	**Load**	**Time** [Seconds]
49.5	Pumps	0.00				
49.0			25%	0.0		
48.8					25%	0.0
48.5			25%	0.0		
48.3					25%	0.0
47.5	Generators					

Table 4.10 – Load shedding scheme in the Portuguese system

In addition to the EHV levels, the Portuguese TSO also supervises and maintains the 60 kV busbars and circuit-ends that link the feeders to the high voltage network of the DN, which are the physical border between the transmission and distribution network, as shown in figure 4.21.

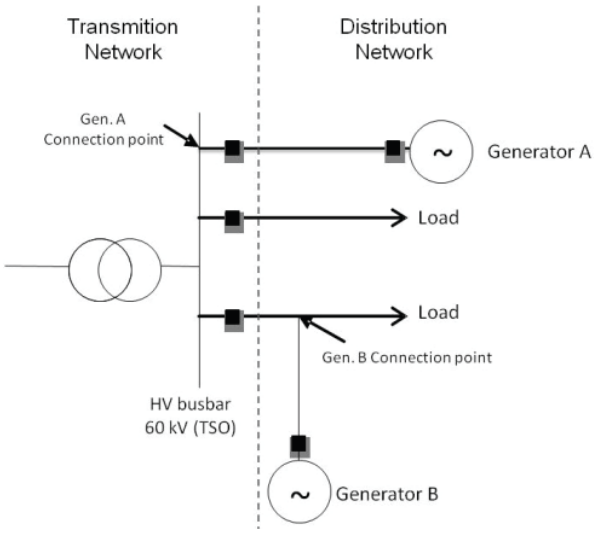


Fig. 4.21 – Single diagram of the TSO and the DSO networks' border [101]

The Portuguese load shedding plan is defined to shed around 50% of the total consumption, dividing 25% of the load in two blocks with a different trigger value, the under-frequency relays in the transmission network acting as backup to the ones installed in the distribution network in case of redundancy. Ideally, the under-frequency load shedding should be performed at the distribution network level, through relay installation in the HV and MV, in order to keep the priority consumers connected.

The relays in the transmission network should only operate as a backup to the distribution network ones and in case of need to shed more load, having trigger values lower than the distribution network ones. In practice, there are four different steps of load shedding. The load which is cut by under-frequency relays installed in the transmission system is much less selective and might cut priority loads. These relays are located in the 60 kV lines circuit-ends at REN's substations. Obviously, there are neither under-frequency relays in 60 kV lines exclusively dedicated to generation, such as wind power plants, nor in circuit-ends of transformers, shunt capacitors and busbar couplers.

The scheme is designed to cope with the islanding of the Portuguese transmission system from the only existing neighbour, Spain, and thereby from the ENTSO-E Continental Europe interconnected system.

With the new forthcoming OH Policy 5, the Portuguese TSO is implementing, in coordination with the DSO, the load shedding scheme presented in table 4.11 on its final stage. Obviously, there will be some intermediate stages before achieving the final one, because the loss of wind generation must be considered.

	Generation		***Distribution Network***		***Transmission Network (backup)***	
Frequency [Hz]		**Time** [Seconds]	**Load**	**Time** [Seconds]	**Load**	**Time** [Seconds]
49.5	Pumps	0.00				
49.0			10%	0.0		
48.8			10%	0.0		
48.6			10%	0.0		
48.4			10%	0.0	25%	0.0
48.2			10%	0.0	25%	0.0
47.5	Generators					

Table 4.11 – Plan for Load Shedding Scheme in the Portuguese System after Policy 5

4.8.6. Voltage stability

In any electricity transmission system, a stable condition must be assured, but power systems are currently more complex and heavily loaded, which means that voltage collapse is becoming an increasingly serious problem. It is possible that, under specific conditions, the system can be placed on a state in which it may not be possible to maintain the voltage levels within secure limits in one or more of the network busbars, because voltage conditions in an EHV grid are directly related to reactive power balance in the systems nodes. Additionally, economic and environmental concerns limit the construction of new transmission lines and generation capacity, thus increasing the stress on the operating conditions and consequently placing the system closer to its stability limits. Voltage collapse can be defined as instability of heavily loaded electric power systems that leads to declining voltages and blackout, which has severe security repercussions and jeopardizes the essential service to final customers. Near the critical point, any small increase of load implies a serious drop in the voltage level.

Adequate reactive power compensation is indispensable to guarantee a reliable system operation, with the suitable quality of service and security levels in the load supply. The voltage values must stay inside the defined acceptable range. Therefore, the equipments used to perform reactive power management must ensure enough control capacity, fulfilling the needs. It is also recommended that these equipments should

be installed as close as possible to the consumption centres, in order to avoid the unnecessary reactive power flows in the network, because they reduce the transmission capacity and increase the system's losses.

System instability can occur if one or more grid elements disconnect by tripping (contingency), the load increases suddenly or the geographical profile of the generation dispatch is abnormal. In case of instability, the system operator must have available an adequate reserve of rapid reactive power participating in the primary voltage control and must act on the electrical grid elements nearest to the area (or busbar) where the problem lies, taking suitable control measures in order to bring the system back to a secure operating condition. The control actions to be applied in a voltage collapse situation are also the actions that are taken in a normal voltage – reactive power control situation, namely:

- To increase the generators' excitation in order to achieve more reactive power injection.
- Automatic devices response, such as Static Var Compensators (if available).
- To connect capacitor banks.
- To change (or block) the transformer and autotransformer tap position.
- To change topology.
- To transfer load to other delivery points through the distribution network.
- To execute load shedding (this is the last action to be applied when reactive power resources are insufficient).

The quality of supply is determined on the basis of the observed voltage deviations of an electrical power system during a given period of time, so voltage stability can be defined as the ability to maintain acceptable voltage values in every busbar. As it was already mentioned, voltage is a local parameter, which must be controlled efficiently through the described control actions, because it depends greatly on the reactive power flows in the system. In the Portuguese transmission system for EHV, the admissible range for voltage variation, in N criterion, is approximately ±10%. In section 4.5.2.2, the acceptable limits for voltage are presented.

In real-time operation, it is important for the system operator to have voltage stability indicators that allow him to react in advance and prevent voltage collapse blackouts. Due to this need an application was developed by the Portuguese TSO that provides useful information directly to the control room operator, allowing the early recognition of an emergency state and to take the required remedial actions in due time. The need to develop a process to identify voltage collapse situations in the Portuguese transmission system arose with voltage problems identified in a specific substation when performing N-1 Contingency Analysis, due to the trip of a 220kV OHL in the Lisbon area that would create a significant voltage drop in one of the end substations during specific operating conditions (namely peak load periods) [5].

Summing up, reactive power management has as goals: to keep the voltage values inside the acceptable range in every busbar, to minimize the reactive power flow in the grid elements to minimize the system losses, in order to maximize the active power transmission capacity and to maintain voltage stability.

4.8.7. Pumped storage

Pumped storage's main purpose is to increase energy efficiency, optimizing the usage of water in hydro power plants by the decreasing discharged water by the dam through its reuse, by the support in maintaining the scheduled cross-border power flow and by "storing" wind energy in the form of water, which can also be reused. The water storage process can be described in the following way: the water is pumped to a higher elevation reservoir from a lower one. In the past pumped storage was operated on a daily basis during the low-cost period, i.e., the off-peak period of the electrical demand, which allows producing electrical energy through hydro power plants in the peak period, using the off-peak stored water. Thus, a daily cycle of efficiency was created.

Nowadays, pumped storage is also used to regulate wind generation, accommodating the exceeding amount of generation, and their daily basis can be adapted to the amount of wind. Wind generation presents a very volatile pattern, which increases the need of pumps available to operate in the system. Figure 4.22 presents the wind generation in four different days.

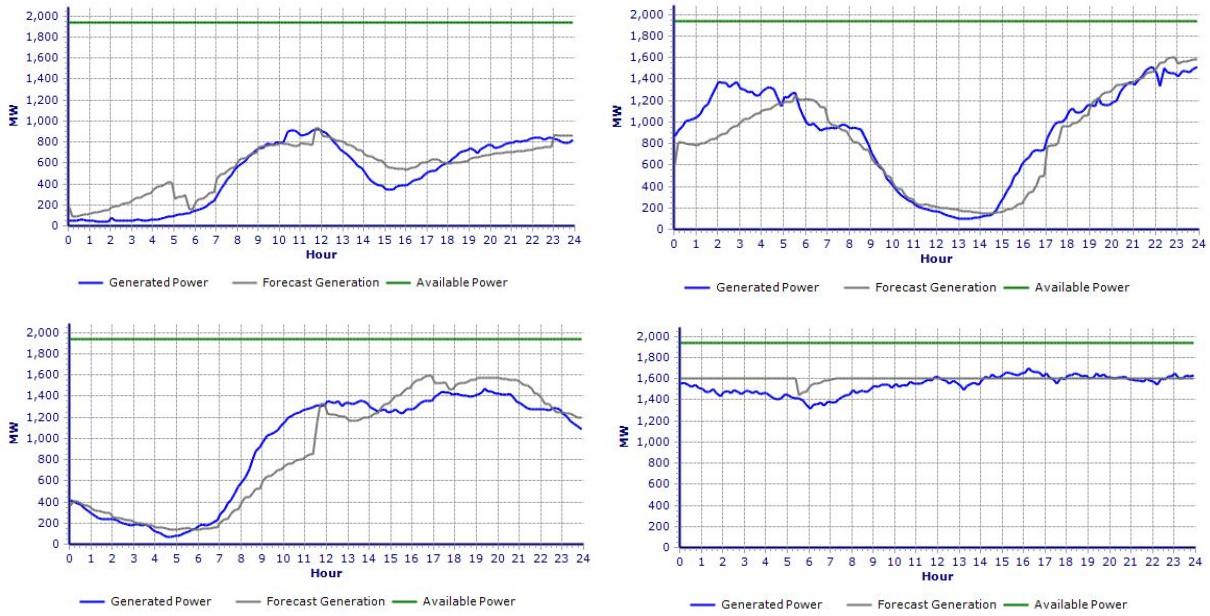


Fig. 4.22 – Examples of Wind generation daily pattern (from December 2009) [102]

Reference [103] presents an analysis of the average hourly distribution of the wind farms peak production, from 2005 to 2008, as shown in figure 4.23. The off-peak period is coincidentally the period where wind generation presents higher values and also where pump storage is more needed, because the load may not be enough to accommodate the total amount of wind in the system.

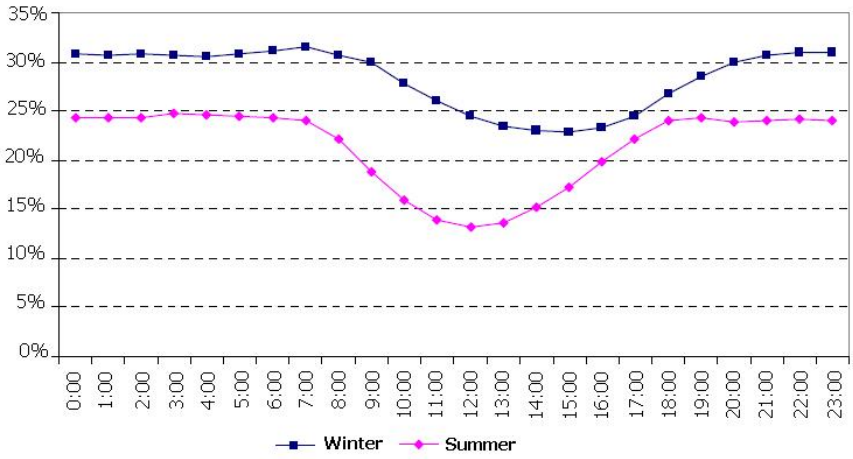


Fig. 4.23 – Wind generation daily distribution [103]

Normally in off-peak periods, from midnight to dawn, the pump storage runs using wind generation, cheap imported energy and thermal power plants that are kept at the technical minimum to be able to supply the morning peak. Depending on the amount of wind, whenever there is a generation surplus, pumps are used not only at night but also during the day.

Pumped storage has the advantage of being suitable for fast generation reserve. Some of the existing units change from pump to generator in a few minutes. The cost of operating a hydroelectric plant is nearly immune to increases in the cost of fossil fuels such as oil, natural gas or coal and it does not produce greenhouse gas emissions. About 70% to 85% of the electrical energy used to pump the water can be regained, taking into account water evaporation losses and conversion losses. This technique is currently the most cost-effective means of storing large amounts of electrical energy on an operating

basis, but capital costs and the presence of appropriate geography are critical decision factors. The usage of pumped storage in a seasonal cycle also allows minimizing the discharge of water by the dam, storing it in the rainfall period.

Reversible turbine/generator assemblies act as pump and turbine. In the Portuguese power system, there are 5 hydro power plants running with reversible units, namely Vilarinho das Furnas, Torrão, Alto Rabagão and Aguieira power plants and, more recently, Alqueva and Frades power plants.

4.9. Operator training and qualification

In recent years, the daily routine of TSOs has become more complex. Control room operators play a decisive role in the good performance of the power system and to achieve all the essential tasks for which it was designed. The operator's ability to manage a large amount of data (information), to adequately understand, decide and execute on time suitable remedial actions, reveals itself as extremely important. Pressured to operate the power system in the most effective way when facing a disturbance, operators are responsible for ensuring a secure and reliable operation of the system, for mitigating a disturbance's impact, limiting as much as possible the affected area, and for restoring the system, returning it to a secure operating state.

It is important to be aware that electrical utilities are confronted daily with unpredictable events in their networks, which may lead to severe security level repercussions in the system, far exceeding all the security principles used for operation and consequently jeopardizing the essential service to the consumers. Operator training using simulators is one of the best ways to provide control room operators with the skills to deal with consequences of unforeseen disturbances that put the system in an emergency situation. When facing an incident, the operators' reaction is decisive to minimize consequences.

Recent incidents, as the ones described in chapter 2, prove that severe contingencies (beyond the reasonable and widely used security limits) actually can happen. The main benefit of operator training is to reduce risks when performing real time operation, but it also allows:

- To standardize operational procedures and to design proper strategies to face emergency situations, improving operation.
- To increase knowledge and awareness, especially in emergency and restorative system conditions.
- To apply and emphasize good practices.
- To improve communication and interaction between participants.
- To evaluate SCADA behaviour/performance in face of extreme situations.
- To distinguish patterns and trends on the SCADA information (that can appear in large amounts).
- To practice accurate methodologies and develop active skills.

As an overall benefit of training, it is possible to identify the improvement of operators' performance and self confidence. Highly trained and experienced operators are more capable of quickly recognising an emergency situation that is developing in the system, and more effectively take the suitable remedial actions to quickly return the system to a secure operating state. Hence, it is possible to conclude that dispatch training simulators help to improve effectiveness in the decision-making process and to decrease the equivalent interruption time, regarding quality of service indicators.

Operational training is defined in the policy 8 of the Operation Handbook [6]. The policy clearly states that each TSO has the obligation to ensure the appropriate qualification of the personnel trained to cope with any kind of events within the system. This obligation implies a very solid and well organized training scheme with a strong theoretical and practical background. TSOs have now a set of requirements and guidelines defined in the policy, regarding to training programs (initial and continuous training), Inter-TSO

training (between neighbouring TSOs), training organization and dispatchers' accreditation and the basic requirements for the dispatch training simulator (DTS).

4.9.1. Portuguese experience

The Portuguese TSO (REN) uses a dispatch training simulator since the beginning of 2001 with the purpose of improving operators' performance efficiency and achieving greater accuracy in their actions, updating and assuring the maintenance of their skills. The DTS is a replica of the SCADA used in real time, which allows the operators to train exactly with the same interface as the real-time system. The need of a DTS won particular acuteness after a major blackout occurred in 9th of May of 2000. This incident's analysis showed clearly the benefits that can be taken from DTS, mainly the ability to train operators to face severe contingencies.

With DTS it is possible to keep on simulating all the past blackouts or relevant incidents, such as the simulation of a national blackout with service restoration through tie-lines or black-start, voltage collapse situations and selected severe contingencies that may occur and even to analyse in advance the system behaviour every time that an important grid element is put into service. Obviously, operators training always require analysis and detailed explanation until the system (after a disturbance) is completely restored and security is ensured again. Of course, it is also possible to analyse the best approach for the restoration process.

Currently, the Portuguese TSO provides two courses every year to its operators, one in spring and the other one in autumn. The courses have two specific parts: theory about the simulations that will happen in sequence. The theory part is given in a classroom environment, presenting and discussing the topic, which allows the gathering of control room operators in the same place. The simulations part is done in a replica of SCADA, using exactly the same man - machine interface. The continuous improvement of control room operator's performance must be a permanent goal. Whenever a relevant incident occurs, the TSO operators' training reveals itself crucial in order to improve their performance in terms of efficiency when confronted with such scenarios.

4.9.2. Joint training between TSOs

The CIGRE Working Group C2.31 has developed an interesting work about joint training between TSOs, which is presented in references [104] and [105]. Joint training is one of the most frequent recommendations from the blackouts described in chapter 2 that have affected a wide area involving several TSOs, thus it is obvious that operator actions when facing emergency and restoration situations is one of the current biggest worries of TSOs in order to improve performance and, consequently, reduce risk.

As mentioned previously, operators' training has many benefits, which are also applied to joint training, although in this specific situation there are additional benefits to be mentioned, such as:

- Strengthened coordination and interaction of control centres across companies and national borders (mainly, between neighbouring TSOs).
- Harmonization of practices and procedures between different companies, including the improvement of mutual understanding.
- Identification of the information that is crucial to be exchanged between different TSOs.

Due to unbundling in the electrical industry and due to recent blackouts, combined training has gained a preponderant role in the utilities' activity. The objectives of combined training are on improving the human aspects in the control centre. The individual performance level of each operator should be improved related to teambuilding and the ability to fulfil the job duties within a group assembled of

different teams from different control centres and entities. The working group has distinguished 3 different categories for combined training: Inter-TSO training, Inter-company training and Intra-company training. [104].

In Europe several approaches of combined training are known [104]. Nordel (Norway, Sweden, Finland and Denmark) carries out joint annual training programmes at Inter-TSO level. The French TSO RTE and the Italian TSO TERNA perform common training sessions at Inter-TSO level. In Belgium, the TSO ELIA regularly performs simulator based Intra-company training for the operators of National and Regional control centres. At an independent training centre in Germany, several ENTSO-E members take part in combined training at Inter-company level (e.g. the Netherlands [106], Austria [107], Czech Republic, Switzerland) and at Inter-TSO level (e.g. Germany, Austria) as well. The Spanish TSO (REE) and the Portuguese TSO (REN) performed in November 2007 a common training session based on the Iberian power system entered in REE's simulator, where also the Portuguese system was modelled. Before the session in Spain, REN organized training sessions with the presence of REE and the Portuguese Distribution company, but without their active participation.

4.9.2.1. Combined training between the Iberian TSOs

On 6th November 2007, the first joint training between REN and REE was held in Madrid with the simulation of an Iberian Blackout and the restoration process of the North-West regions of Iberia, see figure 4.24. This training session follows the recommendations of the 4th of November 2006 Blackout in the former UCTE interconnected system and had the following main purposes:

- Proof of the coordination, organization and hierarchy of control rooms (different entities).
- Improvement identification in the service restoration plan.
- Continuous training of control room operators in order to improve performance.

Fig. 4.24 – Geographical Regions included in the Restoration Process

REE invited to the training session all the players that will be directly involved in the restoration process during a real Iberian blackout situation. With 51 participants, REE gathered in the same environment the following companies: Endesa, Unión Fenosa, Iberdrola, Viesgo, Gas Natural, Hidrocantábrico, Bizkaia Energia, REN and EDP. The training session started at 09:20 and ended at 14:10, i.e. taking approximately 5 hours.

In the restoration strategy, the priority goals were the restoration of strategic loads, the feeding of nuclear power plants (which take a long time to start producing), the restoration of the tie-lines with the

interconnected system (specifically, with the French System), the feeding of thermal power plants and hydro power plants. The Spanish TSO has created several islands through the blackstart of several hydro power plants in the system and The Portuguese TSO has created one island with the blackstart of a natural gas power plant in the region of Porto. As a blackstart demands, the restoration of the supply was extremely slow in the first part of the process and with the increase of the inertia (generating units available) the speed of the restoration increases progressively.

In the Portuguese system, AGC in frequency mode was activated as soon as a number of hydro power plants were connected and a valid frequency measure existed in the system. In the Spanish system, the AGC could not be activated, because of the existence of several islands. The interconnection between Portugal and Spain was made after the interconnection of all the Spanish islands and the interconnection between the Spanish and the French system. With suitable voltage and frequency conditions in both systems, the synchronization between the two affected systems was made through the 400kV OHL in the North by Spanish initiative, although the initial expectations were to connect through the 220kV OHL in the north-east of Portugal.

From the Portuguese perspective, the combined training was a very positive experience. REN has proved to be capable of restoring the system after a complete blackout in a secure way, maintaining frequency and voltage within an acceptable range. All the expectations were exceeded, and it was possible to conclude that joint training has undeniable added value to the players of the Iberian Electrical Power System. Figure 4.25 shows the Portuguese team during training in Spain.

Fig. 4.25 – Portuguese Group during Iberian training

4.10. Conclusion

The Portuguese transmission system operator is responsible for the system planning, design, construction, operation and maintenance of its infrastructures. It is responsible for permanently maintaining the balance between generation and consumption by monitoring the system security, supervising all the equipment and adjusting the cross-border power flows with the Spanish grid.

The Portuguese system is diverse in terms of primary energy sources for generation and includes hydro, combined cycle natural gas, wind, photovoltaic (solar panels), biomass, CHP, fuel and coal power plants. Nowadays the Portuguese government provides big incentives to the use of renewable energy sources, because these power plants help to reduce CO_2 emissions in the electricity generation mix. Due to the latter, the power generation through wind had a significant growth rate since 2000, and it has created new challenges to the system's operation, because of the high intermittency of the primary resource and its behaviour facing disturbances. With the high penetration of wind, the control of the power system in terms of generation reserve has to be re-evaluated, introducing a new issue in system's adequacy. Wind generation adds complexity to the power system's operation, because of its location in the EHV level, far from the consumption, and its intermittent character. Depending on the wind generation units' dynamic behaviour (the ability to withstand voltage dips, to control voltage or even frequency) in the future, they might provide ancillary services to the system. At the moment and because of the bad behaviour of wind farms when facing disturbances, which was seen in the analysed blackouts, the increased need for generation reserve optimization is a new challenge facing the TSO.

Due to the construction of new infrastructures and improvement of the existing ones in the Portuguese transmission system, which is promoted by law and regulation, it is possible to achieve the main goals of the electrical power system that are defined. This causes the network to be dynamic, i.e. the OHL length

and the number of substations (the number of grid elements) is increasing at a high rate and associated with that, also OHLs change their configuration and designation very quickly, creating an additional issue on the development of this work. To solve the latter, the future results cannot depend on a specific grid element; the results must refer to types of elements, such as per km per voltage level, or to specific network and right-of-way characteristics in the case of OHLs. Only after the non-specific indices are addressed, it will be necessary to build up the final index per each grid element. This approach will make the methodology independent of the actual network, allowing it to grow.

In the current competitive environment, the aim is to maximize the transmission capacity of the network, fully using lines' capacity and achieving more efficiency. Since the market price is lower during the off-peak time (normally during the night), the line capacity reserved for the thermal solar radiation input is released. These changes were implemented with the recognition that fixed loading limits were very restrictive, resulting in under-utilization of the conductors. Besides investing in structural changes, the Portuguese TSO has increased the transmission capacity of the network by adopting dynamic rating instead of static limits for overhead lines, which depend on existing ambient conditions variation. The operating limit of electrical lines is determined by the maximum allowed temperature of the conductor and not by its current limit. It is possible to increase the thermal rating at least 10 to 15%, on average, thanks to real time monitoring.

The Portuguese TSO has been continuously striving for system operation improvements by developing efficient processes to analyse and react to severe incidents, such as contingency lists for security analysis and operator training. This is strictly connected with control room operators' performance when reacting to disturbances. In an interconnected system, like the Portuguese one, medium size, highly meshed and with a number of tie-lines connected to the neighbouring countries, the knowledge of the relevant network is crucial to maintain the security of the system. To exchange real-time information of the relevant neighbouring network enables a more accurate security analysis procedure.

Based on historical data, it is concluded that the simultaneous trip of several power lines and the trip of a voltage level in a substation should be taken in consideration and therefore a representative set of contingencies allows us to improve, to anticipate the consequences of incidents and to identify suitable preventive and corrective measures. To complete the security analysis that is currently made by operations planning, new contingency lists are available in the EMS. Obviously, the usual "must run" contingency list is automatically performed in real time operation, but the security analysis can also evolve to a set of more likely contingencies instead of considering all events equally probable. This may be a qualitative improvement that can be drawn at the end of this research work.

In every case that identified contingencies may cause severe incidents to the transmission system, the TSO must prepare remedial actions in order to mitigate as much as possible their consequences. The remedial actions can be preventive or curative and they will be applied to ensure or restore the system's security and the type of remedial actions will be chosen, depending on the costs and on the time that they will take to be implemented and effective. After an incident there is a period of time where the N-1 criterion may not be fulfilled and that occurs until the restoration of the tripped element(s) or the needed remedial actions are taken to place the system again in a secure operating state. During this period, the power system is more exposed to risk, thus the trip of any additional element may cause constraints violations, placing the system out of the normal state.

A TSO must be aware of the system's risk due to contingencies that occur inside or outside its borders in a highly meshed interconnected system. The information exchange and coordination with the neighbours is strongly recommended. In an emergency situation, most of the time, the tie-lines provide mutual support to the endangered system; however a disturbance might also spread into the other system, affecting a wider area. In order to avoid uncontrolled cascading with impact across borders, it is essential to prepare emergency procedures, including coordinated remedial actions. Beyond coordinated remedial actions, also a fast and coordinated restoration procedure is necessary, therefore a good communication between TSOs is crucial for the good performance of the system.

A partial blackout, like the one on 4th November 2006, is one of the most serious emergency situations that can happen in the interconnected system, although the worst scenario, which is a total blackout of the ENTSO-E Continental Europe system, was avoided by the under-frequency load shedding. Regarding the Iberian system, which has a bottleneck in the transmission capacity between Spain and France, the security analysis of major disturbances becomes an issue for both Iberian countries because of the danger of islanding. Due to the importance of such an incident and the aim to restore the system as quickly as possible, communication, efficient emergency procedures, accurate security analysis and operators training are vital.

The failure of the SCADA system is another major disturbance, leaving the control room operators blind and powerless. SCADA is the main tool for system operation, if a disturbance occurs simultaneously with a SCADA failure, the control room will be warned of its severity and consequences by the neighbouring system (permanently controlling the interconnections power flow) and by the distribution system (if there is energy not supplied). Actually, in the 14th of August 2003 USA blackout, the SCADA in one of the utilities failed.

An electrical power system has control parameters, mainly frequency and voltage, which are vital for an adequate operation. In order to control them, the power system has several control methods that ensure the continuity of supply fulfilling the quality of service requirements, such as primary, secondary and tertiary reserves, protection systems installed in each grid element, under-frequency load shedding devices, on-load transformer tap changers, automatic voltage regulation, static reactive power compensation and pumped-storage. When a major disturbance occurs, protection systems and control actions attempt to stop power system degradation, restore the system to a normal state, and minimize the impact of the disturbance. There are four main phenomena that may greatly disturb the system or even initiate a major incident must be prevented, namely: cascade tripping, voltage collapse, frequency collapse and loss of synchronism.

The operator is crucial for a good performance of the power system and to achieve all the essential tasks for which it was designed, thus the continuous improvement of control room operators' performance must be a permanent goal. Operator training using simulators is one of the best ways to provide control room operators with the skills to deal with consequences of unforeseen disturbances that place the system in an emergency situation. When facing an incident, the operators' reaction is decisive to minimize consequences. With DTS, it is possible to keep on simulating all the past blackouts or relevant incidents, to simulate a national blackout with service restoration through the tie-lines or black-start, to simulate selected severe contingencies that may occur and even to analyse in advance the system behaviour every time an important grid element is put into service. The Portuguese TSO uses a dispatch training simulator since 2001, aiming to improve operators' performance efficiency and achieve greater accuracy in their actions, updating and assuring the maintenance of their skills. The need of DTS won particular urgency after the major blackout that occurred on 9th May 2000.

It is not possible to develop a research work that evaluates operational risk in a system's operation environment, if there is not a good understanding of the way an electrical power system works and also how it is operated. This understanding is essential to evaluate the severity of contingencies that is further developed in chapter 8. Therefore, this chapter gives an overview of the Portuguese transmission system, describing a broad set of important aspects, in order to support future decisions in this work. It is important to be aware that operators need decision support tools that can provide them a trigger in case of change of the system state.

Chapter 5.

Portuguese Transmission System Incidents

5.1. Introduction

This research work intends to be directly applied to the Portuguese Transmission System (PTS), thus it is essential to understand concepts and definitions, and properly analyze the historical data that are the basis of the statistical work. As it was already mentioned, incidents are unpredictable disturbances and utilities are confronted daily with disturbances and anomalies in their grids, which need to be recorded and analysed. In this chapter, the incidents are analysed and their causes characterized. The steps taken for each cause are the following:

1. Analyse and evaluate the incidents
2. Identify which are the causes that most affect your system
3. Relate each cause with your system's intrinsic characteristics
4. Analyse how controllable the causes are and which actions to take

This chapter is focused in the analysis and statistics of the EHV voltage level grid elements.

5.2. Concept of incident

An incident is an event that leads to disconnection (not planned) of one or more grid elements – incident elements, which may lead to demand not supplied [64].

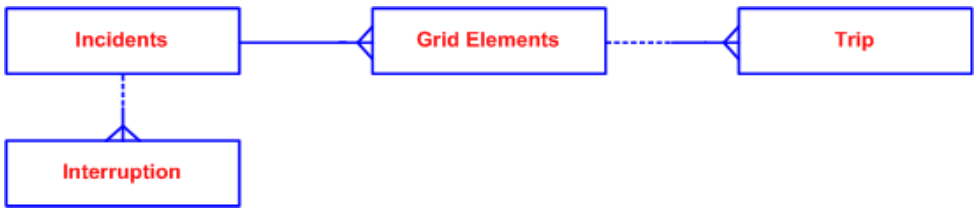


Fig. 5.1 – Incident Structure [19]

Figure 5.1 illustrates that incidents may affect more than one grid elements and that each grid element has a maximum number of trips associated, which is directly dependent on the number of circuit-ends where the grid element is connected (e.g., a line that connects 2 substation has two trips, one for each circuit-end). An incident may or may not cause a consumption interruption, in other words, energy not supplied. When consumption interruption happens, the interruption may be total (cutting all the load of a substation, which is a delivery point injecting power into the distribution network) or partial (cutting the load of some of the feeders connected to the affected substation).

Incident's grid elements can be subdivided in "origin elements" and "affected elements". The definition of origin elements is that these elements are the grid elements affected by a short-circuit (where the fault actually occurs), or in case of absence of short-circuit, all the grid elements removed from service in an untimely way, thus initiating the grid disturbance. Incidents are considered forced outages, independently of the existence or absence of short-circuit. Affected elements are those elements that are removed from service in sequence to the outage of the origin element (often in consequence of short-circuit in the origin element). These affected elements may exist when one of the following events occurs:

- Incorrect operation of a protection relay.
- Overloads associated to the loss of other grid elements during the sequence of events.
- Busbar protection and breaker failure protection operations.
- Zero voltage on a grid's area.

In order to exemplify what has been described, figure 5.2 presents an incident that has removed two grid elements from service. The origin element tripped in consequence of a short-circuit caused by a lightning and the affected element was removed from service by a protection system misoperation.

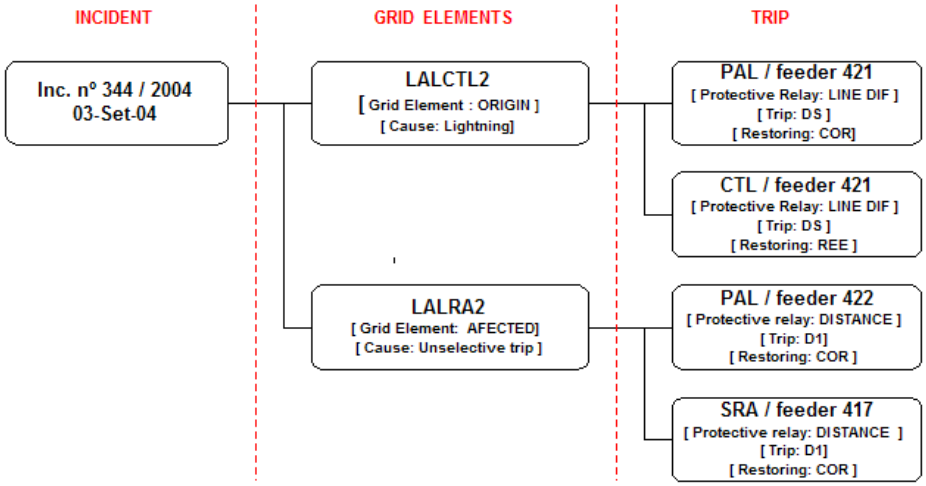


Fig. 5.2 – Incident Example [19]

Any grid element removed from service may affect equally the system security, independently of being origin or affected element. Topological changes resulting from an incident will affect mainly the power flow distribution within the grid elements that remain in service (connected) and the voltage level in the system busbars. After an occurrence of this nature, and depending on its dimension, i.e. the number of affected elements of the grid, consequences may include violations of operating limit, loss of generation units and supply interruption (partial or total) to one or more delivery points.

After defining the concept of incident, origin element and affected element, tables 5.1 and 5.2 summarize the number of grid elements involved in incidents for each year. Thus, it is also possible to conclude that the affected elements represent about 20% of all involved grid elements.

Grid Element	2001	2002	2003	2004	2005	2006	2007	2008	2009
AT	2	0	3	5	2	3	1	3	5
Busbar	1	5	4	2	7	2	3	1	2
150 kV OHL/UC	125	115	183	124	69	98	96	77	71
220 kV OHL/UC	119	145	68	54	179	70	42	50	90
400 kV OHL	38	93	93	57	127	62	37	36	52
TR	12	28	18	10	15	18	12	16	12
IB	0	2	0	0	3	1	1	0	3

Table 5.1 – Total amount of Origin Elements

Grid Element	2001	2002	2003	2004	2005	2006	2007	2008	2009
AT	5	8	9	6	6	4	3	5	7
Busbar	1	5	4	2	7	2	4	3	2
150 kV OHL/UC	150	120	216	151	91	118	110	112	79
220 kV OHL/UC	140	165	74	60	192	73	48	51	94
400 kV OHL	57	103	105	72	143	74	49	42	62
TR	29	58	58	36	51	50	38	41	59
IB	8	5	2	2	7	2	0	4	4

Table 5.2 – Total amount of Origin and Affected Elements

In order to understand the results that are presented in this chapter, the definition of fault is also needed. A fault is any power system abnormality which involves, or is the result of, failure (loss of insulation) of a primary system circuit or equipment and it requires the immediate disconnection of the faulty circuit or equipment from the power system by the automatic tripping of the appropriate circuit-breakers (definition used by REN). If the reconnection of the circuit-breakers that opened to clear the fault leads to another trip, it indicates a permanent fault, where fault local identification and repair or replacement actions need to be carried out in order to reconnect the grid element as soon as possible.

As already introduced in section 3.2, there are several types of contingencies, or in this case faults. In the Portuguese transmission system, faults are classified as follows:

- Independent fault: normally single faults with one origin element.
- Dependent faults: affecting more than one grid element, which can be sub-divided into:
  - Common cause faults (e.g. it is very common for lightning strokes to cause a short-circuit in two OHLs that share the same tower or for forest fires to simultaneously affect more than one OHL in the same corridor).
  - Different cause faults - when grid element disconnection occurs as a consequence of an initiating fault (e.g. protection system misoperation on one circuit-end of a grid element as consequence of a short-circuit on another element).

At this point it is important to mention that grid elements are delimited by circuit breakers, and the protection systems open them to isolate and clear a fault.

Figure 5.3 presents the number of incidents per day of the year, from 2001 until 2009, showing clearly the unpredictable nature of these events, although seasonal patterns can be recognized. Incidents have neither a specific time nor specific day to happen.

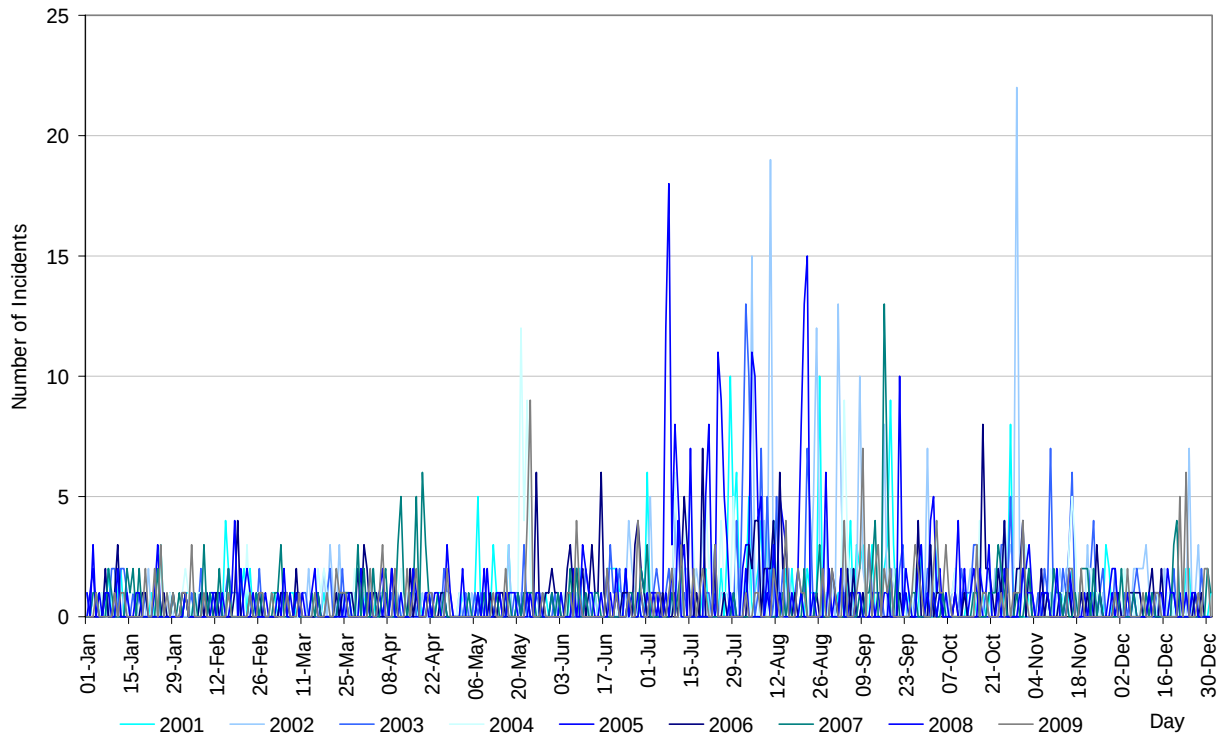


Fig. 5.3 – Number of incidents in the EHV network per day

Next to the seasonal variations shown in figure 5.3, it is possible to conclude that a larger amount of incidents happen in particular periods of the day, regarding the 24 hour period, as presented in figure 5.4.

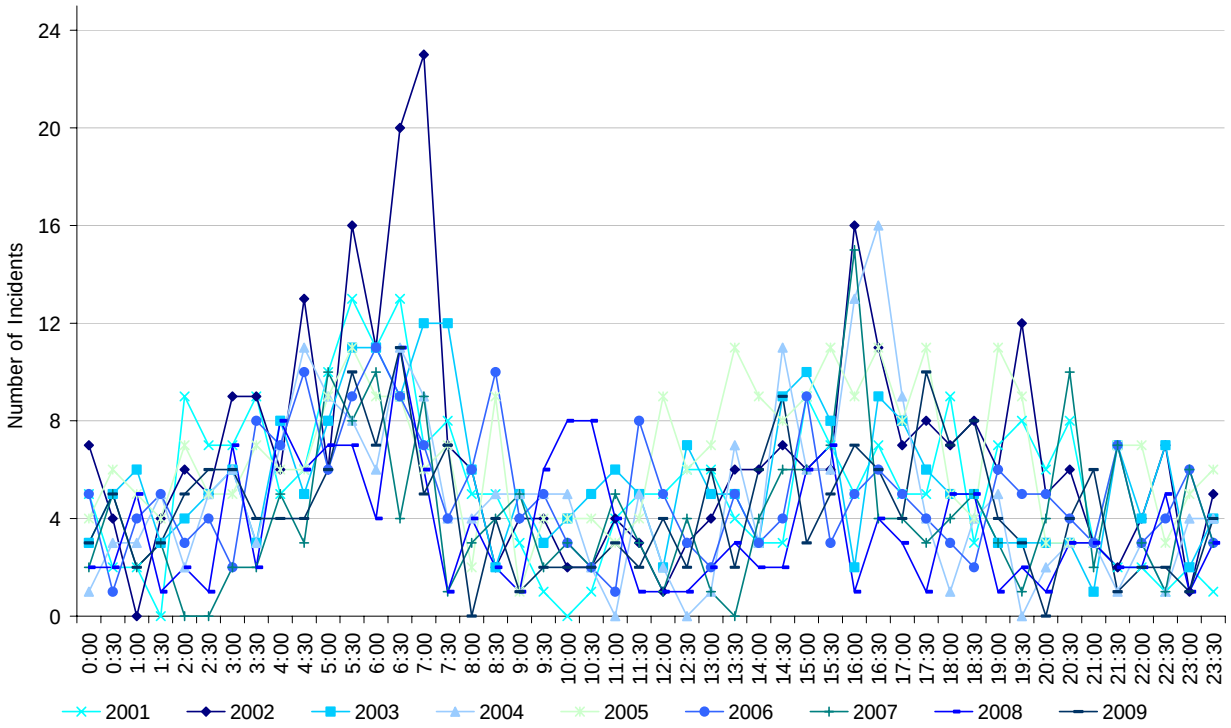


Fig. 5.4 – Number of incidents 24h period distribution in the EHV network

In order to make even clearer the evidence of the periods where incidents more frequently occur, figure 5.5 presents an average in percentage of the number of incidents in each hour.

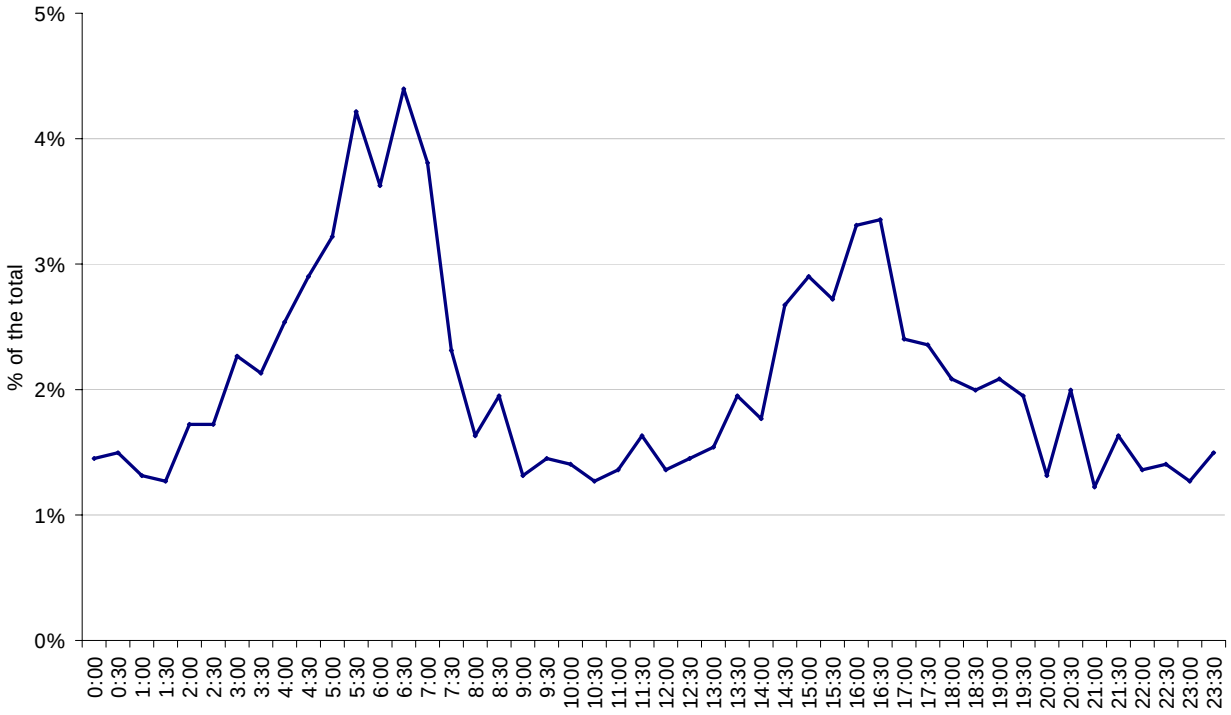


Fig. 5.5 – Number of incidents 24h period distribution average in percentage for the EHV network

5.3. Main causes of PTS incidents

In general terms, the incidents main causes are described in section 3.2.1. From historical data, it is concluded that most incidents originate from overhead lines. From 2001 until the end of 2009, OHLs represent on average about 90% of the incidents with origin in the Portuguese transmission system. Overhead lines, due to their dispersion over a wide geographic area and because of the many different ground characteristics where they are deployed, are more exposed to the action of external factors which cause most of the grid incidents.

The most frequent and usual causes for incidents in the Portuguese transmission system are the following:

- Storks (environmental cause)
- Forest Fires (environmental cause)
- Fog in combination with pollution (atmospheric cause)
- Lightning (atmospheric cause)

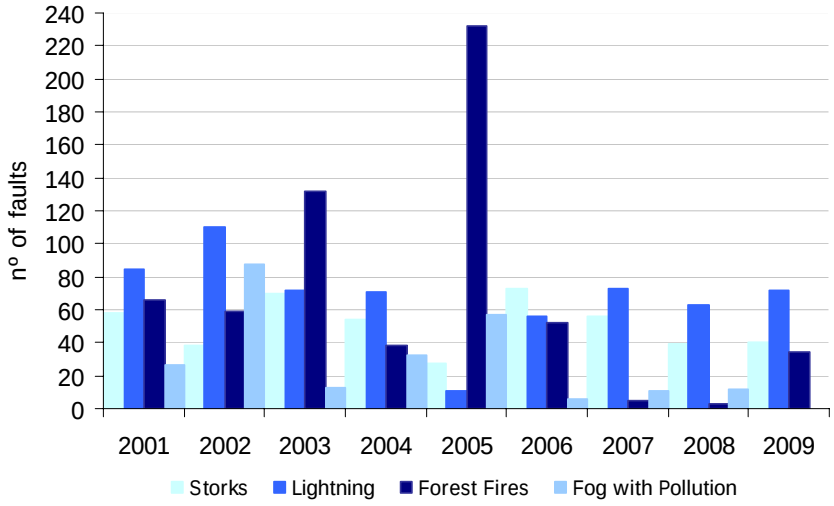


Fig. 5.6 – Number of faults in OHLs caused by the main causes

Figure 5.6 presents the number of faults caused by the main causes. The incident's set of data under analysis is composed of 2572 faults, where 2370 are OHL faults, representing 92% of the total number of faults in the PTS. The faults in transformers represent about 7% and busbars 1% of the total. The four main causes represent about 78% of the faults in the Portuguese transmission system (82% if only OHLs are considered), from 2001 to 2009.

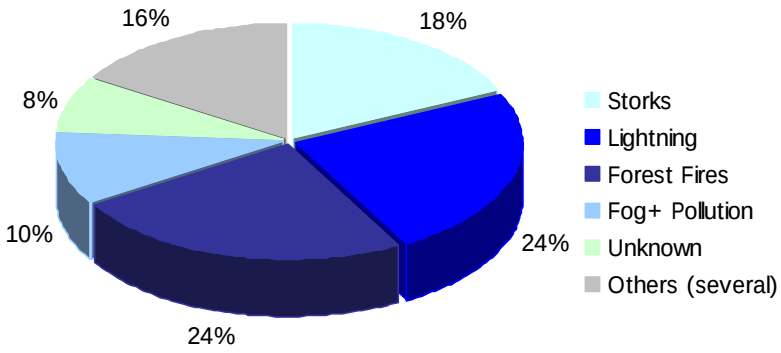


Fig. 5.7 – Percentage of fault causes

In figure 5.7, the category “others” includes internal origin and external causes. The internal origin causes include equipment, protection systems, control systems, maintenance and operation human errors. The external causes include machinery (such as cranes), other networks, vandalism acts and force majeure, among others. External causes only represent around 1% of the total number of faults, whilst internal origin faults represents about 14%. Figure 5.8 shows the weight per year of each sub-cause in the internal origin category, where control and protection systems play a significant role.

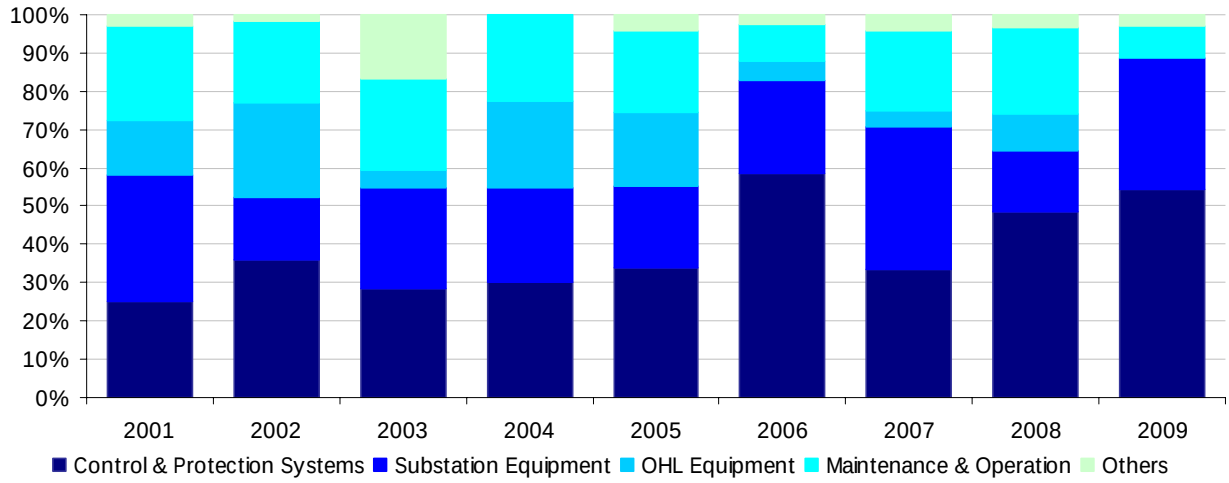


Fig. 5.8 – Quantification of faults caused by Internal Origin

Finally, the unknown causes are the ones that remain unidentified, representing on average about 7.5% of the total. Appendix D presents a more complete overview of the PTS faults during the analysis period. Table 5.3 gives an insight of how much each cause weighs in the total amount of incidents per year.

Cause		2001	2002	2003	2004	2005	2006	2007	2008	2009
Atmospheric	Lightning	28.3%	28.9%	19.5%	28.2%	3.0%	23.2%	39.1%	35.0%	30.6%
	Fog + Pollution	9.1%	23.5%	3.5%	13.1%	15.4%	2.4%	5.7%	6.6%	0.0%
	Other	0.3%	0.0%	1.6%	0.0%	0.0%	0.8%	0.0%	0.0%	5.5%
Environmental	Storks	19.5%	9.8%	19.0%	21.4%	7.0%	28.7%	29.2%	21.3%	17.4%
	Forest Fires	22.2%	15.2%	35.8%	15.1%	57.7%	20.5%	2.6%	1.6%	14.5%
	Trees	0.0%	0.5%	1.1%	0.4%	0.7%	1.2%	0.0%	0.0%	0.0%
	Other	0.7%	0.3%	0.8%	0.0%	0.0%	0.4%	0.0%	1.6%	1.3%
Internal Origin		12.1%	15.7%	11.4%	15.9%	11.7%	16.1%	12.5%	16.9%	14.9%
External		0.0%	0.0%	1.6%	1.6%	0.7%	1.2%	0.0%	2.2%	0.0%
Unknown		7.7%	6.2%	5.7%	4.4%	3.7%	5.5%	10.9%	14.8%	15.7%

Table 5.3 – Overview of fault causes in the system

In order to characterize these causes, information about the intrinsic characteristics of the Portuguese territory is needed, such as geographical, meteorological and environmental data. These causes are independent from each other and affect different areas, so they will be analysed independently. This topic will be further developed in chapters 6 and 7.

5.3.1. Storks

On the blackout described in section 2.3.1, a bird was the initial trigger and neither the only cause nor the single problem. Storks are a very frequent cause for N-1 events, affecting OHLs in the Portuguese transmission system. They are big birds, approximately 1 meter high and with 2 meters of wingspan. It is relevant to refer that storks are protected birds by the Convention of Bonn on Migratory Species,

Convention of Bern on European Wildlife and Natural Habitats and Birds Directive of the EU, because their population was in the past endangered due to pesticides and human intervention.

Nowadays, the population of storks has increased significantly. Concerning the incidents in the Portuguese transmission system, the issue is that stork excrements either pollute the insulators or affect its dielectric vicinity; also nest sticks and other substances fall and may trigger faults [41]. Reference [108] mentions that birds on transmission lines may produce a stream of defecation that results in insulator flashover and that this is a fairly widespread problem. The placement of the nest may block the natural wash made through rain, keeping the insulators polluted.

Fig. 5.9 – Stork nests in an OHL tower & Devices to prevent faults caused by storks

In order to mitigate the number of incidents caused by storks and to adapt the Portuguese transmission grid to their presence, several measures are regularly taken by REN since 1995, namely:

- Possible transfer and relocation of nests to more adequate places in the tower. This is made once a year after the bird nesting season.
- Installation of special devices to inhibit nest build-up at bad locations, to facilitate nest build-up at harmless locations and to protect insulators. Figure 5.10 presents the number of measures to control the effect of storks.

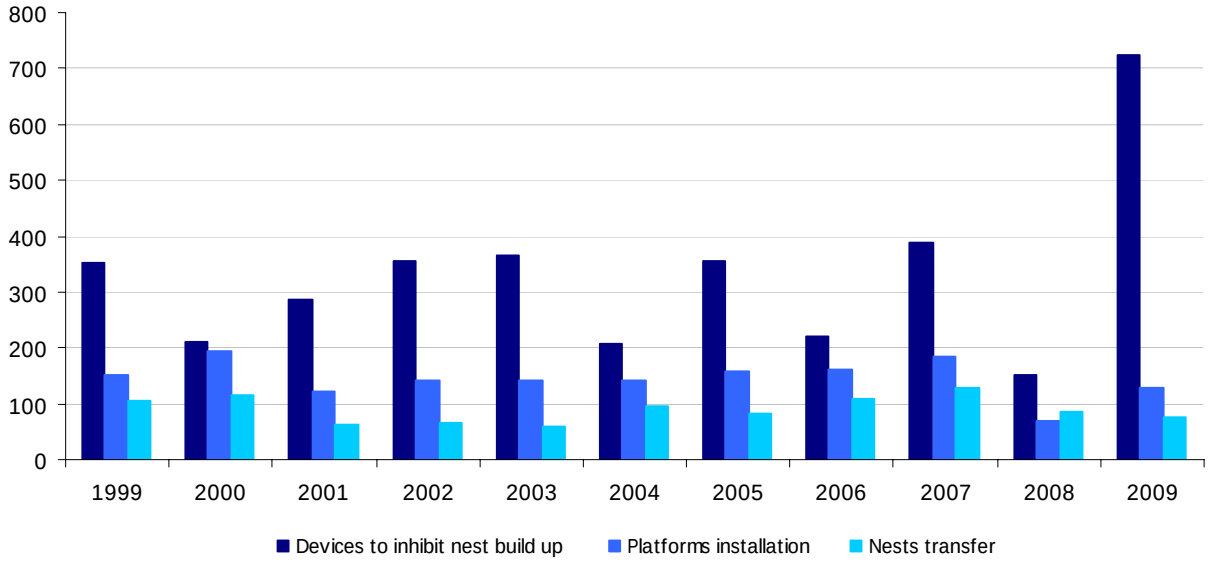


Fig. 5.10 – Number of actions/devices taken to avoid incidents caused by storks

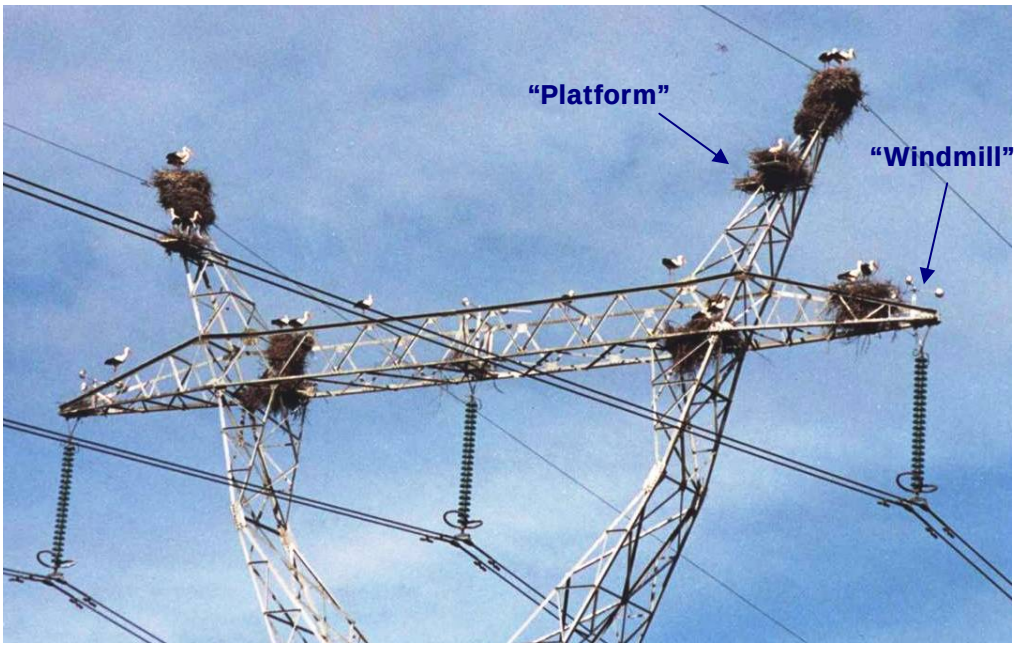


Fig. 5.11 – Installed Devices in an OHL tower

All the described measures have been taken under the permission of the National Environmental Authorities (Nature & Biodiversity Conservation Institute). In spite of the significant increase of the stork population and, as a result, of the number of nests located in OHL towers, the quality of service was not significantly affected, as shown in figure 5.12. Therefore, the applied measures can be considered successful.

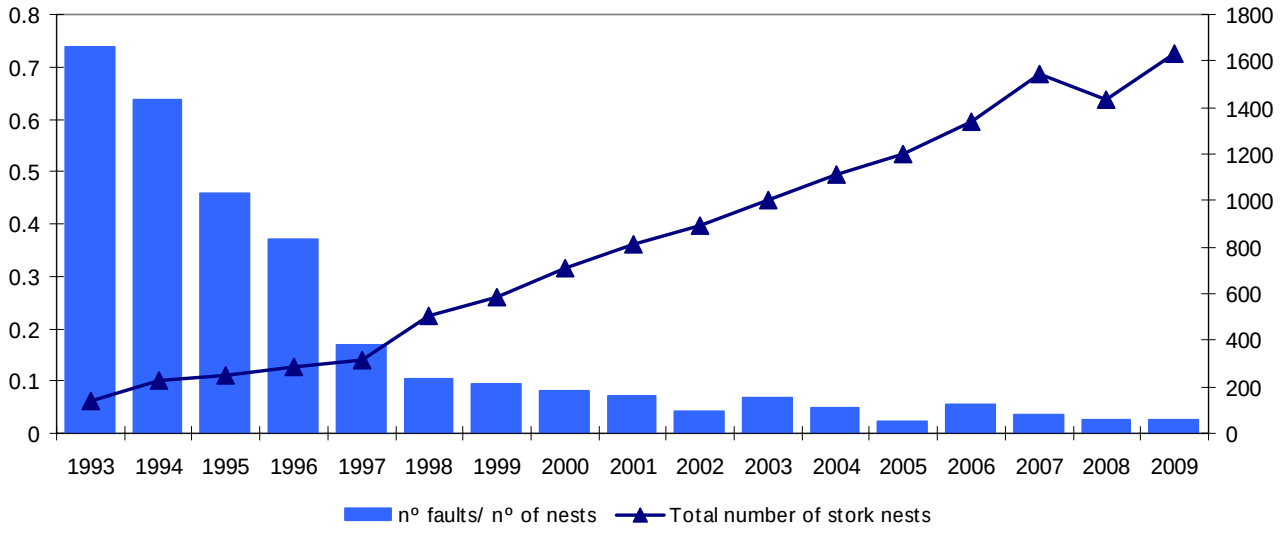


Fig. 5.12 – Comparison between the number of stork nests and the number of faults caused by storks

The regions considered risky in terms of the occurrence of incidents caused by storks are identified in Portugal's map with information about stork nests density per 100 km^2, which is presented in appendix E. With the expansion of the Portuguese transmission network, storks will also be noticeable in areas that now have new OHLs, through their faults, although since the beginning the measures to prevent incidents caused by storks have been installed in new overhead lines. The area where faults caused by storks occur is well identified, affecting a known group of OHLs.

Figure 5.13 presents the occurrence of faults caused by storks on each voltage level. The first conclusion is that the 150 kV level is more affected by this kind of events. Nevertheless, from 2001 to 2009, the evolution shows that the number of faults caused by storks is increasing in the 400 kV network.

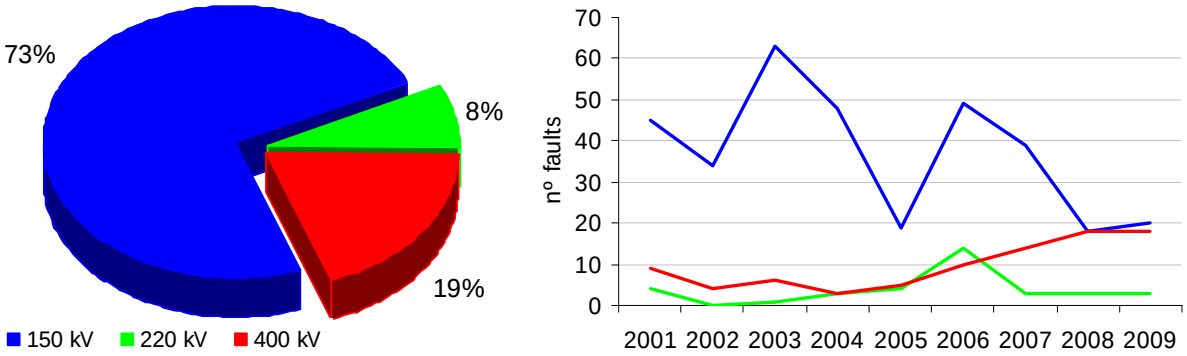


Fig. 5.13 – Percentage and number of faults caused by storks per voltage level

In 2006, there were more faults caused by storks than in the previous years, which may be explained by the reported growth in the stork's population. It is not possible to clearly distinguish a seasonal pattern, although from 2001 until 2009, the worst months were October and November and the least affected month is December, as shown in figures 5.14 and 5.15. Therefore, we would say that there are faults caused by stork during the whole year. The colour coding is the same as in figure 5.13.

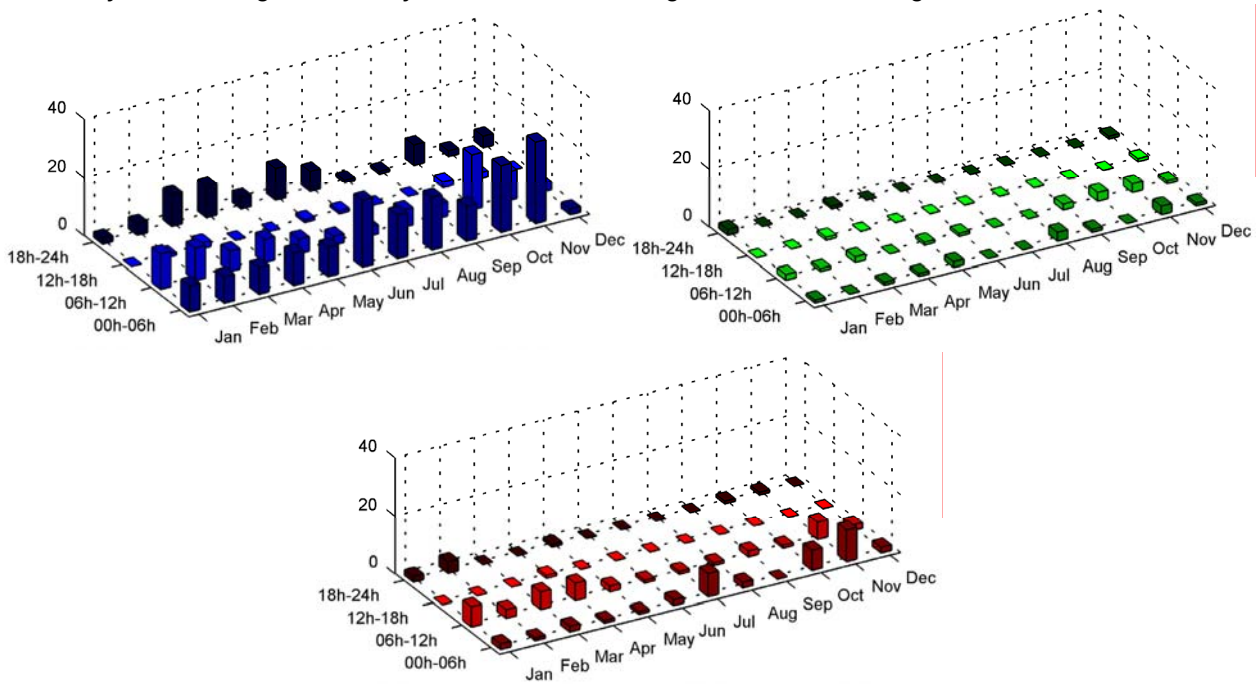


Fig. 5.14 – Faults caused by storks' distribution per month, period and voltage level

In figures 5.14 and 5.15, it is possible to observe that faults caused by storks are much more frequent during the night (approximately half occur from 0h to 6h).

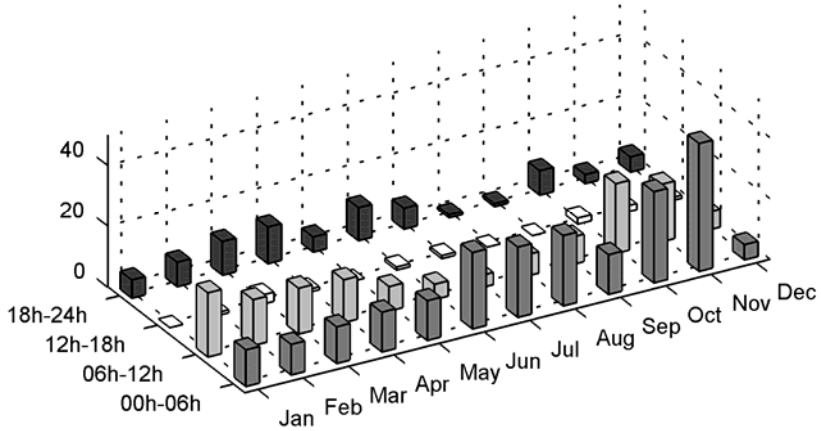


Fig. 5.15 – Total number of faults caused by storks' distribution per month per period

5.3.2. Forest fires

During summer, forest fires can be a major problem in continental Portugal, because of their frequency of occurrence and the area extension that is destroyed, causing big economical, environmental and social damage. The development of a forest fire is greatly dependent on meteorological conditions (direction and wind intensity, relative air humidity and temperature), degree of dryness and vegetable soil, terrain orography, access to the place of fire and the response time of fire-fighters to the event. Forest fires can be caused by several reasons, but the majority of the identified causes have human origin, sometimes accidental or negligent fires, sometimes criminal actions. The natural cause fires correspond to a small amount of the total [109]. Figure 5.16 present an illustration of forest fires in the Portuguese territory.

Fig. 5.16 – Forest Fires in Portugal

A human action in order to prevent forest fires is crucial and makes a significant difference to reach success. Regarding power lines, it is the Portuguese TSO responsibility to maintain the right-of-way clean within a defined area under every OHL that crosses forest, as laid down by law [110]. Figure 5.17 shows the result of this action in the field and with its implementation it is possible to identify three main benefits: the improved efficiency of the fire fighting, the reduced damage to the OHL and the lower risk of incidents caused by forest fires, improving system's security.

Fig. 5.17 – Right-of-way maintained under an OHL

Forest fires of huge proportions may affect several grid elements, in the same geographical area, such as overhead line corridors or the confluence of several elements in the neighbourhood of a substation, as shown in reference [19] and in the blackouts presented in sections 2.1.5 and 2.3.3, or by different forest fires happening at the same time.

A statistical treatment was made of forest fires and incidents' historical data. The worst years were 2003 and 2005, as it is possible to observe in the results presented in table 5.4.

Year	Nº Fires	Burned area (1000ha)	PTS faults cause by forest fires
2001	26533	112	66
2002	26488	124	59
2003	26195	426	132
2004	21870	130	38
2005	35697	338	232
2006	19929	76	52
2007	18722	17	5
2008	13832	17	3
2009	23441[a)]	83[a)]	34

a) Data updated until 15th October 2009 (last faults on 3-10-2009)

Table 5.4 – Overview of forest fires and faults [109]

In general, the Portuguese transmission grid withstood well the devastating forest fires that occurred mainly in the north and central part of the Portuguese territory. In 2005, forest fires have caused 232 short-circuits in PTS overhead lines, which represents six times more than in 2004, four and a half times more than 2006 and around seven times more than in 2009.

Figure 5.18 shows a graph which allows a clear view of the strong correlation between the amount of forest fires and the number of faults in the transmission network caused by them. The correlation factor is about 89%.

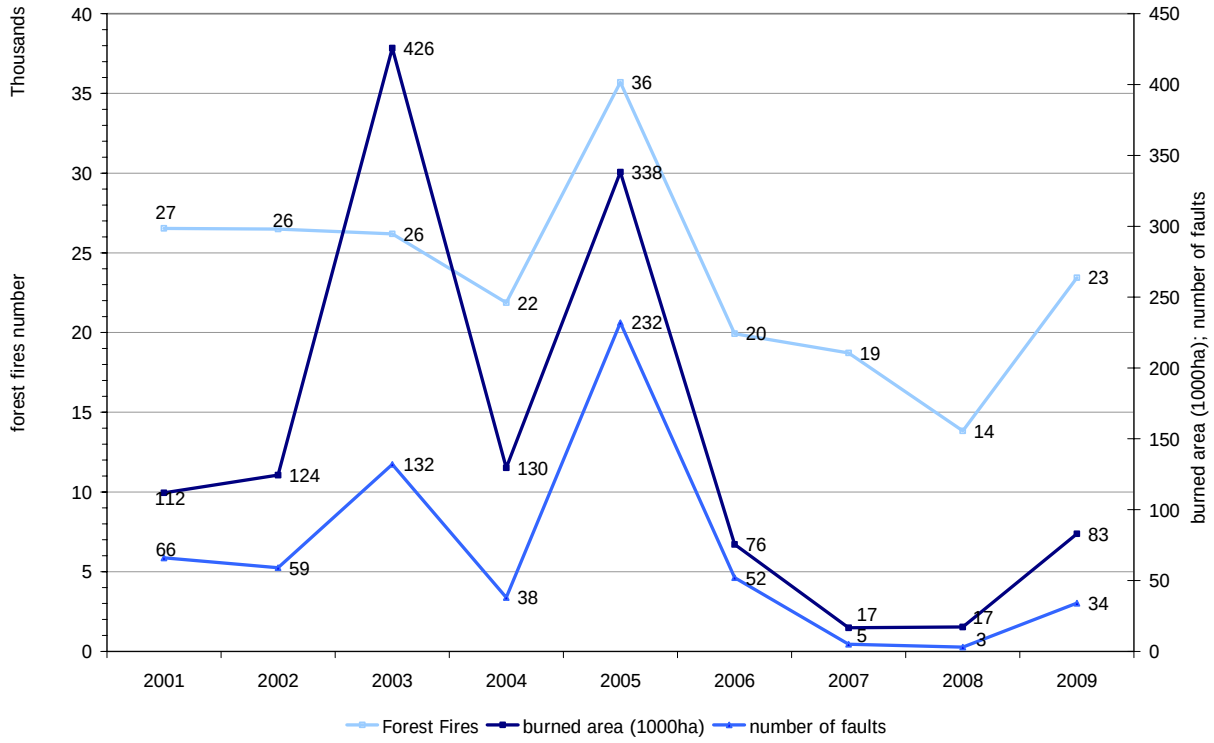


Fig. 5.18 – Yearly amount in the period from 2001 until 15-10-2009

In the most critical days in the summer of 2005, there were periods where several lines were affected by the same forest fire (in the same geographical region) or by different forest fires happening simultaneously (in different geographical regions). For short periods of time, more than three overhead lines were disconnected simultaneously, due to permanent faults or to allow the fire fighters to safely extinguish the fire. Obviously, facing this type of event, the security of a transmission system becomes more vulnerable.

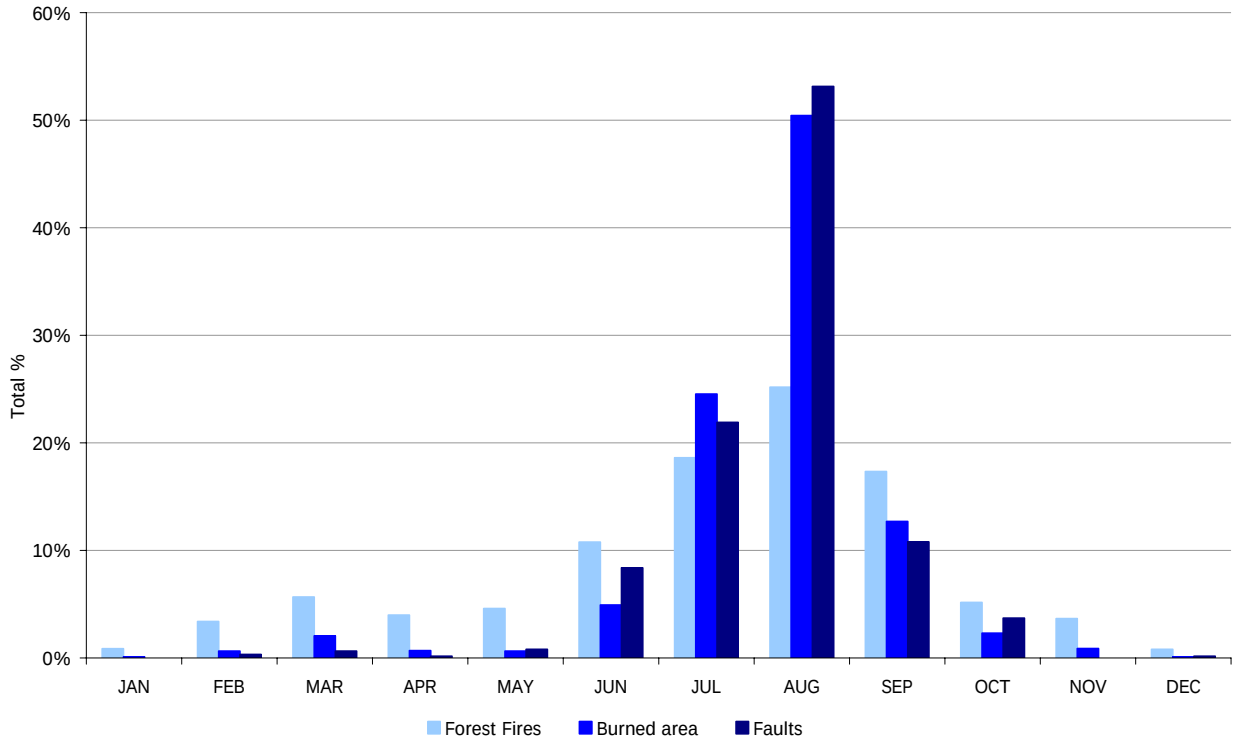


Fig. 5.19 – Month distribution in the period from 2001 until 15-10-2009

Figure 5.20 shows the occurrence of faults caused by forest fires in each voltage level. It is concluded that half of the faults affected the 220 kV network, during the period under analysis. The 220 kV has the largest OHL length in the network. The 400 kV network was more affected than the 150 kV one, although its length is smaller. The voltage level affected by forest fires is strongly dependent on the region where the forest fires actually occurred.

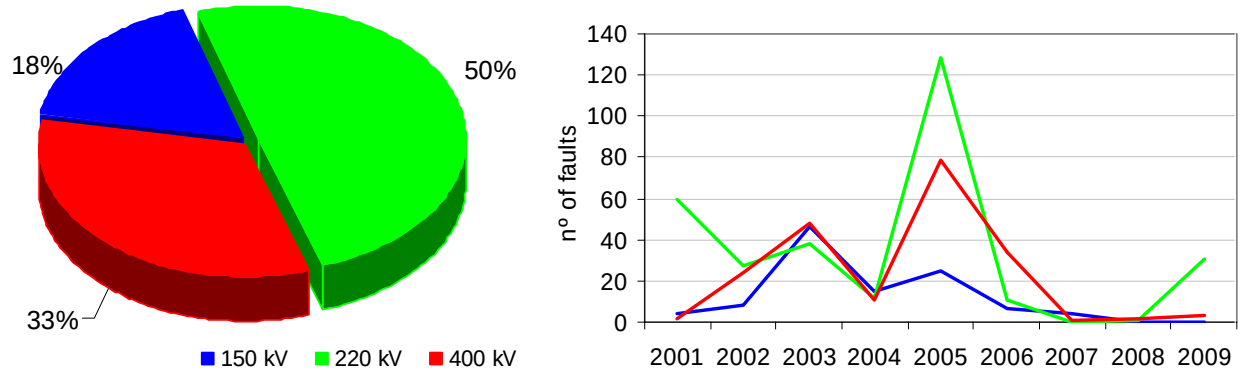


Fig. 5.20 – Percentage and number of faults caused by forest fires per voltage level

Figure 5.20 clearly illustrates the severity of 2005 in terms of forest fires, which is followed by 2003. In 2009 there was an increase in the number of faults when comparing with 2007 and 2008, although after 2006, faults caused by forest fires didn't happen in a significant amount.

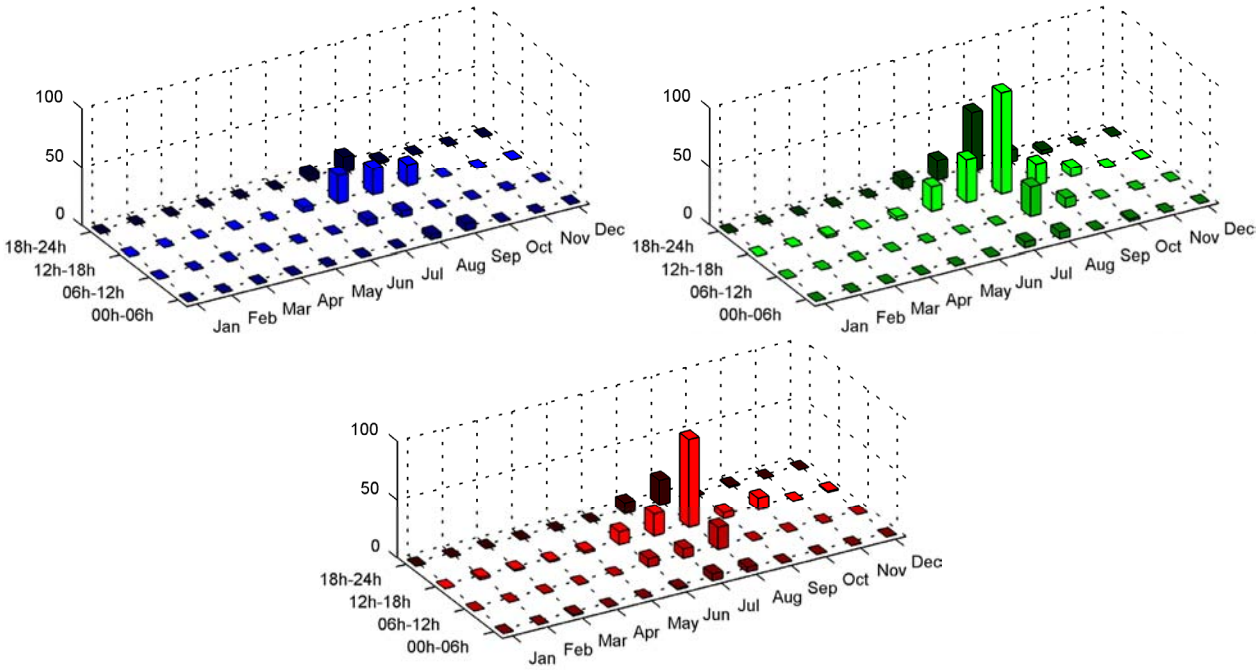


Fig. 5.21 – Faults caused by forest fires distribution per month, period and voltage level

In figures 5.21 and 5.22, it is possible to observe that forest fire season normally begins in June and ends in September and that they are much more frequent during the afternoon period. In fact, about 60% of the faults caused by forest fires occur from 12h until 18h. The colour coding is the same as in figure 5.20.

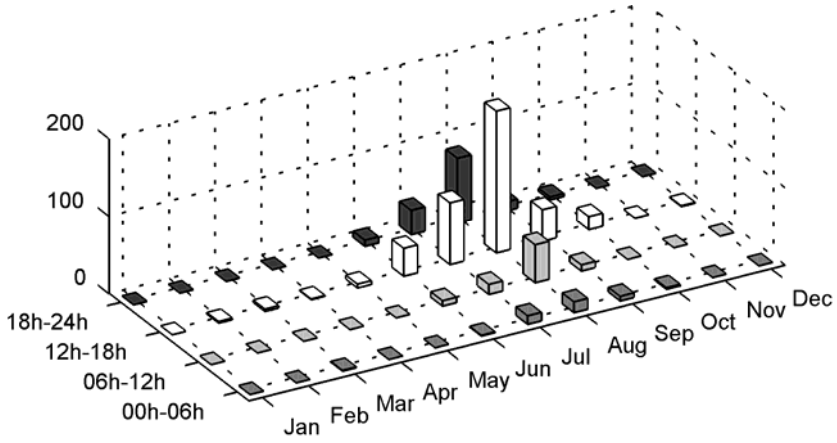


Fig. 5.22 – Total number of faults caused by forest fires distribution per month per period

The faults caused by forest fires outside the sunlight period may be the result of violent forest fires that were not controlled in due time, being active during the night, or by criminal activity in the process of starting the fire. The fire fighters' coordinating entity has a website displaying in real time the active fires in the national territory during fire season and the meteorological institute publishes daily maps with risk of fire per municipality, which are used in this research work to assess risk. This will be addressed in chapters 6 and 7.

5.3.3. Fog in combination with pollution

Incidents caused by heavy fog in polluted areas represent on average about 10% of the total. Favourable conditions for the dirt accumulation on the insulators' surface are created mainly by the lack of rain, causing extended dry periods, and some areas' characteristics, such as prevailing wind speed and direction and external sources of pollution. In the Portuguese case, pollution can be caused by winds coming from the sea being full of salt and also by quarry exploitations. When combined with fog or mist, the accumulated pollution reduces the insulation distance and creates good conditions for phase to ground short-circuits. Hence, the deterioration of the dielectric characteristics of the insulator is caused by the polluting agents that modify the electrical resistance of their surface, such as salt, dust deposit and inert conductor minerals, like carbon.

Fig. 5.23 – OHLs in a foggy environment

Faults caused by fog in combination with pollution occur normally in well identified regions. The regions considered risky in terms of the occurrence of this type of incidents are identified in Portugal's map, which defines the municipalities where mitigation measures were taken and it is presented in appendix F. The southern regions of Portugal, near the coast, including the Lisbon area, are more affected by this cause. The location of most substations near the coast puts great stress on ceramic and glass insulators. This incident's cause affects both OHLs and substations.

Reference [108] refers that contamination flashover requires the occurrence of two events: a sufficient degree of the contaminant composed of some ionic soluble salt, delivered to the insulator and deposited on its surface and a light rain or mist or fog that moistens the surface, but does not create a washing effect. Although the contaminant alone creates no problems, this mixture, contaminant and moisture, produces a conducting film such that a leakage current flows through the contamination layer.

Figure 5.24 presents the occurrence of faults caused by fog in combination with pollution on each voltage level. The faults in OHLs represent 97% and the faults in substations represent 3% of the total caused by fog combined with pollution. In 2009, there were no faults caused by fog in combination with pollution.

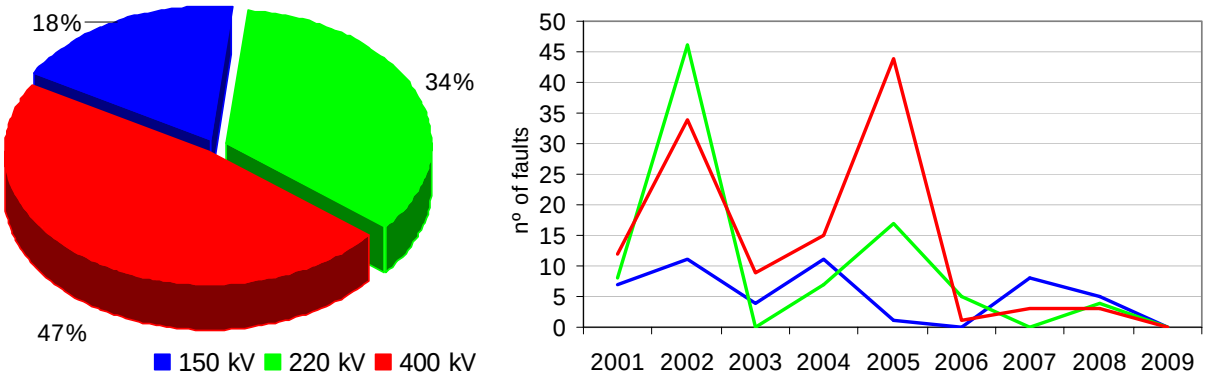


Fig. 5.24 – Percentage and number of faults caused by fog+pollution per voltage level

Inside substations, the incidents caused by fog in combination with pollution are busbar faults. From 2001 until 2009, this has caused 9 busbar faults in the 220kV and 400kV voltage level of two substations located in the Lisbon area, which seem to be more affected by this cause.

The extreme dry weather of 2002 and 2005 aided the occurrence of this type of faults, because of the lack of rain, which was not sufficient to wash naturally the insulators. In particular, 2005 was the worst year in terms of busbar faults in the PTS, as there were 5 busbar faults caused by fog in combination with pollution in REN substations. The colour coding is the same as in figure 5.24.

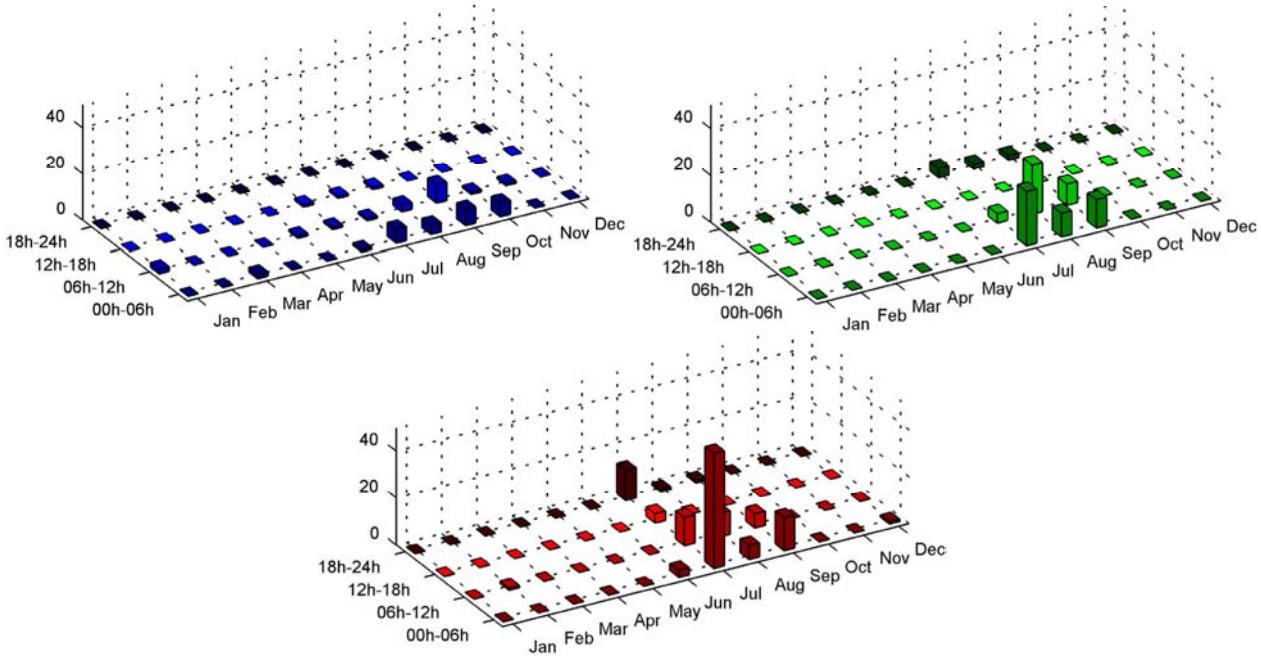


Fig. 5.25 – Faults caused by fog+pollution distribution per month, period and voltage level

Figures 5.25 and 5.26 show that incidents caused by fog in combination with pollution happen mainly during summer, especially in July, August and September. Hence, it is possible to say that it is a seasonal type of fault. The majority of faults happen from midnight to dawn (approximately 57% from 0h until 6h and 26% from 6h until 8h).

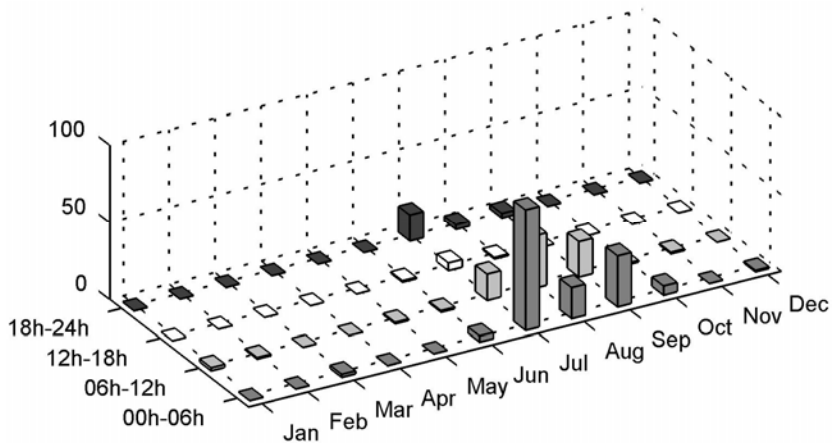


Fig. 5.26 – Total number of faults caused by fog+pollution distribution per month per period

To avoid the risk of this kind of faults, i.e. to improve the performance of the insulators, several actions are taken, such as washing the insulators with a special technique[3] (normally live working), doing manual cleaning (especially in substations), increasing the number of disks of an insulator, applying silicone coating to existing insulators and installing composite (epoxy resin) insulators.

[3] The insulators' washing can be performed on de-energized or live equipment, using de-mineralized water. Washing is usually conducted remotely by using a pressure washer, but it can be done by hand on de-energized equipment.

The Portuguese TSO systematically cleans insulators every year during the summer since the early nineties in OHLs affected by fog and pollution. Since 2004, a program was launched to install composite insulators in new OHLs and replace the existing insulators (glass and porcelain) for composite ones, in the identified critical areas of pollution with a larger concentration of faults. The control actions are illustrated in figure 5.28.

Table 5.5 presents the number of washed towers per year in each voltage level.

Voltage Level	2001	2002	2003	2004	2005	2006	2007	2008	2009
150 kV	769	641	626	632	421	379	177	346	55
220 kV	564	530	460	370	477	525	299	149	91
400 kV	285	358	383	386	378	350	134	96	102
Annual Total	1618	1529	1469	1388	1276	1254	610	591	248

Table 5.5 – Number of towers that were washed per year

Table 5.6 shows the number of installed composite insulators since 2004.

Voltage Level	2004	2005	2006	2007	2008	2009
150 kV	0	2507	1550	408	750	714[a)]
220 kV	1236	4091	270	2548	1816	171[a)]
400 kV	90	622	1597	3169	1630	54[a)]
Annual Total	1326	7220	3417	6125	4196	939[a)]

[a)] approximate values

Table 5.6 – Number of installed composite insulators

Figure 5.27 shows a clear decrease in the number of towers that are washed and also of the number of faults as a result of the installation of composite insulators, which represents the effectiveness of the applied measures. Especially, since 2006, a significant improvement in the quality of service is noticeable.

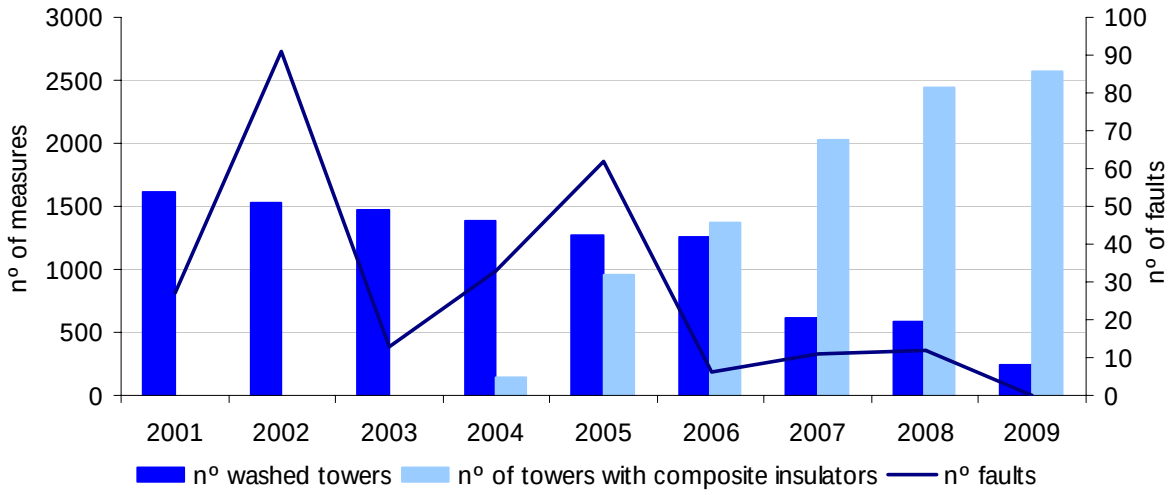


Fig. 5.27 – Overview of the taken measures in OHL

The composite insulators are made of new materials and they present advantages in price, design and pollution performance aspects. They are normally lighter and more compact; thus they can provide more creepage distance for a given axial length. It is relevant to mention that the need for insulator washing disappears with the installation of composite insulators, due to their hidrophobicity. However, this hidrophobicity may be lost under extreme or repeated service/environment stresses. The life time expectation with this kind of insulators is lower than with the glass and porcelain ones, nevertheless this is a new technology that is being installed now in the electrical transmission systems, which means that time is needed to perform a more sustained analysis [111].

Fig. 5.28 – Preventive measure taken in OHL to avoid faults caused by Fog+pollution

5.3.4. Lightning

Lightning is the incident cause that affects all transmission systems! Lightning is the transfer of significant charge between two charged objects. A lightning occurs because of a charge separation between cloud and earth or within a cloud, caused by meteorological processes (it typically occurs during thunderstorms).

After the electrical field reaches a critical level, corona occurs and leaders (conductive and often branched channels of ionized air with a strongly charged tip) are formed. Lightning electrical discharge is visible by the human eye as a flash of light and can occur from cloud-to-cloud and from cloud-to-ground.

Fig. 5.29 – Cloud-to-ground lightning [112]

The electrical discharge consists of an electrical current with an amplitude ranging from 1kA up to 400kA (registered by the detection network), approximately, with a rise time in the order of a few up to tens of microseconds. The duration of one lightning discharge can be from several tens up to several thousands of microseconds. Multiple strokes can occur shortly after each other. Whenever a lightning charge propagates to earth, it must have an “attachment point,” which is the origin of the upward stream of charge.

A lightning current induces a high voltage between the object it strikes and remote objects. Overhead lines are especially vulnerable as they are often located in exposed locations and cover large distances. An exacerbating factor is that lines are often taller than adjacent object, thereby primary targets for lightning.

For instance, when a lightning hits a ground wire, it induces a voltage between the ground wire and the phase conductors and when that voltage exceeds the insulation level, a backflash occurs, electrically connecting the phase with the ground wire. This connection causes a short-circuit in the power system and the short-circuit current maintains the ionized conducting air channel after the lightning has already disappeared. The short-circuit may be single or multi-phase.

The protection systems of the overhead line will trigger due to the fault and, consequently, open the applicable circuit breakers, clearing the fault by disconnecting the faulty line. Subsequently, in the absence of an electrical current, the air loses its conductivity, and therefore the overhead line can safely be re-energized, normally without causing a new short-circuit. The occurrence of a short-circuit immediately after reclosing the breaker indicates the permanence of the fault and damage on the equipment, causing protection systems to operate again and resulting in a forced outage. From 2001 to 2008, only 5% of the faults caused by lightning had an automatic disconnection after reclosing the breaker.

There is no absolute protection against lightning and it is considered an uncontrollable fault cause, although OHL reliability performance is dependent on adequate insulation coordination. Insulation coordination is the process of correlating equipment electrical insulation strengths with expected overvoltage stresses so as to result in an acceptable risk of failure while considering economics and operating criteria [113].

Reference [108] also presents several definitions for insulation coordination. For this work, it seemed adequate to combine some of them. Hence, insulation coordination is defined here as the selection of the insulation strength consistent with the expected overvoltages to obtain an acceptable risk of failure, reducing the probability of equipment damage and taking into account the service environment and the characteristics of the available protective devices. The continuity of service impact caused by failures will also be mitigated.

Concerning overhead lines, the tower geometry, the soil resistivity, the tower footing resistance, the number of ground wires and the insulation level are aspects that will influence the performance of the grid element in case of lightning. This will be further developed in chapter 7.

About 99% of the faults caused by lightning affect OHLs, and the other 1% affects mainly transformers. There was only one event that has affected a 400 kV busbar in 2007. Figure 5.30 presents the occurrence of faults caused by lightning on each voltage level. Through the graph, it is possible to observe that the lower the voltage level, the more affected is the network by this natural phenomenon, which is explained by its lower insulation level.

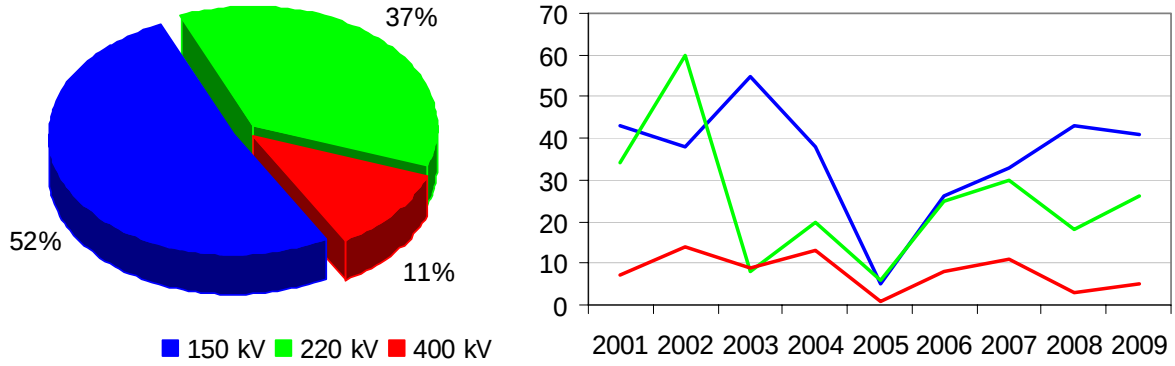


Fig. 5.30 – Percentage and number of faults caused by lightning per voltage level

It is noticeable that in 2005, the number of lightning strokes was considerably smaller than in the other years under analysis, decreasing the number of faults caused by lightning in the transmission system, as shown in table 5.7. The number of lightning flashes was obtained from the data base of the lightning monitoring system, which will be presented in chapter 6.

Year	2003	2004	2005	2006	2007	2008	2009
Nº of flashes	58176	69809	40481	78238	130893	50983	63861

Table 5.7 – Number of lightning flashes in Portugal

This system has been recording data since June 2002, thus it was possible to conclude, from 2003 to 2009, that only around 0.08% of the cloud-to-ground lightning occurring inside the Portuguese geographical boundary caused OHL faults. Figure 5.31 shows the number of lightning flashes and the number of faults caused by lightning per month from 2003 to 2009.

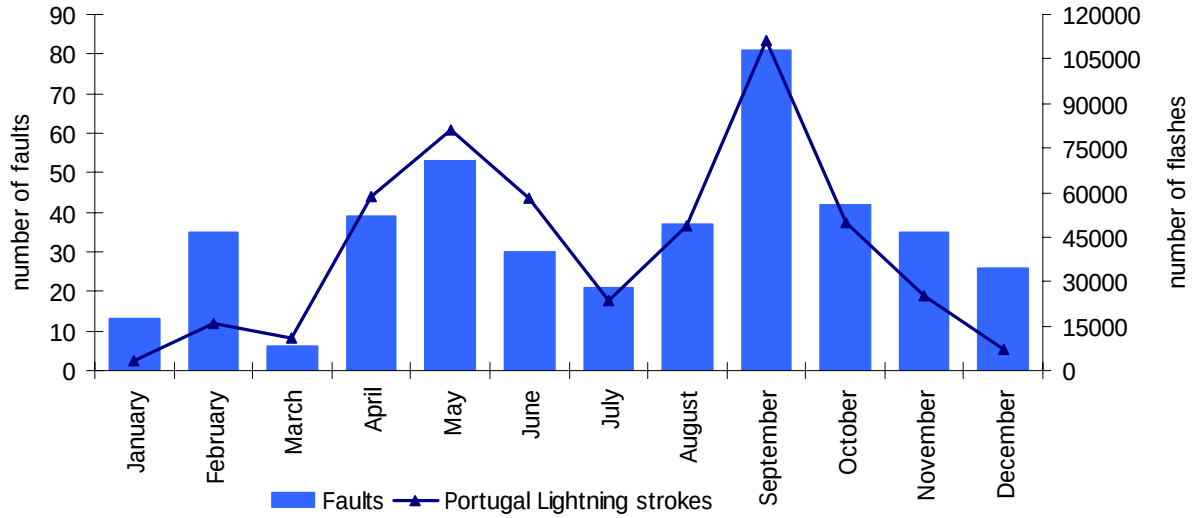


Fig. 5.31 – Number of lightning flashes and of faults caused by lightning from 2003 to 2009

Analysing the cloud-to-ground lightning flashes that have struck inside the Portuguese territory, it can be seen that around 82% occur between 12h and 24h. In figures 5.32 and 5.33, it is possible to observe that faults caused by lightning occur during the whole year and mainly in the afternoon and beginning of the evening period (66% of the faults occurs from 12h until 24h), although the night to dawn also has a significant amount of faults. The colour coding is the same as in figure 5.30.

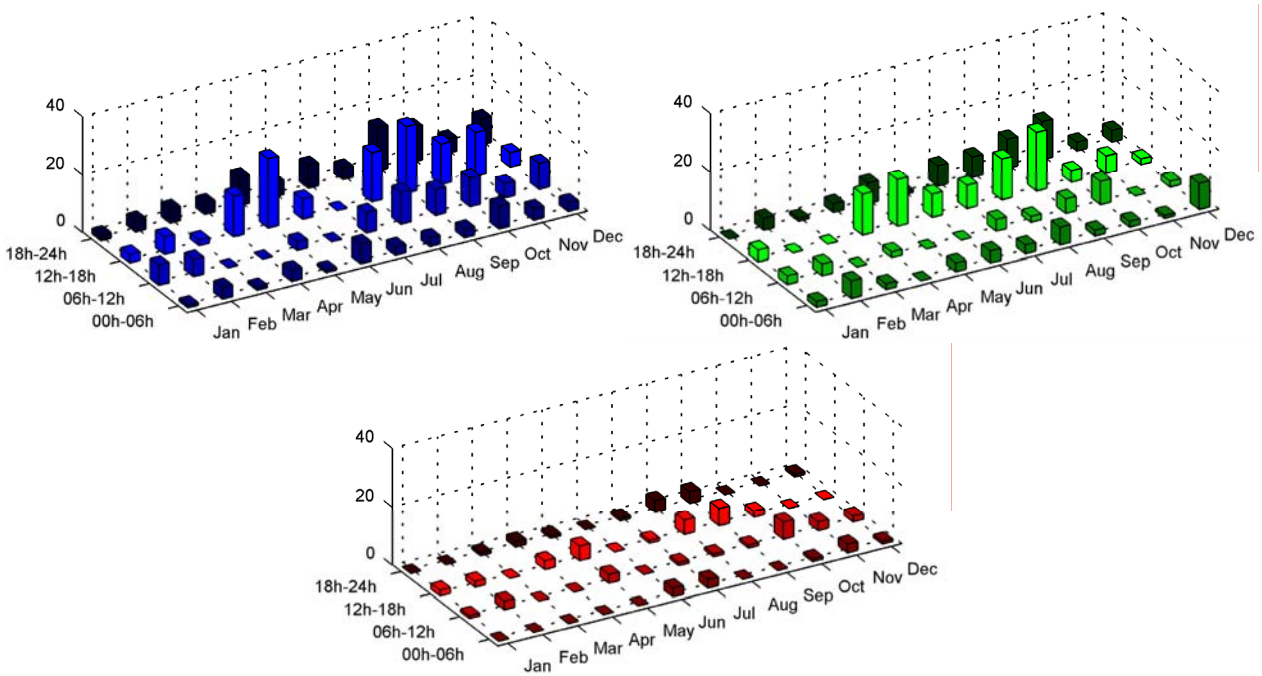


Fig. 5.32 – Faults caused by lightning distribution per month, period and voltage level

In the Portuguese transmission system common cause faults caused by lightning represent about 20% from the total and the length of OHL sharing the same tower also represents on average about 20% of the OHL total length.

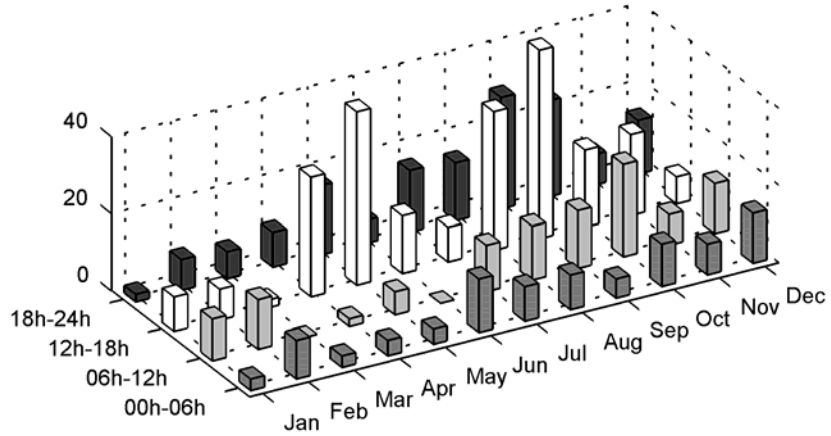


Fig. 5.33 – Total number of faults caused by lightning distribution per month per period

5.3.5. Other causes

There are other causes beyond the presented main ones, which can affect significantly the quality of service in a transmission grid. In this section, the incident causes Maintenance and Operation, Protection System, Obstacles, Ice and Extreme Wind are addressed. Their percentage in the total amount of faults is shown in figure 5.7.

5.3.5.1. Maintenance and operation

Every time when there are people involved in a specific task, there is a chance for human errors. Faults caused by human errors are more likely to happen when the work activity is high. Human errors can be divided in two specific areas: during manoeuvres that are related to operation (local or remote) and during works (maintenance, assembling actions and tests). An example of an incident caused by a human error is the incident of 4th November 2006, described in section 2.2.3.

Analysing all faults since 2001, it is possible to affirm that human errors are not a significant cause in the Portuguese transmission grid faults in terms of amount of events (71 out of 2572 faults), but they are certainly a crucial concern that requires continuous improvement. Figure 5.34 shows the percentage of faults caused by human errors in the Portuguese transmission system from 2001 to 2009.

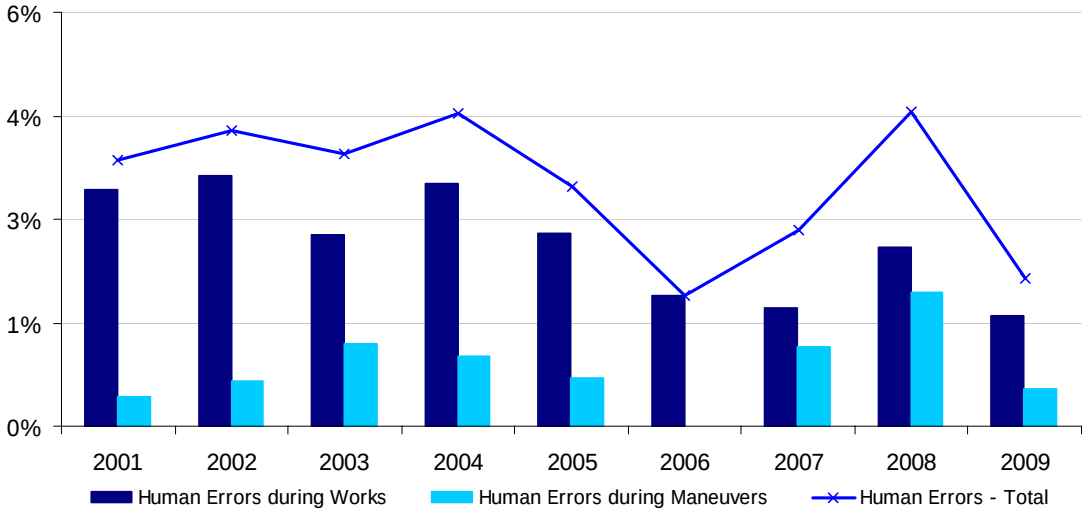


Fig. 5.34 – Percentage of incidents caused by Human Errors in the PTS

From the 71 faults caused by human errors, 68 occurred in bays, of which 6 caused busbars faults, and the other 3 occurred in OHLs, therefore faults caused by human errors will be considered in circuit-ends and in busbars for probability calculation, as presented further in section 7.8. Only 14% of these faults involved a short-circuit.

Human errors are considered neither force majeure nor uncontrollable causes; they are the best example of the need to improve. Many lessons are drawn every time that a human error occurs, therefore additional efforts in order to improve operational procedures and system performance are made. The high level of investment in the Portuguese transmission system is directly proportional to the level of activity (amount of works) in the field and with more activity there are more chances for error. It is relevant to mention that incidents caused by human error usually have severe consequences.

As shown in figures 5.35 and 5.36, faults caused by Human Errors mainly happen during substation's normal working hours (94% of the faults from 6h to 18h). The colour coding is the same as in figure 5.30.

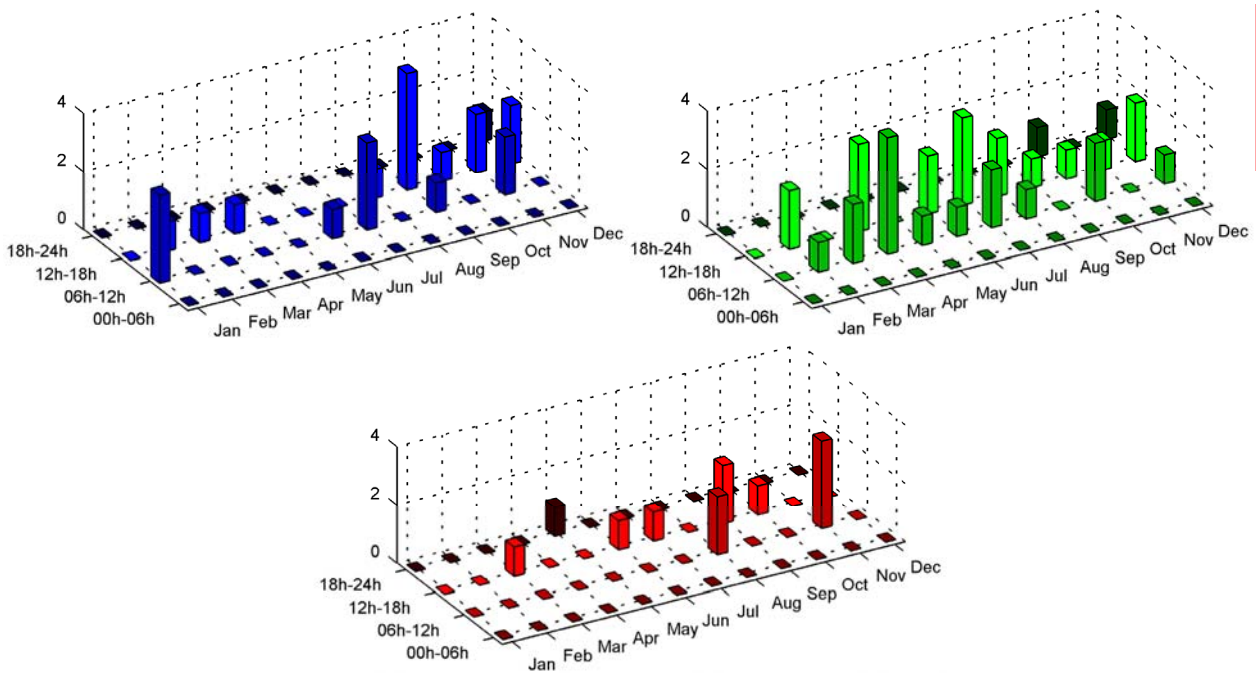


Fig. 5.35 – Faults caused by Human Errors distribution per month, period and voltage level

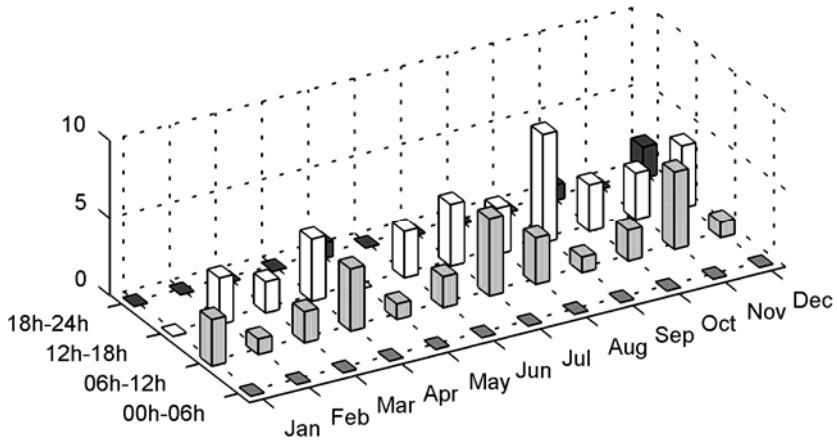


Fig. 5.36 – Total number of faults caused by Human Errors distribution per month per period

5.3.5.2. Protection systems

The correct performance of protection systems is crucial to avoid severe disturbances. Their correct operation with an adequate clearing time is needed to keep the power system secure. Therefore, all grid elements are equipped with protection systems in order to promptly and effectively disconnect any faulty element in a selective manner. The protection system monitors continuously the protected grid element and, when facing a fault, isolates selectively the faulted element as quickly as possible, minimizing consequences and damage for the power system. The most important characteristics of protection systems were defined in section 3.4.

There are mainly two incident types caused by protection systems. First, if the incident is caused by damage of the protection system, the disconnected grid element is considered origin and there is no short-circuit current related to the event. Second, if the incident is caused by lack of selectivity or coordination of a protection system while sensing the short-circuit current on another grid element, the disconnected grid element is considered affected, because the forced outage was triggered by an external fault. There are many reasons for incorrect operation of a protection system, such as damage on the system, incorrect parameters, lack of coordination or selectivity, among others, but the final result is always to remove a grid element from service that would stay connected if everything had worked well.

In order to understand what happened in the Portuguese transmission system since 2001, an analysis of the forced outages caused solely by incorrect operation of protection systems is made. Figure 5.37 is entirely based on incidents data base (GestInc), considering the disconnected grid elements by incorrect operation of protection system over all disconnected grid elements in the EHV grid. The faults caused by protection system misoperation represent around 7% of the total number of faults, including origin and affected element. Considering only origin elements, they represent approximately 3%.

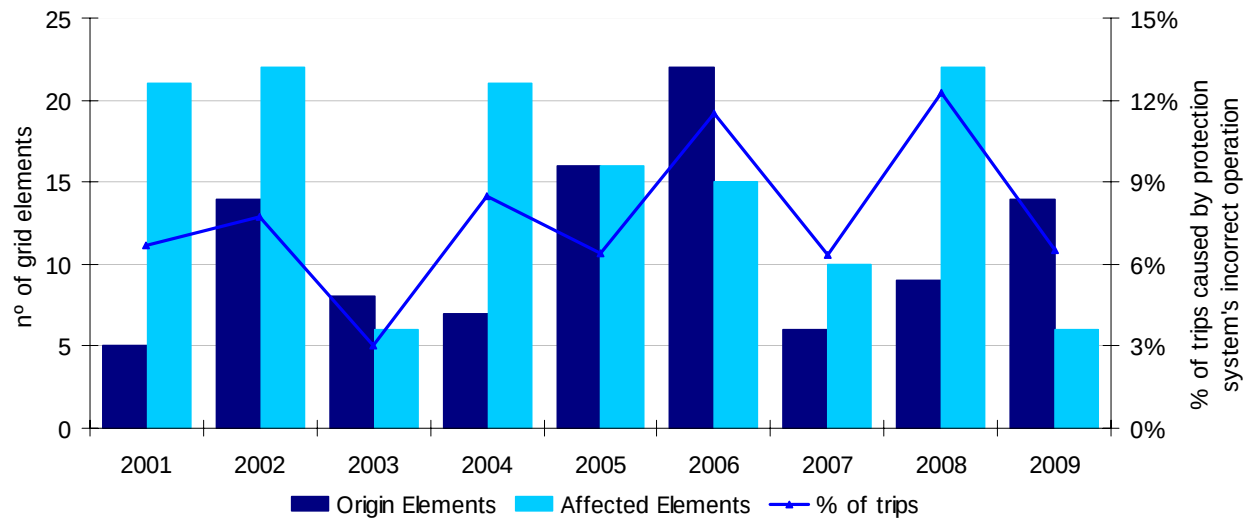


Fig. 5.37 – Origin and affected elements disconnected by protection system's incorrect operation

Figure 5.38 resents the protection system's performance in terms of:

– $\text{Reliability} = \dfrac{n^o\ of\ correct\ operations}{n^o\ of\ correct\ operations + n^o\ of\ incorrect\ operations} \times 100\,(\%)$,

where $n^o\ of\ incorrect\ operations = FO + UO + NS$

$FO = failure\ to\ operate$

$UO = untimely\ operation\ or\ inadvertent\ tripping$

$NS = non - selective\ operation$

– $\text{Security} = \frac{n^o\ of\ correct\ operations}{n^o\ of\ correct\ operations + UO + NS} \times 100\,(\%)$

– $\text{Dependability} = \frac{n^o\ of\ correct\ operations}{n^o\ of\ correct\ operations + FO} \times 100\,(\%)$

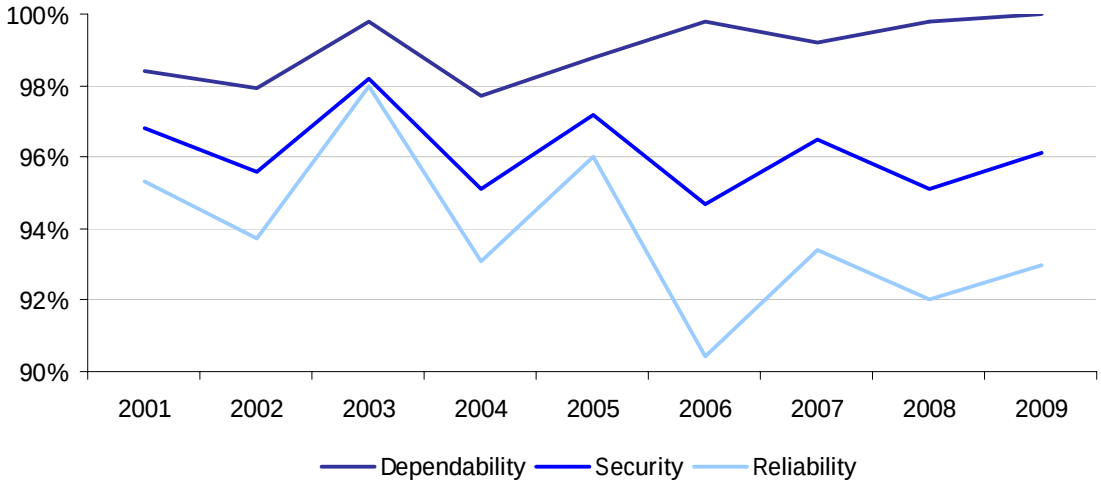


Fig. 5.38 – Protection System's performance

As it was mentioned in section 3.4, the compromise between dependability and security tends to put dependability first. Reliability in this context measures the ability of the protection system to not fail, to not act without selectivity and to not act untimely. Another crucial issue related with protection systems performance is their operating time, because longer short-circuits may have more severe consequences in terms of system security, such as sudden loss of generating units.

Figure 5.39 shows that a protection system's incorrect operation can occur at any moment.

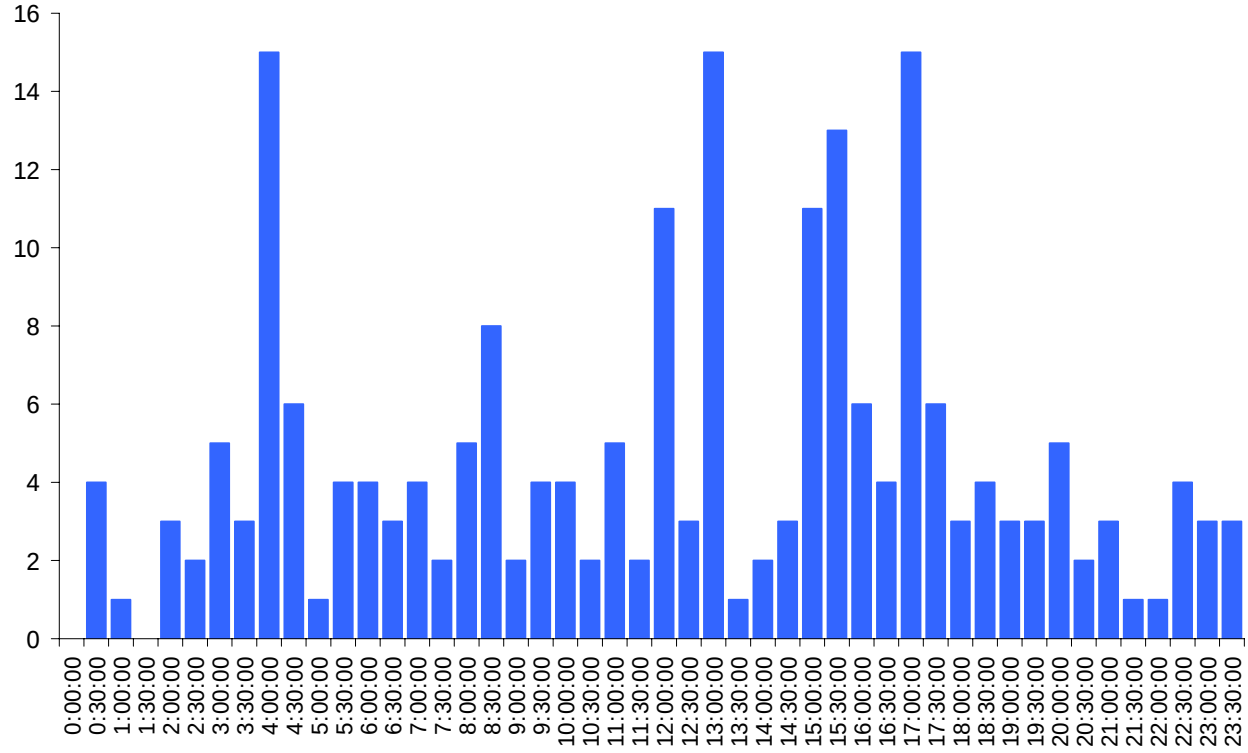


Fig. 5.39 – Hour distribution of faults caused by Protection System Incorrect Operation

Figure 5.40 presents the average operating time of protection systems in the Portuguese transmission grid.

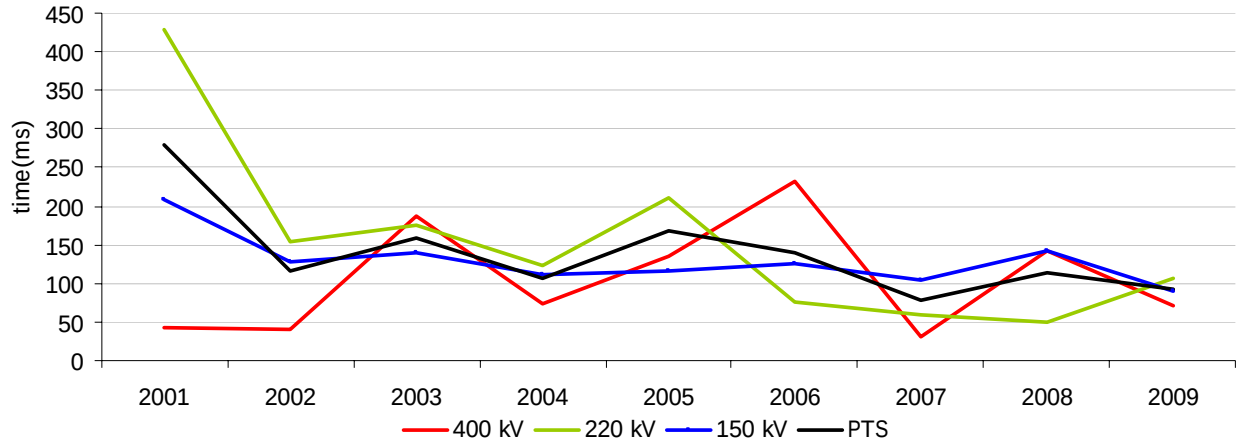


Fig. 5.40 – Protection systems operating average time per voltage level

Through the cumulative probability functions of the protection systems' operating time it was possible to build table 5.8 [114-117].

Year	2005	2006	2007	2008	2009
Probability (t<150ms)	86.3%	88%	90.6%	91.6%	96.6%

Table 5.8 – Probability of operating time less than 150ms

Concerning OHLs, the protection system is composed of two independent systems, having normally distance protection as the main function. Since 2004, REN started a systematic implementation of line differential protection functions, which have the advantage of being a highly selective unit protection and faster when compared to the distance functions. Teleprotection and communication failures between circuit-ends (bays) are greatly responsible for longer clearing times when the distance function operates. Hence, in case of distance relay operation it is important to analyse the trips in 2nd or 3rd zone and how many of those were caused by Teleprotection failure. Figure 5.41 shows the percentage of faults cleared in 2nd or 3rd zone considering all the EHV faults (including all grid elements), the number of faults cleared in 2nd or 3rd zone of the distance relay and the number of faults where teleprotection failure occurred. On average, the faults cleared in 2nd or 3rd zone of the distance relay represent around 5% of the total number of EHV faults from 2004 until 2009. In 2005, the exceptional amount of faults caused by forest fires, which are normally more resistive short-circuits, explain the increase of faults cleared in 2nd and 3rd zone.

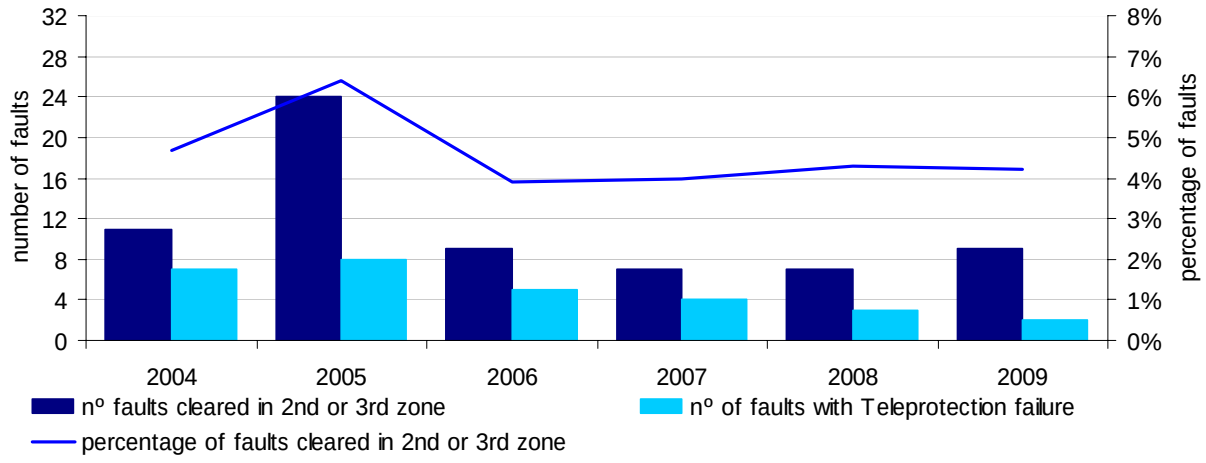


Fig. 5.41 – Protection System's performance

5.3.5.3. Obstacles (vegetation)

The potential for a short circuit caused by an electric arc between a line and an object on the ground, such as a tree, or possibly by direct contact with a grounded object, is another frequent cause that appeared in the blackouts described in chapter 2. The high loading levels of transmission OHLs may result in overheating of conductors, which causes them to sag, increasing the chances of a flashover with a tree.

Analysing all incidents since 2001, it is possible to state that trees are not a significant cause of faults in the Portuguese transmission grid. Faults caused by trees represent less than one per cent (0.5%) of the total amount. After analysing the faults caused by trees, it is possible to conclude that they are mainly single-phase (phase to ground) and permanent faults, because what is causing the fault normally does not disappear after the short circuit.

In order to prevent faults caused by obstacles, the Portuguese TSO is applying two main preventive measures. As already mentioned in the section 5.3.2, REN is responsible for maintaining the right-of-way clean within a defined area under every OHL that crosses forest, which is regulated by law (DL n. º 124/2006 from June, 28th). With this first measure, the occurrence of faults caused by trees in the PTS will be even less likely. The second measure is to use laser technology, flying over each OHL right-of-way, aiming to calculate the distance between the OHL and the obstacles which are beneath the conductors.

5.3.5.4. Ice

Ice storms are a cause for major disturbances in many northern countries. This extreme weather condition leads to extensive damage and long periods of power outage. Reference [118] presents the consequences on the German transmission system after facing an ice storm in November 2005. About 80 towers were broken and 200 thousand people were affected by the blackout. In this ice storm, Belgium and the Netherlands were also affected. Reference [119] mentions another ice storm that hit eastern Canada and North-eastern United States in 1998, where more than 1.4 million households were without electricity.

Fig. 5.42 – Damage in Germany [118]

The Portuguese transmission system never had to face such an event. Up to now, ice only has caused grid disturbances in extreme winter, in high lands and in lower voltage levels (U< 150kV). In EHV overhead lines, it affects mainly the ground wires. In this work this cause is not taken into account.

5.3.5.5. Extreme wind conditions

Wind speeds above approximately 160 km per hour, as specified in the applicable standard EN 50341-1:2001 [120], regarding construction characteristics, is a concern to the Portuguese TSO, because it can cause severe damage to OHL pylons. On December 23rd 2009 at dawn, Portugal faced such a severe event, as described in section 2.3.4, which was similar to what happened in France in 1999, also presented in section 2.2.1.

Figure 5.43 shows an example of the destruction caused by strong wind. This event justifies the introduction of wind speed measurements in the online risk assessment. Combining the synergies with wind power forecast, the Portuguese TSO is receiving real-time measurements of wind provided by the wind farms connected to the transmission network.This data will be used in the near future for risk assessment in real time. However, it was not possible to do historical data analysis with wind speed measurements, because their availability is quite recent. Therefore in this thesis this parameter is not taken into account.

Fig. 5.43 – Destroyed pylons on the 23rd December 2009

5.4. Number of OHL faults per length

The number of faults per km (or per 100 km) is a widely used indicator. Figure 5.44 presents the number of faults per km, including all the incident causes, in the Portuguese transmission network for each voltage level. To calculate this yearly indicator, equation (5.1) was used.

$$Iq_{ij} = \frac{n^o\ of\ \ faults_{ij}}{C_{ij}} \qquad (5.1)$$

where i is the year, j is the voltage level and C_{ij} is the OHL total length affected in the ith year and jth voltage level.

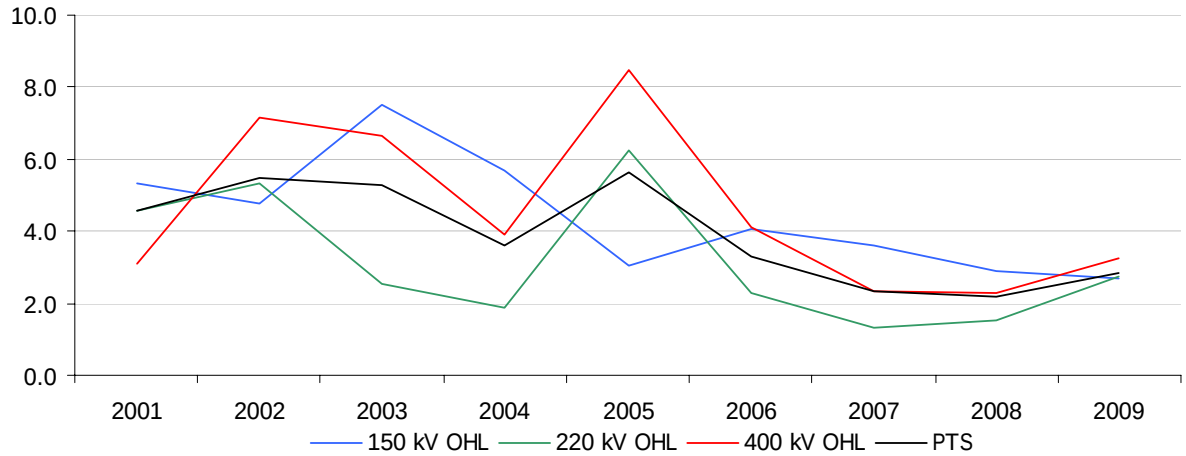


Fig. 5.44 – Number of faults in OHL per 100km (including all the causes)

The total number of circuit kilometres varies every year and in the 8 last years the exposed length has increased. The average number of faults per km per voltage level in the period under analysis is presented on table 5.9.

Element type	Average number of faults per 100 km
150 kV OHL	4.4
220 kV OHL	3.2
400 kV OHL	4.6
PTS OHL	3.9

Table 5.9 – Average number of faults per 100km per voltage level

The number of faults per 100 km lacks accuracy, because for each cause it takes into account the total length of line per voltage level, while some causes only affect well defined regions (normally identified per municipality). Concerning some causes, such as storks and fog combined with pollution, the total length of OHL affected will be much smaller than the total length of line per voltage level. Due to this, a matrix with data per OHL tower, identifying which OHL segment is exposed to which risk, was built, containing the required information for analysis. This will be further developed in chapters 6 and 7.

The results presented in figure 5.44 may be different than the ones published in the yearly REN's quality of service report, because in this work no fault aggregation[4] was considered, contrary to what is done by the TSO when classifying and recording incident data.

5.5. Busbar faults

The busbar faults represent about 1.0% of the Portuguese transmission incidents, in the EHV voltage level, from 2001 until 2009. Although this type of fault is much less frequent than OHL faults, they are usually permanent faults with more severe consequences. Most of the faults occur because of fog combined with pollution and equipment damage.

Cause	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**Total**
Lightning							1			1
Fog associated with Pollution		3		1	5					9
Internal Origin: Maintenance and operation		2	2		1			1		6
Internal Origin: Equipment			2	1	1	1	2		2	9
Internal Origin: Systems						1				1
Environmental - Others	1									1
Total	1	5	4	2	7	2	3	1	2	27

Table 5.10 – Number of busbar incidents in the PTS

In order to clear busbar faults in due time, the busbar differential protection (BDP) is extremely relevant. On general terms, considering the classical substation topology (see section 4.4), the busbar protection only opens the bus coupler plus the circuit breakers connected to the faulty busbar, "saving" the other busbar grid element, i.e., saving half of substation's voltage level normally without supply interruption. The availability decreases during works that remove a busbar from service or do not allow a balanced distribution of the grid elements between the 2 busbars. With the absence of a busbar differential protection, when facing a fault, all the protection systems of the connected OHLs will operate in the opposite circuit-ends (normally in second zone of the distance protection relay), disconnecting the whole voltage level and also what is supplied from it.

[4] For incidents caused by fog in combination with pollution or forest fires occurring inside a time period of 10 minutes, being the cause identified as exactly the same for all the faults, they will be aggregated in the same incident, representing only one fault in OHL per km index for the Portuguese transmission system.

Table 5.10 shows that, on average, there were 3 busbar faults per year in the Portuguese transmission system, when considering the period under analysis. The majority of REN substations have busbar differential protection and from the 27 busbar faults, the busbar differential protection cleared 24 faults, 3 were cleared by the opposite circuit-ends and 4 had supply interruption. As it was already mentioned, this analysis only considers EHV busbars.

5.6. Incidents involving the loss of an EHV level

Due to the non-negligible number of incidents with at least the total loss of an EHV level inside a substation, an evaluation of these incidents sub-set was performed with the following criteria: all incidents that caused zero voltage at an EHV level were considered; all cases of single feeder were excluded, because an N-1 outage provokes zero voltage.

Table 5.11 shows the number of incidents with total loss of an EHV level in the PTS, per year, during the analysis period, where 12 are independent multiple contingencies (with only one cause) and 8 are dependent contingencies (normally combining two or more causes).

	2001	2002	2003	2004	2005	2006	2007	2008	2009	Total
150 kV	1		3		1			1	2	8
220 kV	1	3		1	2					7
400 kV	1	2	1				1			5
Total	3	5	4	1	3	0	1	1	2	20

Table 5.11 – Number of incidents with total loss of an EHV level in the PTS

The incidents that have caused the loss of an EHV level represent less than 1% of the total number of faults.

5.7. Contingencies general statistics

Through historical data, it is possible to identify which disturbances affect simultaneously several grid elements. Hence, the likelihood of such contingencies (N-k, with k>1) must be taken into consideration. In order to understand how many grid elements are out of service simultaneously, from 2001 until 2009, a global analysis of the data was performed. Thus, we have made a detailed analysis of all the forced outages, considering each grid element independently. The criteria for the analysis were the following:

1. Consider all grid elements that go out of service automatically (by protection systems or automatic devices) with the exception of the grid elements tripped by zero voltage functions, after a blackout situation. To determine the value of k, all grid elements simultaneously out of service, including origin and affected element, were considered.
2. Only the EHV grid elements were considered, including lines, transformers and autotransformers.
3. If only one circuit-end of the grid element trips and it will not fulfil the task of transmitting power, it was also considered.
4. In the busbar faults and breaker failure situations, all the involved elements that are in accordance with criterion 1) were considered.
5. The assumption is made that if the grid element is still out of service after one hour, from that moment this element will not be considered in the analysis. It is assumed that in a time period shorter than one hour control room operators are normally able to restore N-1 security criteria, independently of the disturbance dimension and extent of the damage.

Table 5.12 presents the number of contingencies in each N-k group.

Contingency Type (N-K)										
k	1	2	3	4	5	6	7	8	9	>9
N-K	2080	283	44	20	6	4	0	3	0	3

Table 5.12 – Number of contingencies in each N-k group

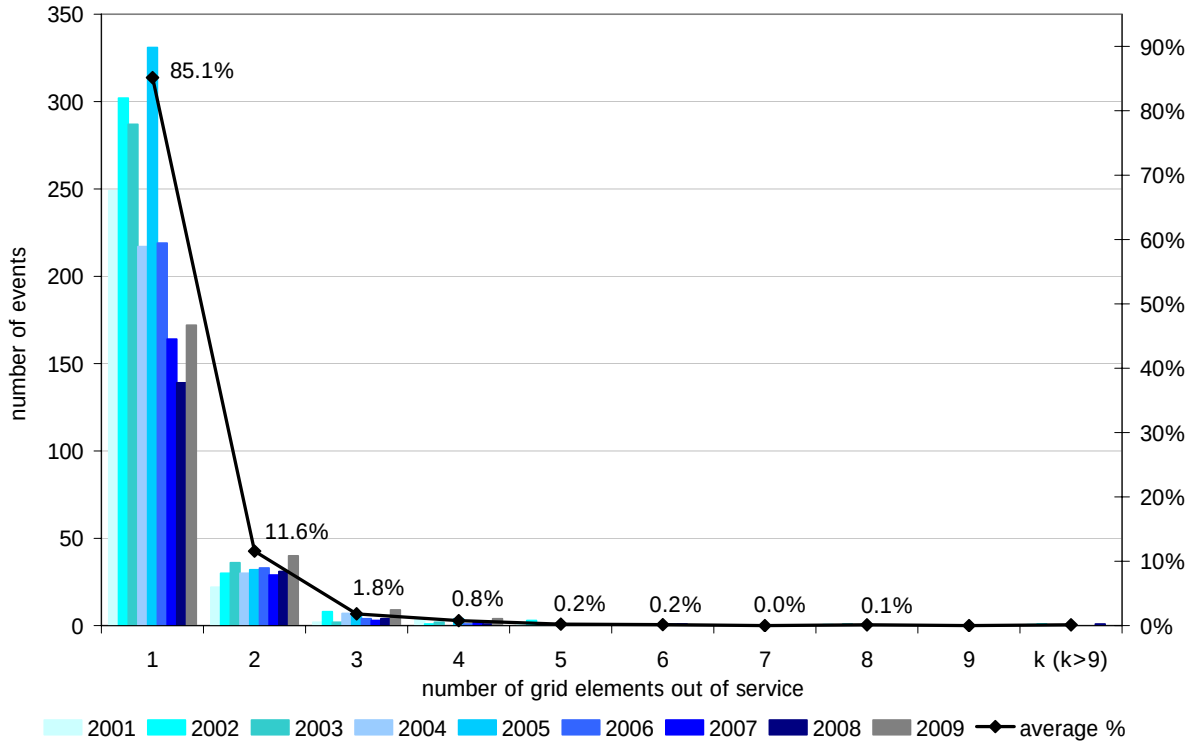


Fig. 5.45 – N-k characterization for the PTS incidents

As presented in figure 5.45, N-1 and N-2 contingencies are dominant in the Portuguese transmission grid, therefore they cannot be considered as rare events. The consideration of N-k where k>2 is mainly relevant in the forest fire season and when considering busbar faults. These situations are included in the contingency lists presented in section 4.5.2.1.

5.7.1. Independent and dependent contingencies

The definition of independent and dependent contingencies was presented in section 3.2. Faults are mainly independent contingencies, but dependent contingencies also occur. Table 5.13 presents the type of faults distribution in the Portuguese transmission system from 2001 to 2009.

Type of contingency	2001	2002	2003	2004	2005	2006	2007	2008	2009	Total
Independent	249	303	288	222	334	222	170	140	178	2106
Dependent	32	42	42	33	40	36	29	36	47	337
Total	281	345	330	255	374	258	199	176	225	2443

Table 5.13 – Faults in the PTS per type of contingency

From the 337 dependent contingencies (about 14% of the total), 155 are common cause, which represents about 46%. The common cause faults affect normally OHLs, which share the same towers during the whole or part of their path, mainly for faults caused by lightning. The extreme wind condition that occurred on the 23rd of December 2009 has disconnected simultaneously two double circuit overhead lines. These faults are also common cause. Table 5.14 presents the dependent contingencies distribution.

Type of dependency	2001	2002	2003	2004	2005	2006	2007	2008	2009	Total
Common cause	16	20	27	13	16	15	11	19	18	155
Different causes	14	17	6	13	10	8	8	11	5	92
Functional dependence	2	5	9	7	14	13	10	6	24	90

Table 5.14 – Dependent contingencies in the PTS

The increase of the functional dependence of faults is caused by new substations which are in the beginning temporarily connected through a single feeder. In case of a fault in the only OHL connected to a new substation, all equipment, such as busbars and transformers, will be disconnected. Busbar faults also belong in this category.

After common cause faults, hidden failures are the most significant cause of double contingencies in the system, as already mentioned in section 3.4.1. Table 5.15 shows the statistics of hidden failures in the system from 2001 to 2009. Hidden failures are normally affected elements and their cause is classified as protection systems.

Type of dependency	2001	2002	2003	2004	2005	2006	2007	2008	2009	Total
Hidden Failure in 150 kV	4	2	2	7	1	3	5	13	0	37
Hidden Failure in 220 kV	5	7	2	2	6	6	3	2	2	35
Hidden Failure in 400 kV	2	6	1	2	0	1	0	2	4	18
Hidden failures Total	11	15	5	11	7	10	8	17	6	90

Table 5.15 – Hidden Failures in the PTS

5.8. Quality of service

Present day quality of service requirements that are imposed to the electrical utility companies force them to develop efficient processes to record and organize incident data, which allow cross-reference and fast access to the information and a greater reliability in data collection and in statistic indicators calculation. In this way, it is possible to identify more accurately which are the critical points and how effective are the changes applied to the system, in order to assure the fulfilment of the quality of service Regulation[5]. REN, as the National transmission grid concessionaire, publishes every year the quality of service report, in which statistics and indicators obtained from GestInc and other sources are presented. The yearly quality of service reports [114-117], [121-124] are available in [102].

The PTS security of supply is characterized by the system performance indicators, established in the quality of service regulation. In the system performance indicators calculation short (≤ 3 minutes) and long (> 3 minutes) interruptions are distinguished. The general indicators, regarding system's global performance, are the following:

- Energy Not Supplied (ENS)
- Average Interruption Time (AIT)
- System Average Interruption Frequency Index (SAIFI)
- System Average Interruption Duration Index (SAIDI)
- System Average Restoration Index (SARI)

To assess the performance of the transmission network in each grid node that feeds the distribution network or EHV direct clients, individual indicators are used. These indicators are:

- Duration of interruptions
- Number of interruptions

[5] Published attached to the "Despacho" nº 5255/2006 of 8th of March – Diário da Republica, 2nd Series of Direcção Geral de Geologia e Energia

Figure 5.46 presents the data organization and flow.

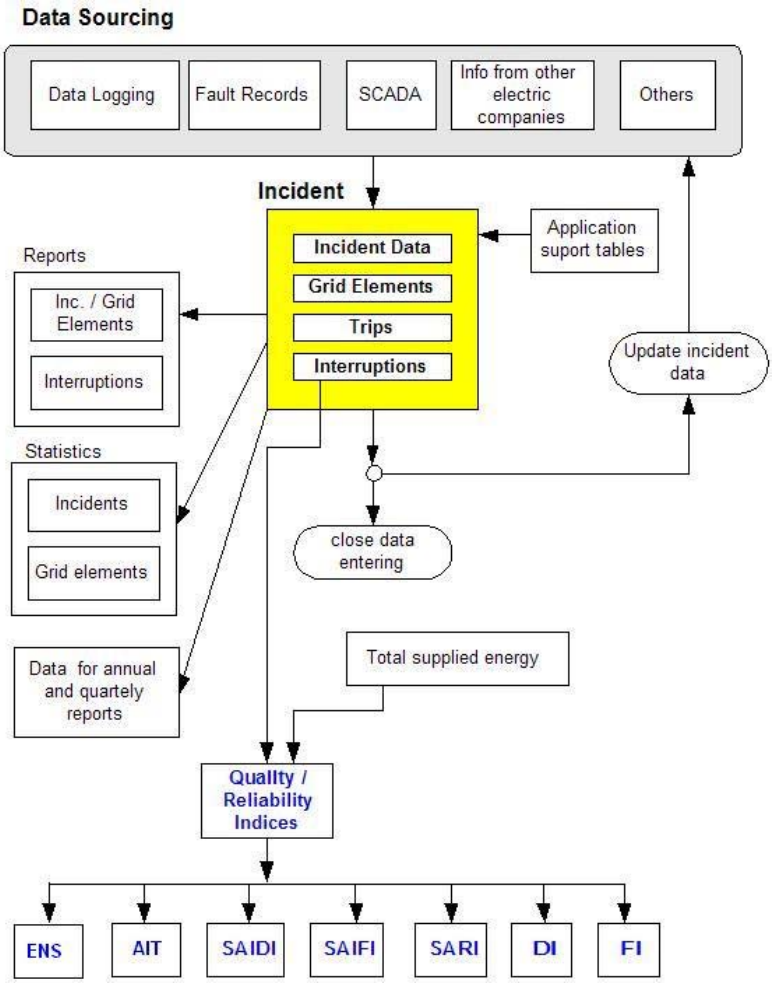


Fig. 5.46 – Indicators Organization [64]

Figures 5.47 and 5.48 present the two main indicators of continuity of supply - Energy Not Supplied and Average Interruption Time. The other indicators mentioned previously can be found in references [114-117], [121-124]. The green part of the columns refers to force majeure causes or to exceptional severe incidents, such as the ones described in sections 2.2.3 and 2.3.

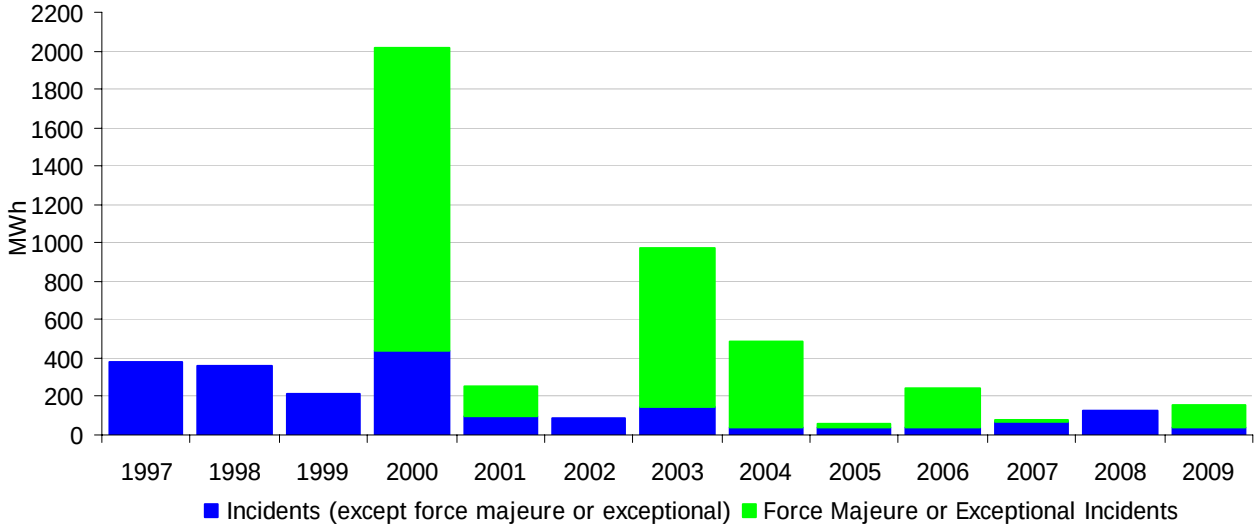


Fig. 5.47 – Energy not supplied in the Portuguese Transmission System

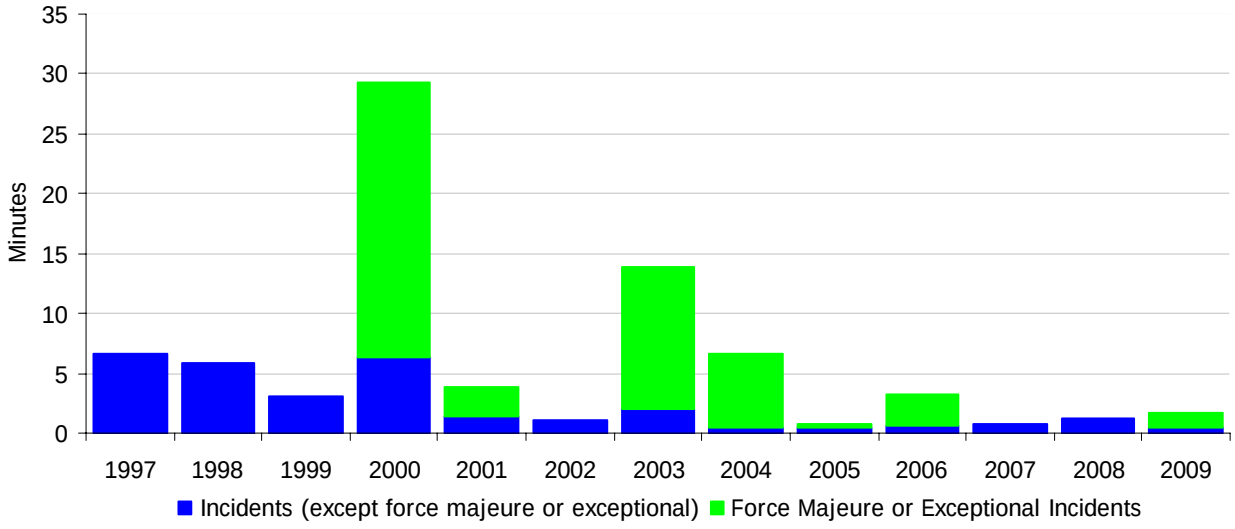


Fig. 5.48 – Average interruption time in the Portuguese Transmission System

To the described indicators, which are the most relevant in terms of incidents, the voltage quality can be added. In the Quality of Service Report (QSR), an analysis of harmonic content, flicker, three-phase system unbalance, deviation of the effective value of voltage and frequency is made for the voltage waveform measured at the busbars of 65 substations and PTS interconnection points, covering all the delivery points where measurement is feasible. Also the availability of the transmission equipment (power lines and transformers) is presented in the annual QSR.

5.9. Conclusion

Incident analysis is a crucial activity to maintain a power system's good performance. At the present time, quality of service requirements are imposed on the electrical utility companies and force them to develop processes to record and analyse efficiently every incident, in order to withstand severe incidents with as little consequences as possible and in this way contribute to risk reduction.

In the recent past, the decrease in the number of incidents and the improvement of quality of service indicators, which directly translates the system performance level, can be described as the result of a multi-disciplinary effort, including several actions on the field, that produce sustainable results. The results obtained point to:

- An adequate planning with the purpose to guarantee service continuity.
- High volume of investment targeted to increase reliability, transmission capacity (also to incorporate new generation plants) and renew assets; this includes uprating of existing OHLs with improved screening against lightning, replacement of insulators, replacement of OHLs in the end of life for complete new ones of higher voltage level in the same right-of-way, refurbishment and replacement of transformers, among others.
- Adequate maintenance strategies, using preventive maintenance techniques and live work techniques, as well as the corrective maintenance every time it is necessary. As preventive measures, it is possible to enumerate all the actions mentioned in section 5.3 of this chapter.
- Strict coordination of the programmed outages, which is done yearly and revised regularly during the year, preferably scheduling the outages in more favourable system operating periods, with the expectation of a lower load, a more balanced generation pattern (with both hydro and thermal) and a favourable forest fire condition, having as main purpose to minimize the consequences of

an unexpected contingency during works. The strict coordination implies the arrangement of several different works for the same grid element in the same period.

- Efficiency of technical and human resources (updating existing technologies, e.g. installing differential protection schemes in OHLs, and regular personnel training).

The period of analysis was chosen from 2001 to 2009, because of the availability of reliable input data. In the future, with an increasing amount of data, the statistical meaning will increase and further conclusions will be drawn. The majority of PTS incidents initiate in OHLs, representing on average about 91% of the total. Most of the incidents with repercussion in PTS that happen in overhead lines are due to the action of environment (storks and forest fires) and adverse weather (such as lightning and fog combined with pollution). OHLs are most affected, because of their dispersion all over the country and consequent exposure to the action of external factors, which cause most of the faults in the network.

Through figure 5.49, it is possible to observe that with the network development the exposed length has increased, but nevertheless the number of incidents has decreased. Particularly in 2004, some of the worst performing OHLs have been removed from service, resulting in a decrease of the total length and also of the total number of faults in OHLs. The increase of faults in 2005 is caused by an extremely dry year and the severity of the forest fires. From 2006 to 2009, the effect of the improvement actions was noticeable, illustrating that the future will not be equal to the past. The large number of faults in 2009 was mainly due to the increase of the number of faults caused by lightning and by forest fires.

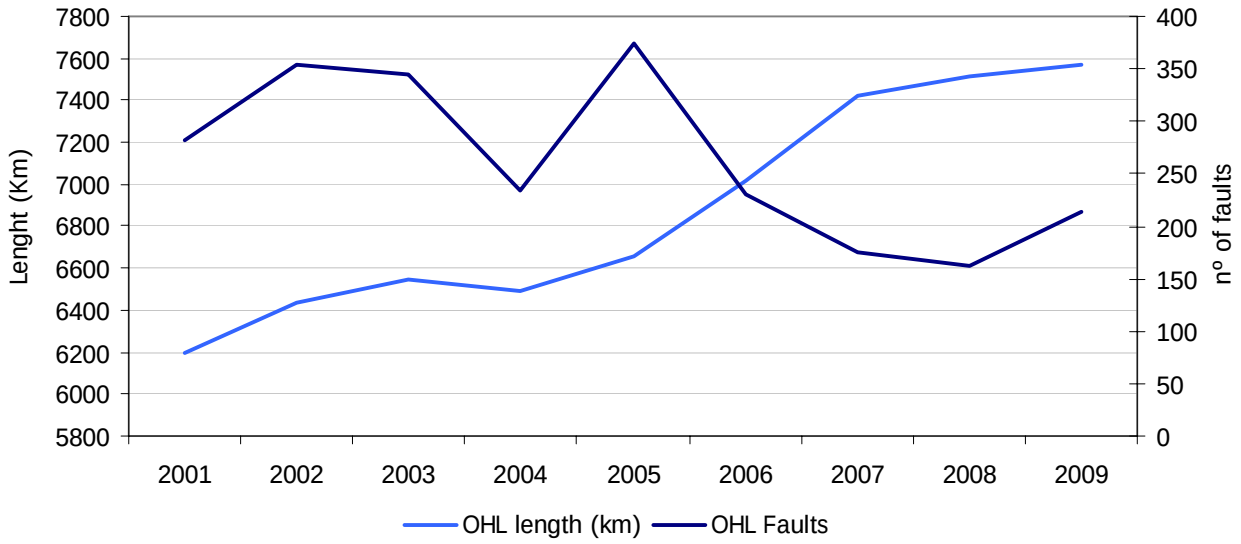


Fig. 5.49 – OHL total length evolution versus the number of OHL faults

The four main causes of faults in the Portuguese transmission system are storks (environmental cause), forest fires (environmental cause), fog in combination with pollution (atmospheric cause) and lightning (atmospheric cause).

The analysis performed in this chapter shows the characteristics of each cause (geographical, meteorological and environmental), their number of faults depending on the time, month and the impact of improvements. It was concluded that it is extremely important to identify the seasonality, location and time of occurrence of the faults, because it will support the decision of considering or not that cause in the risk assessment methodology at each specific moment.

The fault dependence with some specific characteristics was evident with the detailed analysis, and table 5.16 sums up some of the conclusions.

Incident's Cause	Season	Daily period	Location
Storks	All year	50% - from 0h until 6h	Well known stork's areas
Lightning	All year	66% - from 12h until 24h	Whole country (depends on lightning location)
Forest Fires	Summer	60% -from 12h until 18h	Whole country (depends on fire location)
Fog & Pollution	Summer	57% - from 0h until 6h	Well known polluted areas

Table 5.16 – Faults Characterization per cause

Forest fires and lightning are fault causes that can occur all over the Portuguese territory. In case of both lightning and forest fires, there are regions more propitious than others, such as mountain areas or municipalities with a higher risk of fire, respectively, because of their intrinsic characteristics. The lightning density and the forecasts concerning the risk of forest fire will be used in order to determine the severity of each region. This will be further developed in the following chapters.

Despite the increase of the stork population in Portugal, REN's actions taken since 1995 in order to mitigate the influence of these birds in OHL incidents allowed to control the number of faults caused by storks. These actions included the installation of nesting platforms and nesting inhibitor devices and also the relocation of nests. "The plan does not chase the birds from the tower, the aim is to ensure a peaceful coexistence of stork and OHLs" [90]. Nowadays the faults caused by storks happen during the whole year, which may be an indication that storks might be no longer migrating to southern lands and that they have perfect conditions to procreate in Portugal.

The faults caused by fog in combination with pollution and forest fires are extremely dependent on the meteorological conditions and on a specific season (mainly after a dry and hot period). Nevertheless, the measures described are of great importance in order to avoid and reduce faults. Since 2006, it was also possible to notice that the number of faults caused by fog in combination with pollution has significantly decreased. For instance, in 2007, the rain during summer and the increase in the number of composite insulators resulted in a decrease of washed towers and faults and in 2009 there were no faults.

Regarding forest fires, the summer of 2005 was the most critical. There were periods where several OHLs were affected by the same forest fire (in the same geographical region) or by different forest fires happening at the same time (in different geographical regions). For short periods of time, more than three overhead lines were disconnected, due to permanent faults or to the fire fighters' work to extinguish the forest fire. Obviously, facing this type of event, the security of a transmission system becomes more vulnerable, with the temporary loss of the N-1 criterion. The definition of OHL corridor was developed as a response to forest fires and enables a reliable, adaptable and effective management of the system's security.

The recent responsibility, attributed by law to the Portuguese TSO, of maintaining the right-of-way clean within a defined area under each OHL that crosses forest, has created great expectations in terms of fault avoidance and in terms of the efficiency of the fire fighting. This measure will also avoid faults caused by trees, which occur rarely in the Portuguese transmission system. The significant decrease in faults caused by forest fires in the last 3 years gives an indication that forest fires will likely lose importance as an incident cause.

Lightning is an uncontrollable cause and insulation coordination is the only measure to mitigate faults caused by this force of nature. In the analysis period, faults caused by lightning present a quite regular yearly pattern with the exception of 2005, where the decrease in the number of flashes was significant.

Other causes were mentioned in this chapter: maintenance and operation (human errors), protection systems, obstacles, ice and extreme wind. Human errors will always happen, and sometimes behind other

causes a human error is hidden, e.g. an incident caused by a tree or an incorrect parameter in the protection system settings. Hence, their presence in the occurrence of faults may be beyond the statistical results. In order to reduce the risk of human error a set of conditions are needed, such as:

- Accurate and strict procedures to follow in maintenance, assembling and tests.
- Adequate decision support tools to perform the required tasks.
- Good coordination between all involved parties, especially if there are more than one work running simultaneously.
- Personnel training in their working domain.

Concerning incidents caused by protection systems, they are normally associated with severe events caused by a sequence of failures (cascading events), where the protection system's incorrect operation is actually part of the sequence. Unexpected hidden failures, occurring mainly in protection systems, may cause multiple dependent contingencies with multiple and different causes. It is important to be aware that everything that does not have real-time diagnosis may only be detected with the occurrence of a fault, such as short-circuit, which will trigger the failure. As already mentioned in chapter 2, every time that some equipment fails and causes an incident, one of the actions resulting from the incident analysis is to check that equipment in particular as well as all the others of the same model that are installed in the system. In this way, it is possible to avoid the repetition of the same failure. It is also important to have accurate commissioning and testing procedures that will help minimize the risk of misoperation.

Extreme wind conditions have caused a large disturbance in the Portuguese transmission system on 23rd of December 2009. Faults caused by extreme wind conditions are rare, but they normally affect several grid elements and leave a trace of destruction that takes a long time to repair. The combination of wind power forecast and the real time measurements of wind provided by the wind farms connected to the transmission network should be used for probability calculation, also of common cause faults. However, it was not possible to do historical data analysis with wind speed measurements, because their availability is quite recent.

This chapter does not address faults in generation units, damage detected during maintenance, or planned outages, which goes beyond the scope of this work. It provides a deep insight on the incidents in the Portuguese transmission system and clearly shows that the design measures and actions applied to mitigate the controllable causes have doubtless decreased the number of faults, reducing the likelihood of incidents. Therefore, all the changes in procedures, practices and improving actions implemented during the analysis period will be reflected in the incidents of the future, decreasing their frequency and severity, which will be certainly judged every time by incident analysis. A good characterization of faults and consequent improving actions will translate into improved reliability.

Chapter 6.

Information Gathering and Organization

6.1. Introduction

Probabilistic evaluation requires a consistent collection of relevant system and component data [Roy Billinton, Porto, October 2008]. It is vital to have detailed information for decision support.

An assessment methodology needs information as input, which must be adequately organized to be used and processed. One of the most challenging tasks of this research work was the information gathering and organization, which represents a big challenge for any TSO, allowing the evaluation of the network status and the development of methodologies that will improve the system performance and efficiency.

In the beginning of this work, initial ideas were drawn, aims were defined and information needs were identified. As every work that is starting, also this one had a naïve stage, the information identified to be gathered was the ideal, but soon the author realized that part of the ideal information was not available or it was too expensive to acquire (such as meteorological information).

In order to develop a risk assessment methodology for operational system's security, the variables that influence the occurrence of contingencies have to be used in the analysis. The behaviour of an OHL is dependent on the several different factors, to which it is exposed, such as meteorological and environmental conditions. In chapter 5, the detailed faults characterization was made, because historical data and statistics are crucial to decide what is important to be included in the analysis, and it was concluded that it is important to consider the following influencing characteristics:

- Incidents data (grid elements historical performance)
- Network data
- Geographical data
- Weather data
- Environmental data
- System improvements

6.2. Information gathering

The information gathering is an extremely time-consuming task, which depends on the cooperation between different departments of the TSO organization, but it is an indispensable effort because detailed information is crucial for the accuracy of the developed methodology.

The information available in an organization, such as a utility, is normally spread through different departments and occasionally it is not even well structured. When digging into the search of information, the difficulties appeared. The process of asking, obtaining and organizing all the requested information is slow, but despite all, the added value obtained through the organized information source that is created by this work will be significant. It will provide to the Portuguese TSO a reliable and organized data source, from 2001 until 2009, of which the need was already identified. With the effort of many colleagues from different departments of the Portuguese TSO, raw information slowly arrived. The data that was readily available was the incidents' historical data which are organized in GestInc (REN's incident data base).

From the data that was possible to acquire, two matrices of input data were built in MsExcel workbooks, specifically towers and incidents, respectively. In the towers matrix all the detailed information related to towers is stored, namely:

- Number of the tower
- Name of the OHL
- Voltage level
- Tower coordinates (in two different coordinates systems – Datum Lisboa and WGS84)
- Municipality (where the tower is located)
- Type of insulators (if composite or not)
- Number of stork nests
- Presence of pollution at the location
- Geometrical characteristics (tower height and distance between ground wires)
- Soil resistivity (according to the place where the tower is located, in Ohm.m)
- Tower footing resistance (measured or calculated values, in Ohm)
- Number of ground wires
- OHL segment (distance to the adjacent tower in meters)

Integrated in the towers MsExcel workbook, there is a worksheet with municipalities' characteristics, such as:

- Municipality name and number
- Municipality area (km^2)
- Number of towers
- Number of stork nests
- Number of towers with nests
- OHL length (per line and total)

The incidents matrix contains the general incident information and the information relevant for system's security purposes, such as:

- Fault's date
- Fault's time
- Fault's grid element
- Type of fault (mono, bi- or three phase)
- Voltage level
- Fault's cause
- Type of element (origin or affected)
- Temperature
- Fault clearing time
- Lightning flash characteristics (of most likely lightning stroke)

With the development of the methodology, other matrices are built, such as daily forest fire risk value per municipality combined with current active forest fires information, being the last available in [125]. For the forest fire risk, Portuguese Meteorological Institute (IM) calculates the risk level based on the Fire Weather Index (FWI) and makes available on their website the results per municipality, the actual value for the day (d) and the forecast for the next day (d+1) [126].

The available information used for the calculation of the fault probability is shown in figure 6.1. The information can be divided in off-line and online information.

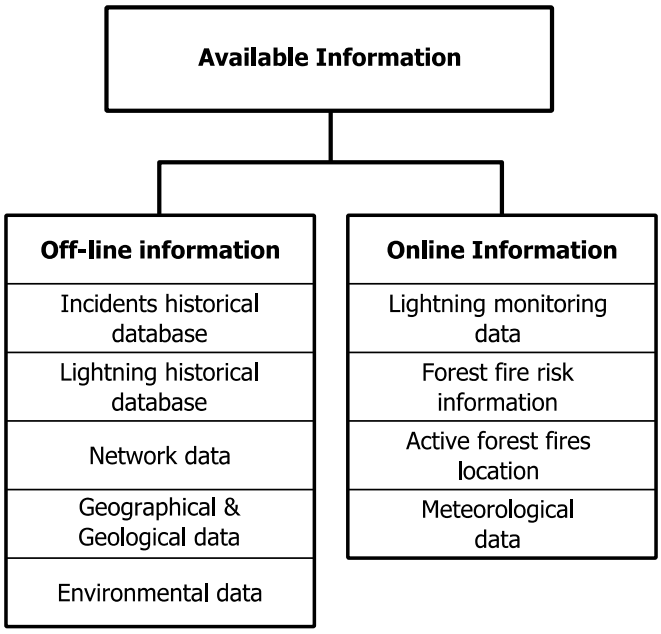


Fig. 6.1 – Information type scheme

6.2.1. Network data

The network data consists of all the equipment installed in the Portuguese Transmission System (PTS). For this specific work, the network data consists of overhead lines, transformers, autotransformers and protection systems, including obviously all their relevant characteristics already presented above as necessary information, such as voltage level, OHL length, tower design, tower footing resistance, insulator type per tower, conductor diameter and system technology, among others.

In the PTS, the tower height within an OHL typically varies between 20 and 60 meters, because of terrain characteristics. Within the same OHL, towers of several types can occur. For each OHL, the characteristics of all towers were individually identified, namely the tower total height and the distance between ground wires. In case of old transmission lines, where there is no accurate source of information, an identified dominant type and height was used, based on the planning department's data base. The vast majority of the Portuguese transmission OHLs has two ground wires.

6.2.2. Geographical data

The geographical data consists of the coordinates of all OHL towers in the network and the municipalities' official administrative borders. The exact borders of each municipality were obtained from the Portuguese Geographical Institute [127].

The PTS has approximately 16700 towers in 2009. Every tower is exposed to the risks that are present in its specific location, such as stork presence, cloud-to-ground lightning density, risk of pollution combined with fog and forest fire risk on a daily basis. The Portuguese TSO uses a tool called RENMap, which provides several layers of information and it was used as a start point for this work. The towers information layer contains the OHL code, the tower number, the tower type, and the tower location (in Cartesian coordinates, Datum Lisboa).

At the start of this work, about 60% of the tower coordinates were known, containing all the towers of the most recent OHL and only the angle towers of the old ones. Recently, a laser measurement of obstacles in the OHL path has been systematically performed, which combines the search for obstacles with tower coordinates measurement. With laser measurement and construction data, including new and uprated OHLs, the towers matrix has grown up to around 95% of the towers.

There are different levels of accuracy in the data. The most reliable information source is the construction data, which are measured on site. The laser measurements have an error that can reach some tens of meters, but for this work that is negligible. The results of the laser measurements are given in geographic coordinates (WGS84, as commonly used in GPS receivers). To represent the other 5% of the towers, some virtual equidistant towers were placed, mainly for older OHLs, where only angle towers information exists, providing a better approximation of the total amount of towers per municipality. At this moment (end of 2009), the expected uncertainty in the total number of towers is less than 1%. The data selection process is presented in figure 6.2.

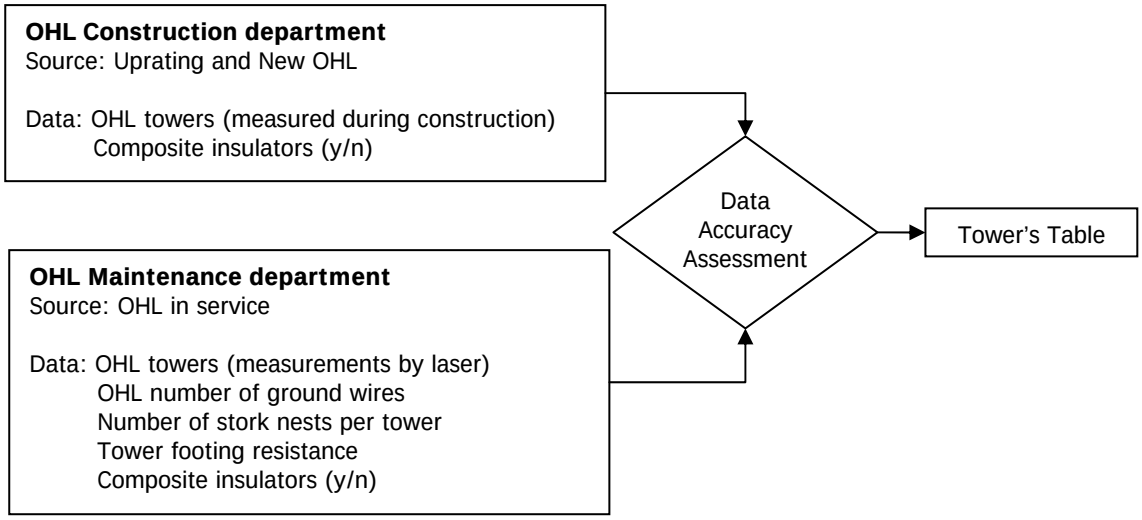


Fig. 6.2 – Tower information sources flowchart

Due to the fact that RENMap uses Cartesian coordinates (Datum Lisboa), while the border information and the recent location measurements are in geographic coordinates (WGS84), a coordinate conversion was needed. This conversion was done using the software TRANCOORD version 2.01 from the Portuguese Geographical Institute [18].

For better geographic visualization of the network, a Google Earth file (.kmz) was created with all the towers, the municipalities' official borders and the nearest soil resistivity for each tower. Additionally, the OHL representation by connecting all the respective towers is also available, as in figure 6.3.

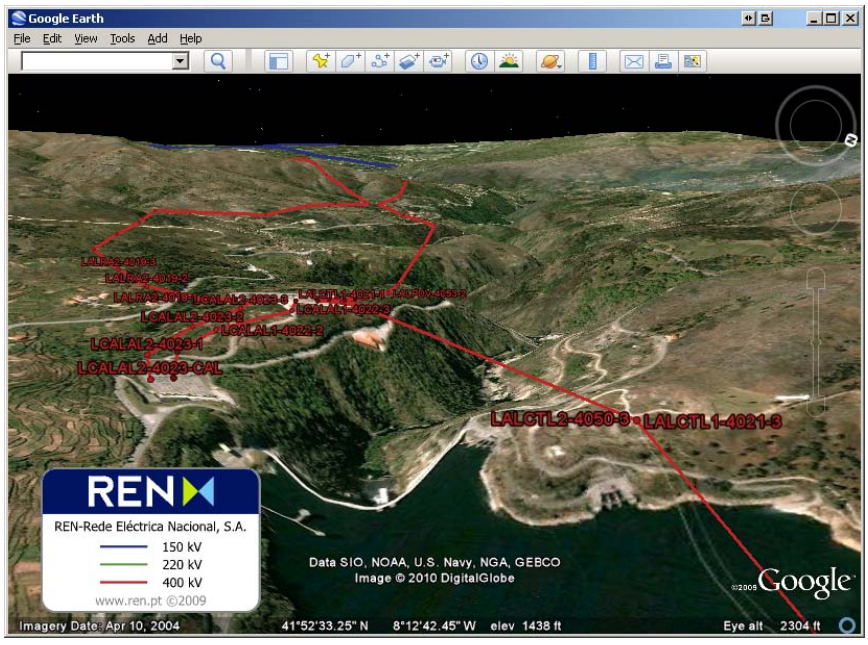


Fig. 6.3 – Part of REN Transmission System visualised in Google Earth

6.2.3. Geological data

The geological data consists of the soil resistivity value in the vicinity of each tower. Reference [128] provides updated maps of soil resistivity for continental Portugal, for depths of 1.5 and 4 meters and for dry and wet weather conditions, taking into account geological information and characteristics, and also weather conditions (precipitation). The dry weather maps were built up from about 1600 field measurements made in dry conditions. The 1.5 meters deep map for wet weather was estimated considering the average precipitation rates for August and May. According to [128], August and May are respectively the most dry and wet month, concerning the amount of water in soil. The results are presented for areas of approximately 25 km^2, so variations in smaller areas are not covered. The 4 meters deep soil resistivity values where used in this work, because of the grounding network geometry and of less significant variation with precipitation, thus being valid for the whole year. It was also noted that the deeper layers have a more uniform space variation. Figure 6.4 shows the soil resistivity map for the 4 meters depth, which is constituted by squared areas of approximately 25 km^2. For each tower in the PTS, the nearest soil resistivity measure was considered.

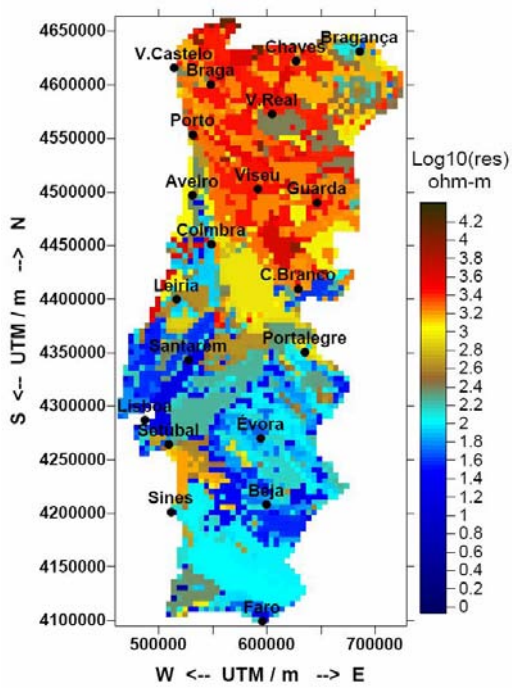


Fig. 6.4 – 4 meters deep soil resistivity map [128]

6.2.4. Weather data

The weather is a very important factor when severe incidents are under discussion, such as dry periods that cause severe forest fires (as in Portugal and in Greece), exposure to pollution agents, wind storms and ice storms that cause structural damage. In the literature, it is possible to find many examples and some were presented in chapter 2. During this work, many incidents are evaluated and the correlation between weather conditions and the events is considered important in order to evaluate what is meaningful to include in the methodology. Ideally, the author would have liked to include in the analysis more weather information than is actually available.

The available weather data only consists of temperature measurements, lightning information and risk of forest fires daily index (based on the fire weather index). Unfortunately, relative humidity and precipitation were not available and, regarding wind speed, there was not enough historical data for the analysis.

The Portuguese Meteorological Institute (IM) owns an historical database that has, in 10 minute intervals, measurements of temperature, humidity, wind speed, direction and atmospheric precipitation from several weather stations spread through the Portuguese territory. They also calculate the risk of forest fire per day, in order to assess the respective risk in each municipality, and they provide lightning information which is registered in the real-time monitoring system (LMS). The latter is accessible through the Portuguese TSO. Lightning data is available in the monitoring system data base since 2003.

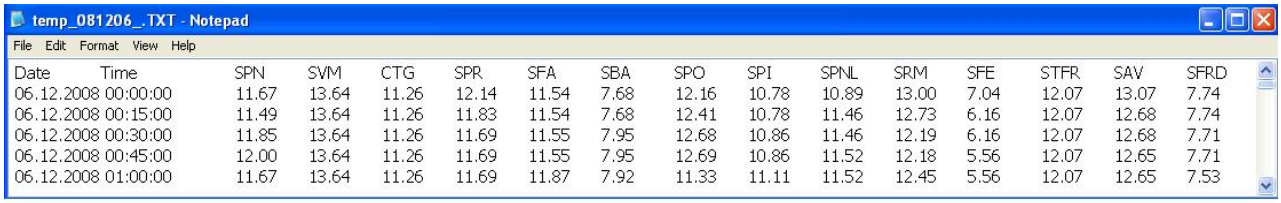
The risk of forest fire index is published daily by IM through risk maps divided per municipality. The daily risk of forest fire is being automatically downloaded from IM's webpage [126]. There is almost no historical map available, but only some reports that sum up the past information. Therefore, the FWI based risk index is going to be assumed as meaningful and it will be used directly, because there is only little data to evaluate its meaning and to analyse the best way to use and incorporate it. The used temperature measurements are mainly the ones located in REN substations, where the historical data is available through the SCADA system. All the available information is taken into account.

About the humidity, wind speed and precipitation no information is available, because it has revealed itself too expensive to acquire. Thus, no historical analysis was performed.

6.2.4.1. Temperature

For temperature measurements, two sources are used:

- Measurement points installed in several substations, which are available through the SCADA system (recorded every 15 minutes). This information is stored daily in text files (.txt), as in figure 6.5. The number of substations with temperature measures is increasing significantly, because new substations and refurbished ones are always equipped with measurement points.


temp_081206_.TXT - Notepad

File Edit Format View Help

Date	Time	SPN	SVM	CTG	SPR	SFA	SBA	SPO	SPI	SPNL	SRM	SFE	STFR	SAV	SFRD
06.12.2008	00:00:00	11.67	13.64	11.26	12.14	11.54	7.68	12.16	10.78	10.89	13.00	7.04	12.07	13.07	7.74
06.12.2008	00:15:00	11.49	13.64	11.26	11.83	11.54	7.68	12.41	10.78	11.46	12.73	6.16	12.07	12.68	7.74
06.12.2008	00:30:00	11.85	13.64	11.26	11.69	11.55	7.95	12.68	10.86	11.46	12.19	6.16	12.07	12.68	7.71
06.12.2008	00:45:00	12.00	13.64	11.26	11.69	11.55	7.95	12.69	10.86	11.52	12.18	5.56	12.07	12.65	7.71
06.12.2008	01:00:00	11.67	13.64	11.26	11.69	11.87	7.92	11.33	11.11	11.52	12.45	5.56	12.07	12.65	7.53

Fig. 6.5 – Temperatures result file (December 2008)

- Daily temperature measures (maximum, minimum and average values) in a few municipalities, namely: Aveiro, Beja, Bragança, Coimbra, Faro, Guarda, Lisboa, Portalegre, Porto, Setúbal and Tavira; this information is provided by REN, in an Excel workbook, and its source is IM.

In order to choose a temperature value per fault, choices had to be made, due to the limitation of data access. Homogenous zones of temperature were recognized through the maps of average medium, average maximum and average minimum temperatures, available in IM's website [126]. As an example of the maps, figure 6.6 shows the average maximum temperature in January and July 2009. Through all the monthly maps of temperature analysed since 2001, it was possible to observe that Continental Portugal has different patterns of temperature between the regions located north and south of the Tagus river and between coastline and inland regions.

Reference [129] has also analysed IM maps and presents four geographical clusters in order to represent climatic zones in continental Portugal, specifically: Littoral North (including Braga, Porto, Aveiro and Coimbra), Interior North (including Bragança and Guarda), Tagus valley and Alentejo (Lisboa, Setúbal and Beja) and Algarve (including Faro and Tavira). In order to solve border problems or to select other value due to bad data, this information was taken in consideration, improving the selection's coherence.

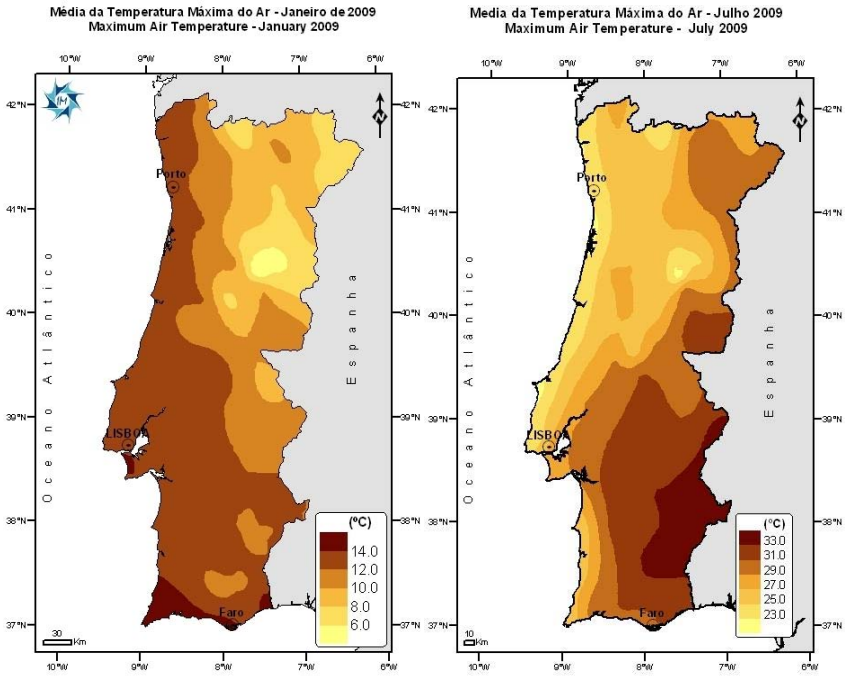


Fig. 6.6 – Maps of the average maximum daily temperature in January and July 2009 [126]

Due to the amount of measurements available (15 minutes values in several substations), SCADA measurements were considered more accurate than the daily ones and therefore used to select a temperature for each fault, following specific criteria, namely:

- Date and time comparison: the selected value has exactly the same date as the measure (incident's date = measure date) and the value time is equal or within an interval until 15 minutes before the fault's time (incidents time – 15 minutes < value time ≤ incidents time), which means it is the last measurement just before or simultaneous with the event.
- Proximity: the selected value is the nearest from the incident's origin grid element. This selection criterion is important because in the end of 2008 only 14 substations had temperature measurement. Hence, the nearest measurement point has to be selected ($min(distance_{ij}), \forall i, j$, where i represent the measurement point and j represents the grid element location). In case of OHL, the selected point is the closest to the bigger segment of that OHL. In the end of 2009, 20 substations had measurements, 6 more than in 2008.

Due to the large amount of data from 2001 to 2008, including around 2920 SCADA text files and more than 2330 incidents, two VBA macros were developed:

1. To populate an Excel worksheet with the temperature values of all the SCADA measurements per incident, fulfilling the first criterion.
2. To select per grid element which measurement is the best to consider, according to the second criterion, after running the first algorithm. This macro fills in a new column with the selected value for each incident. The reason to define every time a new measure (which is most likely to be the same as previously) is due to the fact that new measurement devices are being installed in REN substations, increasing the number of measurement points and the proximity to some of the grid elements. From 2001 to 2008, the number of temperature measurement points in substations increased from 5 up to 14 and it will continue to increase.

After running the two macros, the non-coherent or non-existing data identification and replacement is performed manually, because they occur rarely. In case of bad quality of the substation measurements, the value is replaced by the measure of the nearest substation, if the average temperature of the region is the same. The temperature maps provided by IM, as shown in figure 6.6, are used to make this check, considering the fault month and year. In case of no substation measurement nearby, the daily

temperature measures provided by IM are used. This analysis was only performed from 2001 to 2008, because the drawn conclusion was that no cause is strongly correlated with temperature, therefore in 2009 no further analysis was done. Nevertheless at the end of 2009, 20 substations have temperature measurements.

6.2.4.2. Lightning

Lightning monitoring systems are used internationally, such as in the USA [130], Sweden [131], UK and Ireland [132], the Netherlands [133], Austria [134], South Africa [135], Israel [136] and China [137], and many others.

In 2007, the Portuguese TSO has acquired a real-time monitoring system that provides the control room operators with real-time information on the lightning detected in the national territory, giving geographical and amplitude information.

In the control room the lightning detection data is presented to the operator on an ordinary PC, with a user-friendly interface, which allows in real-time:

- To identify and keep track of the development of thunderstorms.
- To correlate lightning with fault occurrence (i.e., with protection systems operation).
- To activate additional security measures, such as the cancelation of planned outages; a closer look is taken at N-2 contingencies, especially when two lines share the same towers and right-of-way along their length and the implementation of remedial actions identified as necessary (for instance the implementation of a special topological scheme).

Figure 6.7 presents the lightning detection sensors location in the Iberian Peninsula.

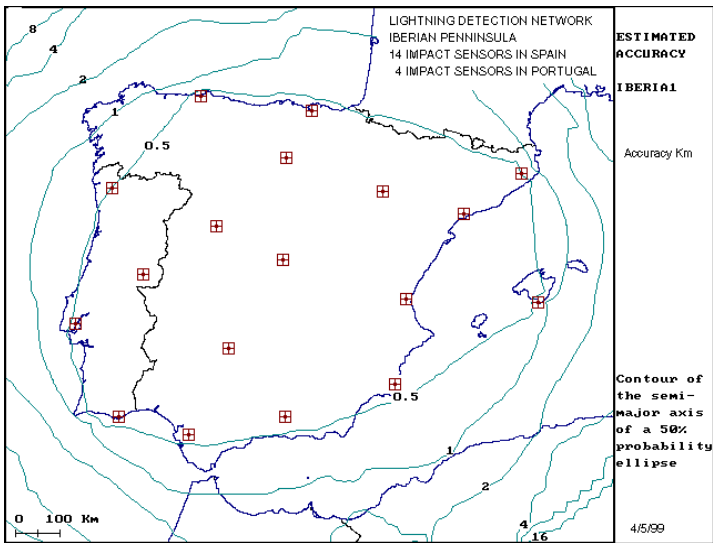


Fig. 6.7 – Lightning monitoring system detection network

The software used to visualize and import the data is "Jobs v5.3 – Visualization and Analysis of Lightning Data" from Météorage, France. This system has already been working since June 2002 in the Portuguese Meteorological Institute, which is the owner of the detection network and the complete historical database of cloud-to-ground lightning records, which are used in the development of this work.

The network is composed of detection and communication equipment, allowing the population of an historical data base. Nowadays, the whole system has 18 detectors, 4 in Portugal in addition to 14 in Spain. Since December 2002, lightning detection data is shared between both countries, improving the

accuracy of the measurements. In the Portuguese case, the information is shared with the 5 nearest detectors in Spain. Multiple sensors are used to detect lightning.

Figure 6.8 presents the user interface of the lightning monitoring system, which has geographical representation and allows monitoring the progression of lightning within the Portuguese territory.

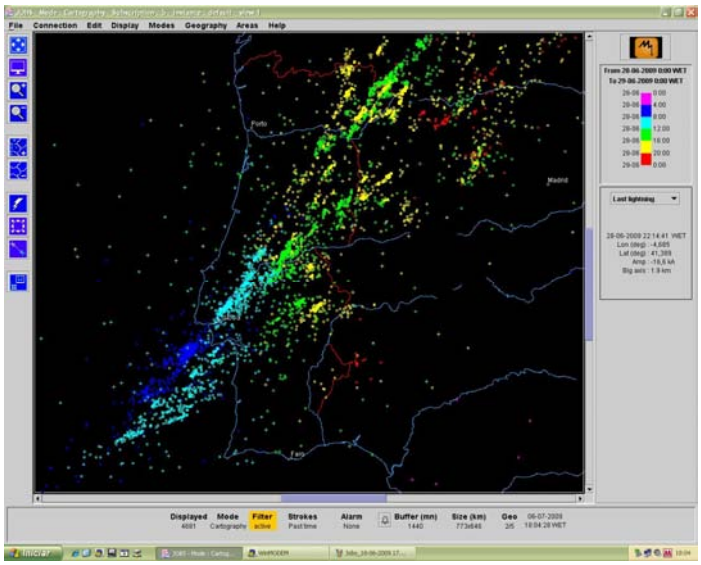
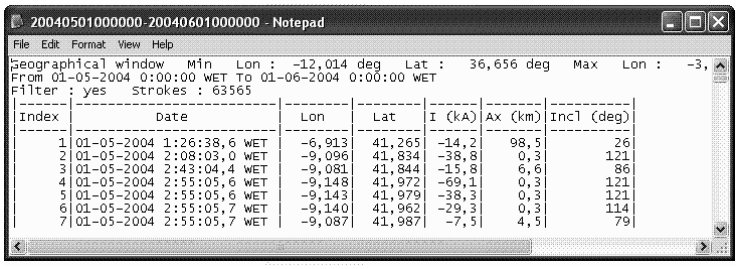


Fig. 6.8 – Lightning monitoring system user interface

According to reference [138], three methods are used to locate the lightning discharge, regarding latitude and longitude (in WGS84): magnetic direction finding, time of arrival and the combination of both (which improves accuracy). The system also provides the measurement of the intensity, polarity and orientation of the discharge. After being detected, the lightning information is immediately transmitted to the data centre via virtual private network (VPN). The information is automatically stored in an ASCII file, as shown in figure 6.9.



20040501000000-20040601000000 - Notepad

File Edit Format View Help

Geographical window Min Lon : -12,014 deg Lat : 36,656 deg Max Lon : -3,
From 01-05-2004 0:00:00 WET To 01-06-2004 0:00:00 WET
Filter : yes Strokes : 63565

Index	Date	Lon	Lat	I (kA)	Ax (km)	Incl (deg)
1	01-05-2004 1:26:38,6 WET	-6,913	41,265	-14,2	98,5	26
2	01-05-2004 2:08:03,0 WET	-9,096	41,834	-38,8	0,3	121
3	01-05-2004 2:43:04,4 WET	-9,081	41,844	-15,8	6,6	86
4	01-05-2004 2:55:05,6 WET	-9,148	41,972	-69,1	0,3	121
5	01-05-2004 2:55:05,6 WET	-9,143	41,979	-38,3	0,3	121
6	01-05-2004 2:55:05,7 WET	-9,140	41,962	-29,3	0,3	114
7	01-05-2004 2:55:05,7 WET	-9,087	41,987	-7,5	4,5	79

Fig. 6.9 – Lightning detection data file

The software provider estimates a location error in the Portuguese territory smaller than 500m for the ellipse's major axis with 50% of probability and an efficiency of more than 90% for lightning with a current peak bigger than 5 kA [138]. The ellipse circumscribes a region centred in the recorded stroke location, within which there is a 50% probability of occurrence. Not all lightning strokes are detected. The detection efficiency will be dependent on the number of sensors, their configuration and geometry. Reference [135] gives a very good insight about detection efficiency and location accuracy of a lightning monitoring system.

In order to analyze the performance of the lightning monitoring system, several steps were performed towards the identification of which lightning has caused each incident from 2003 on. The second half of 2002 was not considered in the calculations, because it was the beginning of the detection network where the LMS was still under testing (time to correct infancy problems) and actually the performance was much lower than in the following years under analysis.

For the first three steps, an application was developed in SQL using Microsoft Access. The fourth step used Google Earth geographical interface, presented in section 6.2.2, which displays the geographical representation of the Portuguese transmission system, and because it is just a visualization tool, this step was made manually. The given steps towards this result were the following:

1. To select only the lightning data that is located inside a defined area, which is a rectangle that includes the Portuguese territory plus 100 km around it. The increase of 100 km is justified by the maximum error found on the detection network records.
2. To compare the date and time of the selected lightning with the SCADA date and time for each incident, both having time synchronization by GPS. The comparison aims to find faults that occurred almost simultaneous with the lightning, i.e., the time of the incident can be up to 3 seconds later as the lightning time. This assumption was made considering the worst clearing time for the fault, which means the distance relay operating in zone 3. The output of this step is a matrix identifying all possible lightning per incident.
3. To check for each incident if the selected lightning strokes are located exactly or in the vicinity of the affected OHL (considering the detection error associated to each lightning – it is defined as an ellipse and its semi-major axis and angle is given in the detection information). For each incident, if a lightning fulfils also this requirement of being exactly or in the vicinity of the OHL path, it is considered to be the cause of the incident. If more than one lightning fulfils the requirement, the biggest amplitude and the lowest detection error will determine the choice.

This analysis was performed per month, because of the huge amount of lightning strokes. Regarding just the detection of lightning that causes faults in the transmission system, the performance of the network detection was measured, as in (6.1).

$$\eta_{LMS} = \frac{n^o \ of \ \ faults \ with \ a \ detected \ \ lightning \ associated}{total \ number \ of \ \ faults \ caused \ by \ lightning} \qquad (6.1)$$

From 2003 to 2008, the performance of the lightning monitoring system was on average 75%. For 2009, the performance has increased to about 93% and the average from 2003 to 2009 is now 77%.

Since 2007, the availability of the real-time lightning monitoring system has reduced the degree of uncertainty when classifying faults caused by lightning. Before that time, the uncertainty in the identification of the cause lightning was much higher. The presence of lightning as the cause of a fault could only be confirmed by a technician in the vicinity (normally in one of the circuit-ends of the affected OHL). This local information was combined with the lightning data displayed in IM's website [126], just providing the geographical representation, with a cross, of the detected lightning per period of time.

With the installation of the lightning monitoring system, in 2007, REN also gained access to a historical lightning database, going back until the second half of 2002. Through the historical data analysis, we have detected some faults (exactly 7), which were previously classified with the cause Unknown, with a plausible lightning to be associated.

In the case that no plausible lightning to be associated with a fault is detected by the monitoring system, but the fault and the lightning flashes are witnessed by a technician, the cause will obviously be classified as lightning. This exact situation happened on 28th of November 2008, where the fault happened close to a substation and it was witnessed by one technician that reported the fact to the control room.

The monitoring system does not detect every lightning stroke that occurs. According to the software provider, lightning strokes are not reported by sensors if their wave shapes are abnormal or if the signal is below the sensor threshold.

6.2.4.3. Wind speed

For this work wind speed was not considered because of the lack of historical measurements. In the near future, because of the large amount of wind farms being connected in the PTS and making wind measurements available, it will be possible to evaluate wind and include it in the work.

Wind speed is a very important factor in the calculation of an OHL thermal rating that once again influences the security margins (the risk of thermal loading only increases for wind speed < 0.6ms^{-1} that on average occurs during 190 hours per year, which represents 2.2% of the time of the year [139]). The availability of wind generation is also very important for operations and security assessment. The likelihood of loss of wind generation when facing a short-circuit and the requirements of generation reserves are further developed in chapter 8.

The faults identified as caused by wind are rare. From 2001-2009, 22 faults were classified as caused by wind, although there are three more classified as unknown with a high probability of being faults caused by wind, located in the OHL with the biggest span length in the network. From the 22 faults, 13 occurred in 2009 because of exceptional wind conditions and 6 in 2003 during the same day affecting only two OHL, whose design was changed afterwards. Additionally, there was a fault in 2004, classified as conductor fall, which was caused by vibrations due to wind.

6.2.5. Forest fires

There are two types of forest fire information included in this research work, namely daily risk of forest fire, made available by Meteorological Institute, and online active forest fires per region, made available by the Portuguese Civil Defence.

6.2.5.1. Risk of forest fires

As already mentioned, daily risk of forest fires is being automatically downloaded from the Meteorological Institute (IM) webpage [126] and it is used directly. Figure 6.10 presents an example of the daily risk of forest fires per municipality.

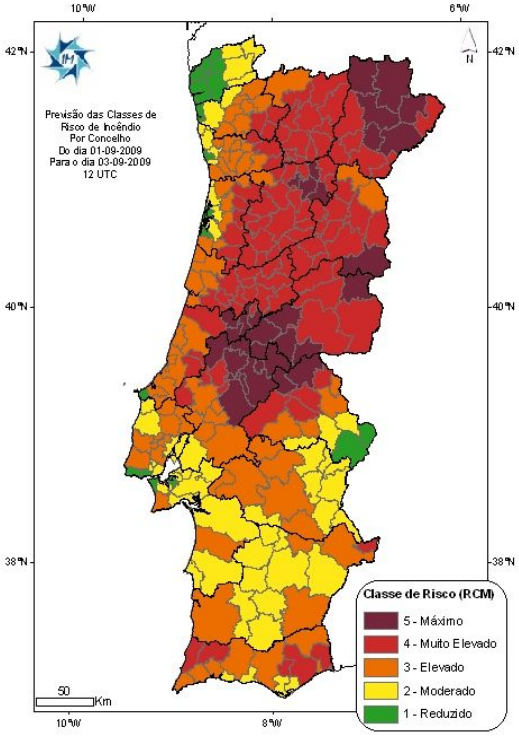


Fig. 6.10 – Risk of forest fire for 3-09-2009 [126]

The Canadian Forest Fire Weather Index (FWI) system consists of six components that account for the effects of fuel moisture and wind on fire behaviour. The first three components, the fuel moisture codes, are numeric ratings of the moisture content of litter and other fine fuels, the average moisture content of loosely compacted organic layers of moderate depth, and the average moisture content of deep, compact organic layers. The remaining three components are fire behaviour indices, which represent the rate of fire spread, the fuel available for combustion, and the frontal fire intensity. Their values rise as the fire danger increases. Calculation of components is based on consecutive daily observations of temperature, relative humidity, wind speed, and 24h rainfall [140].

The risk level based on the Fire Weather Index (FWI) is available per municipality for the current day (d) and for the next day (d+1). An automatic process was developed to take the risk of forest fire per municipality from the image provided daily by IM, presented in figure 6.10. The information can be downloaded as .jpg file format. The automation of all processes is needed, in order to make the methodology adequate to be used in the control room.

Two algorithms were created in Python in order to produce a valid input to be used by the probabilistic method presented in chapter 7, namely: file download and file processing. File download simply downloads the two images, one with risk level for the current day and another with the forecasted risk level for the next day. File processing first identifies where each municipality is located in the image and then takes out the corresponding risk level per municipality based on the colour of the pixels where the municipality is located, using a free library *"Python Imaging Library"*.

Reference [141] presents a detailed analysis of the forest fires that occurred in 2007. Instead of using the FWI directly, the Daily Severity Rating (DSR) is calculated and compared with the actual number of occurrences, as shown in figure 6.11 [141].

DSR is also a numeric rating that represents the difficulty of controlling fire, i.e. reflects the expected efforts required for fire suppression, and it is based on the FWI, as in equation (6.2).

$$DSR = 0.0272 \cdot (FWI)^{1.77} \tag{6.2}$$

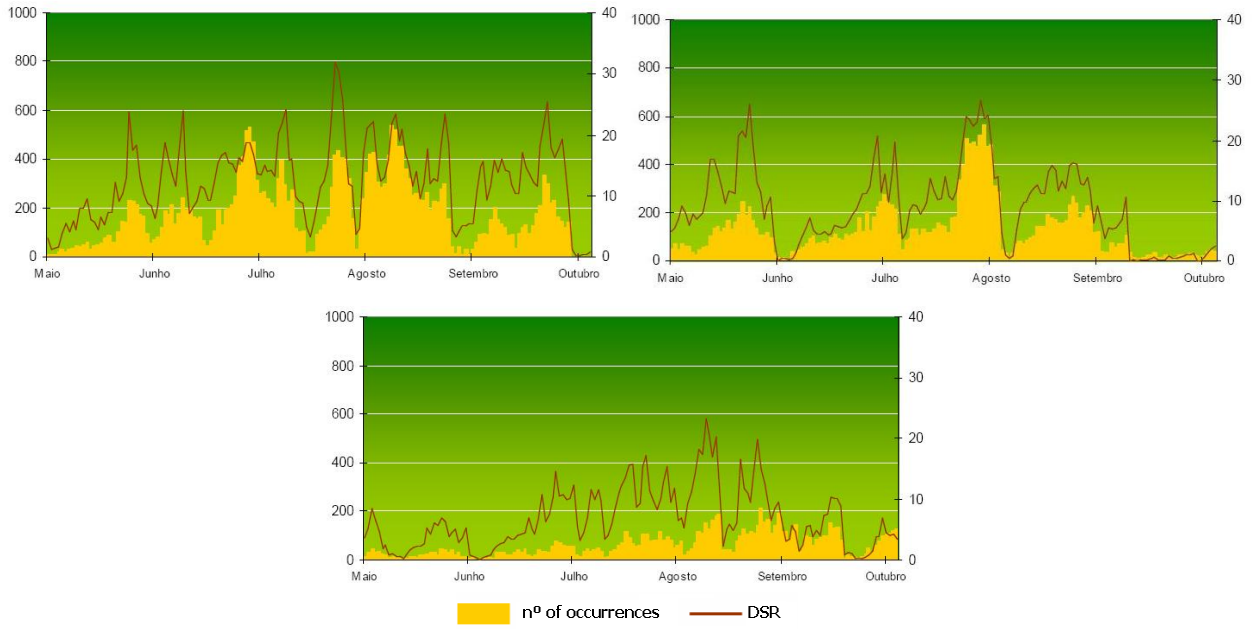


Fig. 6.11 – Evolution of the number of forest fires and the DSR for 2005, 2006 and 2007 [141]

Equation (6.2) derives from a deterministic model developed by Williams (1959) and later modified by Van Wagner (1970) [142], [143]. Through figure 6.11, a strong correlation between the number of forest fires and the calculated DSR is acknowledged, excluding 2007 that was an exceptional year with a very low number of occurrences. The DSR index that is based on FWI, is not publicly available.

6.2.5.2. Active forest fires

The Portuguese Civil Defence makes available on their website [125] online forest fire information of forest fires that last for more than two hours or with more than 10 vehicles or with at least 3 fire-fighting airships involved. The information can be downloaded in three different file formats, namely MsExcel (.xls), MsWord (.doc) and Google Earth (.kml).

An automatic process that saves the active fires file in the .kml format every 30 minutes was developed. These files have the information of the forest fire start time, end time (if the case) and the municipality where it occurred.

With this information available online, it is possible to change the parameter that refers to forest fire risk per municipality in the probabilistic method according to the actual active fires, and therefore including current conditions. For historical data analysis purposes, this information is stored on a daily basis, having in each file 24 hours of data.

6.2.6. Environmental data

The environmental data are very much related with the geography, i.e., with intrinsic characteristics of each place, such as stork presence and pollution areas. This information is gathered by the maintenance division, which has the responsibility to promote actions on all the controllable causes. Considering storks, the Portuguese TSO has the obligation to deliver a yearly report to the National Institute of Nature Conservation and Biodiversity (ICNB) that identifies which towers per OHL have stork's nests and how many, giving the opportunity to estimate the density of the animals located on OHL towers per area. Regarding pollution, the towers that are washed and inside areas with pollution are identified.

6.2.7. Incident data

Since 2001, the Portuguese TSO has an application called GestInc, which has as main purpose to organize and manage a large set of information, which is essential to future data availability [64]. The author has participated in the development of the data base, in the definition of the current incidents' fulfilment criteria and in the daily incident analysis, which allows a high confidence level on the coherence of the existing data. Through incident data, it is possible to calculate historical fault failure rates per cause, per voltage level and even per period of time, as will be presented further in chapter 7.

Furthermore, the most probable lightning record is also included in the incidents data base in order to locate the fault and to analyse the type of lightning that most affect the performance of the grid.

6.2.7.1. GestInc - Incident data base

REN has developed an application to manage all the incidents' information, increasing the effectiveness on data entering and treatment and allowing a more accurate event analysis. This application GestInc was developed by internal staff and is being used since the beginning of 2001, containing all incident records until now. Due to the fact that the application was developed inside the company, it is easy to adapt and

improve, depending on the identified needs. Through its use, it is possible to identify added value to the company, namely:

- increased effectiveness on data entering and treatment
- more accurate event analysis
- faster detection of anomalies in Protection and Control Systems
- quick and easy access to the Incidents and Interruptions data through the company intranet
- better calculation of quality of service indicators
- immediate imported records location with access through the application
- substation maintenance support (e.g. number of switching operations and interrupted current)
- decision support tool for corrective and preventive maintenance

The centralization of the grid's operation and supervision, associated with local event logs import capacity, speeded up the data gathering process and the incident analysis activity, allowing the creation of a reliable historical reference and a prompt data base population. The development of information technologies and the present-day automation level of substations offer a large set of data to analyze, allowing a strict treatment, integration and data presentation, having access to more trusty results and interpretations. The remote control effectiveness and efficiency is increased by the greater reliability of the available data.

After each incident, a detailed incident analysis is performed, because it is always important to identify weak points, errors and most of all to learn from mistakes. GestInc provides a useful way to analyze severe incidents, examining the detailed sequence of faults of a particular occurrence after it has happened. This application was developed in MsAccess and Visual Basic for Applications, presenting a Client-Server architecture. The executable file is placed on the user's personal computer, while the data base resides on the server. New versions are automatically updated in the personal computers. Each incident record is supported by a set of tables, of which the most relevant are the following:

- Grid Elements – PTS and border Elements record that are subdivided in: lines, busbars, transformers, capacitors and power generators.
- Delivery points – all the delivery points where the electric energy is delivered either to clients or other grids.
- Electrical facilities – all REN's substations, power plants, EHV Clients and Spanish Electrical Transmission Grid border substations.
- Incident Causes – all causes and their types used on incident classification, in accordance with quality of service regulation.
- Restoring Agents – all agents (entities and automatic devices) that close the breakers, manually or automatically, after a trip or a non-expected opening, putting the element back into service.
- Fault types – fault characterization (phase identification).
- Protection Relay and Trip types – all existing relays that may act in case of incident and associated trips.

Figure 6.12 presents the display where incident's data are filled in. This display is divided into three embedded windows, being the higher level window related to the incident's common data. The grid elements related to the incident are in a second level, which contains several records, depending on the number of grid elements involved in the occurrence and associated to each one of these is linked a third level window, which has its trip detailed information. The interruptions display is an independent one, which consists of two embedded windows, containing the energy not supplied by delivery point. It is also important to mention that this application is an auditable data source for the Electrical Industry Regulator in security of supply and indices calculation components. This data base automatically generates REN's quality of service key performance indicators. Further details about the described application can be found in reference [64].

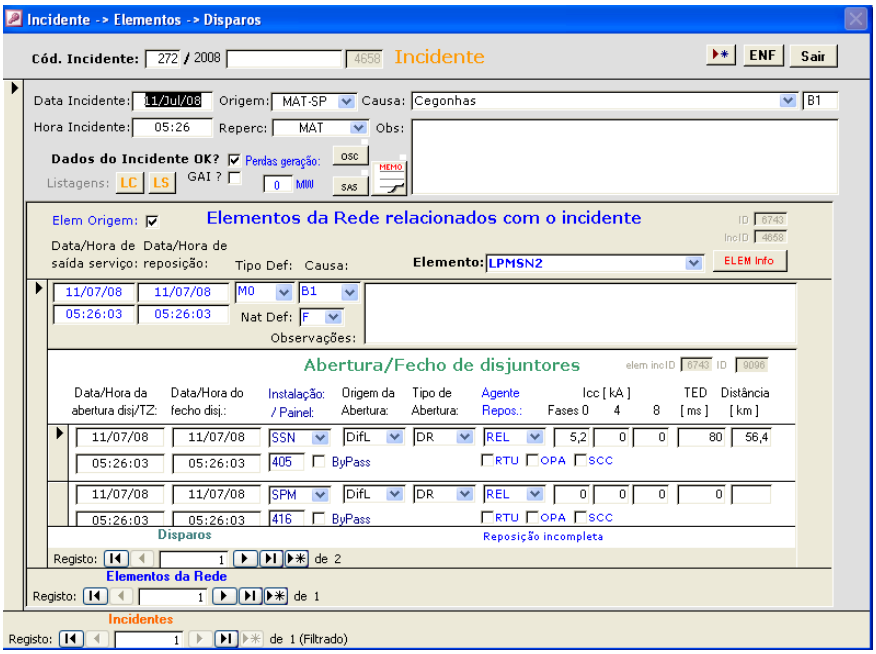


Fig. 6.12 – Main Incident's Register Display

6.2.7.2. Incident's analysis process

The process begins with information gathering, so to perform incident analysis and populate the application data base, the following information is needed:

- SCADA (supervisory, control and data acquisition) records.
- Chronological data logging of involved substations.
- Involved feeder fault records.
- Incident cause identification.

After the population and validation of GestInc, incident information stays available to all interested users, in a systematic way, i.e.: Quality of Service, Protection and Control Systems, Substation Maintenance and Line Maintenance Departments.

For major and relevant incidents, a multi-disciplinary group meets to perform an in-depth analysis of the occurrences, producing if necessary detailed reports, actions and recommendations to be performed. The incident analysis organization is illustrated in figure 6.13.

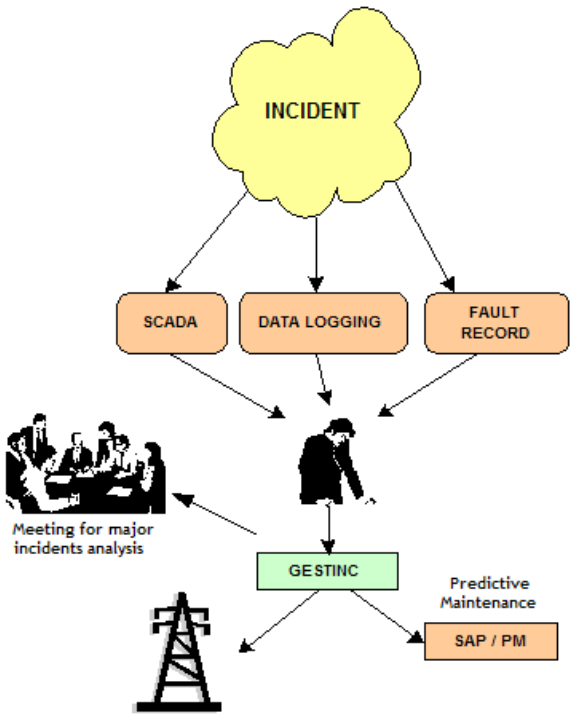


Fig. 6.13 – Incident analysis organization [64]

6.2.8. Operational information

System's operational information is used to evaluate severity, and it consists of State Estimator snapshots, which must include information about planned and programmed outages, load forecast, generation pattern (market driven), wind generation forecast and wind actual production.

6.3. Data preparation algorithms

Several algorithms were made in order to prepare and combine raw data to be introduced in the probabilistic method.

6.3.1. Number of towers per OHL per municipality

For each municipality the number of towers (with and without composite insulators) and the number of stork nests were determined using Matlab's 'inpolygon' function. To calculate the length of an OHL per municipality, the OHL was intersected with the municipality borders, again using Matlab.

6.3.2. Lightning density calculation

In order to determine the number of flashes per year that terminate on transmission overhead lines, the number of ground flashes that can affect an OHL needs to be calculated. Around each OHL a contour was drawn with a width that depends on the tower height and the distance between ground wires. The width of the resulting corridor is typically several hundred meters. The latter is further presented and developed in chapter 7. The number of lightning strokes that affect this area depends on the lightning density Ng in this area. Through the lightning historical data, three possible Ng values were calculated, namely:

- Contour: the line historical number of ground flashes is counted per OHL, in the mentioned corridor around the line, and divided by the contour area.
- Mesh of 4 km^2 squares: the historical number of ground flashes is counted per squares of 4 km^2. The corridor is intersected with the mesh and, for each resulting sub-area, the corresponding density is used.
- Per municipality: the historical number of ground flashes is counted per municipality, see figure 6.14. Analogous to the mesh method, each OHL contour is intersected with the municipality borders.

Orographic and geographic features affect the flash density, such as proximity to rivers and terrain elevation changes (mountains and valleys) [144]. Lightning density maps provide regional detailed information. The lightning activity varies significantly from year to year in most areas (the yearly density maps can be found in appendix G), but the average is the most important thing to consider when performing risk assessment for lightning impact. From the lightning data, maps with lightning distribution density (Ng) were created, from 2003 to 2008, which will allow evaluating the risk of lightning per region.

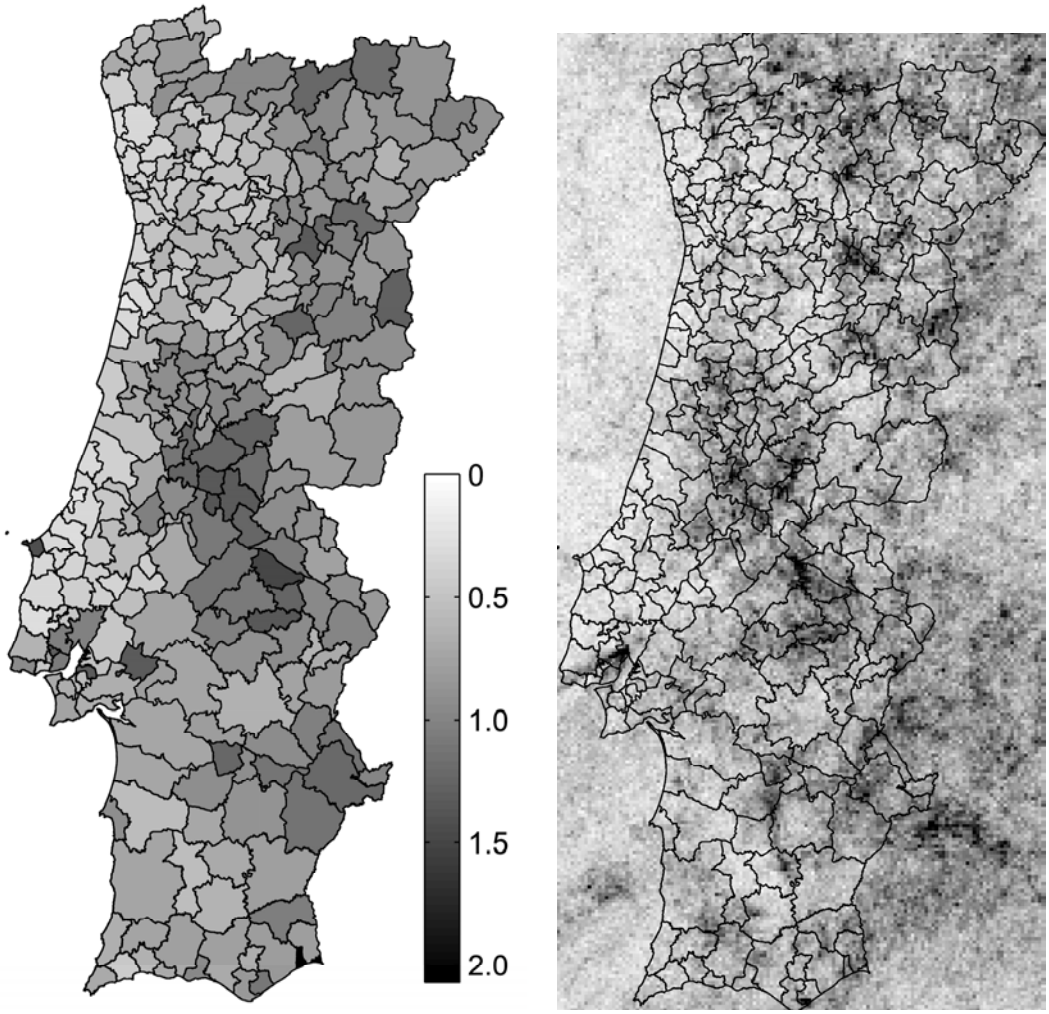


Fig. 6.14 – Lightning density per municipality and 4km^2 mesh (2003-2009)

6.3.3. Soil resistivity per tower

The soil resistivity in the Portuguese mainland is available for a mesh that consists of approximately 25 km^2, as mentioned in section 6.2.3. For each square, the coordinates of its centre and the typical resistivity value are given. For each tower, the nearest square centre was determined and the corresponding soil resistivity is used for further analysis.

6.3.4. Statistics of online lightning observation

The online lightning observation is one of the inputs to calculate the probability of lightning affecting a certain OHL. This observation, yes or no, is used as a multiplier to the lightning probability calculated from historical seasonal and geographical lightning data. The value of this multiplier must depend on the size of the area for which the yes/no observation is made, and how often this information is updated: if a single lightning flash somewhere in the Portuguese mainland would result in a “yes” observation for an entire day, there are many days per year where lightning would contribute to the total risk. Reducing the area and the update interval results in a more accurate observation, which must result in a higher value of the multiplier, represented as $\left(N/P\right)^{-1}$ in chapter 7.

For the online observation of lightning, the Portuguese mainland was divided in two regions: the north and the south, as shown in figure 6.15. This division was selected to be in accordance with the evaluation interval, which is expected to be 1 hour. This was the interval chosen for the calculation presented in chapter 7.

For this geographical division, the effect of the duration of the update interval is determined. For several interval durations, the number of intervals per year is determined during which there was lightning. This analysis is performed using the historical lightning data from 2003-2008, because it was used to calculate probabilities in 2009.

The resulting percentages, along with the multiplier value, presented further in chapter 7, are used in the online risk assessment.

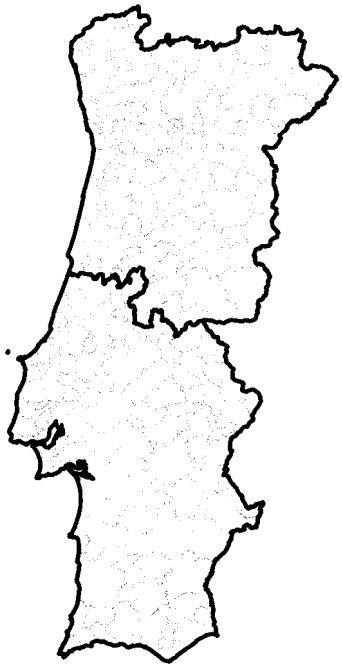


Fig. 6.15 – Division of Portugal in north and south for online lightning observation

6.4. Input information update scheme

The update of all this information is an additional concern. Table 6.1 presents the “bring up to date” frequency for input information. Through these data, many calculations are performed.

Information Type	**Update frequency**
Incidents historical data	Daily analysing incidents and populating the data base
Fault statistics	Every year in January
Municipalities administrative borders	With every update of the Portuguese Geographical Institute
Tower characteristics and coordinates	For each topology change
OHL length and length per municipality	For each topology change
Tower footing resistance	With new measurements
Number of stork nests per tower	Every year in January with the report for ICNB
Towers with composite insulators	Every year before Summer season
Polluted areas	Every year in January
Lightning data	Online and monthly to export previous month historical data
Weather conditions	Online
Fire Weather Index	Every day
Active forest fires information	Online
Operational information	For every snapshot (available every 30 minutes)

Table 6.1 – Update frequency for input information

6.5. Conclusion

All the input information used in this research is presented in this chapter, how it is obtained, organized and pre-processed and how often it needs to be updated. Information organization represents a big challenge and an extremely time-consuming task for a TSO, but it allows the development of methodologies that will improve the system performance.

In order to incorporate the intrinsic characteristics of Portugal that influence the occurrence of faults and the actual risk, based on current conditions, information gathering and knowledge is crucial. The available information used for the calculation of the probability of fault occurrence is the following:

- Incidents' historical data
- Network data
- Geographical and geological data, containing OHL tower coordinates, composite insulators location: tower soil resistivity, and municipalities' official administrative borders, among others
- Environmental data, containing stork nests per tower and regions with identified pollution sources
- Meteorological data and forecast, containing lightning data (historical and online data monitored by the control room operators) and risk of forest fires forecast based on FWI (available for the current and next day)
- Active forest fires information

GestInc, the incident data base, contains every incident that occurred in the PTS since 2001. Hence, it constitutes a crucial base to perform the characterization and the analysis of the historical data. With harmonized population criteria and accuracy in the process of incident analysis, the data since 2001 is considered of high quality to be used. This application allows the management of the entire incidents' information, increasing the effectiveness of data entering and treatment with strict criteria and therefore obtaining an accurate event analysis and highly reliable records.

The input data used in the risk assessment methodology has to be reliable and constantly updated to be able to provide credible indices. Near future information must be integrated in the model, such as lightning data, forest fires risk and meteorological information. The network, geographical and environmental data and characteristics were gathered and organized for this research. For meteorological, forest fires and operational data, which are used online or valid for a short period of time, automatic updates and interfaces were created to include them, in real time, in the methodology. It is important to point out that each country or region has its own intrinsic characteristics that must be included in the study.

There is no such thing as perfect information, but for this work data collection and organization becomes crucial to obtain better results. This forces the TSO to maintain a promptly updated and well structured asset database with all the required information, keeping this methodology running in the TSO. The need for field input data makes this methodology easier to implement within a TSO structure, where the asset owner and the system operator are the same entity, and joins together, in a unique way, two different realities: system operation and field information, increasing veracity in the results. A combination of field and system operations information is introduced and it can be used in benefit of each other in a broader way than only the risk assessment methodology, such as performance evaluation and asset management.

When comparing to the initial point of our work, data gathering was an issue where we have placed lots of effort with good results. After defining the relevant data, several data preparation algorithms were developed to obtain the necessary inputs for the methodology in an adequate format.

A Geographical Information System (GIS) constitutes the perfect information technology (IT) platform for the organization of all the data used in this methodology. After including all the information in the GIS, it shall be the perfect input data source through time. In order to develop this methodology, the needed

information was gathered and, after concluding it, the next step should be aimed at including all the data in the GIS. Finally, due to the requirement of regular information updates, the GIS must be updated on time and an easy interface to transfer data into the methodology needs to be built.

Chapter 7.

Probabilistic Method

7.1. Introduction

The application of probabilistic methods in power system has become an important topic for researchers and engineers, because by combining consequences and probability, it is possible to evaluate the risk of contingencies. The probability of occurrence of a fault has to consider the actual conditions, identifying which are the areas more exposed to risk. As well as historical fault data, it must also include network characteristics, geographical, geological, environmental and weather data in the calculation. Therefore, near future and current information must be integrated in the model, such as real-time lightning data, forest fires risk, active forest fires and meteorological information, increasing realism in the results. Without the use of this information, the simple use of the historical average failure rate for operational risk assessment would overestimate the risk during periods of normal weather and strongly underestimate the risk during periods of adverse weather.

Facing an adverse weather situation, such as lightning occurrence or a high risk of forest fires, there are TSOs that additionally include specific N-k events, with k>1, in their "must-run" contingencies list, but their likelihood is still the same. The deterministic security assessment does not consider the effect of longer overhead lines, which are more exposed to the action of external factors due to their dispersion over a wide area than the shorter ones; neither the inherent characteristics of the geographical area where they are deployed nor the actual presence of the fault's cause, which increases significantly its probability.

In order to incorporate the intrinsic characteristics of Portugal that affect the likelihood of the occurrence of faults and thus actual risk, information gathering as described in chapter 6 is crucial.

The probability results that are presented in this chapter for the second semester of 2009 uses information until the end of 2008, which was updated in the beginning of January 2009. However, some of the presented data that is not directly used as input may already consider 2009. To calculate probabilities in 2010, all the inputs that are used have to be updated with the data until the end of 2009.

7.2. The probability of fault

The probability of fault occurrence on a line can be modelled using the Poisson distribution with a constant fault rate [21]. From the Poisson distribution formula, the probability of no fault in the time period t is given by equation (7.1) and the probability of fault in the time period is calculated as in equation (7.2).

$$Probability_{no\ fault} = \frac{e^{-\lambda \cdot t}(\lambda \cdot t)^0}{0!} = e^{-\lambda \cdot t} \qquad (7.1)$$

$$Probability_{fault} = 1 - e^{-\lambda \cdot t} \qquad (7.2)$$

where λ is the average failure rate for the considered period and t the period duration. If $\lambda t << 1$, equation 7.2 can be approximated by $\lambda \cdot t$. The average failure rate can be replaced by the frequency of

fault occurrence, obtained from historical data, since the duration of a fault is always extremely short [21].

7.3. Correlations

In order to assess the importance of some of the available variables that were considered as meaningful, aiming their integration in the methodology that is being developed, several correlation calculations were performed. Correlations between faults, relative humidity, wind speed and precipitation were not done, because of data unavailability. These meteorological data types may be meaningful when analysing events caused by pollution combined with fog.

7.3.1. Temperature

Temperature is a crucial parameter to determine the transmission capacity of grid elements (such as OHLs, transformers, auto-transformers, phase-shifters, etc.), because it influences directly the thermal loading of components. Figure 7.1 presents the absolute value of the correlation of faults per cause with the temperature and it is concluded that no cause is strongly correlated with temperature. Hence, temperature is not a sufficient parameter to model a probability of occurrence for any cause. The correlation with temperature was performed from 2001 to 2008.

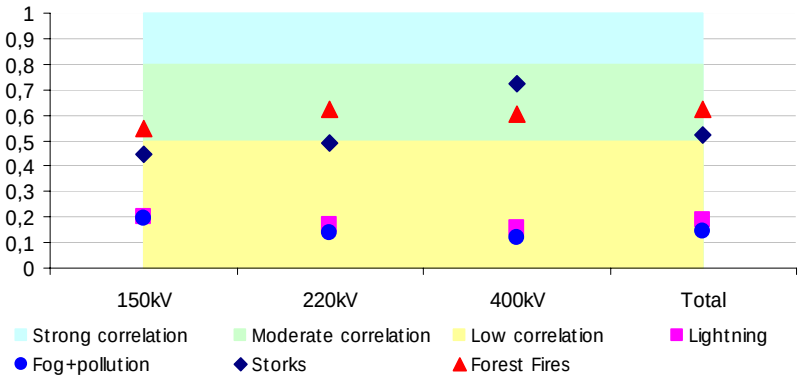


Fig. 7.1 – Correlation coefficient of fault causes with temperature

The correlation between faults per cause and the maximum temperature of the day, on which the fault occurred, was also calculated. Once again, only forest fires present a strong correlation with temperature, about 71%, which is slightly higher than the correlation with the temperature measured just before or simultaneous with the event.

7.3.2. Number of forest fires

From 2001 until 2009, there is a strong correlation, around 90%, between the amount of forest fires in the Portuguese territory and the number of faults caused by them. With the improvement measure described in section 5.3.2, the expectation is that this value will decrease, as well as the amount of faults caused by forest fires, significantly reducing their risk.

7.3.3. Number of lightning flashes

From 2003 until 2009, the correlation between the number of cloud-to-ground flashes in the Portuguese territory and the number of faults caused by lightning per month is 85%. In figure 5.31, the correlation is visible.

7.3.4. Working hours

From 2001 to 2009, 94% of the faults caused by maintenance and operation errors occurred in working hours (considered from 6h to 18h). Hence, for this cause, the division between working periods and non-working periods is important. The majority of these faults happen during work activities inside substations.

7.4. Influence of different causes in the system

Every power system has its own intrinsic characteristics, such as topology, type of generation available, geography, geology, weather, environment, among others. Many of the characteristics may change depending on the current conditions, time of day, month, and season. The current conditions and the intrinsic characteristics of the network must be included in the calculation in order to assess short-term risk, identifying when and which are the areas more exposed to failures.

Due to the fact that the main causes, presented in section 5.3, are dependent on length and on the characteristics of the Portuguese territory, the implementation of this methodology needs accurate information. Most of the geographical information associated with each cause is available per municipality. This is also the main data structure adopted by this method.

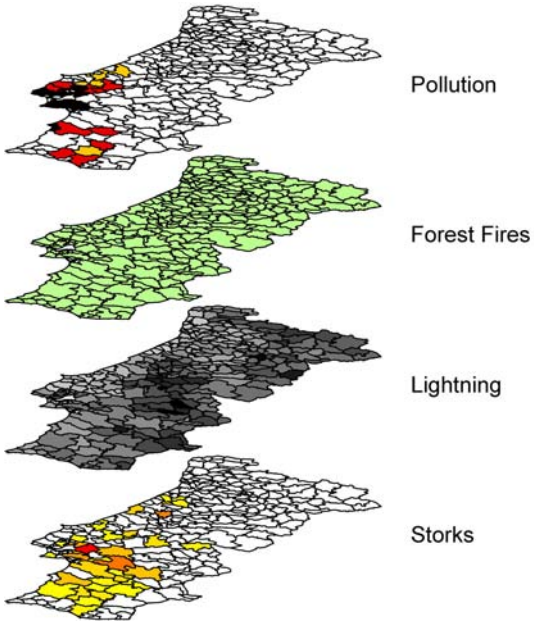


Fig. 7.2 – Geographical influence of the four main causes

Figure 7.2 shows the geographical influence of the four main causes, representing areas at risk for the occurrence of faults caused by each of them. The results presented on the maps per municipality are the following:

- For pollution, it identifies which municipalities are on the insulator's wash plan and the relative degree of pollution.
- For forest fires, Fire Weather Index (FWI) is daily available from the Portuguese Meteorological Institute [126].
- For lightning, it presents the lightning density calculated from 2001 to 2008.
- For storks, it presents the number of stork nests located in OHL towers.

In terms of length, forest fires and lightning can affect any location of the grid, therefore the total network length is considered, but storks and fog combined with pollution only affect a well defined area of the network. Storks affect approximately 35% of the network's length and fog combined with pollution less than 20%, already considering the installed composite insulators.

As already mentioned in chapter 5, the four main causes affect mainly the circuit-part of an OHL. In addition to these causes, OHL faults can also be caused by OHL equipment failure or a small group classified in this work as "others", which includes trees, animals (other than storks), acts of vandalism, design errors, and proximity with external objects (like cranes), among others. Faults classified with cause "others" rarely occur individually and therefore they had to be merged to have meaning.

The performance of transformers is influenced, in addition to faults caused by the transformer components, e.g. trip caused by Buchholz relay, also by the intrinsic characteristics of the location where the transformers are installed and the current conditions, such as local fauna. For busbars, the main causes of faults are fog in combination with pollution, within an identified area, and internal origin group of causes, such as equipment, human errors and protection or control system anomalies. Internal origin group is composed by causes that affect equally the bays associated with other grid elements. For OHLs and transformers, this group of causes, when not causing busbar faults, is always associated with the circuit-ends, except for the OHL equipment.

The different fault causes are assumed to be statistically independent, which makes it possible to calculate the probability of an OHL circuit-part, transformer, busbar or circuit-end, considering all causes, as in equation (7.3).

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i) - \sum_{j=1}^{n}\sum_{\substack{i=2 \\ j<i}}^{n} P(A_j A_i) + \sum_{j=1}^{n}\sum_{\substack{i=2 \\ j<i<k}}^{n}\sum_{k=3}^{n} P(A_j A_i A_k) - \ldots + (-1)^{n-1} \cdot P(A_1 A_2 \ldots A_n) \qquad (7.3)$$

where A_i, $i = 1,2,\ldots,n$ are the probability of occurrence of random events due to each $cause_i$.

7.5. Grid elements for probability calculation

7.5.1. The overhead line

An OHL connection between two substations consists of three different and independent parts as shown in figure 7.3, namely the circuit-part and two circuit-ends. Each circuit is divided into n segments composed by n-1 towers and the two end substations' terminating structures. Each segment is located within a region, which is consequently affected by its intrinsic characteristics, such as environmental and geological, and also by current conditions, such as weather and forest fires. The faults caused by OHL equipment are included in the circuit-part.

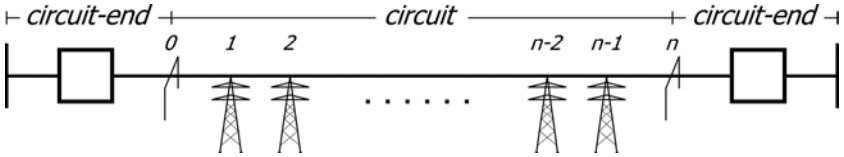


Fig. 7.3 – Overhead line scheme for probability calculation

The total length of an OHL is given by (7.4), where l_i is the distance between two towers, including the terminating structures. For each tower, the coordinates are defined in WGS84 GPS coordinates

$(latitude_i, longitude_i)$ and the distance between two towers is calculated using the great-circle distance formula after converting the coordinates from degrees to radians, as in (7.5).

$$lenght_{total,OHL_i} = \sum_{i=1}^{n} l_i \quad (7.4)$$

$$l_i = r \cdot arccos(sin(latitude_i) \cdot sin(latitude_{i+1}) + \\ + cos(latitude_i) \cdot cos(latitude_{i+1}) \cdot cos(longitude_{i+1} - longitude_i)) \quad (7.5)$$

where r is the radius of the earth.

The length of each OHL per municipality was calculated from the municipality borders and the OHL towers coordinates.

The underground cables represent in 2009 less than 1% of PTS total length and are affected by different problems, such as digging activities and cable junctions (weak points). However, in the PTS historical data from 2001 to 2009, there are no records of faults in this type of grid element. Therefore and for the moment, they will not be considered in the analysis.

7.5.2. The transformer

The transformers and autotransformers are also composed of three independent parts, the unit and two circuit-ends, as shown in figure 7.4.

Fig. 7.4 – Transformer scheme for probability calculation

7.5.3. The busbar

The busbar scheme for probability calculation considers all busbar faults, i.e. faults located in the inner area defined by the current transformers (independently of their cause) as shown in figure 7.5.

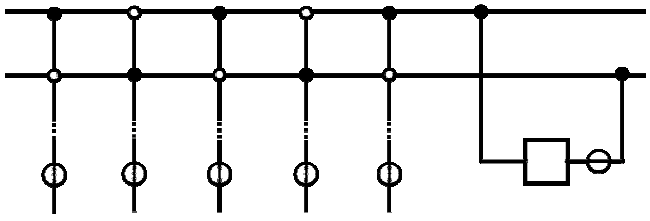


Fig. 7.5 – Busbar scheme for probability calculation

7.6. Probabilistic method for OHL circuit-part

For each cause that depends on length (namely storks, lightning, forest fires, fog combined with pollution, OHL equipment and others), the probability of fault is calculated taking into account the yearly average failure rates, the geographical, geological, environmental and weather influence, and using weighting factors based on location which will affect the considered length at risk and the current conditions. The total probability of faults in an OHL circuit-part is determined by the probability of occurrence of each individual cause, where the probability of $cause_i$ per OHL_k is equal to (7.6).

$$prob_{cause_i,OHL_k} = \left\lfloor \lambda_{cause_i}(m,p,u) \times LR_{cause_i,OHL_k} \right\rfloor \cdot t \qquad (7.6)$$

where m is the month, p is the day period, u is the voltage level and t is the analysis duration (for online assessment this is typically 1 hour); $\lambda_{cause_i}(m,p,u)$ is the average failure rate and LR is the length at risk of OHL_k, both per cause.

7.6.1. Failure rates

In case of OHLs, the failure rates are calculated yearly in order to take into account the significant changes in length of the Portuguese transmission network in the last years. The historical number of faults per km is calculated per cause, month, day period and voltage level for each year as in (7.7).

$$Iq_{k,cause_i}(m,p,u) = \frac{n^o\ of\ \ faults_{k,cause_i}(m,p,u)}{C_{k,cause_i}(u)} \qquad (7.7)$$

where again m is the month, p is the day period and $C_{k,cause_i}(u)$ is the OHL total length affected by the i^{th} cause in the k^{th} year and voltage level u. Therefore, for each cause, the failure rate is expressed as number of faults per km, per month, per day period and per voltage level.

The average failure rate based on historical data was calculated dividing the faults in four day periods (of 6 hours each: 0-6h, 6-12h, 12-18h, 18-24h) per month, after performing the full characterization of all incidents regarding all causes, location, time and season of occurrence. The analysis also included the actions taken to improve performance for each cause, when applicable, and it is presented in chapter 5.

The independent failure rates for the causes that are not dependent on length are integrated in the circuit-end probability. The seasonal and time characteristics are directly incorporated in the failure rates, but the remaining information is included in the “length at risk” value, which is defined further ahead in this chapter.

The choice of the 4 period divisions was made to have some statistical meaning, because when applying shorter periods many values would be zero. With more data, results have more statistical meaning and it may be possible to shorten the duration of the periods, with the limit of 24 periods of 1 hour each, depending on the number of zeros in the failure rate per cause matrix. At the moment, the few periods that still have zeros, mainly in seasonal causes, are accepted just like any other number. Failure rates are updated every year in January with the rest of the statistics of faults.

Equation (7.8) represents the yearly average failure rate scaled to the considered day periods, where T is the average number of hours per month in each of the four day periods and n the number of years under analysis.

$$\lambda_{cause_i}(m,p,u) = \frac{1}{nT} \cdot \sum_{k}^{n} Iq_{k,cause_i}(m,p,u) \qquad (7.8)$$

For each cause, the failure rate is expressed in number of faults per km, per month, per day period and per voltage level. For short-term analysis, performed every hour using State Estimator snapshots, T is equal to approximately 183 hours, because of the daily 6 hours periods per month.

7.6.2. Length at risk calculation

The considered "length at risk", in km, associated to each fault depends on the cause and on the location. It is calculated for every OHL per cause per municipality, as in (7.9) and subjected to (7.10). Due to this fact, for each cause, different weighting factors (α) were defined for each of the 278 municipalities.

$$OHL_k \ length\,at\,risk_{cause_i,municipality_j} = length_{municipality_j,OHL_k} \cdot \alpha_{cause_i,municipality_j} \qquad (7.9)$$

$$length\,at\,risk_{cause_i,OHL_k} = \sum_{j}^{n} OHL_k \ length\,at\,risk_{cause_i,municipality_j} \leq lenght_{total,OHL_k} \qquad (7.10)$$

7.6.2.1. Storks

For storks the information about the number of nests per tower and the number of towers with nests, is available per municipality and is updated yearly, enabling the calculation of the length affected by storks per each OHL. This weighting factor aims to take into account the size of the stork population, since the number of animals also determines the likelihood of the influence on adjacent municipalities.

In case of storks the borders cannot be strict; storks fly and also stand in nearby towers without nests. Hence, it may happen that the affected length occasionally surpasses the j[th] municipality border. In fact, if one tower does not have nests, but it is located in the vicinity of other towers with nests, there is a non-negligible chance of faults caused by storks. Actually, the chance increases near food sources. From the 278 municipalities, only 37 have towers with stork nests and the affected area where the faults occur is identified. Thus, for each municipality *j*, the weighting factor was defined as in (7.11).

$$\alpha_{storks_j} = \left(total\ number\ of\ stork\ nests\ located\ in\ towers \Big/ total\ number\ of\ towers \right)_j \qquad (7.11)$$

Figure 7.6 presents the relation of stork nests and towers with nests with the number of towers per municipality in the end of 2008. It is possible to observe that only two of the municipalities (Montemor-o-Novo and Golegã) have a α_{storks} bigger than 1, representing a very high density of storks in the area.

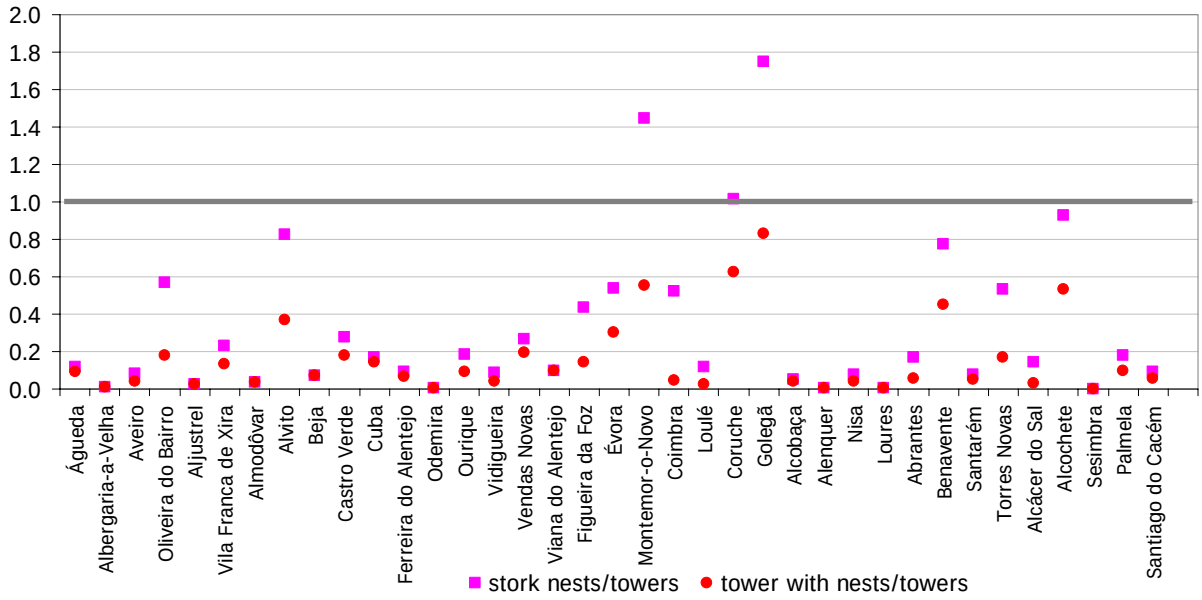


Fig. 7.6 – Relation of stork nests and towers with nests with the number of towers per municipality

7.6.2.2. Fog in combination with pollution

For fog in combination with pollution, the affected OHL towers are identified by the need to wash, which is based on maintenance department experience. For this work, it is identified which municipalities are on the insulators' wash plan and their relative degree of pollution. It is confirmed by the analysis of faults' historical data that the identified regions are the ones where these kinds of faults actually occur. For each municipality and for each OHL, the factors are defined as in (7.12) and (7.13).

$$\delta_{fog_j} = \begin{cases} 1 & if\ the\ j^{th}\ municipality\ wash\ area = yes \\ 0 & if\ the\ j^{th}\ municipality\ wash\ area = no \end{cases} \tag{7.12}$$

$$\alpha_{fog_j} = \delta_{fog_j} \left[\left(\frac{NT_{total} - NT_{composite}}{NT_{total}} \cdot 1 \right) + \left(\frac{NT_{composite}}{NT_{total}} \cdot \beta \right) \right]_{OHL_k} \tag{7.13}$$

where NT is the number of towers of OHL_k and β a performance index to take into account the risk reduction by the installation of composite insulators. For contingencies caused by fog in combination with pollution, the substation terminating structure is also included, because it is equally equipped with composite insulators when necessary and flashovers can occur at this location.

Composite insulators are being applied since 2004 in areas where fog combined with pollution causes faults, in order to improve the performance of OHLs, in other words, the expected value of β is much smaller than one. A limited number of those OHLs have been totally equipped with composite insulators. Up to now, the number of faults due to fog combined with pollution in the OHLs that were completely equipped with composite insulators has become zero after the installation, confirming a very low value of β. Therefore, without enough historical data, for now, β cannot be precisely determined and is assumed to be equal to zero.

In the OHLs that are partially equipped, some faults caused by fog combined with pollution still occur. In one 400kV OHL located in the Lisbon area, there were two faults (one in 2007 and another in 2008) of which it was not possible to determine the exact location, so they could be located inside or outside of the composite area. Assuming the worst and less likely case, to consider the faults inside the composite area β would be equal to $2/185 = 0.01$ (for the OHLs with composite insulators, the number of faults after installation divided by the total number of faults before insulators in the period under analysis). As shown in figure 7.7, in OHLs with a low percentage of composite insulators, the risk level is dominated by the non-composite insulators. Only on areas with a high percentage of composite insulators, their performance determines the risk level.

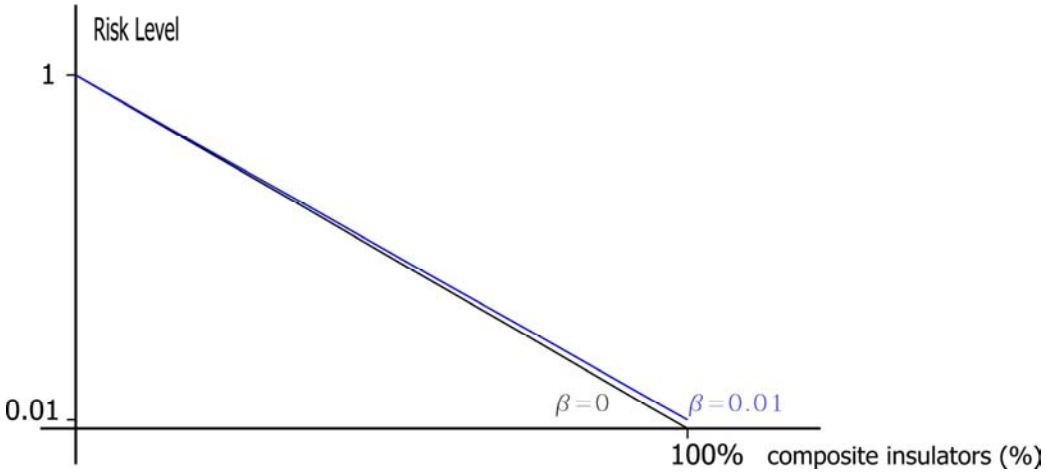


Fig. 7.7 – Analysis of the installation of composite insulators in the PTS from 2001 to 2009

The table supporting this calculation, which contains all the faults caused by fog combined with pollution and the indication of the installation of composite insulators per OHL, from 2001 to 2009, is presented in appendix H. In order to determine the value of β, this analysis will be performed once a year.

7.6.2.3. Forest fires

For forest fires, the risk level based on the daily calculation of the Fire Weather Index (FWI) is made available by the Portuguese Meteorological Institute and provides significant information about the OHLs that may be in danger in a certain day. For each municipality, a risk indicator with 5 levels (from reduced to very high) is presented. Online, the information of the active forest fires in the country, given by the Civil Defence coordination centre, must also be considered, changing only if needed the level of risk in the affected municipalities.

In order to determine the weighting factor α_{fire_j} per municipality, a frequency analysis based on historical data was made for each risk level. Despite the little amount of historical data available, since 2007, for each fault caused by forest fires until the end of 2009, the location of the forest fire and the risk level of the respective municipality were identified. Using these data, a frequency analysis was made and the cumulative frequency was calculated, as in figure 7.8. The knowledge acquired based on experience, after several years of incident analysis, is also used to prove and ensure the effectiveness of this index.

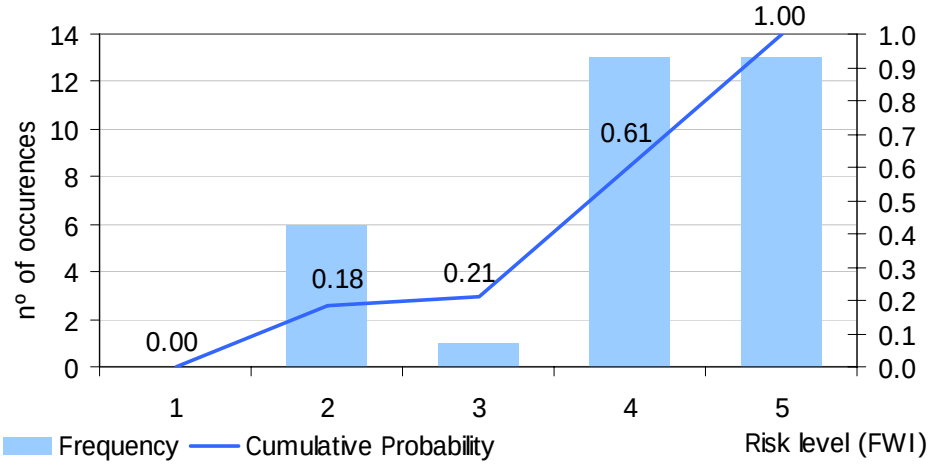


Fig. 7.8 – Risk level of the municipalities where forest fires caused faults (2007-October 2009)

Hence, for each risk level, the cumulative probability value is used, as in equation (7.14), and in case of an active forest fire in a municipality, the respective risk level will be equal to 1, independently of the previous one. The α_{fire_j} values will be updated every time a new event occurs.

$$\alpha_{fires_j} = \begin{cases} Risk\ level_j = 5 \vee active\ fire_j = yes & \Rightarrow \alpha_{fires_i} = 1 \\ Risk\ level_j = 4 & \Rightarrow \alpha_{fires_i} = 0.61 \\ Risk\ level_j = 3 & \Rightarrow \alpha_{fires_i} = 0.21 \\ Risk\ level_j = 2 & \Rightarrow \alpha_{fires_i} = 0.18 \\ Risk\ level_j = 1 & \Rightarrow \alpha_{fires_i} = 0 \end{cases} \qquad (7.14)$$

Due to the fact that the probability of occurrence of faults caused by forest fires is based on average failure rates, it may occur that the failure rate is zero (normally in periods of winter months) and the risk of forest fire is high, like it happened in March 2009 in a 400kV OHL that tripped because of a forest fire at 4h00. This is considered an exceptional event, because forest fire season starts in May and ends in October. However, with more years of history, the number of periods where the failure rate is zero will decrease and these abnormal events will have a very low failure rate.

7.6.2.4. Other causes

For lightning, a completely different approach was adopted and is described in section 7.6.3. For the remaining causes affecting OHLs' circuit-part, such as OHL equipment, α_{cause_i} is equal to 1, since they affect the total length of each OHL, and the probability is calculated as in (7.6). No special current conditions are considered, because they can happen unexpectedly anywhere and at any moment.

7.6.3. Lightning backflash rate

Lightning assumes a preponderant role as one of the primary causes of faults in transmission systems all over the world. OHLs are good attachment points for lightning and their route affects the exposure of the line to lightning. The location of the towers, e.g. top of mountains, ridges or in a valley and the soil resistivity of the OHL path are route characteristics that influence the performance of an OHL. A simplified method to evaluate the risk for lightning flashovers in OHLs was developed, which is used to predict the chance of faults caused by lightning, as part of the probabilistic methodology. To describe the stochastic nature of lightning parameters, a simplified probabilistic method for predicting lightning performance of an OHL was developed based on CIGRE and IEEE methods [108]-[145], which are internationally accepted.

The simplifications introduced in the method are considered acceptable, because of the low level of precision of the input data and largely unknown seasonal and daily variations in parameters, such as soil characteristics (e.g. tower footing resistances may exhibit significant seasonal variations). It is therefore considered that an exact prediction of lightning effects in this case will not contribute significantly to the accuracy of line lightning performance estimation. There are two main concerns when evaluating the performance of an OHL due to lightning:

- Shielding failure flashover rate
- Backflash failure rate

The shielding failure rate is the number of flashovers that terminate on the phase conductors. The purpose of the ground wires is to act as collectors of the flashes (shielding) and as much as possible to prevent flashes from terminating on the phase conductors and causing a flashover. The flashover happens if the voltage on the grounded structure produced by the stroke exceeds the line critical flashover voltage (CFO). It may be uneconomical to shield the conductor in a way that absolutely no flashovers occur. Therefore, the location of ground wires of an OHL is normally chosen, on the design level, in such a way that the shielding failure flashover rate (SFFOR) is less than a specific number flashes per 100km-year. The Portuguese regulation, EN50341-3-17 [146], defines that the geometry of the shield wire(s) shall be such to ensure that a flashover due to a direct lightning stroke into the phase conductors is reduced to one per 100 km of line per year. The SFFOR is not considered in detail in the estimation. Its effect is included by introducing a scaling factor (see eq. (7.29)) in the estimation of the backflash failure rate, thus approximating results with historical data.

The vast majority of strokes and flashes terminate on the tower or on the ground wires. A voltage is built up on the tower but also a voltage is induced on the phase conductors, together resulting in a voltage across the line insulation. If these voltages are equal to or higher than the line CFO, backflash occurs, thereby electrically connecting the phase with the tower or ground wire. According to [145], flashovers within the span are possible, but insignificant compared with the flashovers at the tower. Therefore, span flashovers will be neglected.

Reference [108] states that the negative downward flash is the primary concern, because it represents the majority of the flashes that affect power systems (about 85% to 95% of the flashes to tower having heights less than 60 meters on a flat or rolling terrain). In Portugal, the analysis of lightning data recorded by the lightning monitoring system (LMS), between 2003 and 2008, shows that the positive flashes

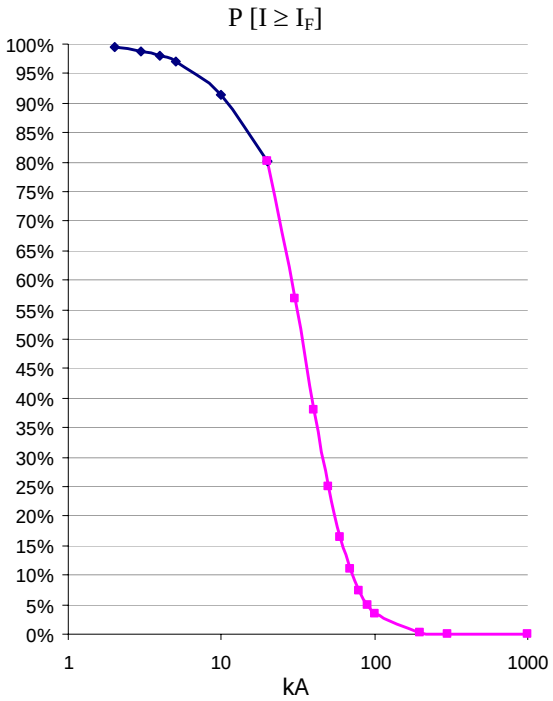
represent approximately 20% and the negative flashes 80% of the total amount, which is comparable to what is presented in international data.

Tower height is also a very important factor in the OHL performance, because more strokes are collected by the taller structure in the surroundings. The majority of OHL towers have heights of less than 60 meters; therefore for risk of fault caused by lightning calculation, only negative downward strokes are going to be considered. This is an accepted approach when evaluating the risk of lightning for overhead lines, because they are more prevalent [145]. This is also valid for the Portuguese transmission system (PTS), as mentioned in section 6.2.1.

7.6.3.1. Data for backflash rate calculation

In order to incorporate the characteristics of Portugal, the Portuguese network and the actual conditions for the calculation of OHL probability of faults, information is again crucial. The following information was utilized:

- Historical fault data: based on the incident data base described in section 6.2.7.1.
- Network data per tower: containing tower geometry, number of ground wires, tower footing resistance, the insulation level and the conductors' diameter (for the last two, typical values per voltage level are used).
- Geographical and geological data per tower: including OHL tower coordinates, soil resistivity in the location or vicinity of the tower and the municipalities' official administrative borders.
- Lightning data: historical and online data monitored by control room operators and imported from the LMS available in the Portuguese TSO, as described in section 6.2.4.2.
- The current amplitude distribution for the first stroke of negative downward flash approximated by the lognormal distribution as in equation (7.15), where M is the median and β the logarithm standard deviation. Using the distribution parameters suggested by CIGRE, namely M=61.6 and β= 1.33 for I < 20 kA and M=33.3 and β= 0.605 for I > 20 kA. Figure 7.9 shows the CIGRE reference cumulative distribution for negative lightning current amplitudes, first stroke.



$$f(x) = \frac{1}{\sqrt{2\pi}\cdot\beta x}\cdot e^{-\frac{1}{2}\left[\frac{ln\left(x/M\right)}{\beta}\right]^2} \qquad (7.15)$$

Fig. 7.9 – CIGRE reference cumulative distribution
For negative lightning current amplitudes, first stroke.

The shielding failure domain comprises peak current amplitudes of less than 20 kA and the backflash domain comprises of those currents above 20 kA [145]. In chapter 5, it was mentioned that the first lightning stroke may be followed by one or more subsequent strokes, following the breakdown path of the first. The first stroke is considered to be the most severe in creating a line flashover condition [108]; therefore subsequent strokes are neglected in this work.

In case of lightning, the period under analysis for the probabilistic method begins in 2003, because of the reliability of the lightning data recorded by the lightning monitoring system, and ends in December 2008.

7.6.3.2. Tower footing resistance

Soil resistivity and consequently tower footing resistance have a significant impact in the OHL performance, because the tower voltage is highly dependent on them. For each tower in the PTS, the nearest soil resistivity measure was considered. The grounding geometry of the towers in the Portuguese case is mainly composed of four independent rod electrodes connected to each tower's foot with on average 2.1 meters length and buried into the soil (normally 80 cm deep), as shown in figure 7.10.

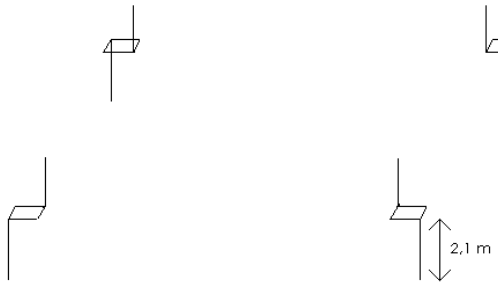


Fig. 7.10 – Typical rod

Due to the fact that tower footing resistance (R_{TF}) measurements only exist for about 60% of the towers of the Portuguese transmission system, the soil resistivity value is used to estimate the tower footing resistance for the towers without measurements. The correlation between the nearest soil resistivity values with the measured tower footing resistance is around 31%, because the soil resistivity was obtained from the resistivity map presented in figure 6.4, which is rather indirect. Some of the used measurements are more than 5 years old. Figure 7.11 shows the tower footing resistance measurements versus the corresponding soil resistivity value.

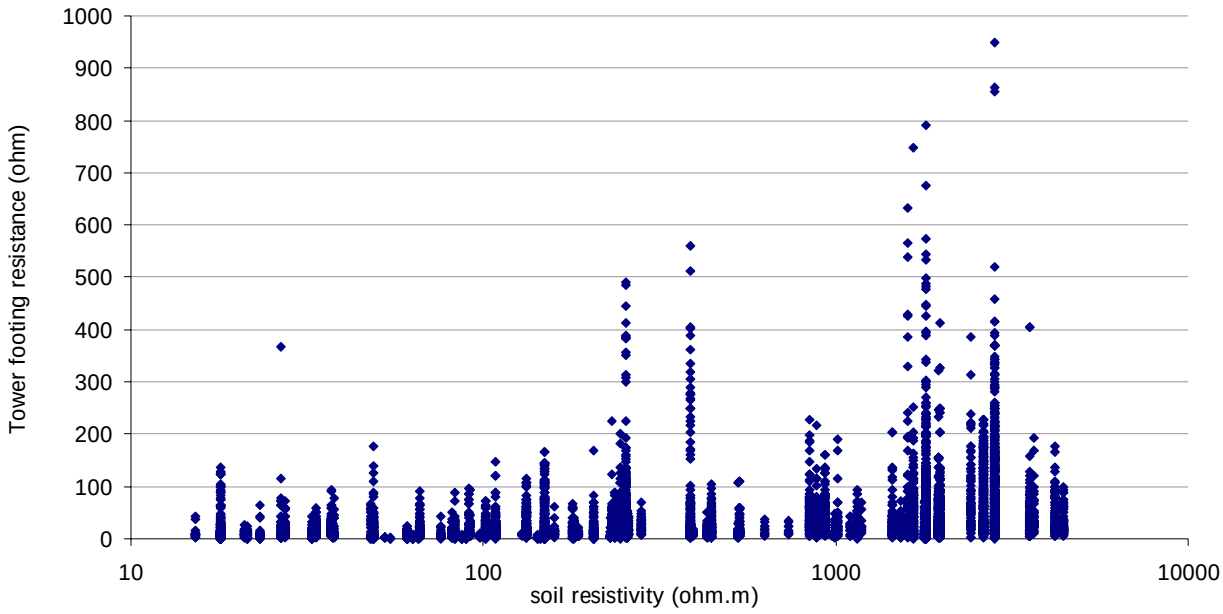


Fig. 7.11 – Tower footing resistance measure versus soil resistivity values

Tower footing resistance is a local measurement that depends on the tower rods (see figure 7.10) in contact with the earth, on the electrode condition and on soil resistivity. The latter is also dependent on many factors, such as soil type and humidity. The used soil resistivity may not represent exactly the soil resistivity of the exact tower location, although it is the best input available (as described in sections 6.2.3 and 6.3.4). The towers located in a high resistivity soil may worsen the entire OHL performance, even if they are just a small group.

A power law is used for R_{TF} estimation, because it has a better approximation than the linear one, as shown in figure 7.12. Thus, for each tower, the tower footing resistance (R_{TF}) can be estimated using equation (7.16), where ρ is the nearest soil resistivity value. Figure 7.12 shows the power approximation of the tower footing resistance.

$$R_{TF}\left(tower_i\right) = 2.809 \cdot \rho^{0.31}\left(tower_i\right) \qquad (7.16)$$

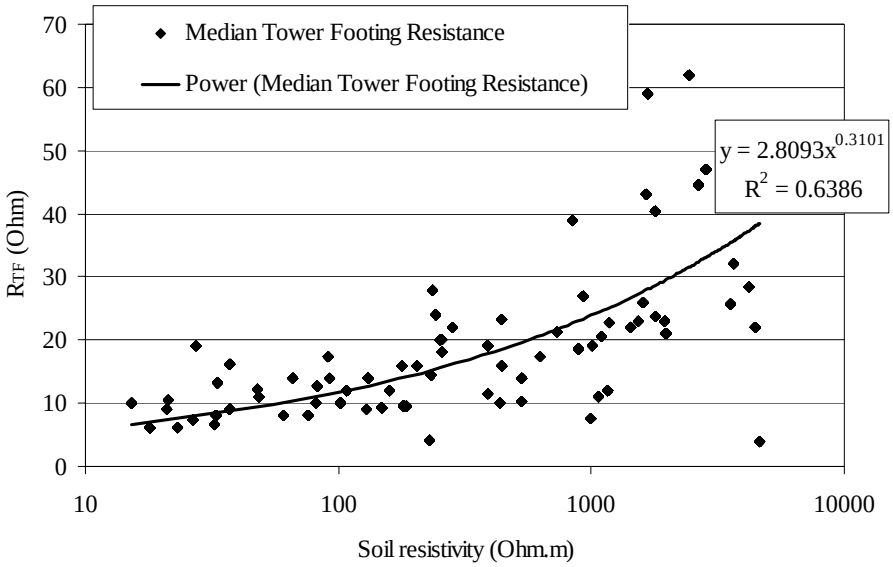


Fig. 7.12 – Tower footing resistance approximation curve

This approximation was based on median values of the tower footing resistance for each soil resistivity value, in order to prevent outliers.

7.6.3.3. Number of lightning flashes and density calculation

The cloud-to-ground flash density provides the basis for the estimation of frequency of lightning effects in electrical power systems. In order to determine the number of flashes per year that terminate on transmission overhead lines, the density of ground flashes (Ng) needs to be calculated. Through the lightning historical data, three possible Ng values were calculated: inside a contour which represents the attractive radius of each OHL, inside a mesh of 4 km^2 squares and per municipality, as presented in section 6.3.2.

There is the expectation that the first method takes into account the local effects of the route of an OHL, for example running in a valley or on top of a hill. However, the historical number of lightning strokes counted in the corridors might be too small for statistical evaluation. The second method uses smaller regions than using municipality data, but bigger than the OHL corridor method and does not take into account the exact route of the OHL. Reference [147] assumes that the area of 4 km^2 is sufficiently small to represent regional variations in flash density. The third method is the basis of the rest of the information used in this work, and uses irregularly sized municipality areas, which are in general smaller in the north and larger towards the south of Portugal. This method was applied because it corresponds to the structure of the other inputs used in this works.

7.6.3.4. OHL exposure to lightning incidence

For the estimation of the number of strokes, the generalized expression derived by Eriksson [108] for the average attractive radius (R_A), in meters, on each side of a transmission line, as in equation (7.17) was used.

$$R_A = 14 \cdot h_T^{0.6} \tag{7.17}$$

where h_T is the total tower height in meters.

An exposure width (EW) is calculated as in equation (7.18) for each OHL. The contour around each OHL, from the beginning until the end, is calculated joining all the exposure widths at each tower and drawing a semi-circle at the end tower, having as radius half of the calculated width at that tower as shown in figure 7.13.

$$EW_{tower_i} = \left(2 \cdot R_A + S_g\right)_{tower_i} = \left(28 \cdot h_T^{0.6} + S_g\right)_{tower_i} \tag{7.18}$$

where R_A is the attractive radius and S_g is the distance between ground wires, in meters. In case of only one ground wire, S_g is equal to zero.

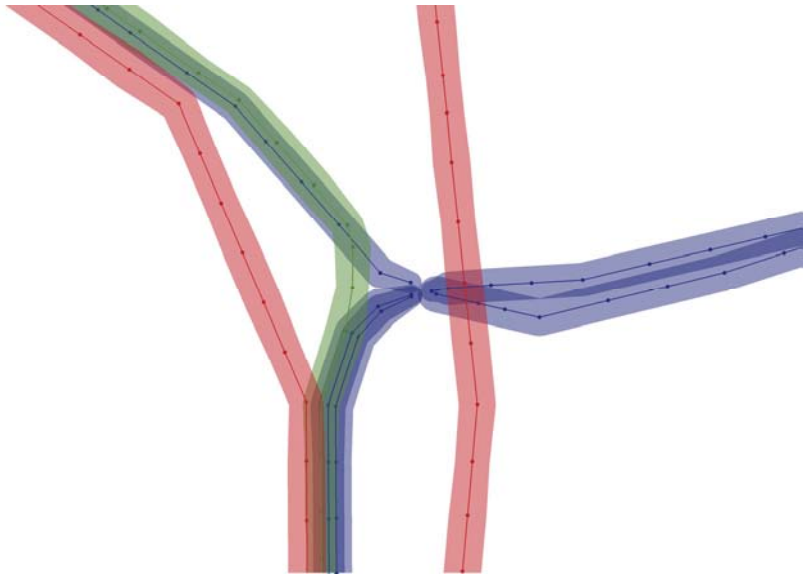


Fig. 7.13 – OHL contour exemplification near a substation

Normally, an OHL begins and ends at a terminating support structure in a substation that is normally lower than the towers and has a ground wire all over that structure, so the distance between ground wires is considered zero. These structures are standardise and assumed to have specific dimensions according to the voltage level, which were used in this work.

A fault inside a substation has generally more severe consequences than a fault in an OHL, thus substations are better shielded and the grounding network has a meshed structure, resulting in a much smaller impedance than the tower footing resistance of an OHL. Therefore, the attractive radius of the terminating support structures will be smaller than the radius for towers. Usually, the effect of end structures falls inside the last tower radius.

The number of cloud-to-ground flashes within the contour of each OHL, from 2003 to 2008, was calculated using the three methods presented in section 6.3.2. For the contour, the number of lightning flashes is directly counted inside the contour. For the other two methods, the contour is divided into sub-areas by intersecting it within the applicable border, being either the municipality borders or the mesh.

The area of each sub-area is calculated, defined as the exposure area (EA), and multiplied by the lightning density of the corresponding municipality or mesh square. Summing the sub-areas of each OHL, it results in the lightning exposure NL_{OHL_i} as in (7.19), where j represents each sub-area.

$$NL_{OHL_i} = \sum_{j=1}^{n} EA_{OHL_{i,j}} \cdot \frac{NL_{DA_j}}{DA_j} \qquad (7.19)$$

7.6.3.5. Critical current calculation

The critical current I_C is the lowest lightning current amplitude that causes backflash. To calculate the critical current, some additional simplifications were assumed, namely:

1. The tower impedance (Z_T) and the effect of the decrease in crest voltage caused by adjacent spans are neglected; because the tower impedance is neglected, the crest values of the tower voltage and the final voltage are identical. Also the reflection from neighbouring towers is neglected.
2. Corona effect is neglected, which would decrease the ground wire surge impedance, thus increasing the coupling factor, enhancing the contribution of ground wires protection. The coupling factor, which is the ratio of mutual impedance between ground wire and phase conductor with the ground wire surge impedance for a stroke in the ground wire, is assumed to be 0.3.
3. The positive polarity gradient for critical flashover voltage (CFO) is assumed to be constant at 560kV/m. The CFO for backflash is 560*S, where S is the insulator's string length in meters.
4. As a simplification, the ground wires surge impedance is assumed to be 330Ω, in case of two ground wires, and 550Ω, in case of only one ground wire. In order to determine these values, equations (7.20), (7.21) and (7.22) were used, considering the average tower height and the average distance between the ground wires (see table 7.1).

   The surge impedance applied to one conductor is given by equation (7.20) [108], where h is the conductor's height and r the radius.

$$Z = 60 \cdot ln\left(\frac{2h}{r}\right) \qquad (7.20)$$

   In case of two conductors, separated by a distance d_{12}, the mutual surge impedance between conductors is shown in figure 7.14 and given by equation (7.21) [108].

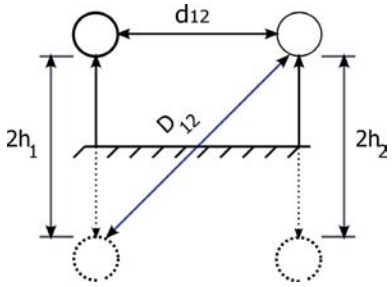


Fig. 7.14 – Conductors' scheme

$$Z_{12} = 60 \cdot ln\frac{D_{12}}{d_{12}} \qquad (7.21)$$

   The combined surge impedance of the two conductors (Z_e) is given by equation (7.22).

$$Z_e = \frac{Z + Z_{12}}{2} \qquad (7.22)$$

Conductors	Average Height (m)	Average Diameter (m)	Average distance between wires (m)	Mutual impedance (ohm)	Surge impedance (ohm)	Equivalent Surge impedance (ohm)
1 Ground wire	38	0.016	0	-	549.5	549.5
2 Ground wires	38	0.016	12	110.8	549.5	330.1

Table 7.1 – Surge impedances for one and two ground wires

5. For the critical current calculation, the equivalent impedance (R_e) is assumed as the parallel between the ground wires surge impedance (Z_g) and the measured footing resistance (RTF), ignoring the ionization around the grounding structure, mainly composed by independent rods, as in equation (7.23). During a lightning stroke, it takes time to build the ionization, thus it is reasonable to neglect it.

$$R_e = \frac{Z_g \cdot R_{TF}}{Z_g + R_{TF}} \tag{7.23}$$

It was decided to include the power frequency effect on the calculation, which will give higher values of backflash rate. The presence of an AC voltage on the phase conductors increases the chance of backflash.

The travelling impulse wave on the ground wires induces a surge voltage on the phase conductor equal to the coupling factor C times the voltage on the ground wires ($C \cdot V_{TT}$). According to [108], using the simplified CIGRE Method, with all the mentioned simplifications, the crest voltage on the tower (V_{TT}) and on the phase conductor (V_C) are defined as in equations (7.24) and (7.25). The crest voltage across the insulation (V_I) is defined as in equation (7.26). The meaning of the various parameters is illustrated in figure 7.15.

$$V_{TT} = R_e \cdot I \tag{7.24}$$

$$V_C = CR_e \cdot I - V_{PF} \tag{7.25}$$

$$V_I = (1-C)R_e \cdot I + V_{PF} \tag{7.26}$$

where I is the stroke current in kA, C is the coupling factor and V_{PF} is the power frequency voltage at the instant of stroke termination in kV.

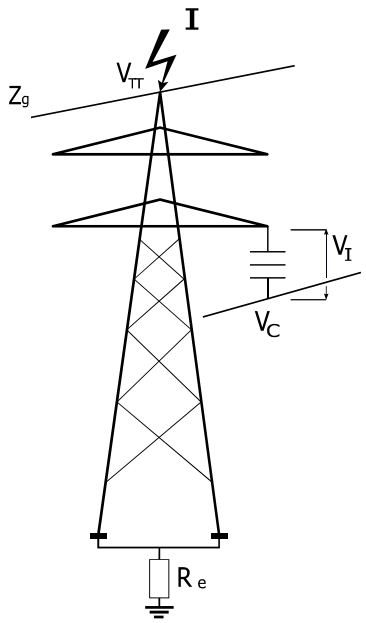


Fig. 7.15 – Surge Voltage at the tower and across the insulation

The power frequency voltage at the instant of stroke termination is given by equation (7.27), Where V_{L-L} is the system nominal voltage (150, 220 or 400 kV). In this work a conservative value of K_{PF} equal to 0.7 is used independently of the conductors' configuration [108].

$$V_{PF} = K_{PF} \cdot V_{LN} \tag{7.27}$$

$$V_{LN} = \frac{\sqrt{2}}{\sqrt{3}} \cdot V_{L-L} \tag{7.28}$$

For a backflash to occur, the voltage across the insulation, as in equation (7.26) must be equal to or greater than the CFO of the insulation. Therefore, the critical current, the minimum current that causes flashover, is determined as in equation (7.29).

$$I_C = \frac{CFO - V_{PF}}{(1-C) \cdot R_e} \tag{7.29}$$

7.6.3.6. OHL backflash rate estimation

The probability of a flashover is the probability that the stroke current I equals or exceeds the critical current I_C. The value of P(I_C) is determined through CIGRE reference cumulative distribution for negative lightning current amplitudes, first stroke, as shown in figure 7.9. The backflash rate (BFR) is the multiplication of this probability by the number of flashes, NL, that terminate on the ground wire and is calculated as in equation (7.30).

$$BFR = NL \cdot P(I_C) \tag{7.30}$$

Due to the fact that each tower within an OHL has different characteristics and the entire OHL performance is influenced by the individual performance of each tower, the I_C (critical current) is calculated per tower. Afterwards, also per tower, the probability of flashover is determined as mentioned. Per OHL, the average of the probability of all its towers is calculated, as in equation (7.31).

$$P_{av}[I_C, OHL_k] = \frac{1}{n} \cdot \sum_{i=1}^{n} P(I_{C,i})_{OHL_k} \tag{7.31}$$

where n is the number of towers that compose the kth OHL, $I_{C,i}$ is the ith tower critical current and $P(I_{C,i})_{OHL_k}$ the probability of flashover of the ith tower.

In order to apply the described methodology to the Portuguese TSO, a scaling factor (SF) per voltage level is introduced, fitting the calculated values to the actual historical fault data, which consists of the ratio between the total number of faults per voltage level and the sum of $NL_{OHL_k} \cdot P_{av}[I_C, OHL_k]$ for all the OHLs of each voltage level. Thus, instead of equation (7.30), equation (7.32) is used per OHL.

$$BFR_{OHL_k} = SF \cdot NL_{OHL_k} \cdot P_{av}[I_C, OHL_k] \tag{7.32}$$

where BFR_{OHL_k} is expressed in number of faults per year.

7.6.3.7. OHL backflash rate results

Due to the fact that the vast majority of strokes and flashes terminate on the tower or on the ground wires, shielding failure is not considered. Therefore, the expected number of faults caused by lightning will be equal to the BFR.

The described method was applied to all PTS overhead lines and, to assess the quality of the prediction per OHL, the actual number of faults per year was compared with the calculated expected number of faults (BFR_{OHL_k}), within the period under analysis. For new OHLs and for existing ones with significant changes in the topology, the proportion of the time in service was taken into account.

Figures 7.16, 7.17 and 7.18 show the relation between the expected number of faults and the actual number of faults in the respective voltage level, during the six years under analysis. The BFR value per OHL is presented in appendix I.

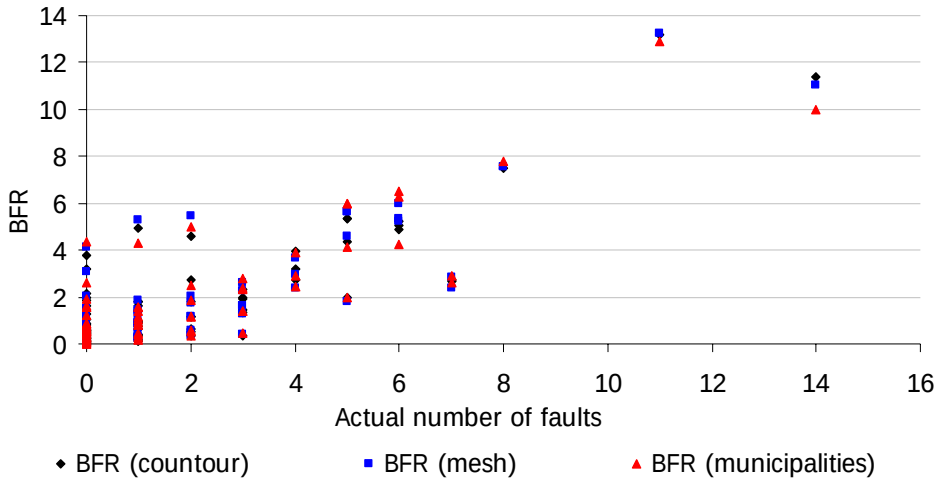


Fig. 7.16 – Expected number of faults versus actual number of faults for 150 kV network

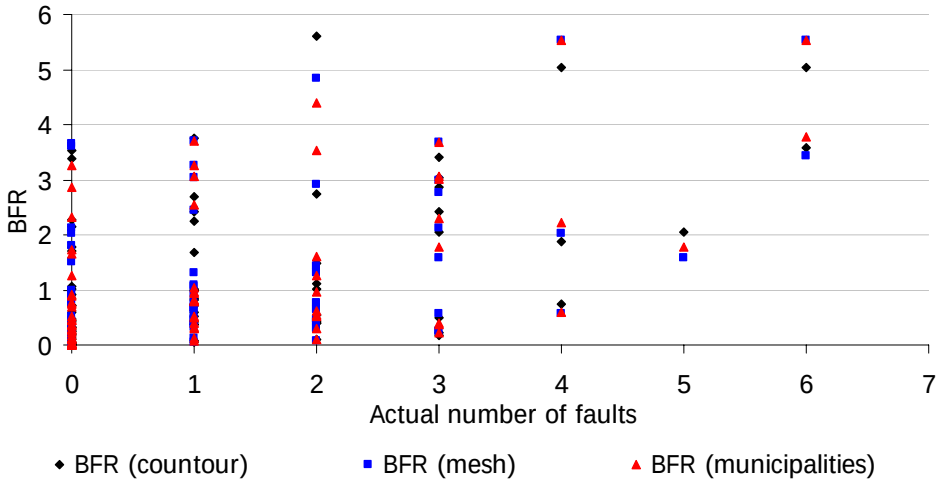


Fig. 7.17 – Expected number of faults versus actual number of faults for 220 kV network

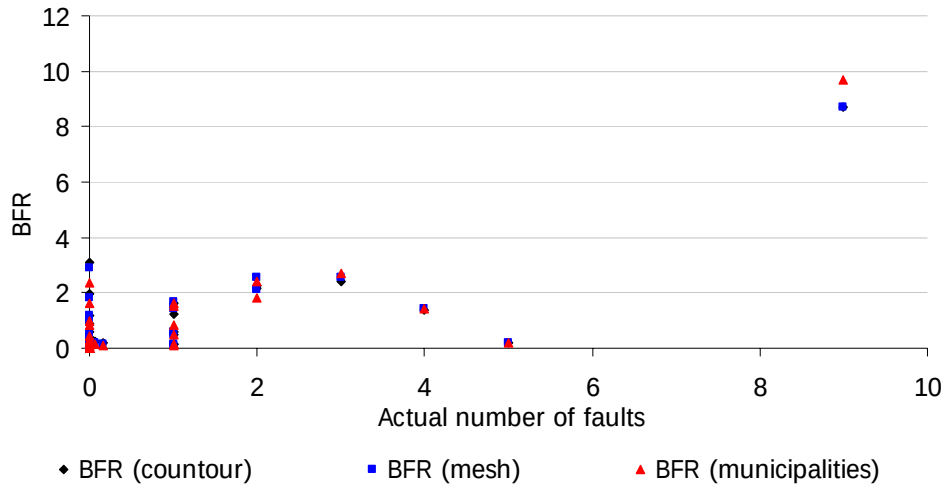


Fig. 7.18 – Expected number of faults versus actual number of faults for 400 kV network

In table 7.2, the calculated correlation values are presented.

Voltage level	Contour	Mesh	Municipalities
150 kV	0.85	0.84	0.84
220 kV	0.55	0.54	0.58
400 kV	0.78	0.79	0.81

Table 7.2 - Correlation between the expected number of faults and the actual number of faults

It is possible to conclude that the three analyzed options give very similar results. The results for the 150 and 400 kV present a strong correlation with the past data, giving a good estimation of faults. The correlation for the 220 kV is weaker, thus decreasing the trust in the estimation.

For phenomena as unpredictable as lightning and with so much inaccuracy and lack of data, a moderate correlation between the expected and the actual number of faults was expected and indeed achieved.

To complement this analysis, the absolute error was calculated per OHL, being the difference between the estimation and its actual values. In order to assess how close the predictions are to the eventual outcomes, without considering their direction, the mean absolute error (MAE) was calculated, as in equation (7.33).

$$MAE = \frac{1}{n} \cdot \sum_{i=1}^{n} \left| f(x_i) - y_i \right| \qquad (7.33)$$

where $f(x_i)$ is the prediction and y_i the actual number of faults in the period under analysis.

Voltage level	Contour	Mesh	Municipalities
150 kV	1.0	0.99	0.99
220 kV	0.85	0.88	0.84
400 kV	0.51	0.50	0.48

Table 7.3 – Mean absolute error between the expected and the actual number of faults

Through the results presented in table 7.3, it is possible to conclude that on average the prediction error is ± 1 fault per OHL in six years, representing ± 0.17 faults per OHL per year. These numbers can be compared with the results presented in figures 7.16 to 7.18.

For each voltage level and considering all OHLs, the maximum absolute error was 4.4 faults in the 150 kV, 3.4 faults in the 220 kV and 4.8 in the 400 kV for the six years, approximately, where the minimum absolute error is zero in all voltage levels. After analysing the worst results, it was identified that in most of those OHLs, the tower footing resistance was mainly predicted through soil resistivity or the quality of the measurement is dubious.

Due to this big variation, the root mean square error (RMSE) was also calculated, as in equation (7.34), because it gives higher weight to larger errors.

$$RMSE = \sqrt{\frac{1}{n} \cdot \sum_{i=1}^{n} \left(f\left(x_i\right) - y_i \right)^2} \qquad (7.34)$$

Table 7.4 results are not more than the average magnitude of the error of the fault estimation per voltage level, which gives an insight about the dispersion of the data under analysis. Once again, the three methods have very similar results.

Voltage level	Contour	Mesh	Municipalities
150 kV	1.43	1.47	1.44
220 kV	1.29	1.32	1.25
400 kV	1.06	1.05	1.00

Table 7.4 – Root mean square error between the expected and the actual number of faults (6 years)

7.6.3.7.1. Simulations with IEEE FLASH

In order to compare the results of the presented method with the IEEE FLASH method [144], [148], [149], additional calculations were performed for 10% of the PTS overhead lines (6 of 150kV, 8 of 220kV and 6 of 400kV). For the subset under analysis, only the municipalities' method was used in the comparison. In table 7.5, the calculated correlation values are presented.

Voltage level	IEEE flash	Municipalities
150 kV	0.75	0.98
220 kV	0.90	0.86
400 kV	0.83	0.84

Table 7.5 – Correlation between the expected and the actual number of faults

The MAE is 0.69 for the IEEE FLASH results and 0.13 for the presented method results, considering only the 20 OHLs under analysis. The difference between the errors of each method is justified by the scaling factor applied (see equation (7.32)) that approximates the results with the actual number of faults.

Figures 7.19, 7.20 and 7.21 illustrate both methods results per year and the comparison of the simplified method with IEEE FLASH results confirms the validity of the simplifications made.

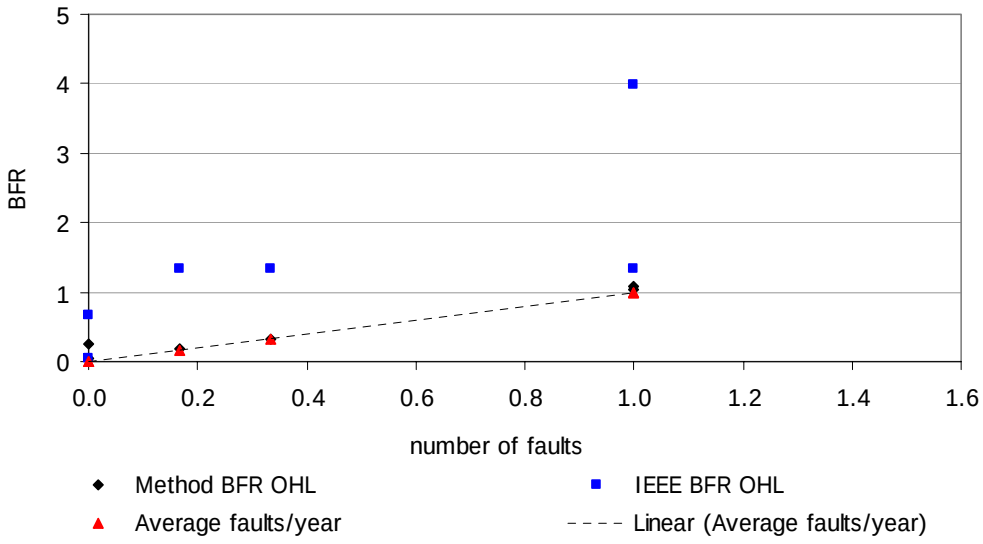


Fig. 7.19 – The two methods results versus actual number of faults for the 150kV OHLs

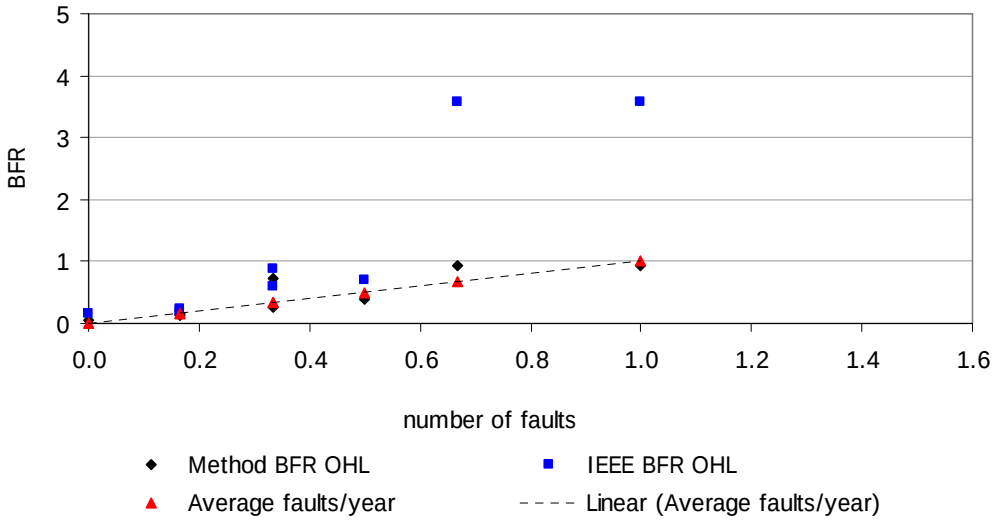


Fig. 7.20 – The two methods results versus actual number of faults for the 220kV OHLs

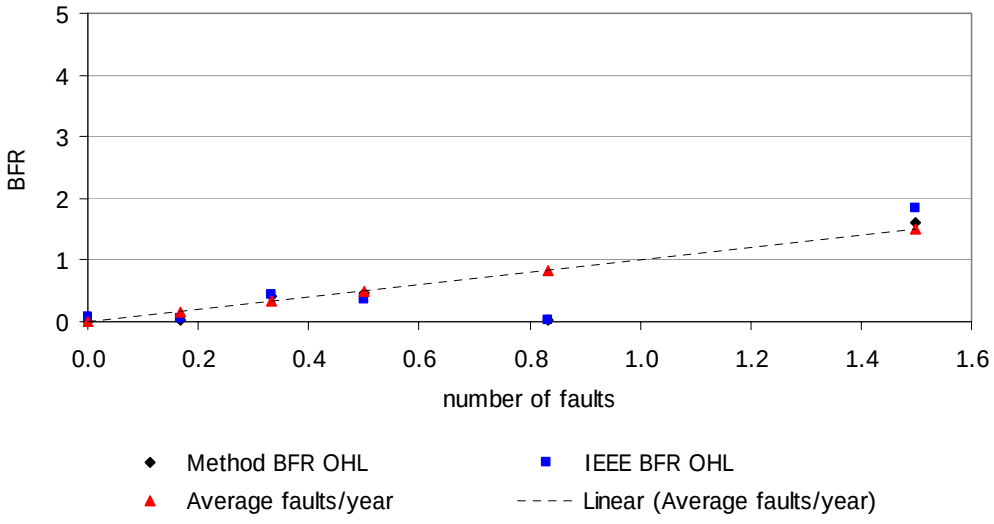


Fig. 7.21 – The two methods results versus actual number of faults for the 400kV OHLs

7.6.3.8. Online conditions

There is only risk of faults caused by lightning when there is actually lightning activity. Therefore, the online conditions presented by the lightning monitoring system and the meteorological institute forecast must be considered. In addition, for short-time period analysis, such as 1 hour, as it is intended to be done in the overall risk assessment methodology, it is not reasonable to consider the BFR per OHL per year simply divided by the number of hours within 1 year. In fact this would underestimate the risk when it is present, because there are many periods without lightning and some periods with a high concentration.

Due to this fact, the estimation of how often the observation "lightning occurs" within a specific period and location is made, calculating N/P where N is the number of periods that have lightning and P the total number of periods, within a specific area. This calculation was performed using the LMS recorded data from 2003 to 2008. For instance, dividing a year in one hour periods (8760 periods), around 24% of the considered periods have at least 1 lightning flash recorded within the country. Considering periods of 24 hours and the whole of Portugal, 80% of the days had lightning activity. Therefore, the expected number of faults caused by lightning, per OHL, for the next t (duration of the analysis in hours) is determined as in equation (7.35).

$$probability_{OHL_k} = BFR_{OHL_k} \cdot \frac{t}{8760} \cdot \delta_j \qquad (7.35)$$

The duration and location of the analysis and the online conditions are taken into account with δ_j, as in equation (7.36).

$$\begin{cases} \delta_j = 0, & \textit{without lightning activity or forecast} \\ \delta_j = 0.5 \cdot \left(\frac{N}{P}\right)^{-1}, & \textit{with only lightning forecast or LMS unavailability} \\ \delta_j = 1 \cdot \left(\frac{N}{P}\right)^{-1}, & \textit{with actual lightning activity} \end{cases} \qquad (7.36)$$

where j represents the North or South part of the country.

After analyzing the lightning historical data, it was concluded that often the lightning activity would only affect the north or the south of Portugal, thus the division North/South of the country by using the accurate borders of the centre districts. If a right-of-way of an OHL is located both in North and South, the proportion of the length will be calculated in case of lightning activity in only one region.

The $(N/P)^{-1}$ value, also called multiplier, depends on the duration of the analysis. Dividing the country in North and South, the N/P value is similar for both areas as shown in table 7.6. Therefore, we use the average for both areas. Further details were presented in section 6.3.4.

Interval Duration (hours)	North		South	
	N/P (%)	$(N/P)^{-1}$	N/P (%)	$(N/P)^{-1}$
24	62.0	1.6	61.5	1.6
12	46.2	2.2	46.4	2.2
8	39.8	2.5	38.7	2.6
6	34.3	2.9	34.4	2.9
4	28.7	3.5	28.6	3.5
3	25.1	4.0	25.3	4.0
2	20.7	4.8	20.9	4.8
1	**14.6**	**6.8**	**15.1**	**6.6**
0.5	10.2	9.8	10.9	9.2

Table 7.6 – Multiplier for North and South

7.6.4. Common cause faults in overhead lines

The risk of multiple contingencies cannot be neglected in the analysis of the probability of fault occurrence. The historical data analysis enabled the identification of the components that are susceptible to common cause failures. It was concluded that common cause failures mainly happen due to lightning, affecting OHLs that share the same towers during the whole or part of their path. As already mentioned in section 5.3.4, about 99% of the faults caused by lightning affect OHLs and 20% of those are common cause faults. The length of OHLs sharing the same tower represents on average 20% of the OHL total length. In section 5.7.1, an analysis of the fault dependency in the Portuguese transmission system was presented. As shown in table 7.7, the amount of common cause faults is significant, considering the total amount of faults caused by lightning in the Portuguese transmission system.

Year	Total	Independent	Common Cause
2001	84	50	34
2002	110	78	32
2003	72	46	26
2004	71	49	22
2005	12	10	2
2006	56	34	22
2007	73	56	17[a)]
2008	63	29	34
2009	72	60	12
Total	613	412	184

One common cause contingency has at least two faults.

a) One common cause contingency affecting three OHLs – two sharing the same tower and one in a very near parallel path.

Table 7.7 – Number and Types of faults caused by lightning

Beyond lightning also forest fires may cause common cause faults. After analysing the faults caused by forest fires, which affect several OHL, the drawn conclusion is: the same forest fire may affect OHL corridors that are composed of more than one OHL, but they rarely fail simultaneously (less than 5% of the faults affect more than one OHL in less than 5 seconds). After analysing the historical data, from 2001 to 2009, forest fires only affect simultaneously two OHLs, which normally share the same towers and right-of-way. Therefore, the majority of faults caused by the same forest fire that affect more than two OHLs mainly occur with intervals of some minutes, and even if some OHLs are disconnected in the same period, the fault does not necessarily occur at the same time. The quasi-simultaneous (less than 5 seconds difference in the trip of more than one OHL) is considered as common cause, because they are disconnected at the same time. The non-simultaneous trips give the operator the opportunity to reconnect the OHL before others trip because of the same forest fire. These are considered independent faults, even if it was not possible to restore them. Another cause of common cause faults, as mentioned in chapter 5, is extreme wind conditions. On the 23rd of December 2009, there were two common cause faults because of extreme wind speed, but these were the only two situations recorded in the considered period for analysis and there is no historical data of wind measurements to evaluate how often wind speed above 160km/h occurs, as the multiplier calculated for lightning (see table 7.6). Therefore, no calculations are performed, but this is recommended for future developments.

Common cause failures are dependent events; two events A and B are said to be dependent if

$$P(A \cap B) \neq P(A) \cdot P(B) \tag{7.37}$$

Dependence can be classified as intrinsic or extrinsic, as already described in section 3.2. In this work only common cause faults from extrinsic dependencies are analysed, where a common cause failure is defined as the failure of more than one component due to a common cause. Figure 7.22 presents the reliability model for common cause forced outages.

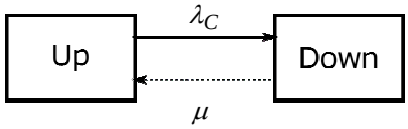


Fig. 7.22 – Model for common cause forced outages [21]

The repair rate (μ) is beyond the scope of this work, although it is important to mention that a common repair rate for a common failure only happens if the automatic recloser reconnects the OHLs within the same timeframe. Otherwise, with human intervention the OHLs are reconnected independently and with different response times.

7.6.4.1. Beta factor model

Reference [10] presents one of the simplest methods for modelling the impact of common cause faults, which is the beta-factor. In order to illustrate the method, consider a simple redundancy of two identical components B1 and B2. Each component is further divided into independent failure and both affected by common cause failure (CCF), as shown in figure 7.23.

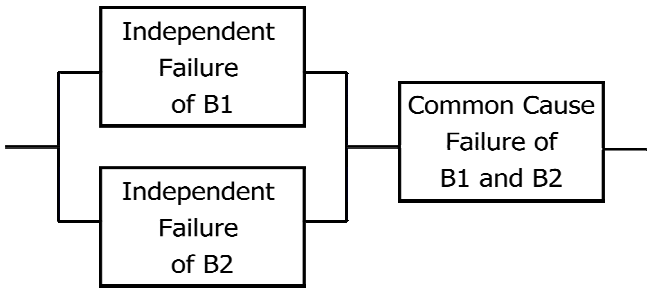


Fig. 7.23 – Reliability block diagram for CCF events

The beta-factor model assumes that: Total component failure frequency (λ_T) = Independent failure frequency (λ_I) + common cause failure frequency (λ_C).

The factor β is defined as in equation (7.38) and λ_C and λ_I are calculated as in equations (7.39) and (7.40), respectively.

$$\beta = \lambda_C \Big/ \lambda_T \tag{7.38}$$

$$\lambda_C = \beta \cdot \lambda_T \tag{7.39}$$

$$\lambda_I = (1-\beta) \cdot \lambda_T \tag{7.40}$$

The failure probability of the two parallel components B1 and B2, considering both independent and common cause faults, is calculated as in (7.41).

$$Q_s = (\lambda_I \cdot t)^2 + (\lambda_C \cdot t) \tag{7.41}$$

Where $\lambda \cdot t$ is an approximation for the probability of fault occurrence modelled by the Poisson distribution with a constant fault rate, as already mentioned in section 7.2.

A point estimate for β is given by equation (7.42).

$$\beta_{estimated} = \frac{2n_2}{n_1 + 2n_2} \tag{7.42}$$

where: n_1= number of independent failures and n_2= number of common cause failures.

For common cause faults that only affect two identical grid elements, $\lambda_C \cdot t$ is used to calculate the probability of occurrence which will be multiplied by the respective severity to obtain the risk of the specific contingency.

7.6.4.2. Results

With the historical data analysis and the total failure rate per OHL or segment of OHL, it is possible to apply the β-factor model for common cause faults in parallel identical OHLs (or segments) that already have common cause faults in their history. This method is valid for OHLs that share entirely the same right-of-way, which can be considered identical components having the same failure rate; this is true for the OHL that mainly trip because of faults caused by lightning. For OHLs that only share part of the total right-of-way, the division into segments is needed and the failure rate has to be calculated for each OHL segment independently. Therefore, the location of the faults has to be determined in order to achieve an accurate statistical analysis.

In case of lightning faults, the backflash failure rate (BFR) is calculated per OHL based on the probabilistic method for lightning performance of an OHL, which was presented in section 7.6.3. This method uses tower geometry, tower footing resistance, insulation level, conductors' diameter, geographical and geological information, to calculate the BFR, which are the same for OHLs that share the same towers. Therefore, these parallel OHLs have exactly the same BFR value.

The common cause failure probability will be used for risk calculation of N-2 contingencies that are included in the security assessment whenever there is probability of lightning. In the case when one of the parallel OHLs, which share the total right-of-way, has more independent faults than the other, but the same number of common cause faults, the maximum of the λ_C is used. In the case of two OHLs that share only part of the right-of-way, which is normally the length of the shortest OHL, λ_C will be calculated considering the shortest OHL, because it corresponds to the common path (see figure 7.24). Assuming that for N-2 only common cause faults occur, the probability of the common cause occurrence will be $\lambda_C \cdot t$.

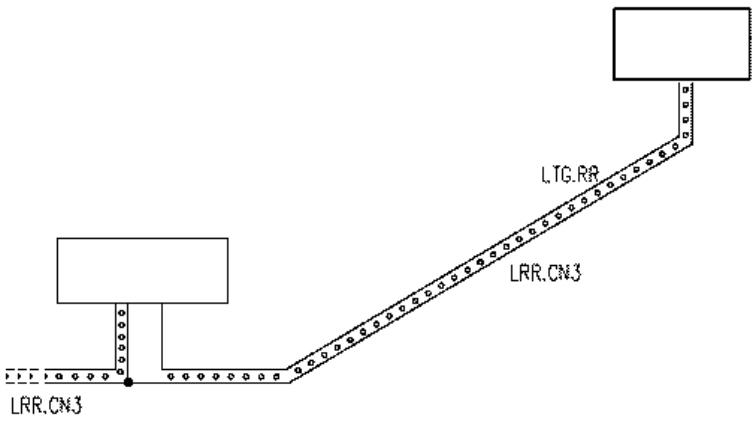


Fig. 7.24 – Example of two OHL sharing part of the right-of-way

Table 7.8 presents the results for the common cause failure rate for faults caused by lightning, from which it is possible to conclude that some OHLs, where β =1, only have CCF faults when affected by lightning.

OHL Names	U(kV)	λ_T (BFR) per year	N° of CCF per year	β	λ_C per year
LPMFF1+LPMFF2	150	0.1978	0.33	1	0.1978
LPMFF4+LFFQAJ	150	0.1011	0.33	1	0.1011
LOQET1+LOQET2	150	0.4836	0.67	1	0.4836
LSNOQ1+LSNOQ2	150	0.9958	0.67	0.9	0.8851
LORVI+LPDVVI	150	0.3986	0.17	0.5	0.1993
LFFTRF1+LFFTRF2	150	0.0173	0.50	1	0.0173
LFRCC1/RDA+LFRCC2/RDA	150	0.1388	0.50	1	0.1388
LMDRPDV1+LMDRPDV2	150	0.6505	2.00	1	0.6505
LPOTN1+LPOTN2	150	0.0837	1.00	1	0.0837
LSNPO2+LSNSI	150	0.3143	0.33	1	0.3143
LVGCL2+LVGCL3	220	0.2975	0.50	1	0.2975
LCGRM2+LCGRM3	220	0.0827	0.00	0	0.0000
LVRVG1+LVRVG2	220	0.1612	0.33	1	0.1612
LCLMC+LCLEJ2	220	0.5031	0.50	1	0.5031
LVGRR1+LVGUR	220	0.4246	0.17	1	0.4246
LRRVM1+LRRCT	220	0.0857	0.33	1	0.0857
LRRCN3/TG+LTGRR	220	0.0378	0.33	0.8	0.0303
LCFFE1/SSE+LCFFE2/SSE	220	0.9238	0.50	0.9	0.7918
LCCFE1/FTL+LCCFE2/FTL	220	0.1319	0.50	1	0.1319
LCFVC1/GVA+LCFVC2/GVA	220	0.5092	0.17	1	0.5092
LALCTL1+LALCTL2	400	0.0202	0.50	0.6	0.0121

Table 7.8 – CCF Rate Results per year for per N-2 events caused by lightning (2003 to 2008)

Figure 7.25 shows the OHL corridors with the worst performance in terms of a higher number of faults per km, regarding faults caused by lightning.

Fig. 7.25 – OHL corridors geographical representation with the higher number of faults per km

In the case of forest fires, the failure rate of independent faults is based on historical data combined with the information of risk of forest fires or active forest fires within a region (e.g., municipality) where the towers of each OHL are located. The information about forest fires will be updated hourly in real-time. Corridors can be affected quasi-simultaneously by forest fires, causing N-k contingencies with k equal to 2, 3 or 4. As already mentioned, these faults represent around 5% of the total number of faults caused by forest fires and many of the corridors defined in the C list up to now did not have any simultaneous trip. Based on historical data, only two OHLs were disconnected simultaneously by the same forest fire and, in case of parallel OHLs, the β-factor model is adequate.

Table 7.9 presents the set of parallel OHLs that were affected simultaneously by the same forest fire and the β value for each pair.

OHL Names	U(kV)	β
LORVI+LPDVVI	150	0.50
LFRCC1/RDA+LFRCC2/RDA	150	1.00
LSNPO2+LSNSI	150	0.50
LVGCL2+LVGCL3	220	0.67
LVGRR1+LVGUR	220	0.25
LCFFE1/SSE+LCFFE2/SSE	220	0.80
LCFVC1/GVA+LCFVC2/GVA	220	0.31

Table 7.9 – OHL pairs and β for N-2 contingencies caused by the same forest fire (2003 to 2008)

However, often within an interval of a few minutes, more than 2 OHLs are disconnected by the same forest fire and they cannot be immediately restored because the fire underneath is causing a permanent fault or fire fighters are working in the corridor. This situation is similar to a cascading event, where OHLs may trip in sequence, although with the uncertainty of a forest fire the sequence is undefined. Table 7.10 presents the groups of OHLs that have tripped non-simultaneously, but were out of service at the same time because of a forest fire.

OHL Names[6]	U(kV)	Years of occurrence
LPTPN+LPTMG	220	2001
LPNVG1+LPNVG2	220	2001, 2002, 2005
LRRLV+LLVRM	400	2002
LBLRM1+LBLRM2	220	2002
LLVRM+LPGRM	400	2002
LBLRM1+LLVRM	220/400	2002,2006
LFTFR+LZRFR+LPGFR	150/400	2003
LPMSN2+LPMSN3	400	2003
LPRBL1+LBLPI	220/400	2003,2004,2005
LPGRM+LPGFR	400	2003
LPNCF1+LPNCF2	220	2003
LPTPN+LBTPN	220	2003
LSNOQ1+LSNOQ2	150	2004
LRRUR+LRARR2	220/150	2005
LRRLV+LRRPI	400	2005
LVGUR+LVGRR1+LVGVM4	220	2005
LPRBL1+LPRBL2/PB+LBLPI+LLVRM	220/400	2005
LVCPR1/MRT+LVCPR2/PP+LAGPR2/MRT	220	2005
LCDVI1/VF+LORVI	150	2006
LRRCN3/TG+LTGRR	220	2006

Table 7.10 – OHL groups disconnected non-simultaneously by the same forest fire

[6] The OHL names were updated to the current designation of the component.

In this case, the best approach is to use the probability of N-1 and N-2 events caused by forest fires and to simulate severity every few minutes, using State Estimator snapshots where OHLs of corridors were already disconnected by previous faults with the same cause. Thus, the severity will be able to reflect the consequences of an N-k event. Even more severe were several forest fires in different regions disconnecting OHLs and creating N-k events with k>3.

For N-3 and N-4 simultaneous events, a specific analysis of the OHL groups that have already tripped together within a corridor needs to be performed, in order to find a common failure rate based on history. This failure rate will be the number of faults per year per each considered group, multiplied by the maximum of the risk of forest fires indices including the municipalities where the corridor is located. For the period under analysis, these failure rates are zero, because this situation has not occurred.

For the N-1 analysis, the total failure rate (λ_T) for both causes is used per OHL in order to always consider the worst scenario.

7.7. Probabilistic method for transformers

The probability of fault occurrence for transformers and autotransformers is based on the average fault failure rate, for each cause, per voltage level and per transformer. Both transformers and autotransformers are added when considering their total number. For probability calculation and statistics, transformers are grouped by the highest voltage level.

The three main causes that affect transformers in the PTS are the transformer itself, its own components and protections (installed in the unit), lightning and a set of other less significant causes. Although the probability in case of transformers is based on historical failure rates, for lightning current conditions are considered, because as previously mentioned without lightning there is no risk of faults caused by it. Therefore, the δ applied for OHLs, as in equation (7.36) is also applied for transformers.

The probability of fault occurrence is calculated as in equation (7.43) for lightning and as in equation (7.44) for the other causes.

$$prob_{lightning,TR}(u) = \lambda_{lightning,TR}(u) \cdot \delta_j \cdot t \qquad (7.43)$$

$$prob_{cause_i,TR}(u) = \lambda_{cause_i,TR}(u) \cdot t \qquad (7.44)$$

where t is the analysis duration (for online assessment this is typically 1 hour).

7.7.1. Failure rates

The historical number of faults per transformer is calculated per cause and voltage level for each year as in equation (7.45).

$$Iq_{k,cause_i}(u) = \frac{n^o\ of\ \ faults_{k,cause_i}(u)}{n^o\ of\ transformers_k(u)} \qquad (7.45)$$

where k is the year; u is the voltage level and i represents the i^{th} cause.

Equation (7.46) represents the yearly average failure rate, with T the number of hours per year of the considered period, e.g. if the failure rate is expressed in faults per transformer per hour, T is equal to 8760 hours.

$$\lambda_{cause_i,TR}(u) = \frac{1}{nT} \cdot \sum_{k}^{n} Iq_{k,cause_i}(u) \qquad (7.46)$$

For each cause, the failure rate is expressed in number of faults per transformer and per voltage level.

7.8. Probabilistic method for busbars and circuit-ends

The probability of fault occurrence for circuit-ends and busbars is also based on the average failure rate, for each cause, per voltage level and in this case either per bay or per busbar. The historical number of faults per circuit-end and per busbar is calculated per cause and voltage level for each year as in equation (7.47), the denominator being the number of elements, bays or busbars per voltage level, respectively.

$$Iq_{k,cause_i}(u) = \frac{n^o\ of\ \ faults_{k,cause_i}(u)}{n^o\ of\ element_k(u)} \qquad (7.47)$$

where k is the year; u is the voltage level and i represents the i^{th} cause.

The yearly average failure rate per voltage level is calculated as in equation (7.48). Therefore, the failure rates are expressed as number of faults per hour per circuit-end or per busbar, respectively, with T equal to 8760 hours.

$$\lambda_{cause_i,element}(u) = \frac{1}{nT} \cdot \sum_{k}^{n} Iq_{k,cause_i}(u) \qquad (7.48)$$

For human errors, it is also considered whether the fault happened or not during working hours, because 94% of these faults occurred between 8h and 18h, from 2001 until 2009. Thus for failure rate calculation, the period from 6h to 18h is considered working hours. Therefore, two failure rates are used: one for faults during working hours, which are much more likely, and another one for faults outside working hours, which are very rare. Thus, in equation (7.48) T is equal to 4380 hours for each period (working and non-working hours).

Some of the factors that may cause busbars faults, generally lie at circuit-end level, namely substation equipment, human errors and protection and control systems, which implies that part of the faults caused by them is associated to busbars and the other part to circuit-ends. These causes do not affect OHL circuit-part or transformers, and beyond them, busbars are also affected by fog combined with pollution and other environmental causes. Fog combined with pollution is a seasonal cause and it is only considered in summer (June, July, August and September), which is in accordance with the historical data. Therefore, two failure rates are used. Outside summer, the failure rate is zero and during summer the failure rate is calculated as in (7.48) with T equal to 2920 hours.

7.8.1. Circuit-ends

The probability of fault in a circuit-end caused by the i[th] cause is given by equation (7.49).

$$prob_{cause_i,end}(u) = \left(\frac{TNF_{cause_i}(u) - BNF_{cause_i}(u)}{TNF_{cause_i}(u)} \right) \times \lambda_{cause_i,end}(u) \cdot t \qquad (7.49)$$

where $TNF_{cause_i}(u)$ is the total number of faults with the i[th] cause in the voltage level u and $BNF_{cause_i}(u)$ is the number of faults in busbars with the i[th] is cause in the voltage level u.

7.8.2. Busbars

For the causes that the circuit-end part has in common with busbars, the probability of fault in the busbar caused by the i[th] cause is given by equation (7.50), where the variables are the same used in equation (7.49).

$$prob_{cause_i,bus}(u) = \left(\frac{BNF_{cause_i}(u)}{TNF_{cause_i}(u)} \right) \cdot \lambda_{cause_i,end}(u) \cdot t \qquad (7.50)$$

Regarding the other causes that affect busbars, the probability of fault is calculated as in equation (7.51).

$$prob_{cause_i,bus}(u) = \lambda_{cause_i,bus}(u) \cdot t \qquad (7.51)$$

7.9. Final fault probability

After calculating the fault probability in all components, separately for each cause, it is time to join the parts and calculate the probability of fault occurrence per OHL and per transformer, including the two circuit-ends, as shown in figures 7.3 and 7.4. For busbars, as shown in figure 7.5, it is only needed to include all the causes when calculating as in equation (7.3).

Figure 7.26 presents the reliability diagram of an OHL or transformer. With $prob_{end}(u)$ the failure probability of circuit-ends, $prob_{OHL_k}$ the failure probability of the k[th] OHL and $prob_{TR_k}$ the failure probability of the k[th] transformer or autotransformer, including all different causes, the final fault occurrence probability will be calculated as in equation (7.52), using $prob_{OHL_k}$ for OHLs or $prob_{TR_k}$, respectively.

$$fault\ probability_{OHL_k} = 1 - \left[(1 - prob_{end}(u)) \times (1 - prob_{OHL_k}) \times (1 - prob_{end}(u)) \right] \qquad (7.52)$$

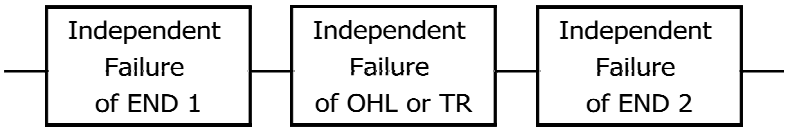


Fig. 7.26 – Reliability scheme for transformers and OHLs

For OHL with three circuit-ends, the equation 7.53 is used. In OHLs the circuit-ends have always the same voltage level.

$$fault\ probability_{OHL_k} = 1 - \left[\left(1 - prob_{end}(u)\right)^3 \times \left(1 - prob_{OHL_k}\right)\right] \qquad (7.53)$$

7.10. Multiple independent contingencies

Multiple independent contingencies are rare and their probability is obviously much smaller than the probability of the dependent ones. The calculation of multiple independent contingencies does not fit in online risk assessment, where the computational time needs to be short and a pre-defined list of contingencies considered more credible is evaluated. The possible combinations for N-k (k>1) contingencies, when considering all grid elements, is enormous and not compatible with real-time risk assessment. Nevertheless, in the operations planning environment, it may be useful to study the combinations of N-2 or even N-3 contingencies.

The probability of multiple and independent faults are calculated as in equation (7.54).

$$probability\left(A_{k_1} A_{k_2} A_{k_3} \cdots A_{k_n}\right) = P\left(A_{k_1}\right) \cdot P\left(A_{k_2}\right) \cdot P\left(A_{k_3}\right) \ldots P\left(A_{k_n}\right) \qquad (7.54)$$

where $P\left(A_{K_i}\right)$ is the probability of fault of the grid element A_{k_i} .

7.11. Interface for manual calculation

The presented probabilistic method is part of an integral risk assessment methodology, which aims to provide control room operators with risk-based security indices for short-term analysis. The final stage of development aims to have the overall process completely automated for online evaluation. However, an application was designed to run on demand past/future scenario simulations for probability calculation and its interface is shown in figure 7.27. With this application, several off-line simulations were performed to evaluate the results of the probabilistic methodology.

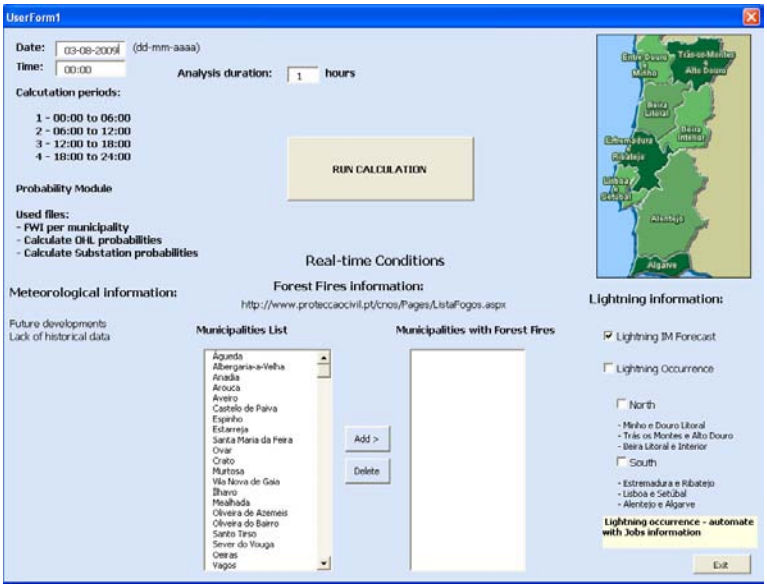


Fig. 7.27 – Interface for manual probability calculation

The input data treatment involving geographical location within the municipalities' borders, such as OHL towers, lightning records, among others, was first done using MatLab, as described in chapter 6, generating the necessary tables to be able to proceed with the probability calculation. The algorithm to

calculate probabilities was fully developed in MsExcel, using VBA for applications. The calculation for one period under analysis takes approximately 40 seconds on a standard laptop, which is compatible with the time requirements for real time simulations and analysis. In the servers available in the Portuguese TSO, it is expected to take around 1/3 of that time.

7.12. Final probability results

In order to evaluate the results of the probabilistic part of the proposed methodology, the probabilities of fault occurrence for all OHLs, transformers and busbars in the system were calculated hourly from 1st June until 31st December 2009. For this calculation, recorded information of active forest fires, of risk of forest fires and of lightning occurrence was used. The use of this information allows the probability calculation as if it was performed in the beginning of the period under analysis.

Every influencing factor takes part in the probability calculation. Storks and fog combined with pollution affect in the same way a whole period of 6 hours depending on the month, because their information per municipality and failure rates are updated in the beginning of each year, where the different seasons and times are well defined. Forest fires and lightning can affect each hour in a different way, because they are based not only on failure rates and on characteristics, but also on current conditions, which are assessed online and updated for each period under analysis. Therefore, the probability result without lightning or forest fire occurrence is based on failure rates affected by the conditions of the location where each OHL is placed and by the OHL characteristics, such as having composite insulators installed, which are updated yearly. For the latter, the result of the probability calculation is similar to what is shown in figure 7.28. The probability variations shown in figure 7.28 are mainly influenced by two causes: storks and fog combined with pollution, but because the line is very short there are not very steep variations. The 400 kV OHL presented in the graph has also a very low BFR, so it is hardly influenced by lightning.

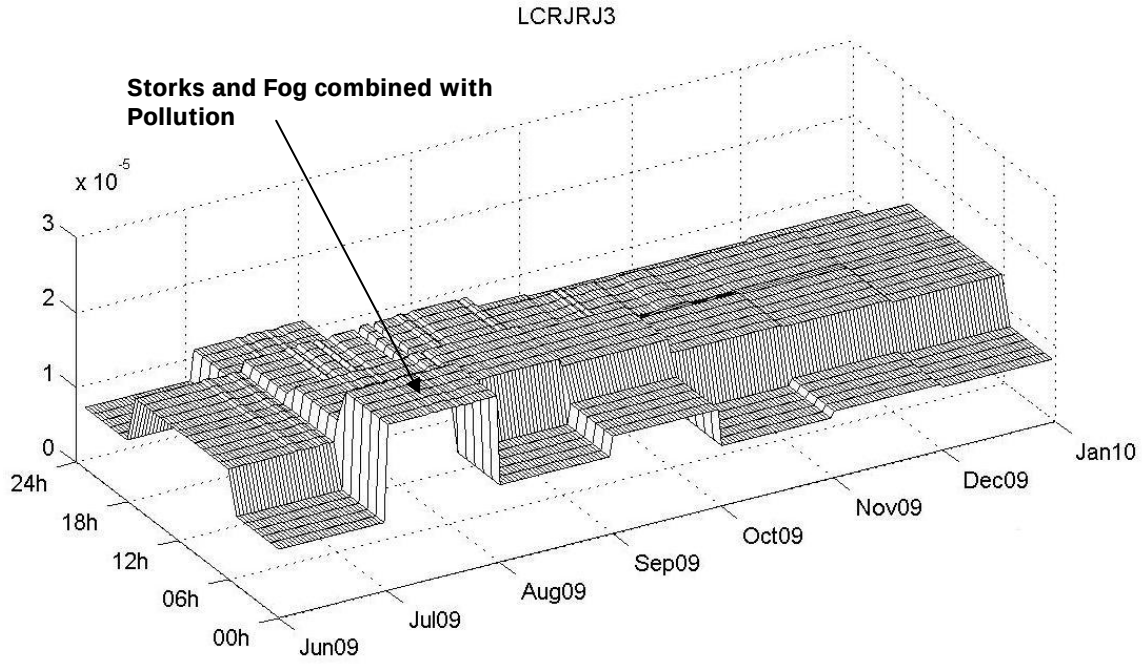


Fig. 7.28 – Very short 400kV OHL that connects a substation to a power plant

Figures 7.29, 7.30 and 7.31 present the probability of fault occurrence results for three OHLs with different characteristics. Figure 7.29 refers to an OHL located in the north of Portugal, where neither storks nor fog combined with pollution affect the overhead lines. On the other hand, it is located in a region where the soil has a very high resistivity value, because it is mainly granite. The peaks in the graph are mainly due to lightning, and because the BFR has a high value, the probability of faults caused by lightning has a significant effect on the final probability and, consequently, on the graph.

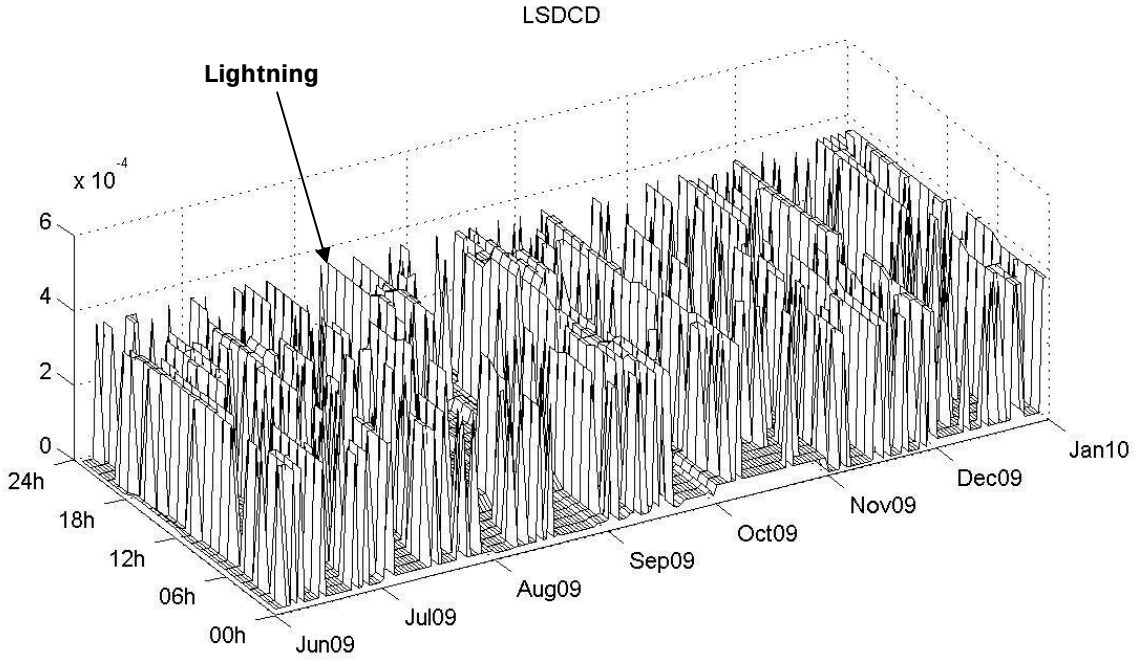


Fig. 7.29 – Probability of fault occurrence for a 150kV OHL

Exactly the same situation happens with figure 7.30, but this OHL is located in the interior central part of Portugal, which was an area very often affected by forest fires in the period under analysis, which influenced greatly its probability during August and in the beginning of September. On the 31st of August, the maximum value for the probability of fault for the presented OHL was reached, because of forest fires, and indeed they have caused 3 faults on the line at around 18h on that day.

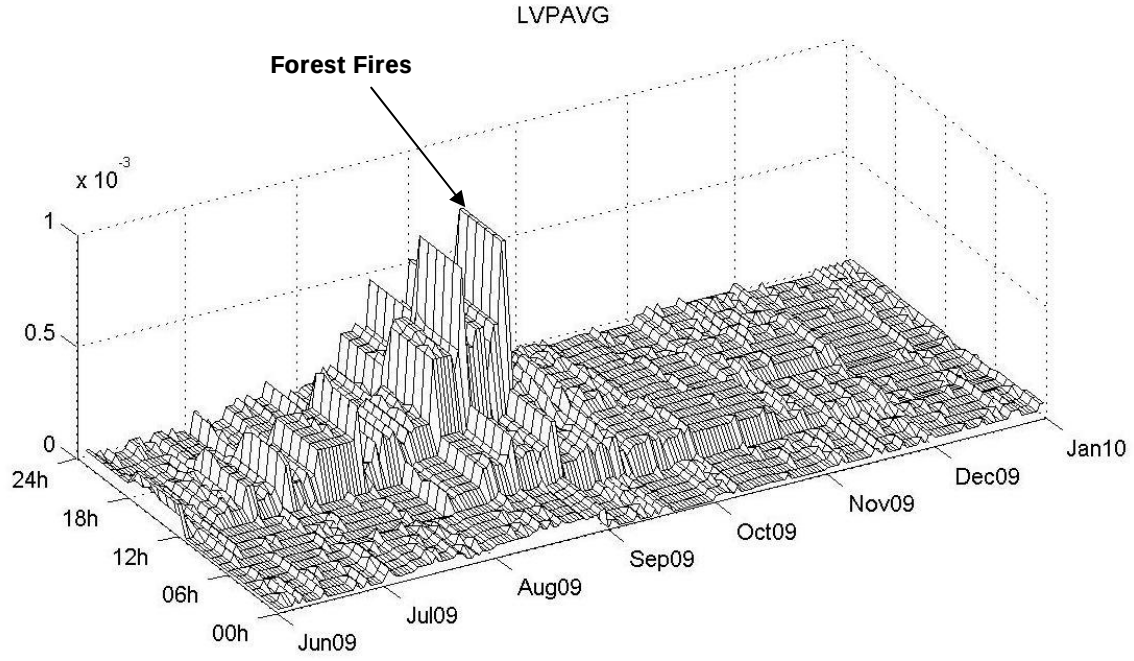


Fig. 7.30 – Probability of fault occurrence for a 220kV OHL

Figure 7.31 shows the probability of fault occurrence for a 400kV OHL located near the coast in the centre of Portugal. Additionally to lightning and forest fires, this specific OHL is also affected by stork and fog combined with pollution. Storks influence is clear in many months during the year, especially in the first two periods of the day. The influence of fog is well noticeable in the first period (from 0h to 6h) of July and the influence of forest fires during August and beginning of September (mainly from 12 to 18h). The small peaks in the graph are the effect of lightning occurrence and because the BFR of this 400 kV OHL is relatively low, the lightning effect is also small.

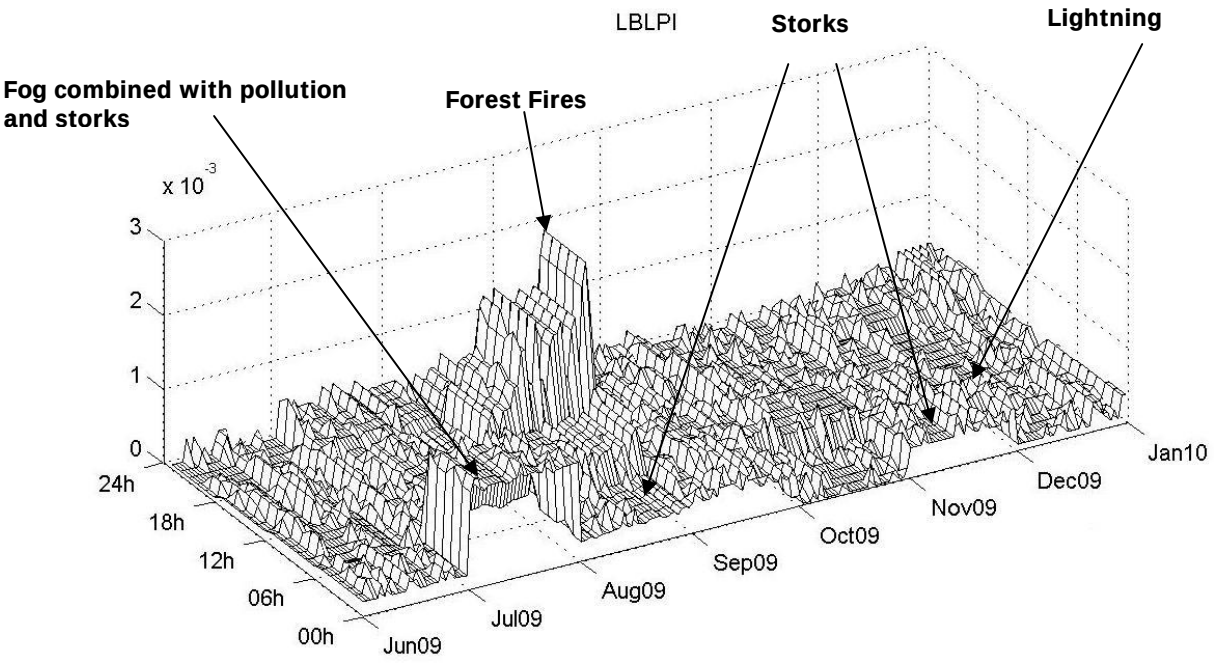


Fig. 7.31 – Probability of fault occurrence for a 400kV OHL

Figures presenting the probability of fault occurrence for the rest of the PTS overhead lines are presented in appendix J.

In order to illustrate the calculation process, some examples are presented. The probability of occurrence is calculated for three OHL (one of each voltage level) on the 30th of August in different periods. The period of analysis is always 1 hour.

Example 1: A 150 kV OHL located in the south part of Portugal near the coast, LSNPO2. The probability will be calculated for the second period of the day at 11:00. Figure 7.32 present the probability of fault occurrence results. This OHL is mainly affected by storks and fog combined with pollution as noticeable from 0h to 6h and from July to October, because of higher probabilities. The peaks in the graph are the effect of lightning occurrence.

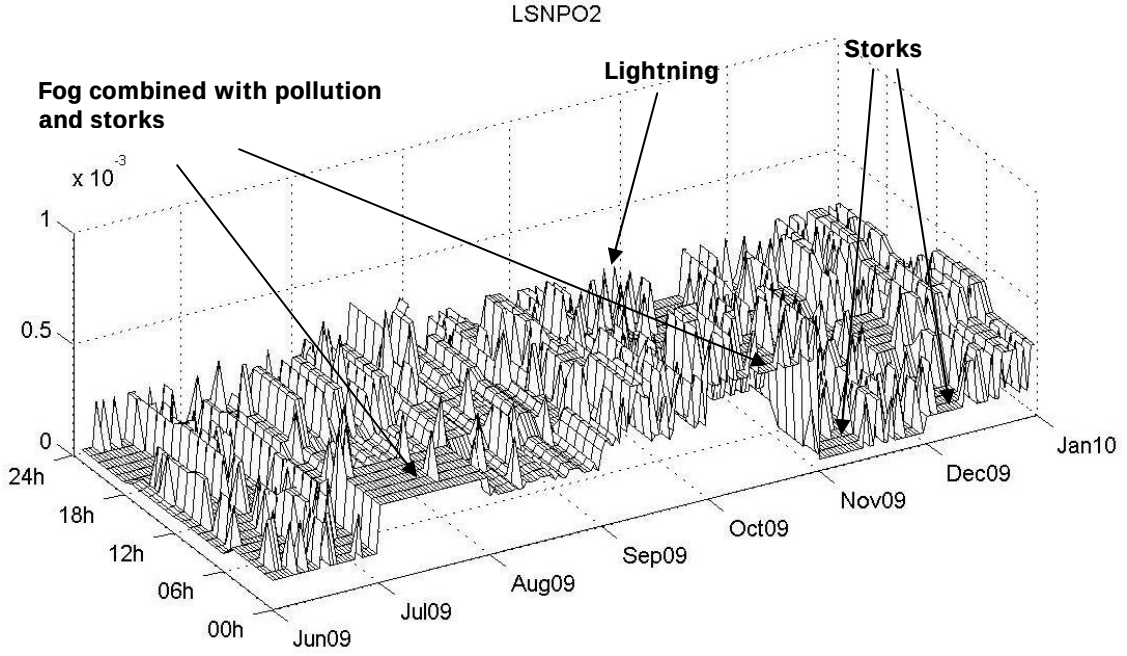


Fig. 7.32 – Probability of fault occurrence for a 150kV OHL

Table 7.11 presents the data per municipality for probability calculation. The total length of the OHL is 95.8km. This OHL does not have composite insulators. The BFR_{LSNPO2} is equal to 0.261 faults per year.

Municipality	Length (km)	α_{storks}	α_{fog}	α_{fire}
Odemira	44.7	0.007	0	0.606
Silves	5.3	0	1	0.606
Monchique	14.9	0	0	1
Portimão	1.2	0	0	0.606
Santiago do Cacém	25.0	0.091	1	0.212
Sines	4.7	0	1	0.606

Table 7.11 – Data for probability calculation for LSNPO2

Table 7.12 shows the failure rate per cause for the OHL circuit-part and probability of fault occurrence per cause for circuit and circuit-end part.

Part	**Cause**	**Failure Rate (per hour per km)**	**Probability**
OHL Circuit	Storks	4.0×10^{-6}	9.6×10^{-6}
	Lightning	with lightning	2.0×10^{-4}
	Fog + Pollution	3.0×10^{-6}	9.3×10^{-5}
	Forest Fires	1.0×10^{-6}	7.5×10^{-5}
	Unknown	6.0×10^{-7}	5.8×10^{-5}
	OHL Equipment	1.0×10^{-6}	1.2×10^{-4}
	External	No faults	-
	Others	No faults	-
Circuit-part probability of fault			1.4×10^{-4}
End	End Equipment		8.9×10^{-6}
	Systems		3.4×10^{-6}
	Human Error		2.9×10^{-6}
Circuit-end probability of fault			7.3×10^{-6}
Probability of fault occurrence for LSNPO2			**1.55×10^{-4}**

Table 7.12 – Probability calculation summary for LSNPO2

Example 2: A 220 kV OHL located in the centre of Portugal near Lisbon and near the coast, LCVRTJ. The probability will be calculated for the first period of the day at midnight. Figure 7.33 present the probability of fault occurrence results for LCVRTJ. In this OHL the BFR is very low so the lightning occurrence effect on the graph is small.

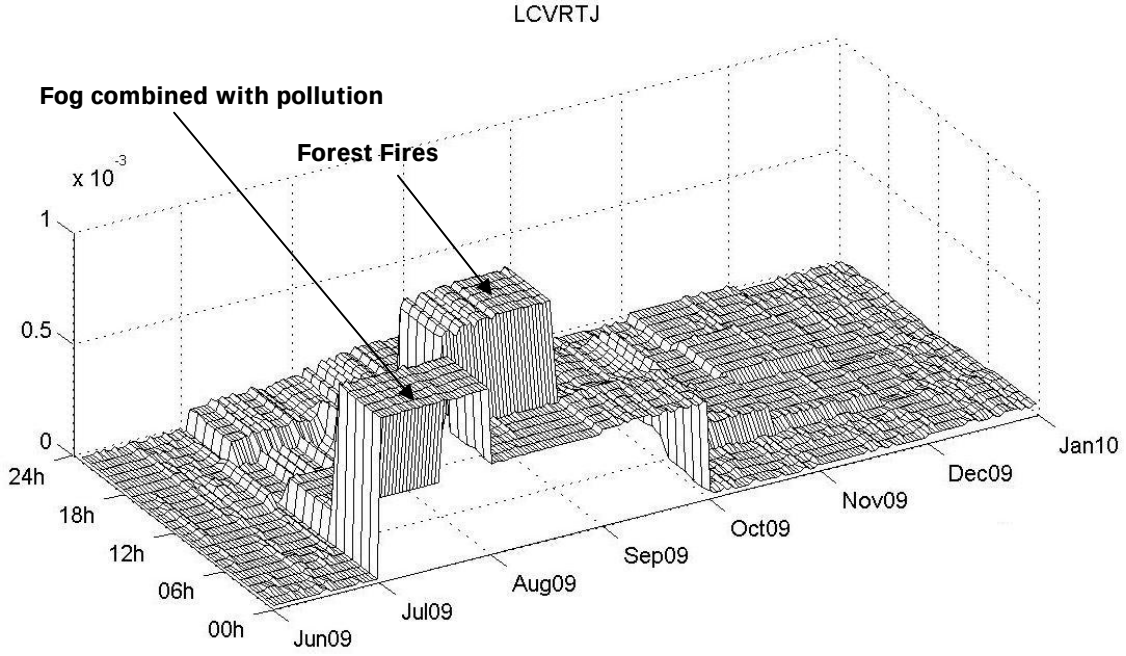


Fig. 7.33 – Probability of fault occurrence for a 220kV OHL

Table 7.13 presents the data per municipality for probability calculation. The total length of the OHL is 46km. This OHL is partially equipped with composite insulators. The BFR_{LCVRTJ} is equal to 0.017 faults per year.

Municipality	Length (km)	α_{storks}	α_{fog}	α_{fire}
Sobral de Monte Agraço	1.4	0	0.25	0.21
Torres Vedras	9.4	0	1	0.18
Amadora	1.6	0	0	0
Cascais	0.3	0	1	0
Mafra	14.4	0	0.79	0.21
Sintra	19.0	0	0.36	0.21

Table 7.13 – Data for probability calculation for LCVRTJ

Table 7.14 shows the failure rate per cause for the OHL circuit-part and probability of fault occurrence per cause for circuit and circuit-end part.

Part	Cause	Failure Rate (per hour per km)	Probability
OHL Circuit	Storks	No storks	-
	Lightning	No lightning	-
	Fog + Pollution	1.2×10^{-5}	3.5×10^{-4}
	Forest Fires	9.8×10^{-7}	9.0×10^{-6}
	Unknown	9.3×10^{-7}	4.3×10^{-5}
	OHL Equipment	No faults	-
	External	No faults	-
	Others	No faults	-
		Circuit-part probability of fault	4.1×10^{-4}
End	End Equipment		9.3×10^{-7}
	Systems		3.2×10^{-6}
	Human Error		2.2×10^{-7}
		Circuit-end probability of fault	4.4×10^{-6}
		Probability of fault occurrence for LCVRTJ	**4.1×10^{-4}**

Table 7.14 – Probability calculation summary for LCVRTJ

Example 3: A 400 kV OHL located in the north of Portugal, LRARR2. The probability will be calculated for the third period of the day at 16:00. Figure 7.34 present the probability of fault occurrence results for LRARR2. The increase of the probability value in August and the peak at the end of the month is mainly due to forest fires.

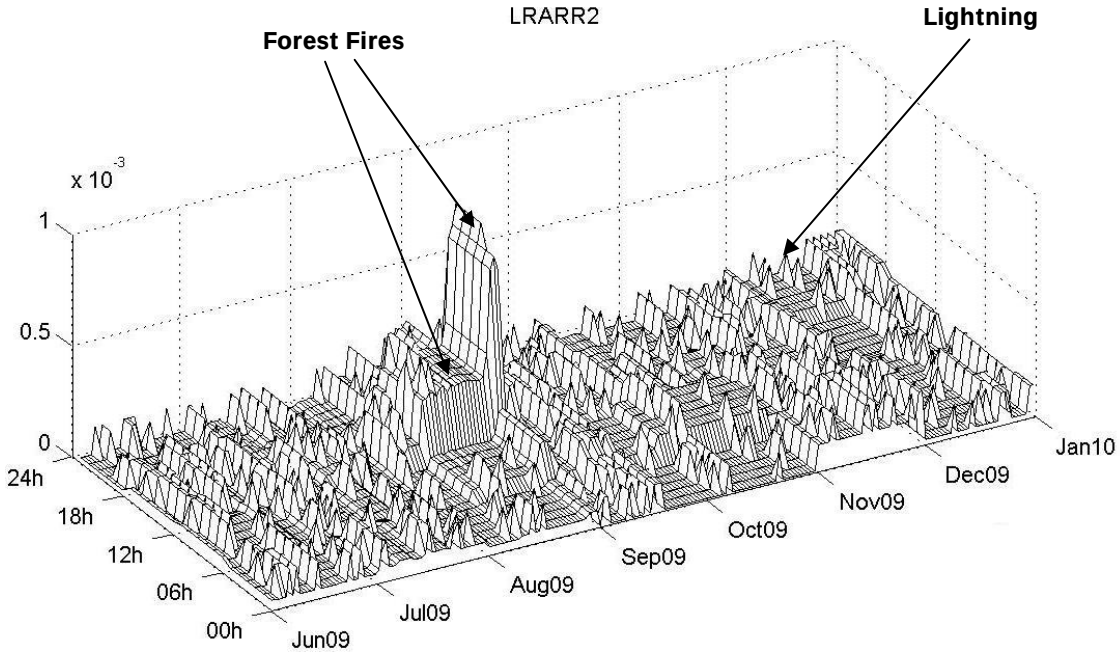


Fig. 7.34 – Probability of fault occurrence for a 400kV OHL

Table 7.15 presents the data per municipality for probability calculation. The total length of the OHL is 34.1km. This OHL is not located in areas with storks or pollution problems. The BFR_{LRARR2} is equal to 0.16 faults per year.

Municipality	Length (km)	α_{storks}	α_{fog}	α_{fire}
Santo Tirso	3.8	0	0	1
Vila Nova de Famalicão	0.3	0	0	0.606
Guimarães	7.1	0	0	0.606
Paços de Ferreira	10.6	0	0	0.606
Paredes	12.3	0	0	0.606

Table 7.15 – Data for probability calculation for LRARR2

Table 7.16 shows the failure rate per cause for the OHL circuit-part and probability of fault occurrence per cause for circuit and circuit-end part.

Part	Cause	Failure Rate (per hour per km)	Probability
OHL Circuit	Storks	No storks	-
	Lightning	No lightning	-
	Fog + Pollution	No pollution	-
	Forest Fires	2.0×10^{-5}	7.8×10^{-4}
	Unknown	2.2×10^{-7}	8.1×10^{-5}
	OHL Equipment	No faults	-
	External	No faults	-
	Others	No faults	-
		Circuit-part probability of fault	8.6×10^{-4}
End	End Equipment		9.4×10^{-7}
	Systems		2.6×10^{-6}
	Human Error		3.7×10^{-6}
		Circuit-end probability of fault	7.2×10^{-6}
		Probability of fault occurrence for LRRRA2	**8.8×10^{-4}**

Table 7.16 – Probability calculation summary for LRRRA2

The minimum probability of fault for OHLs and also transformers occurs when the causes that affect the circuit-part or the transformer itself are not present; consequently, the value will be the result of the probabilities of the two circuit-ends, based on yearly average failure rates. The maximum, minimum and average values of probability of fault occurrence, per month per period, were calculated for all OHLs and are shown in appendix J; this will provide an insight of which are the OHLs that have a higher probability of fault.

Busbars are affected by several causes related with the circuit-end that depend on yearly average failure rates, but they can also be strongly affected by fog combined with pollution when located in areas where that risk exists. The probability of faults in case of busbars is much smaller; it has an order of magnitude of 10^{-6} or 10^{-7}, in case they are affected or not by fog combined with pollution or lightning, respectively (the last cause only has one fault in 2007 in the 400 kV).

Figures 7.35 and 7.36 show the probability of faults for two busbars located in different regions. The first is located in an area affected by fog combined with pollution and the second one not. In figure 7.35, it is possible to observe the reduction in the probability after summer, i.e., after the period where there is risk of faults caused by fog combined with pollution.

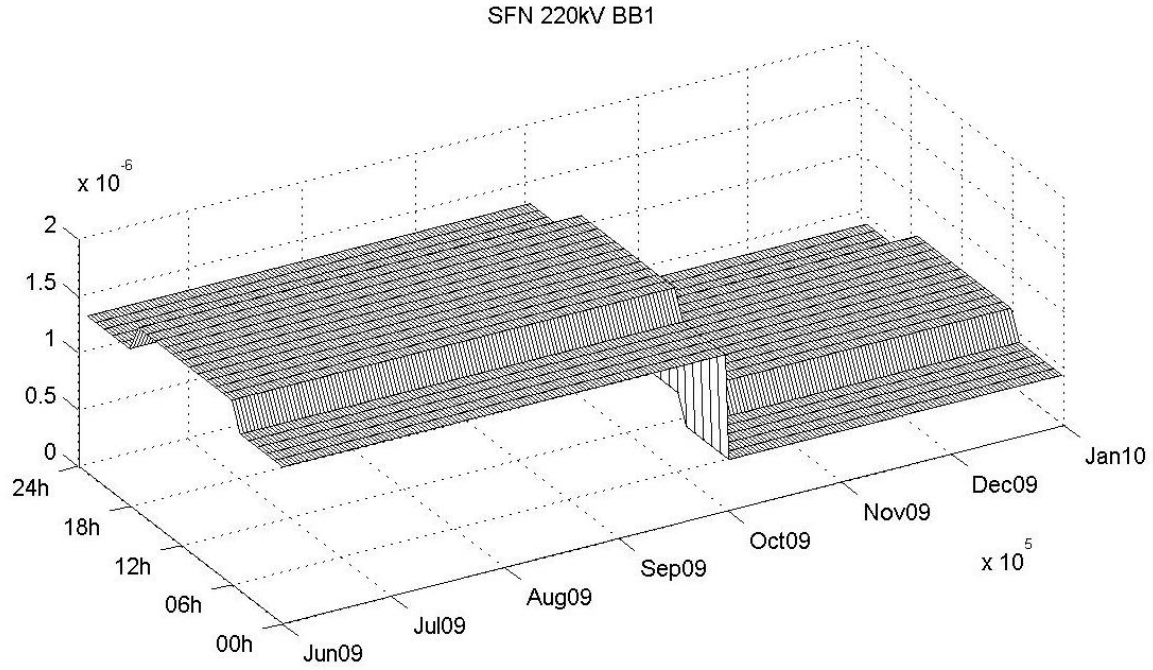


Fig. 7.35 – Probability of fault occurrence for a 220 kV Busbar affected by fog combined with pollution

Figure 7.36 presents an example of a probability plot for a busbar which is not affected by fog combined with pollution.

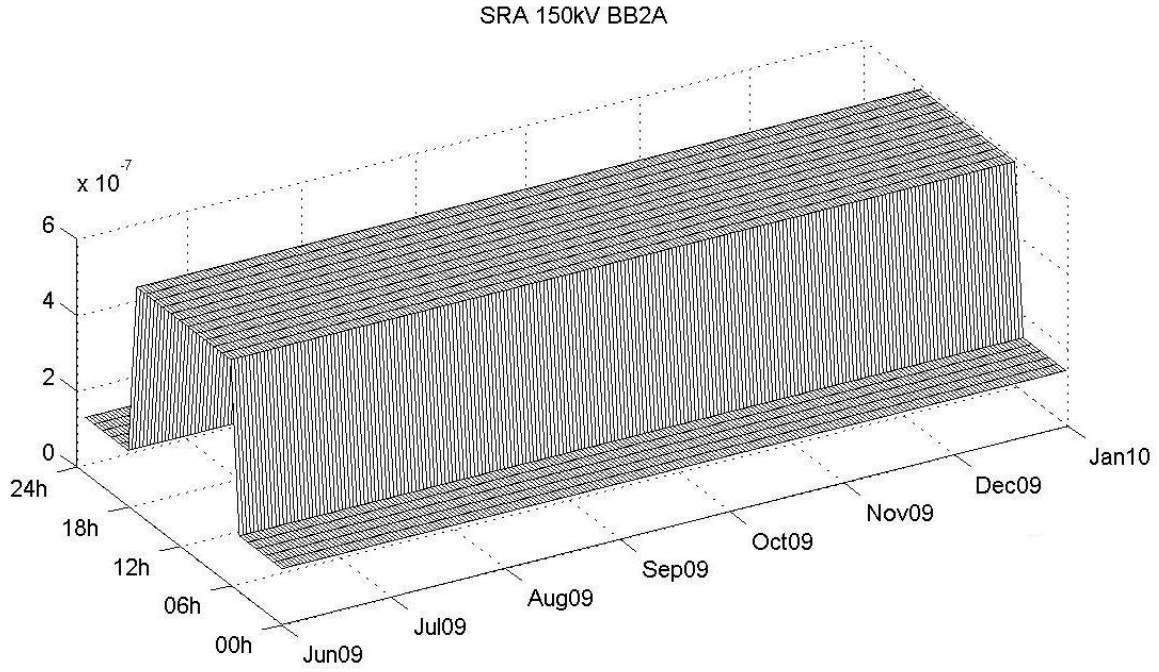


Fig. 7.36 – Probability of fault occurrence for a 150 kV Busbar

Figures presenting the probability of fault occurrence for the rest of the busbars are presented in appendix J.

In the case of transformers, the probability of faults is based on yearly average failure rates and they are rarely affected by lightning and not at all by forest fires. Therefore, the results are much more constant and stable within the year and time periods, as can be seen in appendix J. Table 7.17 presents the probability of fault for transformers per period per type of transformer.

	AT 220/150 kV		AT 400/220 kV	AT 400/150 kV	TR 400/60 kV	TR 220/60 kV		TR 150/60 kV
Period	Min	Max	Min=Max	Min=Max	Min=Max	Min	Max	Min=Max
0h-6h	1.6E-05	2.7E-05	1.3E-05	1.3E-05	1.1E-05	1.4E-05	2.4E-05	1.0E-05
6h-12h	2.2E-05	3.2E-05	1.9E-05	1.9E-05	1.6E-05	1.9E-05	2.9E-05	1.5E-05
12h-18h	2.2E-05	3.2E-05	1.9E-05	1.9E-05	1.6E-05	1.9E-05	2.9E-05	1.5E-05
18h-24h	1.6E-05	2.7E-05	1.3E-05	1.3E-05	1.1E-05	1.4E-05	2.4E-05	1.0E-05

Table 7.17 – Maximum and minimum probability of fault per period per type of transformer

Due to the low number of faults in transformers and even lower in autotransformers, they were joined per voltage level of the primary side, when calculating the respective statistics and failure rates. There were faults caused by lightning in 220/60 kV transformers, which results in maximum (with lightning) and minimum (without lightning) values of probability in the 220 kV machines. For AT 220/150 kV, the probability value to use is the minimum presented in table 7.17, because this type of machine never tripped because of lightning.

Figure 7.37 presents the probability of fault for 400/150 kV autotransformers.

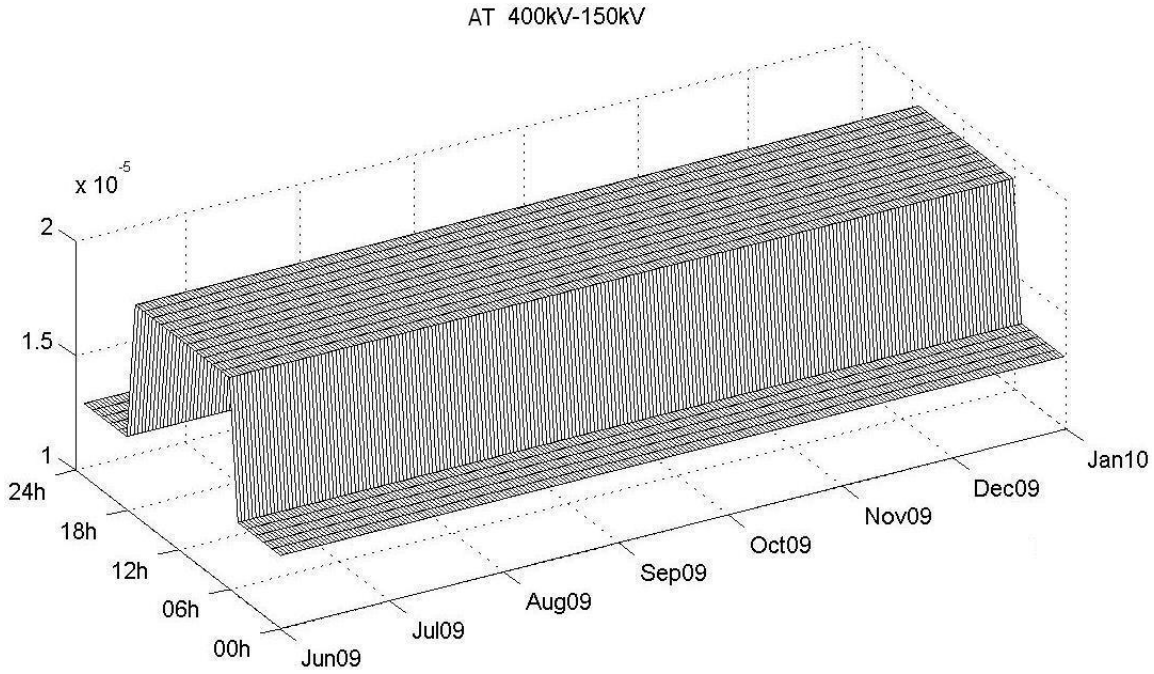


Fig. 7.37 – Probability of fault occurrence for 400/150 kV autotransformers

For the 220kV transformers, the value is not constant per period, because on this voltage level transformers were affected by lightning in the past. The probability due to lightning is included, changing the probability value according to current conditions, as in equation (7.43). Transformers in the North and South are affected differently, because of the lightning exposure areas that were defined to incorporate online conditions. Figure 7.38 presents the probability of fault for 220/60 kV transformers in the North of Portugal. The peaks in figure 7.38 represent lightning occurrence periods, increasing the fault probability.

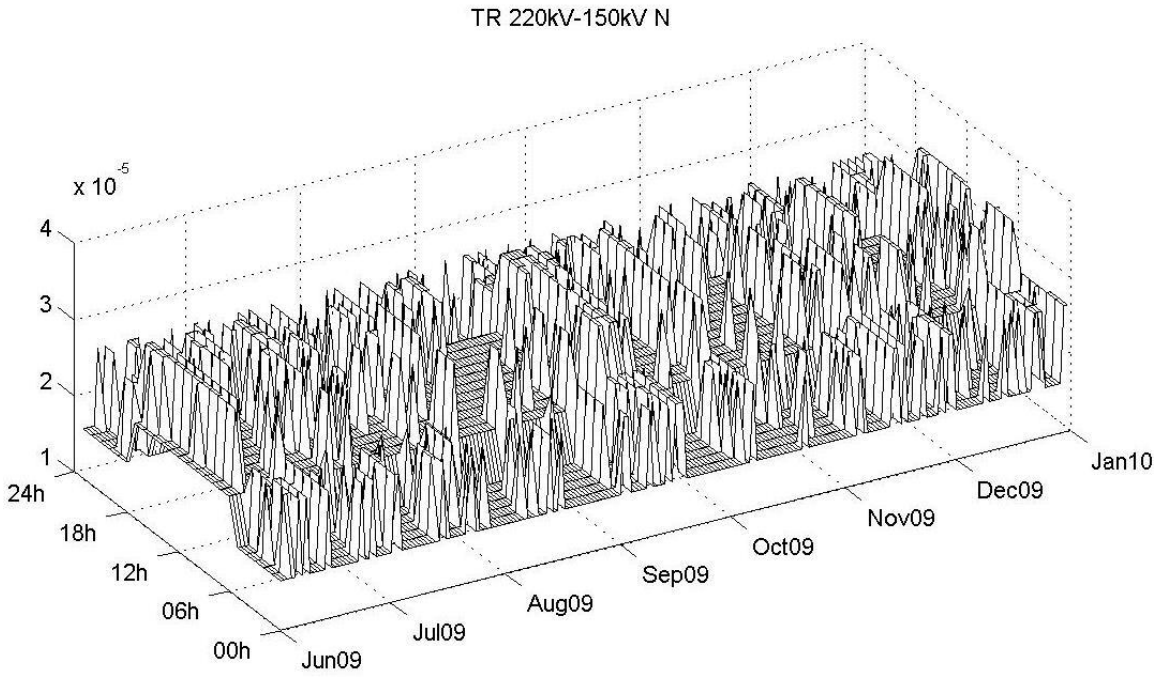


Fig. 7.38 – Probability of fault occurrence for 220/60 kV transformers in the North

Figures presenting the probability of fault occurrence for the rest of the transformers types are presented in appendix J.

Common cause N-2 contingencies were included in this work, considering faults caused by lightning and forest fires. Figures 7.39 and 7.40 show the probability of occurrence of an N-2 common cause faults where it is possible to distinguish the effect of lightning activity (the peaks in the graph) and the effect of forest fires (the higher surfaces mainly noticeable in August). When none of these causes are present, the probability of common cause faults is not considered and in figures 7.39 and 7.40 is presented as zero.

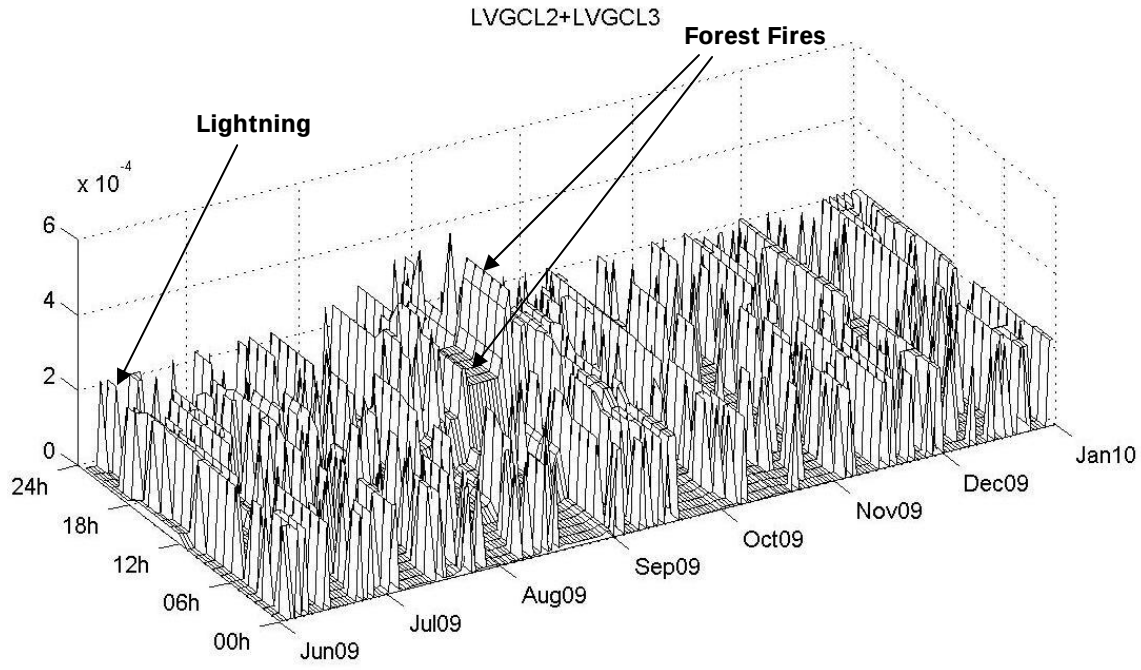


Fig. 7.39 – N-2 contingency composed by two 220 kV OHLs

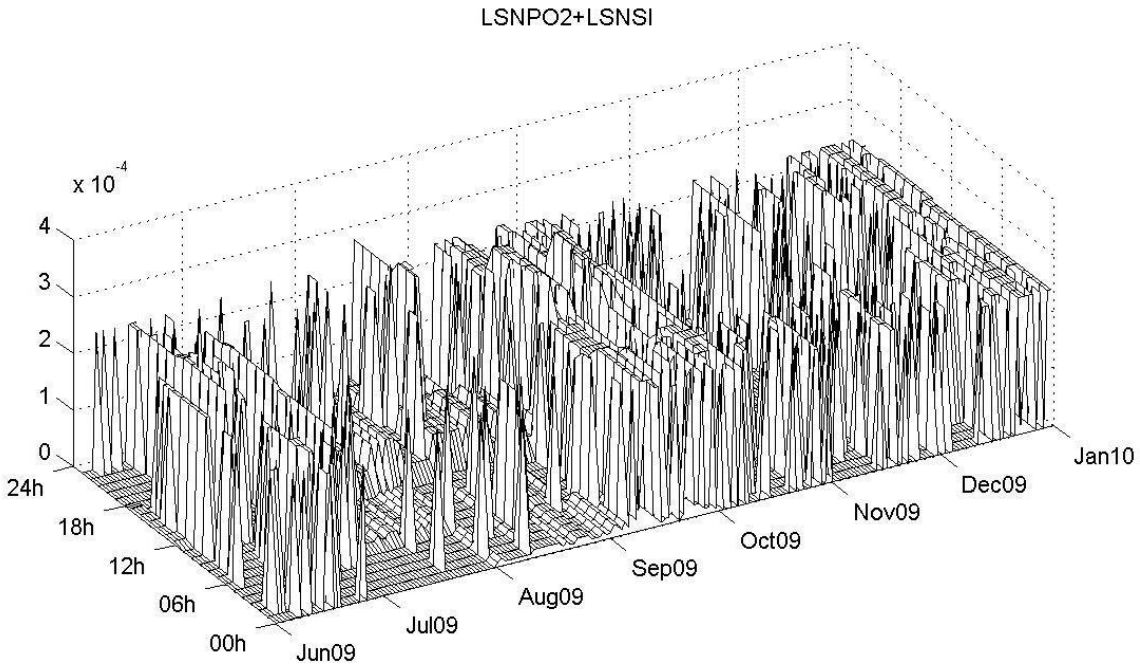


Fig. 7.40 – N-2 contingency composed by two 150 kV OHLs

The probabilities of fault occurrence for the rest of the N-2 defined contingencies are presented in appendix J.

7.13. New grid elements

Due to the rapid development of the Portuguese transmission grid, there are often topology changes and new grid elements in the system. As mentioned in section 4.1, the integration of generation through renewables and the increase of the interconnection capacity are the motor for the quick changes in the network. Due to the latter, even if changes in topology are small, there would not be enough historical data for many grid elements to calculate individual indices. In order to have a sufficiently flexible analysis, we will use average failure rates per voltage level and in case of OHL per km, as mentioned in sections 7.6.1 and 7.7.1, allowing the network to be dynamic.

In case of change of topology, such as the splitting of an existing OHL in two parts caused by a new substation, the old OHL record is closed and the new OHLs are activated in the model. The history of the old OHL is already included in the failure rates and the events of the new ones will be included in statistics for the first time in the end of the year. In case of totally new grid elements, they are included in statistics exactly in the same way.

For both situations, the evaluation of the environmental and geographical characteristics is performed in order to identify to which risks the grid element is exposed. For lightning, the BFR is calculated, considering all the required information presented in section 7.6.3.1.

7.14. Conclusion

In this chapter, we are presenting the probabilistic method to estimate the short-term failure rate of contingencies and to be used online as part of a risk assessment methodology for security evaluation. The described method is fast and therefore compatible with the real-time operations environment. For its development, it was important to gather qualitative data, understand the process and find correlations between variables that were considered meaningful.

The state of the art of research that was presented in chapter 3 does not explicitly include the influence of the characteristics of each network in the probability of fault calculations. The introduction of current conditions and the intrinsic characteristics of network and of its location is the added value of this work, which aims to assess the probability of faults based on short-term failure rates.

For the four main causes of the Portuguese transmission system, which are dependent on length and on the different characteristics across Portugal, this methodology includes all the influencing factors that are considered important in terms of OHL performance. These factors include number and location of stork nests, identified polluted areas, composite insulators location, risk level of forest fire per municipality, active forest fires information, lightning data, and network characteristics.

The data organization is mostly made by municipality, aiming to determine the OHL length and substations exposed to local risks. Therefore, accurate network topology and physical characteristics, weather, geographical and environmental information and also operational experience are needed to determine realistic weighting factors for each cause. The information requirements of this methodology make it mainly possible within a TSO structure, where the asset owner and system operator are the same entity, as mentioned in chapter 6.

For the other causes yearly average failure rates are used, because no other influencing factors were identified, except the working schedule for human error that uses different failure rates according to the time of the period under analysis and the seasonality of busbar faults that are caused by fog in combination with pollution.

Additionally and because we are developing work for system operations environment, current conditions are also included, aiming to assess short-term risk in a realistic way. Here the concept of short-term failure rates is implemented, valuing the current risks that are actually present in each evaluation and including all the influencing factors in the probability calculation. This probabilistic method also ensures the difference between longer and shorter OHLs, where the longer ones are obviously more exposed to risks. This difference is not considered in the normal deterministic contingency analysis, which treats them as equal.

For lightning, a method to estimate the number of faults caused by lightning for short-term analysis was implemented. This method is based on the probabilistic method for lightning performance of an OHL developed by CIGRE. The goal was to keep the calculation as fast and as simple as possible. The systematic inaccuracies introduced by the simplifications are corrected by the scaling factor. It seems to be the best compromise solution with good results, also when comparing it with the results obtained with IEEE FLASH for a subset of the OHLs, because the applied scaling factor improves the estimation results. The comparison of the simplified method with IEEE FLASH results confirms the validity of the adopted simplifications.

The backflash rate calculation includes the factors that are most significant in terms of OHL performance in case of lightning, such as lightning density, number of ground wires, soil resistivity, tower geometry, the insulation level, the conductors' diameter, tower footing resistance, actual lightning conditions from the LMS and faults' historical data. The critical current, the minimum current that causes flashover, is calculated per tower, due to the fact that each tower has different characteristics. The tower footing resistance is one of the most crucial inputs in order to predict OHL performance, regarding lightning, and it varies during the year, thus inherently introducing imprecision into the method. Besides this, there is also lack of data and limited trust in some of the measurements, which is why the accuracy level of the predictions is expected to increase when the quality and completeness of the measurement data improves. The moderate correlation between the expected and the actual number of faults was expected.

The risk of single and multiple contingencies cannot be neglected. Common cause faults occur in electrical power systems under specific circumstances. The most common situation is faults caused by lightning that affect simultaneously OHLs that share the same towers during the whole or part of their right-of-way.

Another possible origin of common cause faults is forest fires affecting a corridor composed by several OHLs. On 23rd December 2009, the disturbance caused by wind (described in section 2.3.4) has caused two common cause faults in two different areas of Portugal and it has increased the awareness of the relevance of having wind speed measurements available online.

Common cause failure rates are needed when assessing the risk of multiple contingencies, in order to calculate the probability of occurrence.

The β-factor model has proven to be adequate to address the N-2 contingencies caused by lightning and by forest fires for parallel OHLs. In case of lightning, most of the OHLs that share the same towers within the same right-of-way have common cause faults with simultaneous trips and the BFR is mainly based on geometry and intrinsic characteristics of their location. In case of forest fires, not more than two OHLs are normally affected at the same time. After analysing the characteristics of the N-2 common cause contingencies, it was possible to conclude that it mainly affects parallel OHLs.

Hidden failures occur at the same time as an initiating fault, normally causing another grid element to trip. The most common event, involving a hidden failure, is an N-2 contingency. These contingencies are considered also dependent as common cause ones, but the causes that affect the involved elements are different. While common cause failures only occur under specific conditions, such as adverse weather and forest fires, hidden failure events can always happen in the system because they do not depend on external factors. In spite of their importance, discussed in section 3.4.1, and its statistics shown in section in 5.7.1, integrating hidden failures in the risk assessment methodology is beyond the scope of this work, therefore it will also be addressed in future developments.

In order to evaluate the probabilistic part of the methodology and its results, probabilities of fault occurrence were calculated from the beginning of June 2009 until the end of December 2009. The results show that the probability of fault increases with lightning and forest fires and also confirm the seasonality and the pattern that is expected for the four main causes. For this calculation, the fault historical data, from the beginning of 2001 until the end of 2009, was considered.

Chapter 8.

Risk Assessment for Operations

8.1. Introduction

The probabilistic nature of power system security has been well recognized since the early days of modern power system operation and control. The aim of the probabilistic approach is to make use of the available information in the decision making process [12]. As it was presented in chapters 5, 6 and 7, there is information of many types and with different time frames that can be used. Decisions to mitigate risk should be based on the expected risk reduction. The risk of a specific contingency can be evaluated by weighting its severity by its probability of occurrence, as in equation (8.1).

$$Risk_k = probability_k \times severity_k \qquad (8.1)$$

where k represents the k^{th} contingency under analysis.

The new environment in power system has created new challenges to the system security assessment. The use of methodologies that take advantage of the day-ahead forecasts and actual real-time conditions in combination with past knowledge, using probabilistic methods, is interesting in the system operation's environment, because it gives a more accurate overview to the control room operators. There is an increasing need to provide control room operators with an online indicator of the security level associated with existing or forecasted (near future) operating conditions.

References [3], [12], [17] point out the need for online probabilistic security assessment, identifying the need to introduce short-term failure rates that take into account the current conditions. In section 3.3, an extensive description of the deterministic and probabilistic methods was made and it is acknowledged that the deterministic approach only assesses the severity of contingencies, in terms of thermal loading and voltage violations, assuming that all considered events are equally likely.

In order to calculate the risk of contingencies, a method was developed to calculate the probability of contingencies considering all the significant influencing factors about which there is enough information. The probabilistic method was described in chapter 7 and the severity calculation is explained in this chapter.

There is no such thing as no risk, also in the deterministic approach there is risk, but it is just not assessed. Low and high risk are treated in the same way. With so many uncertainties, the probabilistic approach is adequate to evaluate power systems' behaviour and performance. Risk and reliability are strictly connected, because operating with a higher risk corresponds to the acceptance of lower reliability.

8.2. Risk evaluation time frames

Risk can be mainly evaluated in two time frames: a longer one in operations planning and a shorter one online in the control room. The uncertainty of the analysis will diminish with the proximity of the period under analysis, because more information is available (such as lightning occurrence, active forest fire information and generation pattern) and also the used forecasts, such as risk of forest fires or wind generation, are more accurate.

In operations planning, the risk methodology can be used to perform the day-ahead schedule technical verification (D-1 analysis), of which the current analysis is as described in section 4.5.2.3. Online, it can be used to perform the analysis for the next hour (H-1 analysis), which has as main purpose to balance the system (generation and load), considering the next hour operating conditions and for that using the tertiary reserve. This analysis is a new concept, which was born inside the Portuguese TSO during this research work, and it is not yet being applied in the Portuguese transmission system. The H-1 analysis has the purpose to assess risk for the next hour, complementing the deterministic security evaluation already performed in the control room.

In addition, the EMS system performs every 10 minutes a contingency analysis, as described in section 4.5.2.6. This real-time analysis has the option to associate to each contingency a probability of occurrence, but does not allow further analysis, except ranking the events per probability. Therefore, it is not enough to evaluate risk.

The online analysis performed for the next hour has accurate data for all the inputs, but with more time in advance the forecast errors increase and the quality of the prediction decreases. Forecast errors introduce some uncertainty in the next period operating conditions. Table 8.1 presents typical error values for the time horizons that are most relevant for this research.

Forecast type	1 hour in advance	1 day in advance
Load	>1%	2%
Wind	5%	20%

Table 8.1 – Average errors per type of forecast

For the next hour analysis, the maximum expected error is the following:

- For the load, around 90 MW, if 9000 MW of peak is considered
- For the wind generation, around 140 MW, if 85% of the total installed power is considered (values at the end of 2009). The maximum simultaneity factor considered for wind generation is 85%.

Therefore, the errors for the next hour have low impact. In case of the hourly D-1 calculation that is performed the day before, the significance of these errors increases. However, the load errors are guaranteed through the tertiary reserve, because it includes the addition of 2% of the predicted consumption in every programming period, as mentioned in section 4.8.3. To cope with wind generation forecast errors, the Portuguese TSO adjusts the tertiary reserve according to the generation needs for balancing the system, ensuring security. The wind generation forecast is updated every 6 hours, correcting the previous prediction.

The probability of contingencies presented in chapter 7 used 1 hour for the analysis duration (t=1 hour), which is suitable both for real-time and for the hourly D-1 assessment. In the hour before, the information that is available is more accurate, not only in terms of wind and conventional generation pattern and load profile, but also in terms of active forest fires and lightning occurrence. For the probability calculation, one hour in advance, current and more precise information is used. One day in advance, the available forecasts for the next day are used, including risk of forest fires and lightning, which are provided by the Meteorological Institute.

8.3. Risk assessment

This research work aims to evaluate operational risk for a short period of time, starting from a known system's state and considering current conditions, wind generation and load forecast, and all the other factors available during the operation. The flowchart of the methodology is shown in figure 8.1.

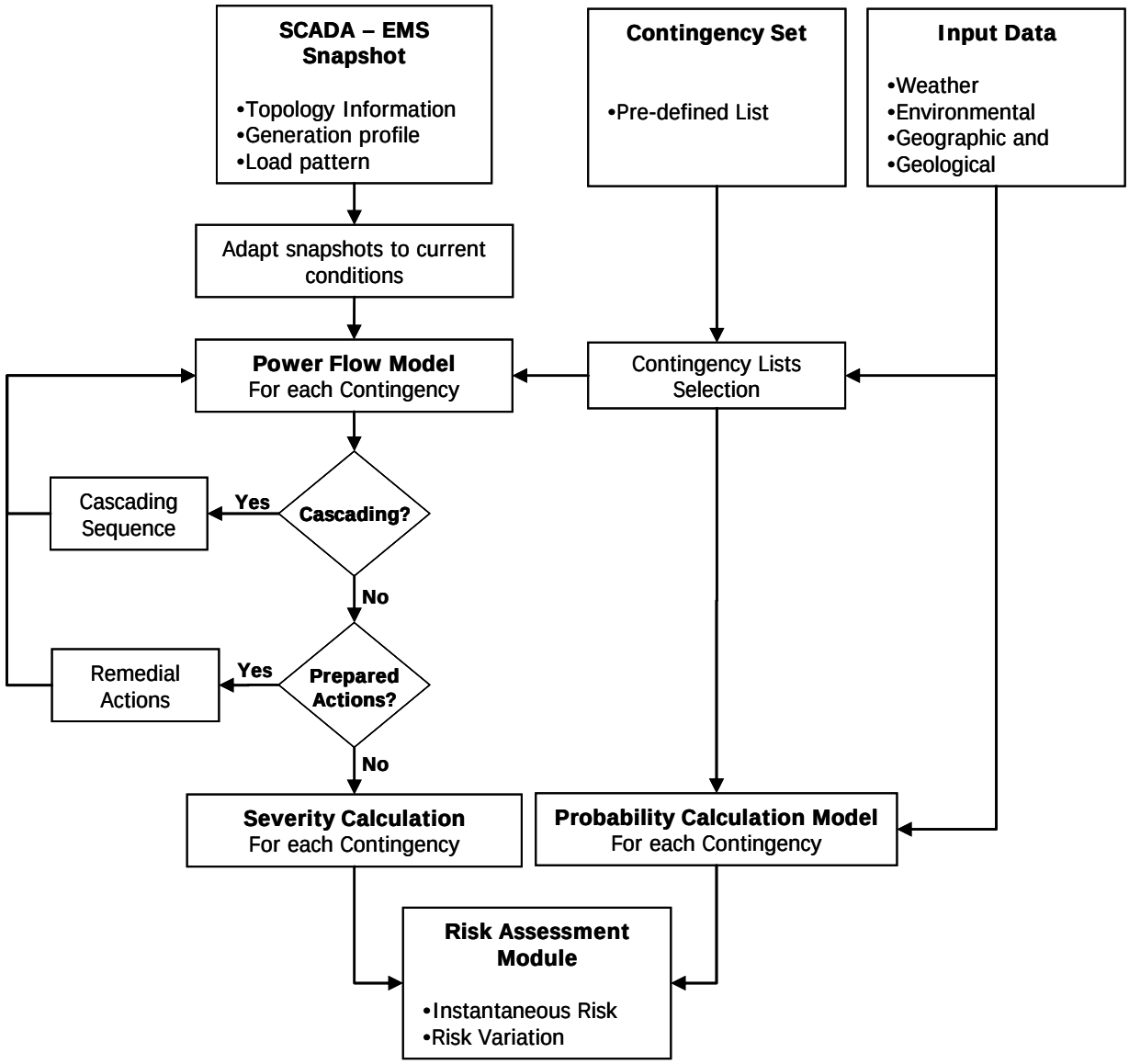


Fig. 8.1 – Risk assessment methodology flowchart

The dynamic inputs to be included in the risk evaluation for an operational environment are presented in figure 8.2. Control room operators need to be aware of all these parameters. The weather forecast includes the lightning and the risk of forest fires forecasts.

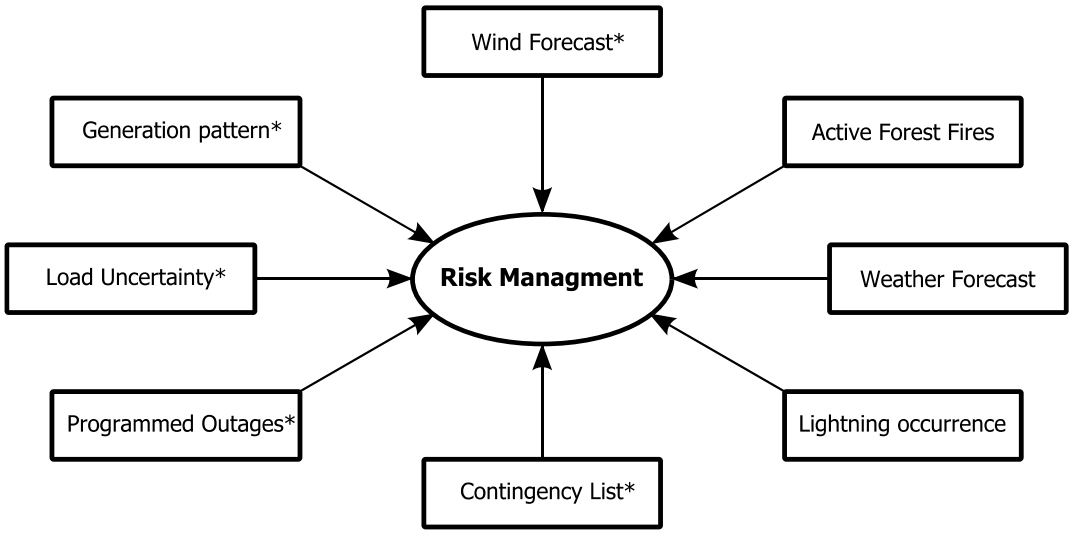


Fig. 8.2 – Risk analysis inputs (*currently used in the deterministic analysis)

Risk management inside a control room is not only about the probability of faults, their consequences also assume a preponderant role and they are affected by many inputs, such as the generation pattern, the quality of the forecasts and the current conditions. The latter must influence the contingency list that is assessed, because of e.g. lightning or forest fire occurrence. The selection of the contingency lists is applicable in the H-1 analysis, after evaluating the current conditions, and in the real-time contingency analysis. For D-1 analysis all the defined contingencies can be evaluated (see section 8.4.1).

The generation pattern depends on the market, which in turn depends on prices and, obviously, prices are strongly dependent on primary energy resources, such as, coal, oil, gas, water availability, and, in some countries, nuclear. Wind energy and some other renewable energy sources are not yet on the market in Portugal, although the regulation allows and they are already on the market in Spain. These energy sources are normally entirely absorbed by the network, except in operating conditions that jeopardize system's security. Hydro, wind or photovoltaic generation, depend on the availability of the corresponding natural resource, which is less controllable than coal, oil and gas, increasing the uncertainty in terms of the available generation capacity.

Planned outages are normally associated with works, such as maintenance, construction, etc., and during work periods inside a substation or in an OHL, the risk of potential accidents and human errors associated with works may increase. The yearly outage plan aims to schedule outages when they have the least impact on the system's performance, i.e. when the consequences of contingencies are least harmful.

The amount of available information clearly influences the system's risk expectation. To be aware of the short-term risk can make the difference between operators taking preventive or post-disturbance actions. After having a measure of risk, the decision-making process is dependent on the operator's judgement and appreciation of the results.

8.4. Severity evaluation

Severity must reflect the consequences of a contingency and the loading condition [17]. Online risk assessment has to consider thermal overload limit violations for each branch (lines and transformers), voltage limit violations for each busbar, the danger of cascading sequences, voltage instability situations, islanding situations, loss of load and loss of generation. System security limits are constraints that maintain the system secure and prevent the electricity market from being operated according only to economic rules.

Dynamic simulations are beyond the scope of this research work, therefore frequency limit violations and small-signal and transient stability are not addressed. For simplification and process celerity, voltage instability is determined by the non-convergence of the power flow analysis. If areas with a high risk of voltage instability are identified, a simple algorithm developed in the Portuguese TSO can be used in parallel with this severity evaluation in order to identify voltage collapse situations without the need for the specific EMS module and to assess the effect of preventive remedial actions [5].

The analysis for the next hour is performed using State Estimator (SE) snapshots that contain system information for the period under analysis, including:

- Expected changes in the topology.
- Wind generation forecast.
- Load forecast.
- Programmed outages.
- Expected generation pattern (which is market driven).

The SE snapshots are automatically created every 15 minutes. The online assessment for the next hour uses the snapshot created at the hour when the analysis starts, containing the current conditions and on which only small adjustments in the expected conditions are needed. Most of the information is available on an hourly basis.

Severity functions are adopted to quantify the impact of each contingency, based on the post-contingency results of the analysed SE snapshot. These results are the same ones that are calculated in the deterministic approach, and therefore they are easily understandable by control room operators.

To evaluate severity, several normalized functions, one per type of impact, are calculated from the results of the power flow simulation, using the same operating limits as in the deterministic criteria. Normalized functions enable the calculation of a global severity index.

In the following sections, for all the severity functions, i represents the i^{th} branch and j the j^{th} busbar.

8.4.1. Analysed contingencies

The TSO must select the exceptional contingencies to include in the contingency list based on specific operating conditions and their risk assessment [6]. A selective analysis of incidents' historical data was made in order to identify credible contingencies, because it is not reasonable to simulate all possible contingencies in a Transmission System.

From the analysis, it was concluded that it is relevant to analyse the contingencies included in the "must run" and busbars list, presented in section 4.5.2.1, adding some more N-2 contingencies that tripped because of lightning or forest fires and are not part of the current "must run" list. After analysing the incidents' historical data, it was concluded that the criterion including only N-2 contingencies of double circuits (OHLs sharing the same towers) with more than 35 km of length is not adequate, because there are shorter double circuits that are frequently affected by common cause faults. The list of N-2 events used in the analysis was presented in table 7.9, in section 7.6.4.2. N-2 events caused by hidden failures were not considered, because they are out of the scope of this research work. Common cause faults due to extreme wind conditions were also not considered, because there was not enough historical data to perform a rigorous analysis.

8.4.2. Thermal overload

Thermal overload occurs when the power flow in a component is above the defined rating. For the post-contingency results, equation (8.2) is calculated for each branch that is overloaded, as an approximation to quantify the severity of the overload.

$$sev_{overload_i} = \begin{cases} \dfrac{S_i - S_{max_i}}{S_{max_i}}, & S_i > S_{max_i} \\ 0, & S_i \leq S_{max_i} \end{cases} \qquad (8.2)$$

After calculating the overload severity for each branch, all overloads caused by the k^{th} contingency need to be aggregated into a common function. In order to give more weight to more severe overloads, the severity is given by equation (8.3), which will prevent that for example 5 overloads of 10% have the same impact as one of 50%.

$$S_{overload} = \sum_{i}^{n} \left(sev_{overload_i} \cdot 100 \right)^2 \qquad (8.3)$$

where n is the number of branches.

8.4.3. Voltage limit violations

Voltage limit violations occur when voltages are outside the defined acceptable range, which is normally quite small. For the post-contingency results, equation (8.4) is calculated for each busbar that is out of the acceptable range. The maximum voltage limit is important to consider, because the higher the voltage, the higher the probability of flashover.

$$sev_{voltage_j} = \begin{cases} \dfrac{v_{min} - v_j}{v_{min}}, & v_j < v_{min} \\ 0, & v_{min} \le v_j \le v_{max} \\ \dfrac{v_j - v_{max}}{v_{max}}, & v_j > v_{max} \end{cases} \quad (8.4)$$

After calculating the voltage severity for each busbar, all voltage violations caused by the k[th] contingency are aggregated into a common function, having the same principle as the overload function, as in (8.5).

$$S_{voltage} = \sum_{j}^{n} \left(sev_{voltage_j} \cdot 100 \right)^2 \quad (8.5)$$

where n is the number of busbars.

8.4.4. Non-convergence index

The non-convergence of the power flow (PF) computation in the post-contingency analysis can indicate a very severe situation in the system. If the power flow diverges, it is assumed that the occurrence of the k[th] contingency results in voltage instability. The acceptability of this approach has been demonstrated in [150] and it is not the objective of this index to determine the exact point at which the voltage collapse might occur. Equation (8.6) presents the non-convergence index. This is one of the most severe results, together with the loss of load, in the severity evaluation.

$$S_{NC} = \begin{cases} 1, & if\ PF\ diverges \\ 0, & if\ PF\ converges \end{cases} \quad (8.6)$$

More complex calculations to assess voltage instability are not compatible with on-line assessment because of computational time.

8.4.5. Loss of load

The loss of load is expressed in MW and its evaluation is of great importance, because when it happens it has a large social and economical impact. For the post-contingency results, the loss of load per busbar LL_j is determined. To normalize the loss of load that resulted from the k[th] contingency to be used in a global severity function, equation (8.7) is calculated.

$$S_{LL} = \frac{\sum_{j}^{n} LL_j}{Total\ Load} \times 100 \quad (8.7)$$

where n is the number of busbars with load loss.

8.4.6. Loss of generation

The loss of generation is also expressed in MW and its evaluation is relevant because of generation reserve schedule. In this analysis, only the loss of conventional generation or generation removed because of the outage, as a consequence of a contingency, are included, assuming that the lost generation does not reconnect in less than 15 minutes. Therefore, the loss of generation caused by a voltage dip is excluded. The latter will be further developed in section 8.10.

For the post-contingency results, the loss of generation on the busbar LG_j is determined. To normalize the loss of generation that resulted from the k[th] contingency to be used in a global severity function, equation (8.8) is calculated.

$$S_{LG} = \frac{\sum_{j}^{n} LG_j}{Total\ Generation} \times 100 \qquad (8.8)$$

where n is the number of busbars with generation loss.

8.4.7. Islanding criterion

Another possible consequence of a severe contingency is the formation of an island. In the 6[th] September 2001 incident, described in section 2.3.2, following the dependent double contingency caused by an initiating fault and a hidden failure, a cascading sequence due to overload occurred and, in the end of that sequence, the grid south of Sines substation was an isolated island. To handle islanding situations, there are two possible approaches. The first method always considers the worst scenario by assuming that everything collapses independent of the balance between generation and load. The second method creates a balance criterion and assumes that if the balance criterion is fulfilled the island is stable. The second method was implemented and the balance condition is given by equation (8.9).

$$Balance\ \ Criterion = \begin{cases} Balanced\ \ island & if\ 1.1\,Generation \geq Load \\ Lost\ \ island & if\ 1.1\,Generation < Load \end{cases} \qquad (8.9)$$

The capacity of frequency regulation in the balanced island, which depends on which generators are connected to the formed island is also evaluated. If an island is lost, the loss of its load and generation is taken into account for the severity calculation.

8.4.8. Cascading analysis

Cascading is a sequence of dependent events. In this research work, only cascading caused by overloads is addressed. There are two types of cascading caused by overload, namely:

- Overhead line sag caused by thermal overload with a subsequent short-circuit caused by increasing proximity to external objects;
- Operation of distance protections under certain conditions.

The transmission capacity of a conductor is limited by the conductor's maximum design temperature, which determines the maximum sag of the conductor, and the rate of annealing, therefore the cumulative loss of strength of the conductor. The thermal expansion caused by the increase in temperature can result in the line dropping beneath its safety clearance. Under certain conditions, this may cause flashover to the ground, resulting in ground fault, outage of this circuit, and weakening of the system with the possibility of cascading events [77]. As conductor temperature increases, the conductor elongates depending on its

coefficient of thermal expansion. Due to thermal inertia, conductor sag does not occur instantaneously. The typical thermal inertia time constant of an overhead conductor is about 10 to 20 minutes [151], allowing temporary overloading without sag concerns and giving the control room operators time to react.

In this research work, it is assumed that control room operators take prompt remedial action immediately after being warned by an overload alarm in order to avoid the thermal expansion. Remedial actions will mitigate the overloads and bring the system back to a secure state.

There are no dedicated transmission line overload protection systems in the Portuguese transmission system. Therefore, whenever there is an overload, which is not eliminated by the protection system, a risk of short-circuit caused by the OHL sag is real. At the moment, there are few special protection schemes implemented in the system to react against overloads, which normally involve generation shedding to reduce/solve overloads. On the other hand, in the presence of a severe overload, the distance protections, based on under-impedance functions, can be misled and interpret it as a remote short-circuit not cleared by the primary protections and consequently trip above a certain threshold and time, especially, but not exclusively, for non-supervised *Zone 3* with mho characteristics.

In case of OHLs, the protection system will allow up to $1.5xI_{max}$ (winter capacity limit in Amps) within a power angle of 30º maximum, which assumes a voltage value near the nominal one. For transformers, the distance protections will allow up to $2xI_{nominal}$ with a power angle of 40º maximum. If these conditions are exceeded and the apparent impedances are within the backup zone reaches of the distance protections (depending on actual reaches of the step zones of protection), the trip will occur in less than 3 seconds.

Below the presented thresholds and with no other fault condition, the protection system will not trip, so it is possible to assume that there is no risk of cascading. Above these current thresholds, there is a significant risk that the grid elements will trip, depending on the actual zone reaches of the distance protections, which take into consideration coordination issues related to short-circuit analysis. As these are difficult to attain for the purpose of this simulation, we shall consider a probability to trip equal to 100%, to verify subsequent severity, in such cases. So, considering the tripping criteria, and after removing the grid elements with currents higher than $1.5xI_{max}$ for OHLs, and $2xI_{nominal}$ for transformers, a new power flow is simulated in order to assess the new severity and verify if there are more grid elements tripping after the ones that were disconnected because of overload.

The identification of possible cascading events is very important for real-time operations and for operations planning. Cascading outages are addressed in this work as follows:

- Identify the contingencies that may lead to cascading.
- Simulate iteratively cascading outages due to consecutive opening of overloaded branches.

For each contingency, the cascading algorithm is run after the power flow simulation if there are thermal overloads $S_i \geq S_{max_i}$, where S_i is the power flow on the branch i and S_{max_i} is the thermal limit of the branch i, both expressed in MVA, which are the units for the results given by PSS/E.

Cascading algorithm:

1. The protection system operates if $\frac{S_i}{S_{max_i}} > 1+\delta, \quad \forall i$, where δ=0.5 for OHLs and δ=1 for transformers (δ is the defined tripping threshold), disconnecting the overloaded branch.
2. Simulate power flow again.
3. Identify possible loss of load, loss of generation and power flow non-convergence.
4. If there are thermal overloads, go to (1).

5. Stop the simulation when:
    a. No overload beyond the tripping threshold occurs
    b. The power flow simulation diverges

For every contingency where the cascading algorithm was run, the severity is calculated in the following way:

- In case of thermal overloads and voltage limit violations, the results of the first iteration are considered.
- In case of load and generation loss, the results of all iterations are included and summed per type in the end.
- In case of islanding, the islanding criterion is applied.
- In case the power flow diverges, the non-convergence index is equal to one.

Cascading events caused by overload can result in N-k (k>1) contingencies that may cause loss of load, loss of generation, islanding or voltage stability problems.

8.4.9. Global severity

The severity evaluation for each contingency is made by several types of impact, namely:

- Thermal overload
- Voltage limit violation
- Voltage instability (non-convergence index)
- Loss of load
- Loss of generation

For each type of impact, an individual risk index $Risk_{type}^{k}$ can be calculated by multiplying the probability of the kth contingency by the result of the severity function for each type S_{type}^{k}, expressing the consequences of the kth contingency which is being evaluated, as in equation (8.10).

$$Risk_{type}^{k} = probability_{k} \times S_{type}^{k} \tag{8.10}$$

Nevertheless, also a global severity function per contingency is going to be calculated as in equation (8.11).

$$Severity_{k} = \sum_{type} \left(\omega_{type} \cdot S_{type}^{k} \right) \tag{8.11}$$

where ω_{type} is the weighting factor to value the importance of each type of severity

Table 8.2 presents the weighting factors to be used in this work per type of severity.

Type of severity	Weighting factor
Loss of Load (**LL**)	54.0
PF non-convergence (**NC**)	500.0
Thermal overload (**OL**)	2.1E-03
Voltage limit violation (**VL**)	3.0E-03
Loss of Generation (**LG**)	4.5

Table 8.2 – Severity weighting factors

The weighting factors were determined based on the comparison of the numerical results of each individual type of severity and also on an engineering judgement of how important each type of severity is. Figure 8.3 illustrates this approach, showing the range of variation for each severity, reflecting their relative importance. As a starting point, the weighting factor for the most important severity type, loss of load, was chosen such that the maximum severity of this type is equal to 1000. The number at the top of each column in figure 8.3 is the maximum severity value per type. Similarly, for all the other severity types a maximum value was chosen and the corresponding weighting factor was thus calculated.

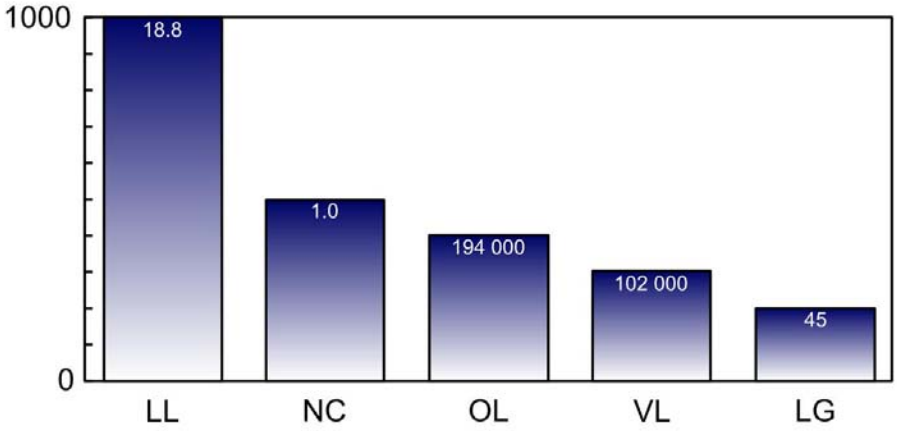


Fig. 8.3 – Relative importance of each severity type

8.5. Risk indices

Operational risk assessment aims to predict the risk of the system during a short period of time. The total risk of the k^{th} contingency is calculated as in equation (8.12) and the total risk of the system (SR) for the period under analysis is given by equation (8.13).

$$Risk_k = probability_k \times Severity_k \tag{8.12}$$

$$SR = \sum_{k}^{N} Risk_k \tag{8.13}$$

where N is the total number of contingencies.

8.6. Severity results

Using a snapshot per hour, the severity was calculated, aiming to obtain an input for the risk-based security assessment. The analysis was made from July until December 2009, based on 4416 recorded SE snapshots.

The snapshots that were used were exactly the ones saved in the date and time under analysis, therefore the simulation starts from a real and well defined system state. The severity assessment uses the following assumptions:

- The protection system of the faulted circuit operates and clears the fault.
- The circuit-breakers always open correctly.
- Automatic re-connection is not considered for the evaluation.
- The repair time of the components is not considered.

– For the existing closed loops through the distribution network that did not have energy not supplied during the time considered for statistical analysis in this work, the loss of load and of generation is considered zero.

Not all contingencies that were simulated have violations. The severity of N-1 OHL contingencies is often zero or it has a low overload, except for exceptional operating conditions that may occur during a limited period of time. Voltage limit violations are rare for N-1 contingencies, normally when they happen the violations are of low severity. Common cause contingencies are also evaluated and obviously their results are more severe. This type of contingencies, as already mentioned in chapter 7, only occur with the presence of a specific cause and its evaluation can be decided based on forecast information. In this work lightning and forest fires were considered. As expected, the contingencies composed of a busbar have generally the most severe consequences, but their probability is lower and more constant than the other contingencies that were analysed.

For this historical data analysis, remedial actions were not considered. Figure 8.4 shows the flowchart of the severity analysis that was performed. The first power flow is just for the SE snapshot validation.

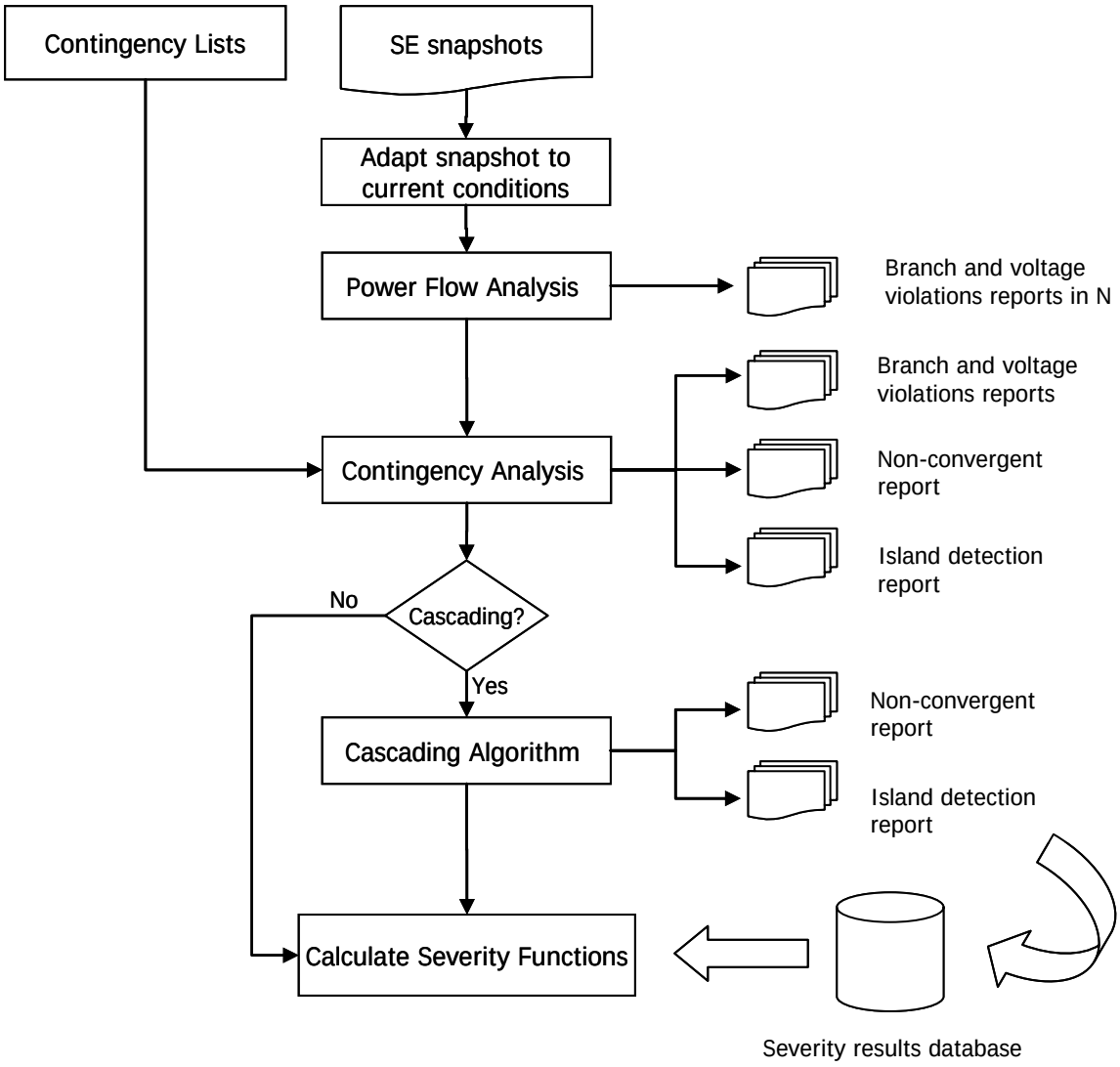


Fig. 8.4 – Severity evaluation flowchart

Figure 8.5 shows the flowchart of the cascading algorithm that is presented in section 8.4.8.

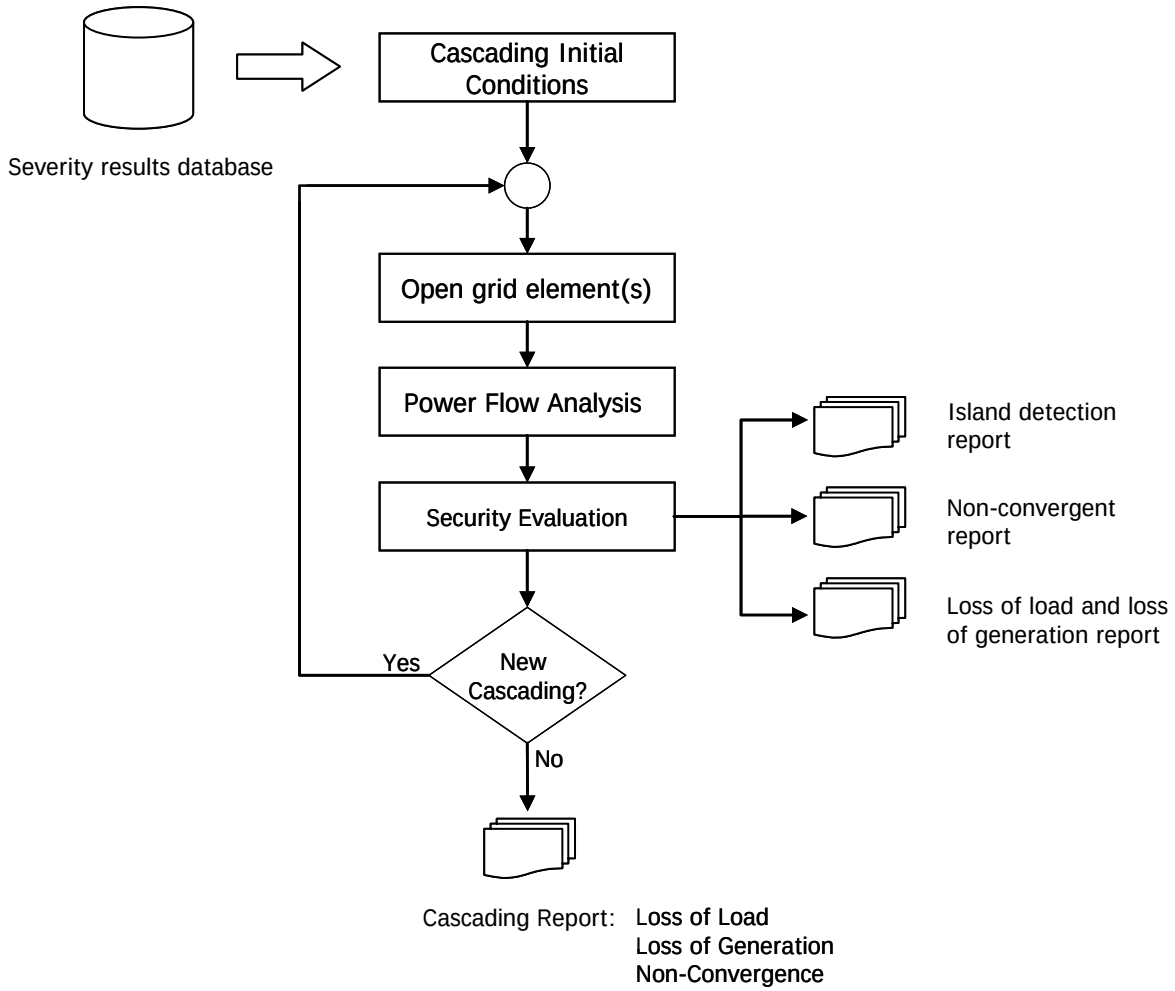


Fig. 8.5 – Cascading algorithm flowchart

In order to illustrate the analysis that was made, figure 8.6 presents the N-2 contingencies on the 23rd of December 2009 at 18h, which was the hour with the highest risk in the second half of 2009. The N-2 contingencies are responsible for the high severity results.

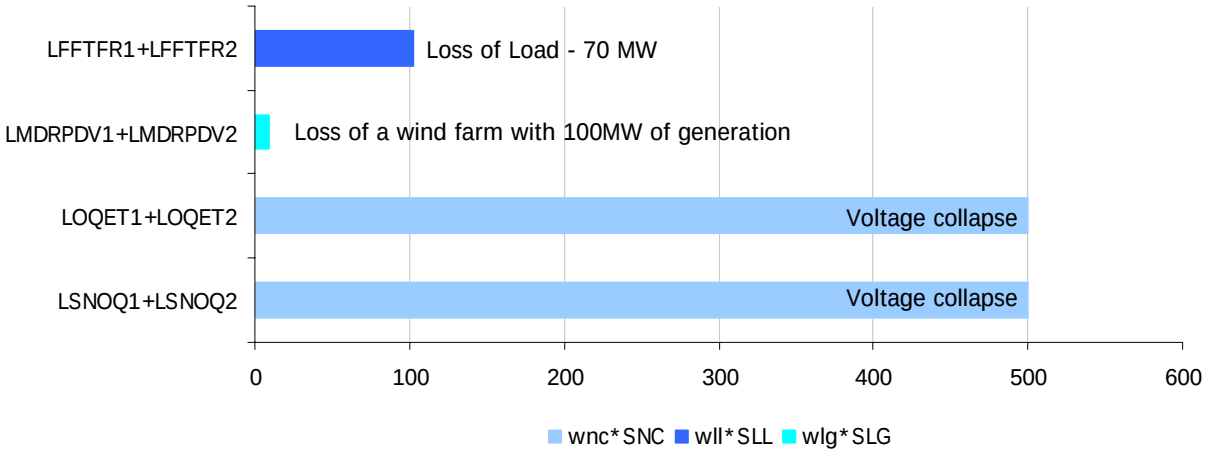


Fig. 8.6 – N-2 severity results for the 23rd of December 2009

Another example is the severity results corresponding to a peak load hour in summer time, e.g. 23rd of August 2009 at 20h. In summer the load in Algarve is significantly higher than in winter. Figure 8.7 presents the most severe busbar contingencies at the defined time. The most severe situations are the following:

1. A contingency on the 220 kV busbar in the vicinity of a natural gas combined cycle power plant (NGCC), and because August was a dry season, that power plant was at the maximum of its production capacity. This contingency resulted in power flow not converging, causing the voltage collapse at one substation.
2. A contingency on the 150 kV busbar in a substation in the south of Lisbon, which connects a coal thermal power plant. This contingency caused the voltage collapse at three substations in Algarve.
3. A contingency on the 150 kV busbar in a substation in Alentejo causes a voltage collapse situation at least in one substation in Algarve.

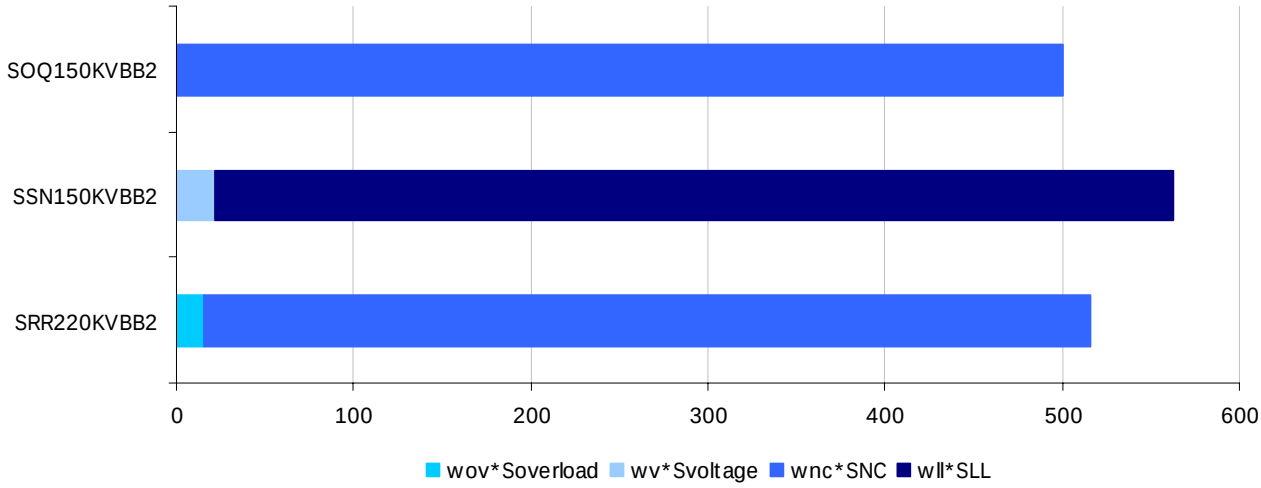


Fig. 8.7 – Specific busbars severity results for the 23rd of August 2009

8.7. Risk results

In order to evaluate the developed methodology, the risk was calculated from July until the end of December 2009, aiming to perform the H-1 analysis based on recorded conditions as if it was performed in real time. With probability and severity results, risk is evaluated.

Figure 8.8 presents the risk trend during the period under analysis. In this figure, it is possible to observe the forest fire influence that in 2009 occurred mainly in the end of July, end of August and mid September.

The high severity values, which occurred in the end of 2009, are justified by the incident of 23rd December 2009 (described in section 2.3.4), which caused the forced outage of 6 OHLs, four in the centre and two in the south of Portugal. The highest peak of risk on the graph corresponds to the total value of risk calculated for the 23rd December at 18h, where the presence of lightning and the disconnected OHLs have caused the system to be more vulnerable. In this example, due to lightning, the two N-2 common cause contingencies in the south have a probability different from zero and both do not converge in terms of severity, resulting in a extreme risk value. If one of these N-2 events had occurred, that would result in a voltage collapse of at least one substation in the Algarve. For the contingency LOQET1+LOQET2, one substation is expected to be lost and for the contingency LSNOQ1+LSNOQ2, three substations are expected to be lost.

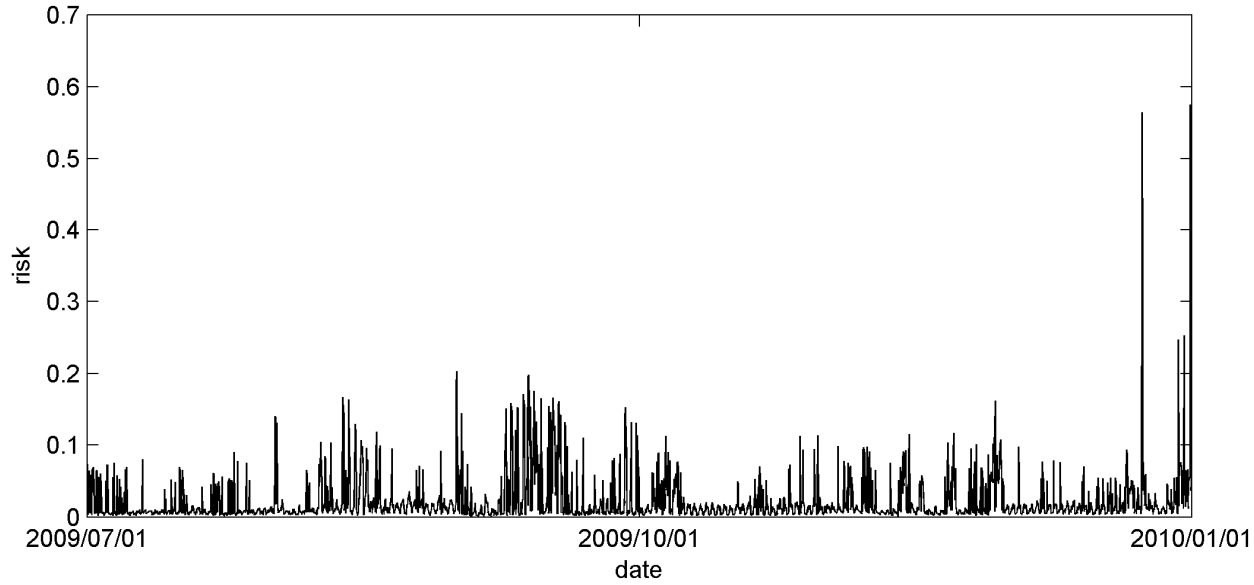


Fig. 8.8 – System's total risk per hour

Figure 8.9 shows the probability versus severity of each contingency, in which is possible to observe that some of the contingencies have a high risk. Figure 8.10 shows figure 8.9 zoomed in the area of the represented rectangle, in order to give an exemplification of a level of risk, and the iso-risk curve that is drawn represents the median of the total risk per hour.

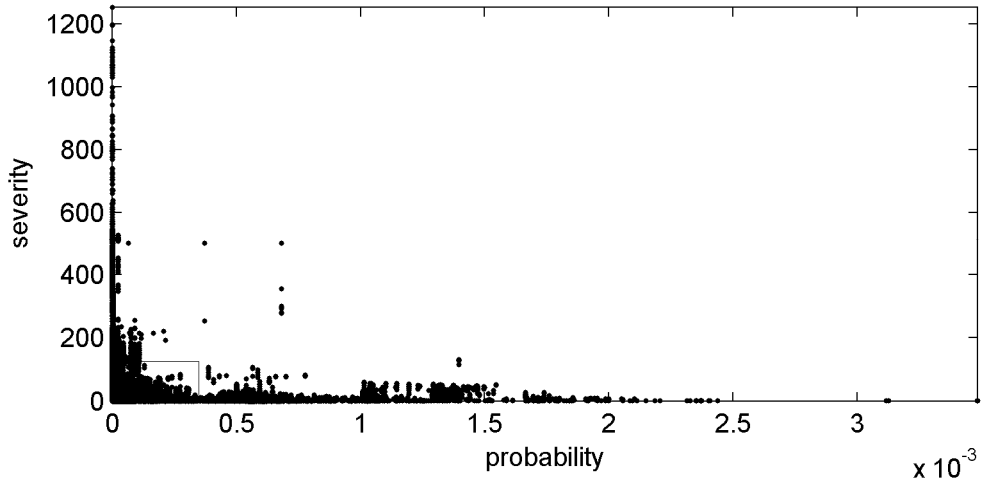


Fig. 8.9 – Probability vs. severity graph of the period under analysis

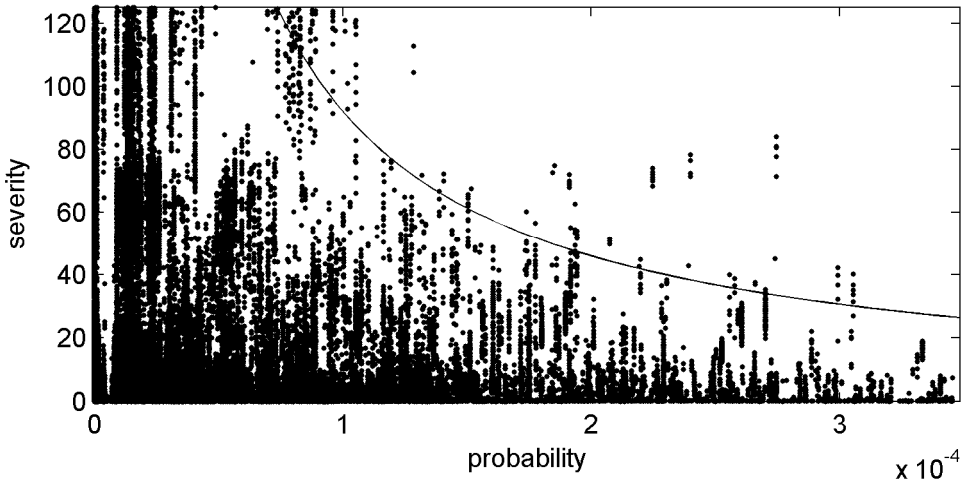


Fig. 8.10 – Zoomed probability vs. severity graph for the period under analysis

In order to show some specific examples of risk, two busbars (B2 220 kV SRR and B1 150 kV SSN), one N-2 event (LSNOQ1+LSNOQ2) and a single contingency (LRMAM) were selected. As acknowledged in chapter 7, the probability of occurrence of contingencies in busbars is very low. The probability of the double contingency is only affected by lightning, resulting in the same value for each severity, i.e. in a vertical line in the figure 8.11, as for busbars. This single contingency is mainly affected by the effect of storks, fog combined with pollution and forest fires, justifying its large variation. Lightning has a small effect because of its low BFR value. In terms of severity, this contingency mainly causes overloads. As expected, the severity result is higher for busbars and double contingencies, because it can result in voltage collapse, loss of load and loss of generation in specific operating conditions. Busbars have a much lower probability than OHLs. The probability of fault graph for each selected contingency can be found in appendix J.

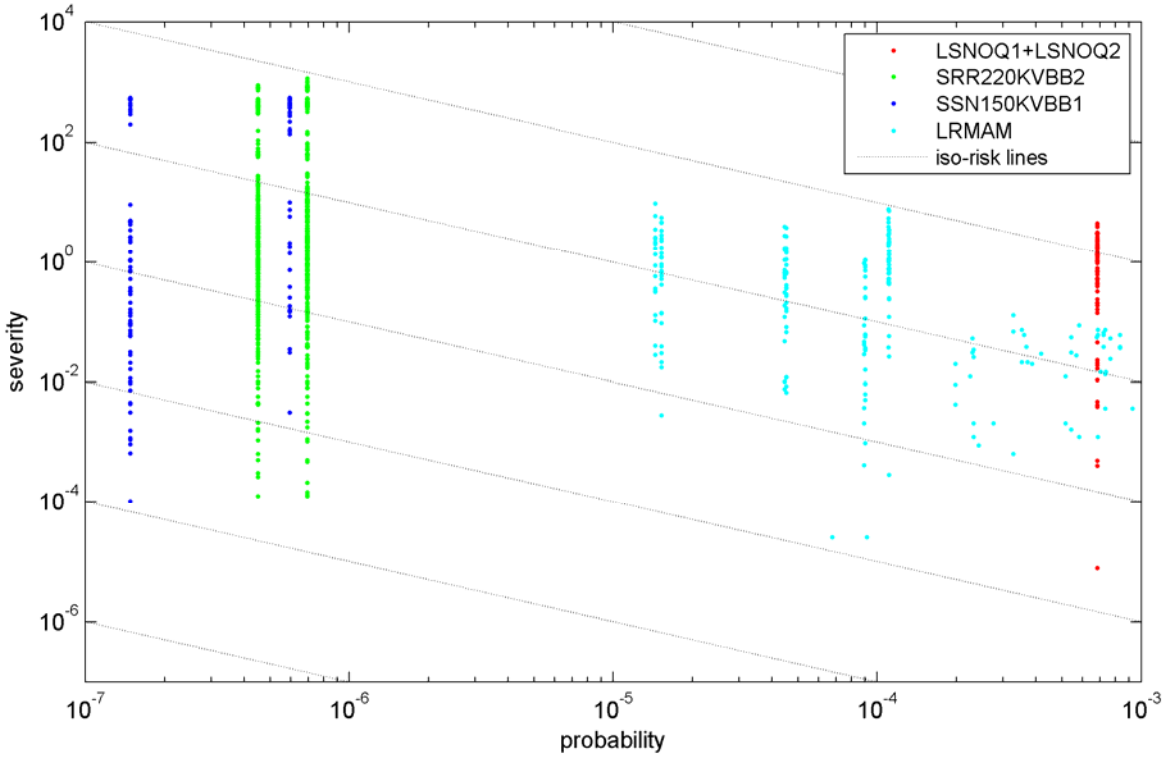


Fig. 8.11 – Probability vs. severity graph of four different contingencies in the period under analysis

In addition, for each selected contingency, the total risk per hour is shown. Figures 8.12, 8.13 and 8.14 clearly show an increase in the risk in the end of the year due to the incident that occurred on the 23rd December 2009. Figure 8.12 presents the total risk per hour of the LRMAM contingency. In the entire period of 6 months, there was only one cascading situation, which corresponds to the highest value of severity. The high risk in this contingency corresponds to a high severity and results from the fact that this OHL was essential in the supply to Lisbon, due to the fact that only 2 OHLs were connected from the 6 OHLs that compose the north corridor.

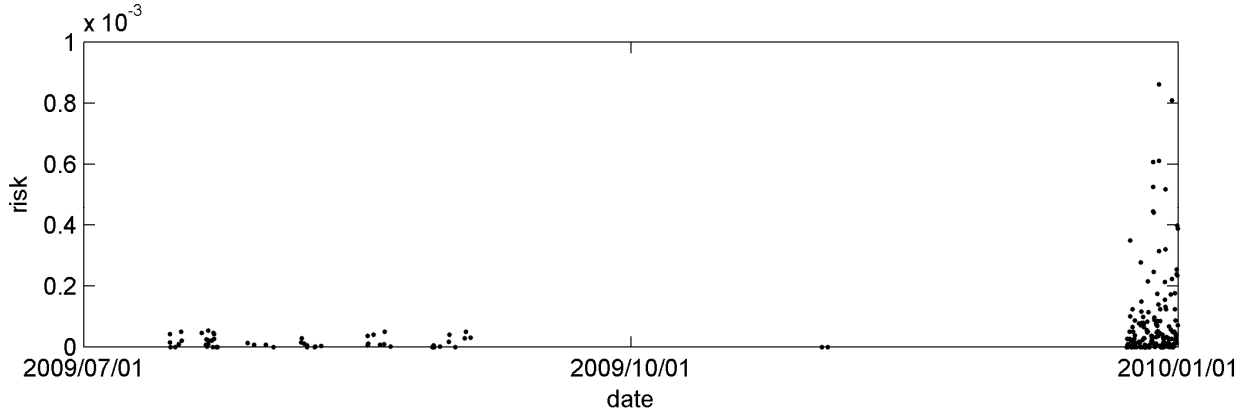


Fig. 8.12 – Total risk per hour of the LRMAM contingency

Figures 8.13 and 8.14 present the total risk per hour of the double contingency LSNOQ1+LSNOQ2 and of the 150 kV busbar of Sines. The increase of the risk in the end of the year is once more due to the incident caused by extreme conditions in December 2009, specifically because of the 2 OHLs (double circuit in the same corridor) that were damaged and could not be reconnected.

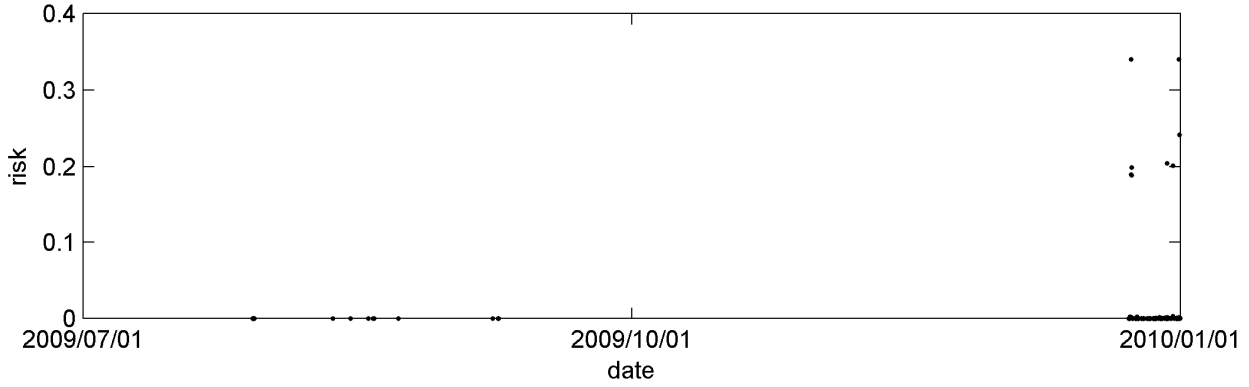


Fig. 8.13 – Total risk per hour of the LSNOQ1+LSNOQ2 contingency

The contingency of the B1 150 kV SSN, for the worst values of risk that correspond to the worst values of severity, causes a voltage collapse at several substations in the south of Portugal. These highest risk points correspond to a special topology in SSN substation, when only one busbar was operational.

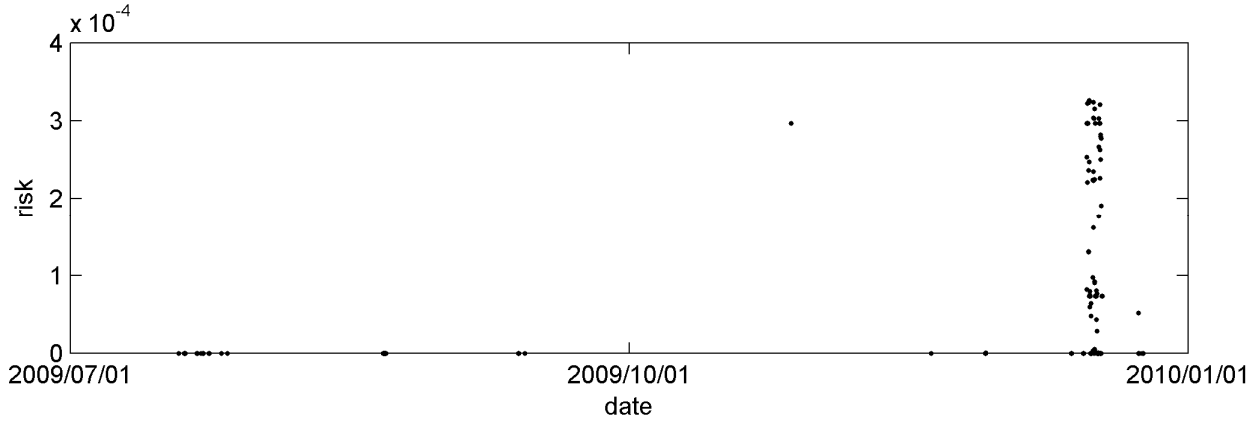


Fig. 8.14 – Total risk per hour of the B1 150 kV SSN contingency

Figure 8.15 presents the total risk per hour of the B2 220kV SRR contingency. The B2 220kV SRR is located near Porto and in the vicinity of a NGCC that is important in dry periods. In the most severe periods, cascading sequences and power flow non-convergence were recorded, having as a consequence, either the islanding of the power plant with another 220 kV substation or the voltage collapse of that substation.

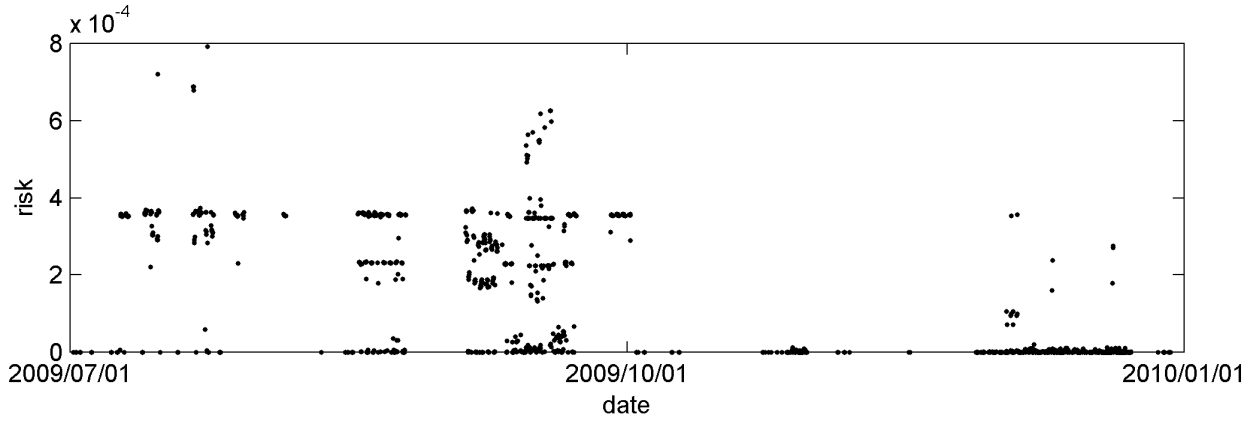


Fig. 8.15 – Total risk per hour of the B2 220 kV SRR contingency

8.8. Computational time

In the risk assessment methodology, the first two parts can run in parallel, i.e. the calculation of the probability of each contingency and the calculation of its severity (including cascading sequence analysis). Taking into account the characteristics of the available servers in the Portuguese TSO to run both methods, where each server has 2 Intel Xeon E5335 running at 2GHz frequency clock, each method is expected to take less than 20 seconds, performing the calculation for the next hour. After these processes, the calculation of risk indices is expected to take approximately 5 seconds for one hour. Therefore, the total computational time for the entire risk evaluation is expected to take less than 30 seconds for periods of 1 hour, which is compatible with online analysis.

8.9. Contingency costs

There are two direct costs that can be evaluated after a contingency namely the cost of energy not supplied and the cost of generation reserve that was needed to start in order to restore security, i.e. bring the system back into a secure state.

In general terms, the energy not supplied in MWh is the interrupted load in MW multiplied by the interruption time in hours. From 2001 until 2009, the average interruption time, considering all load interruptions in the Portuguese transmission system, was around 14.5 minutes, but the median of the values was around 5 minutes. These values include the force majeure ones. Figure 8.16 presents a histogram of the time per interruption caused by faults in the Portuguese transmission system.

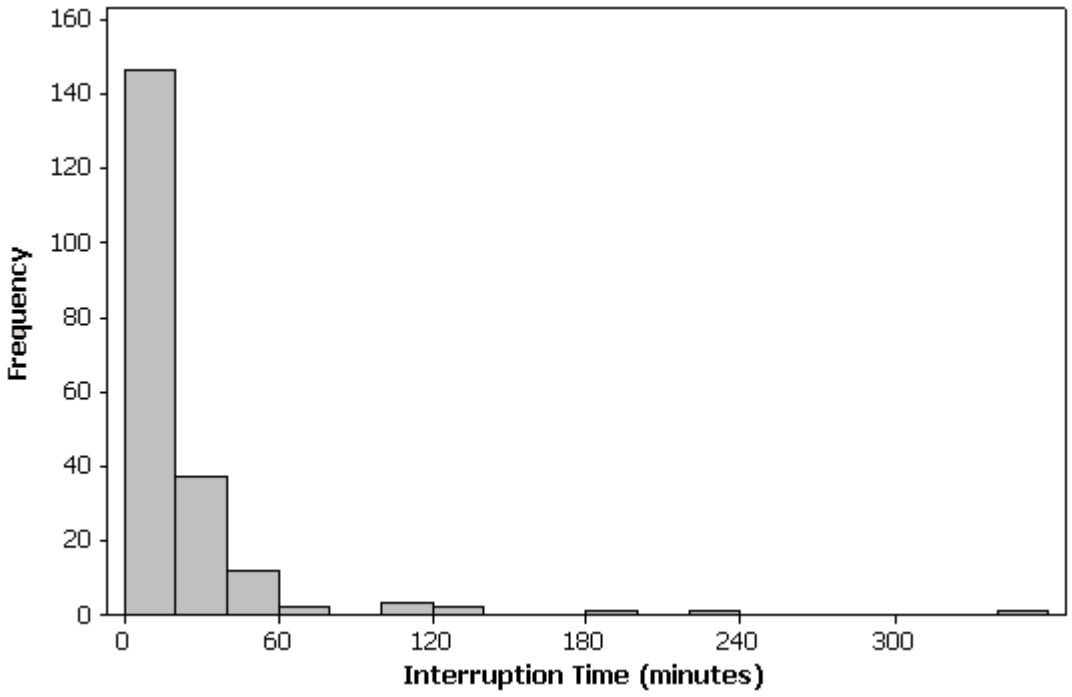


Fig. 8.16 – Interruption time histogram

Due to the fact that different substations have different dimensions, the average and the median of the interruption time per circuit-end that supplies consumption were calculated in the same period, being 7.3 and 2.3 minutes, respectively. Based on experience, it is concluded that 2.3 minutes per circuit-end is a reasonable interruption time to consider. These values can be updated every time that a new interruption occurs. Therefore, depending on the amount of substations without energy, the interruption time will be calculated considering the number of affected circuit-ends that supply load. In this work, for simplification, the average number of circuit-ends per substation is used, considering 11.5 minutes (i.e. 0.19 hours) as the interruption time for calculation per substation.

For each contingency, the cost of the load loss can be calculated by equation (8.14).

$$Cost_{LL}^{k} = f_{cost}\left(LL_k \times TI_k\right) \tag{8.14}$$

where $LL_k = \sum_{j}^{n} LL_j$ is total load loss for the k[th] contingency in MW and n is the number of busbars with load loss. $TI_k = TI_{end} \times NE$ is the interruption time in hours for the k[th] contingency. For severity evaluation, the TI_{end} corresponds to the median interruption time and NE is the number of affected circuit-ends that supply load. $f_{cost}\left(LL_k\right)$ is the function that determines the cost of the interrupted power in €/MWh.

Long-term studies use as the cost of energy not supplied 250 €/MWh for the first MW not supplied and it is assumed that the economical impact of energy not supplied increases as more power is interrupted. Therefore, the cost of energy not supplied grows linearly with the interrupted power, reaching a cost 10 times higher for an interrupted power equivalent to 10% of the recorded load peak, which is around 9 GW. As a result, the cost function is given by equation (8.15).

$$f_{cost}\left(x\right) = 2.5x + 247.5 \tag{8.15}$$

The generation reserve costs depend on the daily market price for the tertiary reserve. It is only needed to start units to reduce the ACE back inside the acceptable range. In Portugal, there is no emergency market and the fastest units are started without considering price and they are paid at their bid price. This is only possible online in the H-1 analysis.

After each contingency, the total loss of generation is determined by summing the generation loss of all busbars, i. e. $\sum_{j} LG_j$ in MW.

The total direct cost of a contingency can be evaluated by the loss of load cost plus the cost of the needed generation reserve, which is determined by the market. This does not include the repair time cost, because it cannot be assessed in advance, nor any other costs that are not directly connected with system operations.

8.10. Wind generation facing disturbances

The impact of wind generation on the transmission system was described in chapter 4. As mentioned in section 4.3.1, short-circuits provoke voltage dips with the duration of the fault clearing time that consequently can cause wind generators to trip.

The analysis of the loss of wind generation associated with each short-circuit is evaluated for each incident, in order to assess its impact on the transmission system operation, regarding the instantaneous deficit of generation in the system, which is automatically compensated by the tie-lines and the restoration of wind farms. This off-line analysis was made by REN for all the incidents since 2006 and, in order to illustrate its results, an example will be further presented. To perform the analysis of the loss of wind generation per wind farm for a specific short-circuit, the algorithm is described as follows:

1. To perform short-circuit simulations (normally three-phase symmetric ones) at each end of the grid element in case of a fault on an OHL or for the busbar in case of a fault inside a substation; from the short-circuit simulation, a voltage pattern is obtained.
2. Through the voltage pattern and each wind farm's characteristics (such as location, protection system settings in the interconnection with the network and fault ride-through capability

condition), it is possible to evaluate which are the wind farms that will lose generation and estimate the total loss of wind generation in MW.

3. The results of step 2 are validated with the faults' historical data for each grid element, if available, containing records of the actual loss of wind generation. This allows the evaluation of the performance of each wind farm and to predict their expected behaviour for each contingency.

The example is the incident described in section 4.3.1 that occurred on 15th November 2009. Figure 8.17 presents the voltage pattern that has resulted from the short-circuit simulation and the complementary symbols that reflect what happen in each wind farm during the fault. For this case, a phase-to-phase short-circuit was simulated in the exact location of the fault, which was recorded by the protection system [152].

From figure 8.17, it is concluded that the wind farms that lost all their units, during the incident of 15th November 2009, were in the area where the voltage was below 0.8 U_N, except two wind farms that are marked with the red circle. If the Fault-ride through had been active in all wind farms and there were no minimum voltage relays active for voltage higher than 0.2 pu, this incident would not have caused loss of wind generation.

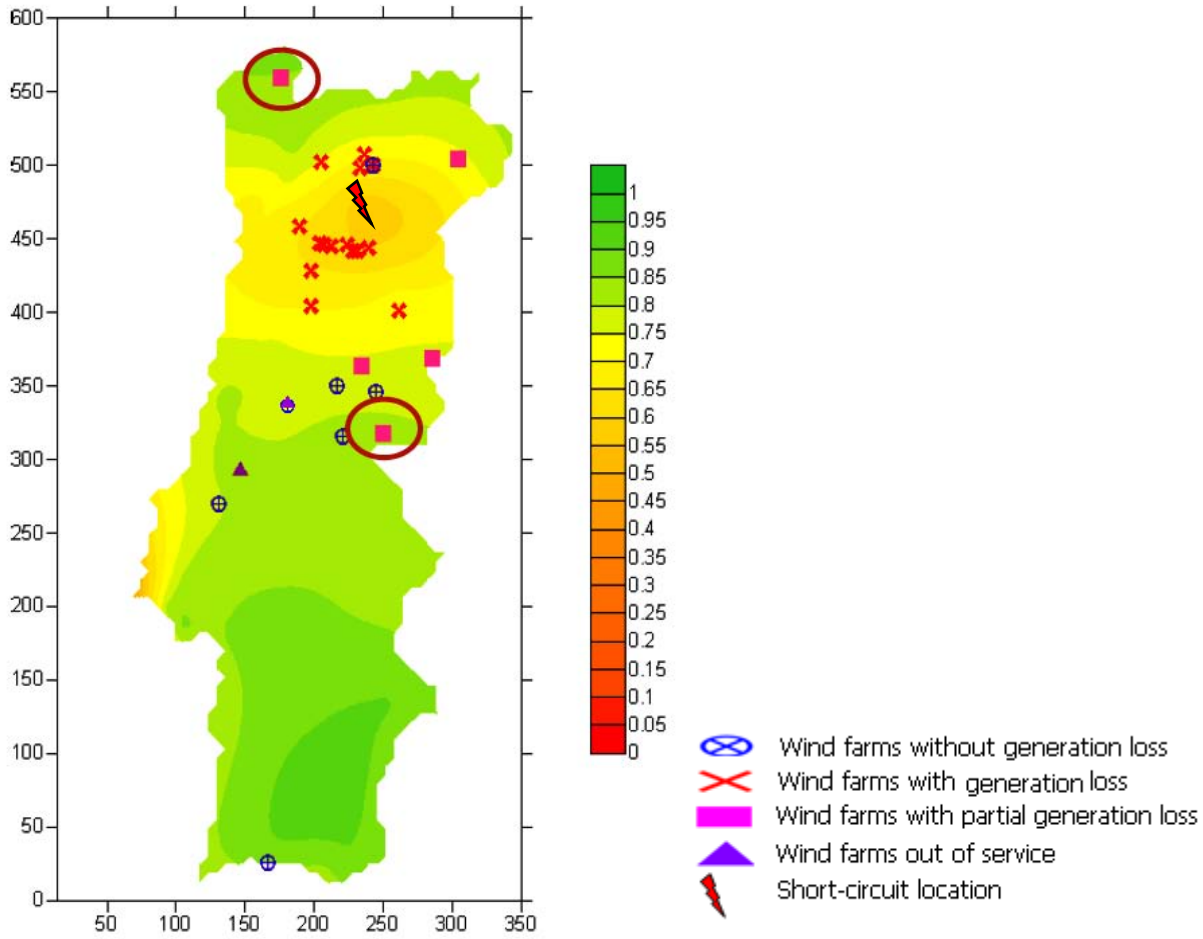


Fig. 8.17 – Voltage pattern in pu and wind farms location [152]

The short-circuit simulation with the proper characterization of the wind farms allows the introduction of the loss of wind generation in the severity analysis, removing from service with each contingency the wind farms that are expected to trip. However, with the introduction of the fault ride-through capability and the change of settings of the minimum voltage relays installed in the connection point to the grid, in several wind farms, in accordance with the voltage curve presented figure 8.18, the relevance of this analysis decreases.

Figure 8.18 shows the characteristics of the short-circuit that occurred on the 15th November 2009 compared with the voltage dip characteristics to be withstood by wind generating units.

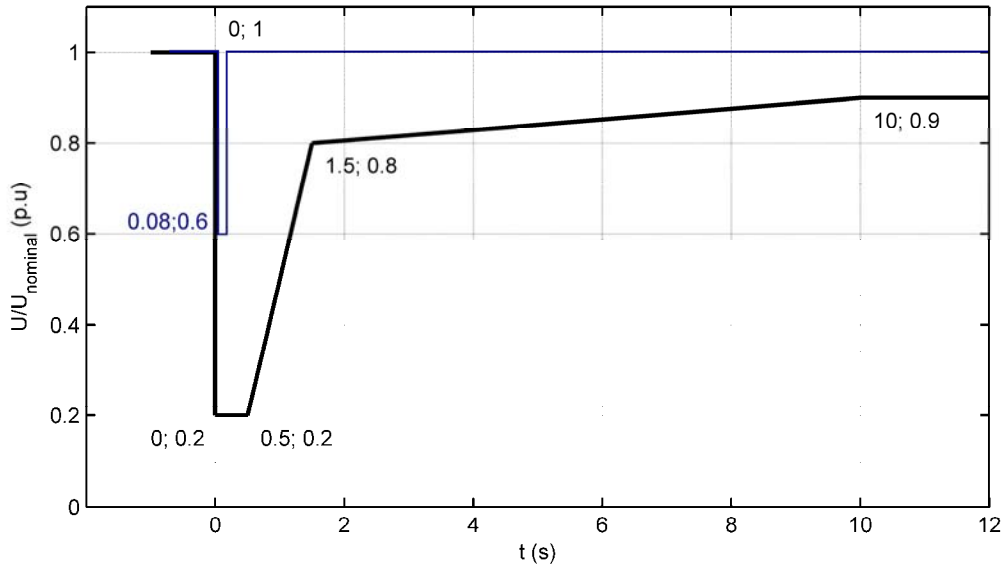


Fig. 8.18 – Characteristic of the 15th November 2009 short-circuit [152]

Figure 8.19 presents the real curve recorded in three different busbars in the 220 kV network at the moment of the incident. The nearest substation from the fault's location that has voltage measurements is SRR and the distance to the place of the fault is around 68km on a straight line.

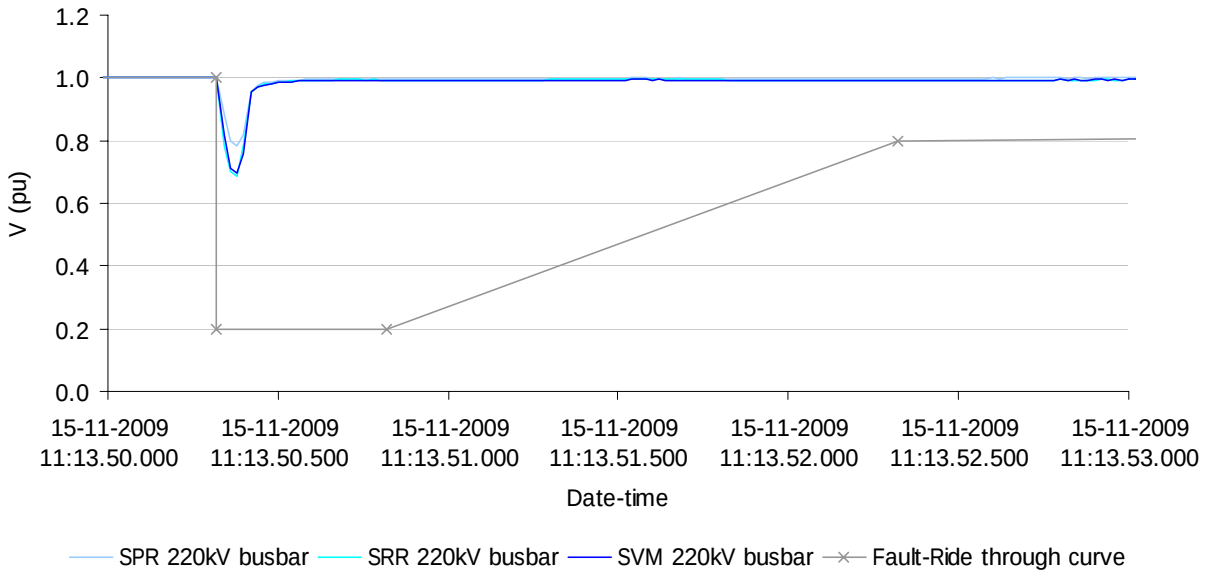


Fig. 8.19 – Voltage measurements recorded in three different substations at the moment of the fault

Another concern regarding the loss of wind generation is the additional generation reserve that may be needed. From historical data, it is concluded that in the Portuguese transmission system the wind farms recovery time, after being disconnected because of a voltage dip, is on average 8 minutes. The ability to restore the loss of power, in less than 15 minutes (see section 4.8.2), indicates that the need of additional reserve will not correspond to the total loss of wind generation and that they will be much lower. For instance, on the 15th of November 2009, 60% of the wind farms with telemetering were connected in less than 15 minutes.

Figure 8.20 presents the voltage dips that were recorded in 2008 [114], and it is possible to conclude that only two of the recorded voltage dips (marked with a circle) were outside of the Fault-ride through capability curve.

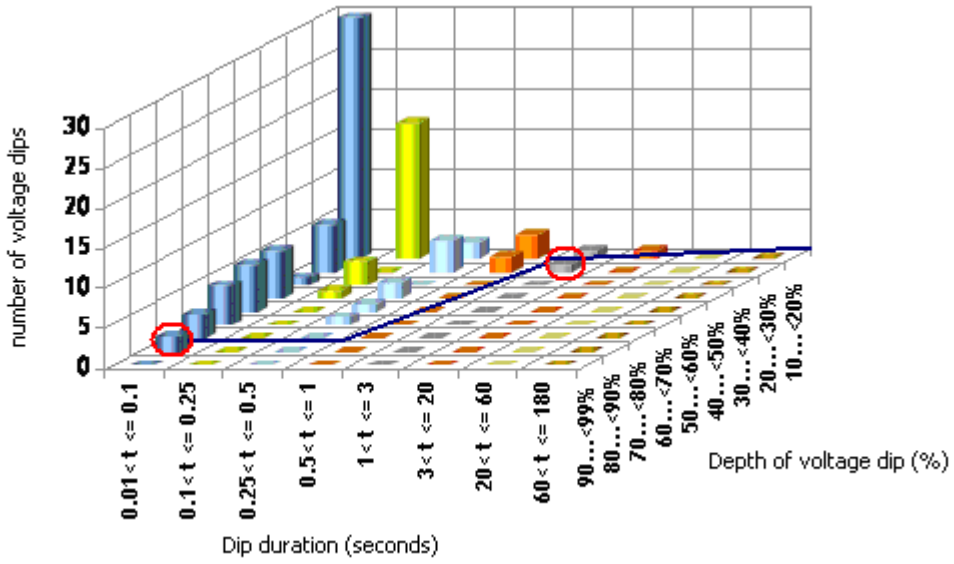


Fig. 8.20 – Voltage dips recorded in 2008

From 2006 to 2009, there were 743 incidents in the EHV network, from which 160 incidents had loss of wind generation, representing about 22% of the total amount of incidents. Figure 8.21 presents the yearly results of the loss of wind generation due to short-circuits in EHV grid elements.

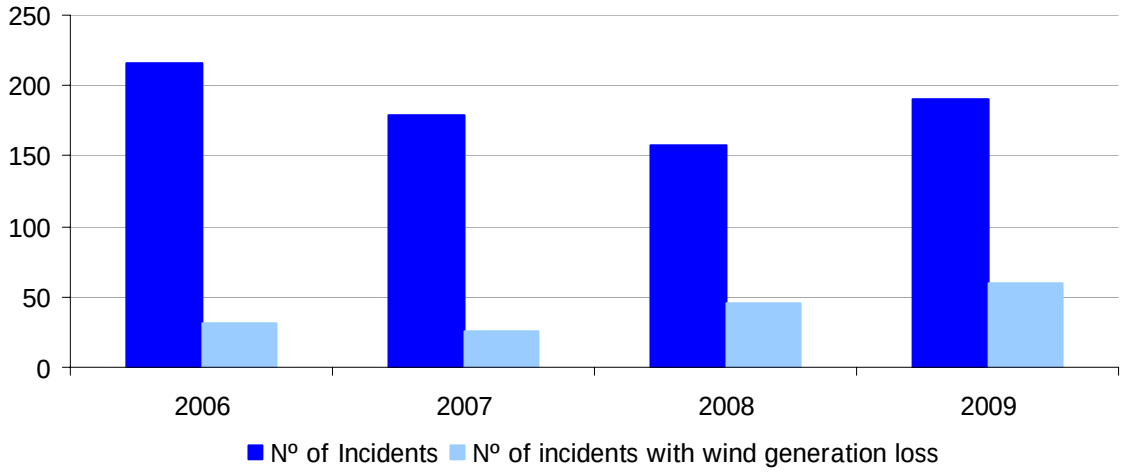


Fig. 8.21 – Total number of incidents and incidents wind generation loss

8.11. Restoration time

In spite of the fact that in the security assessment performed in the control room the restoration time of the grid elements is not considered, the analysis of the time that grid elements take to be reconnected after an incident is a very interesting one.

Figure 8.22 presents the cumulative frequency in percentage of the restoration times for OHLs and transformers. It is immediately concluded that OHLs are reconnected much faster than transformers, which is explained by two features:

- In OHLs most of the faults are fugitive, which means that most of the times the first attempt in reconnecting the component is successful without requiring any inspection or corrective action.
- Most of the OHLs have automatic reclosing implemented at both line ends, which results in the reconnection of the OHL in less than 1 second or in a few seconds, depending on the technology. The majority of OHLs only has single-phase automatic reclosing in 900 ms, although the systems with newer technologies that are being installed already have synchronization check, which also allows a more secure three-phase automatic reclosing. From the OHL faults 42% had a successful automatic reclosing, reconnecting it immediately after the fault. If the fault is permanent, the protection system operates again and disconnects the line after the automatic reclosing. In this case, it remains disconnected, until the fault is found and repaired. Forest fires can cause permanent faults but do not necessarily cause damage, allowing a quick reconnection once the forest fire is extinguished.

When there is no automatic reclosing or it fails to operate, the control room operator manually reconnects the grid elements affected by the incident. The reaction time of operators to a fugitive N-1 OHL fault, without additional failures in the restoration process, goes normally from 30 seconds to a few minutes.

After the operation of the protection system of a transformer, at least an inspection is required before reconnecting. Faults in transformers are normally permanent and therefore the restoration process is slower than with OHLs, because it involves an inspection and if applicable the repair of the damage. The same is true for busbars, because of the chance of damage after the operation of the busbar differential protection system for a busbar fault. Restoration times for busbars are also larger than for OHLs, with an average time of 75 minutes. The advantage of the busbar fault is that, after the inspection, it is possible to isolate the faulty equipment and restore the equipment which is not damaged. Therefore, from different types of components, different restoration times are expected, although efforts are always made to reconnect the grid elements as soon as possible, keeping in mind that a quick restoration is important for the security of the system. The security analysis considers the worst case, which does not assume reconnection during the period under analysis.

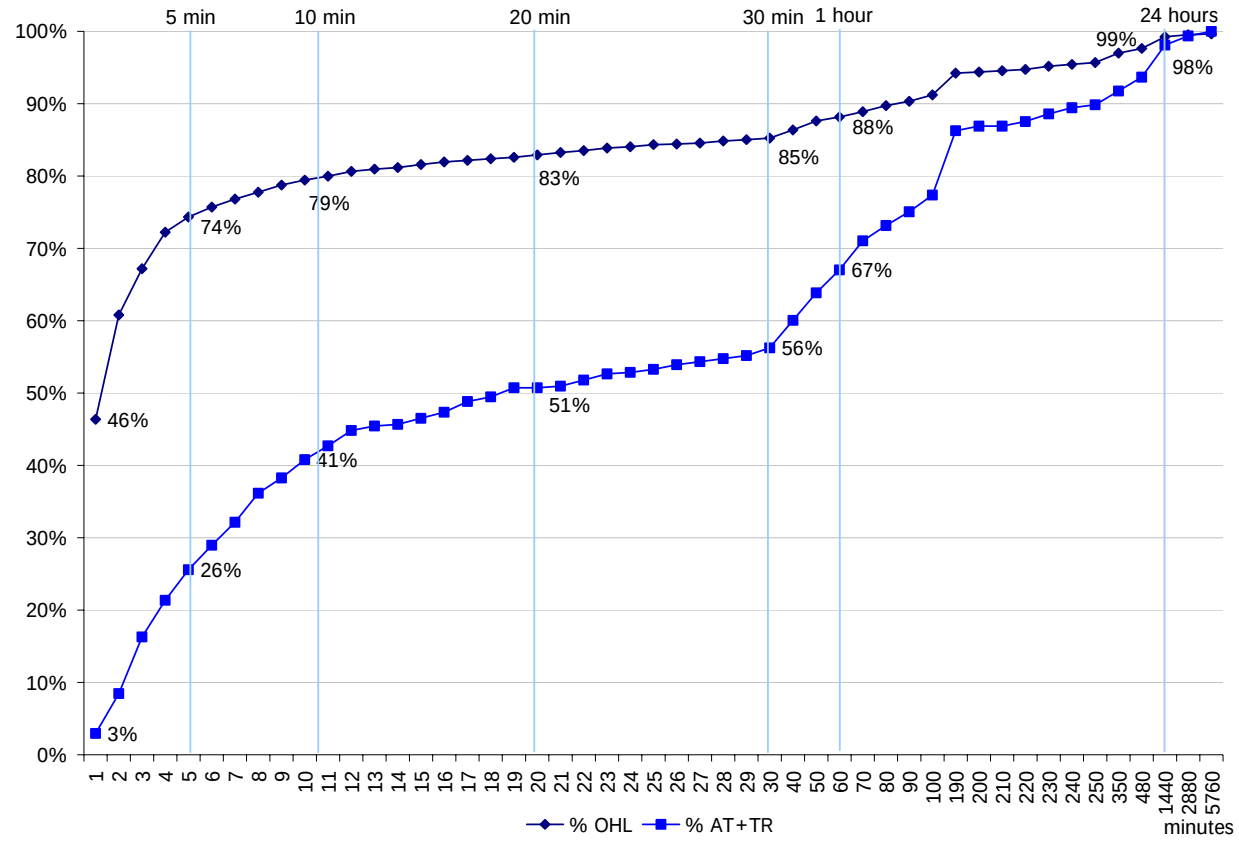


Fig. 8.22 – Cumulative frequency of the restoration time for OHLs and transformers

8.12. The methodology in the control room

In the beginning, the risk assessment methodology, using probabilistic methods, must coexist with the deterministic one, which has been used for many years by TSOs for security analysis. The new methodology needs time to prove itself and to gain the confidence of control room operators, providing enough time to interpret, test and better understand the methodology outcomes with several operating states.

The contribution of the developed methodology can be used at first to introduce additional information in the deterministic analysis and to re-adjust the list of contingencies and the decisions, based on the probability of events. Control room operators will play a decisive role, making their judgements and giving feedback on the methodology results. At this moment a question is raised: Which information is relevant to present to control room operators?

Another question that can be raised is: Is this methodology going to increase or decrease the human resources needs? This methodology may not decrease the number of human resources in control rooms and it will for sure demand highly educated people, able to understand the increasing complexity of the network behaviour and a more challenging security analysis with more vulnerable and stressed networks. The operator will always be the one deciding and taking action and the analysis of the results of the risk assessment will serve as an awareness system. Decisions should be taken at a level where the impacts of the decision are best understood, which means as close as possible to the “process” being controlled, i.e. in the control room. Therefore, relevant information and skills must be available to the decision-maker, i.e. to the operator.

It is not fair to consider the severity as final without including the remedial actions prepared for a specific contingency. If there is a prepared remedial action to be applied for the specific contingency under analysis, it should be implemented and the severity for the specific contingency should be calculated again. Handling contingencies in real time is supported by the analysis performed in the operations planning phase, which defines which remedial actions should be applied to mitigate the impact of a specific event. In advance, remedial actions are fully tested and prepared for when they are needed in real time operation.

8.13. Conclusion

A methodology to evaluate operational risk for a short-period of time was developed, taking into account the probabilistic nature of contingencies and their severity under specific operating conditions. This methodology uses several types of information to calculate risk indices, including current conditions. The risk indices provide an insight to control room operators of the network state and of the constraints that operators face. They have to be simple and fully understood by who operates the system. In the beginning they should be as close as possible to the deterministic results to which operators are used. Both methods, deterministic and probabilistic, should run in parallel and the transition between approaches should happen progressively. The new methodology has to be accepted by control room operators, therefore sufficient time is required to interpret, test and better understand its outcomes with several operating states.

For risk calculation, the probability and the severity of each contingency are needed. The severity evaluation is composed of several functions, aiming to reflect the consequences of each contingency in terms of thermal overload, voltage limit violations, voltage instability, loss of load, loss of generation and cascading sequences. The severity functions per type of impact are defined in such a way that their outcome is a normalized value, which is used in the calculation of a global severity index. To calculate severity for the next hour, current State Estimator snapshots are used, including the expected changes in actual conditions such as programmed outages, wind generation forecast, load forecast and expected

market-driven generation pattern. The probability calculation was described in chapter 7. Regarding risk indices, a global index and one per type of impact are calculated.

Although the knowledge of the probability of events is extremely relevant for system operation, the severity should be the main driver of the decision-making process. Of course, if a certain phenomenon is particularly likely to occur, it becomes a significant contingency even with not so severe consequences, because after an event that weakens the system, another event can always occur that has more severe consequences before the normal secure state is restored.

The sequence of branch tripping, because of an initiating fault, followed by line overloading, may cause a cascading event. There are no dedicated overload protection systems in the Portuguese transmission system, although facing a severe overload, the distance protections can interpret it as a remote short-circuit not cleared by the primary protections and, consequently, trip the overloaded branch. An algorithm was developed to assess cascading events after a contingency, assuming that beyond a defined threshold, the overloaded line or transformer is disconnected. First, the identification of the contingencies that may lead to cascading is made and, afterwards, the iterative simulation of cascading outages due to consecutive opening of overloaded branches is performed. In the end, the subsequent severity is assessed.

The global severity index is based on a weighting concept, where the highest weight is given to the worst severity and the lowest weight to the least critical one. The assigned values can be changed according to experience after the methodology is in use. It is important to make this methodology flexible and easily updatable, i.e., to be valid for now and for the future. In terms of risk assessment, the relevant parameters should be added, changed or removed of the probability of occurrence and of the severity function when needed and according to the evolution of the physical network, terrain conditions and system security requirements.

In addition to the severity calculation, the direct costs of a contingency for system's operation are discussed, where the loss of load costs and the generation costs are addressed. For the load costs, the function used in long-term studies is presented and for the generation cost, the market price needs to be applied. The indication of cost is additional information to the risk index per contingency. Further analysis was not performed.

Furthermore, relevant issues as the wind generation behaviour when facing a disturbance, including a practical example, and the restoration time, with an analysis of the restoration of all faults from 2001 to 2009, are discussed.

In order to validate the severity part of the methodology and to evaluate the calculated values, severity functions were calculated from the beginning of July until the end of December 2009. Also risk indices and the cost of the loss of load were calculated for the same period.

Chapter 9.

Final Conclusions

9.1. Synthesis of the work

Nowadays most of the transmission systems' operating conditions are more stressed due to the introduction of a competitive environment in the power system industry, the regulatory changes causing the unbundling of generation, transmission and distribution, the environmental concerns, which limit the construction of new transmission lines and generation capacity, and the strong incentives to generation through renewable energy sources. In addition, the electricity market presents more unpredictable and less stable power flows and a market-driven generation pattern more unpredictable and less controllable as well. All the described factors have created more vulnerable networks and a more complex security assessment in operations environment. New challenges to the power system security assessment demand the development of new methodologies.

The aim of this work was to develop an adequate risk assessment methodology for system operations, which considers probability and severity of contingencies, to be used for security evaluation in the control room, where currently only classical deterministic methods are applied. The applicability of the methodology directly in the control room was of great concern. Issues like the computational time and operators' understanding and acceptance are important. To be accepted by control room operators, sufficient time is required to interpret, test and better understand the outcomes of the new methodology with several operating states. In order to establish a link between this methodology and the current deterministic analysis, both results should be maintained and the probabilistic and risk information added to the analysis. In the first phase, both approaches have to run in parallel in order to calibrate the new methodology and to prove its usefulness.

Recent blackouts have increased the awareness of TSOs for the occurrence of major disturbances, which are normally the result of a combination of events with the same or different causes. After the initiating event, it may be followed by unforeseen events increasing its severity. The need to improve real-time information and the development of new support tools was mentioned also in many of the blackouts and disturbances presented in chapter 2. This appreciation and usefulness motivates and gives meaning to the development of an online risk assessment tool to be used in the control rooms of the Portuguese TSO.

The developed methodology uses probabilistic methods and takes into account the current conditions and the past knowledge to calculate a risk indicator for the next period under analysis, which provides a more accurate overview to the control room operators. It considers the effect of frequency of occurrence of faults (using historical data from the beginning of 2001 until the end of 2009), physical network conditions, environmental, geographical and geological characteristics, and online conditions, such as lightning occurrence and forecast information, and risk level or active forest fires. This research does not only perform a risk evaluation, considering different probabilities related to different contingencies and their consequences, but also identifies the actions that contribute to risk reduction, inside and outside the control room, such as operator training or composite insulators installation.

An electrical power system is made of thousands of components. From the analysis of the faults' historical data, it is concluded that single and specific double contingencies are not rare events. Incidents are naturally unpredictable and the recent disturbances, presented in chapter 2, have aided in increasing awareness about the risk of unpredictable disturbances and also that a simple initiating fault can have severe consequences. To eliminate the chance of major blackouts or severe disturbances is neither technically nor economically viable. Thus disturbances are a permanent threat to the electrical power

systems, raising the significance of incident analysis activity and of the use of risk evaluation methodologies.

Risk assessment is a topic of the moment for utilities. In the new Policy 3 – Operational Security of the UCTE Operation Handbook, risk analysis appears as a requirement to be fulfilled by all ENTSO-E partners in the definition of N-1 considered by each TSO. It also refers that TSOs have to be aware of the risk in their own system due to contingencies. Cascading sequence effects are also mentioned in the policy as a concern when addressing the N-1 security calculation. Previously, CIGRE has published two task force reports that recommended further study of probabilistic security assessment methods, and the Electric Power Research Institute was involved in efforts to develop probabilistic risk assessment tools for security assessment.

In literature, many reasons are reported to adopt probabilistic methods in the security assessment of transmission systems, namely:

- The deterministic assessment only considers consequences in terms of thermal load, voltage violations and loss of load. It does not consider the probability of events nor cascading sequences.
- Some of the recent disturbances (see chapter 2) proved that the N-1 criterion is not sufficient to guarantee a high security and reliability level, which is the goal of every TSO.
- Under specific conditions, such as stormy weather or forest fires, the likelihood of faults in grid elements increases and this effect must be incorporated in the evaluation. In the deterministic approach, events are equally likely to occur, and there is no differentiation in the probability of occurrence in those periods. Therefore, it does not integrate current conditions in the analysis.
- The deterministic approach does not identify the regions of the network that are more exposed to risk, such as areas with stork nests placed in OHL towers. Many times, this identification is just empirical knowledge, based on the operators' experience.
- With the deterministic approach, it is not possible to include any type of uncertainty in the analysis.

In addition to these reasons, utilities are facing increasing reliability demands and quality of service requirements and, with the current computational skills, it is feasible to perform a large amount of calculations in a short period of time. The increasing quality of service requirements force utilities to develop processes to record and analyse every incident. These processes will constitute a reliable source of historical information, being used to identify problems, to implement improvement actions and to develop methods in order to evaluate risk. The improvement actions applied in order to mitigate the risk of some of the controllable causes of faults have already improved significantly the system's performance, and for the future further improvements are expected.

A risk assessment methodology is essential to support control room operators in the security evaluation of the system, and provides them with indices, allowing them to be aware of inherent risks and to react in advance, but this is just a small part of the whole picture. Risk avoidance and reducing the consequences of contingencies go beyond the security analysis that is performed in the control room. In the Portuguese transmission system, the recent improvement in the quality of service indicators is the result of a multi-disciplinary effort that has achieved a sustainable result. This continuous effort involves efficient planning, investment in new assets and in the renewal of existing ones, adequate maintenance strategies, strict coordination of outages and efficiency of technical and human resources, including regular training to the latter. Control room operators play a main role in the good performance of the power system and in achieving all the essential tasks for which it was designed. The operator's ability to manage a large amount of data, to adequately understand, decide and execute on time suitable remedial actions, is also important.

For the development of the risk assessment methodology, a detailed analysis of the operation of the Portuguese transmission system and of its faults and their characteristics was performed. It is not possible to implement a methodology that evaluates operational risk if there is not a good understanding of the

way the electrical power system works and also how it is operated. This understanding is essential to evaluate the severity of contingencies. Chapter 4 gives an overview of the Portuguese transmission system, describing a broad set of important aspects, in order to support decisions in the course of this work.

The incidents' historical data base of the Portuguese transmission system was used in the characterization of faults, which was performed considering data from the beginning of 2001 until the end of 2009. The majority of incidents initiate in overhead lines (OHLs) and represent 92% of the total. OHLs are most affected, because of their geographical dispersion and consequent exposure to the action of the external factors that cause faults.

The four main causes of faults in the Portuguese transmission system are storks, forest fires, fog in combination with pollution and lightning. From the characterization of faults, it was concluded that it is extremely important to identify the seasonality, location and time of occurrence of the faults, because this supports the decision of which cause must be considered in the risk assessment methodology at each specific moment. The fault dependence on some specific characteristics was evident with the detailed analysis.

Storks cause faults during the whole year, with a decrease in the number of faults in December, in a well known group of OHLs. Half of those faults occur from 0h to 6h. Despite the increase of the stork population in Portugal, REN's actions taken since 1995 in order to mitigate the influence of these birds in OHL incidents allowed to control the number of faults caused by this bird. Storks mainly cause single contingencies.

Forest fire is a seasonal cause, because faults occur mainly in summer, and it can affect the entire Portuguese territory, depending on the location of the forest fire. About 60% of the faults caused by forest fires occur from 12h to 18h. In the most critical days, there were periods where several OHLs were affected by the same forest fire or by different forest fires happening at the same time. The Portuguese TSO is, since 2006 when a new law came into force, responsible for maintaining the right-of-way clean within a defined area under each OHL that crosses forest. This measure has created great expectations in terms of fault avoidance and in terms of the efficiency of the fire fighting, and also avoids faults caused by trees, which occur rarely in the Portuguese transmission system. Forest fires may cause multiple contingencies.

Similar to faults caused by forest fires, also faults caused by fog in combination with pollution are seasonal, occurring mainly during summer, and extremely dependent on weather conditions. More than half of these faults occur from 0h to 6h in well identified areas of pollution. The installation of composite insulators and the washing of insulators are measures of great importance in order to avoid and reduce the number of faults. Since 2006, it can be noticed that the number of faults caused by fog in combination with pollution has significantly decreased.

Lightning is an incident cause that affects all transmission systems and faults caused by it can occur all over the country during the whole year. Two thirds of the faults caused by lightning occur between 12h and 24h. Lightning is an uncontrollable cause and insulation coordination is the most effective measure to mitigate faults caused by this force of nature. Faults caused by lightning are normally single or double common cause contingencies. For both causes, lightning and forest fires, there are regions more favourable than others, such as mountain areas or municipalities with a higher risk of fire, respectively, because of their intrinsic characteristics.

Other fault causes were considered for analysis, namely maintenance and operation (human errors), protection systems, obstacles (vegetation) and ice. Human errors will always happen, and sometimes behind other causes a human error is hidden, although the risk of its faults can be significantly reduced with strict procedures for maintenance, assembling and tests, adequate decision support tools for different tasks, good coordination and communication and personnel training. Protection systems can be

the cause of two types of events: protection system damage or a hidden failure. The first type normally only disconnects the component which is protected by the damaged protection system and the second type normally involves an initiating fault on another grid element located in the vicinity. To reduce the risk of faults caused by protection systems, every time that a protection system fails, the equipment that failed is checked and, if necessary, also the others of the same type that are installed in the network. Faults caused by obstacles (mainly vegetation) represent less than 0.5% of the total amount of faults. Finally, regarding faults due to extreme wind conditions, these are of greater concern, because they cause multiple contingencies with permanent damage.

Several of the fault causes identified in this research are common to other transmission systems. Regarding ice, there are no recorded faults due to this cause in the Portuguese transmission system and, consequently, it is considered an international cause. Nature extreme causes such as earthquakes and hurricanes were not analysed. Nature extreme causes, like lightning, are considered uncontrollable and to improve the performance of the system in such cases may be non-cost effective.

For probabilistic evaluation, a consistent data collection is required. Information gathering and organization represents a big challenge and an extremely time-consuming task for a TSO, but it allows the development of methodologies that will improve the system performance. In order to incorporate the intrinsic characteristics of Portugal that influence the occurrence of faults and the actual risk, the available information was evaluated, selected and used in the probability calculation. It was important to gather qualitative data, understand the process and find correlations between variables that were considered meaningful. There is no such thing as perfect information, but for this work data collection and organization becomes crucial to obtain better results. So, there was a need to overcome the limitations of the available information. Statistical analysis for the estimation of the probability of events and mathematical modelling for the inclusion of all influencing factors that introduce realism in the methodology were made.

For the four main causes of the Portuguese transmission system that are dependent on length and on the intrinsic characteristics across Portugal, this methodology includes all the influencing factors that are considered significant in terms of OHL performance. These factors include number and location of stork nests, identified polluted areas, composite insulators' location, forest fire risk per municipality and active forest fires information, lightning density, online lightning occurrence, number of ground wires per OHL, tower geometry, soil resistivity and footing resistance per tower, tower coordinates and the municipalities' official administrative borders. The data organization is mainly made by municipality, aiming to determine the length of OHLs and the substations exposed to risks. For the other causes yearly average failure rates are used, because no other influencing factors were identified, except the working schedule for human error that uses different failure rates according to the time of the period under analysis.

For lightning, a method to estimate the number of faults caused by lightning for short-term analysis was implemented. This method is based on the probabilistic method for lightning performance of an OHL developed by CIGRE. It seems to be the best compromise solution with good results, also when comparing it with the results obtained with IEEE FLASH for a subset of the OHLs, because the applied scaling factor improves the estimation results. The comparison of the simplified method with IEEE FLASH results confirms the validity of the adopted simplifications. The critical current used to determine the backflash rate is calculated per tower, to take into account the different characteristics of each tower.

The input data for the risk assessment methodology needs to be reliable to provide credible indices. Near future information must be integrated in the model, such as lightning data, forest fires risk and meteorological information. After defining the relevant data, several data preparation algorithms were developed to obtain the inputs in an adequate format. For meteorological, forest fires and operational data, which are used online or valid for a short period of time, automatic updates and interfaces were created to include them in real time in the methodology. This requires the TSO to maintain a common asset database properly organized and promptly updated, with all the required information, to be used as input.

The need of field input data makes this methodology easier to implement within a TSO structure, where the asset owner and the system operator are the same entity, and this methodology joins together, in a unique way, two different realities: systems operation and field information, increasing veracity in the results.

The integration of current conditions and the intrinsic characteristics of the network and of its location is the added value of this work, which aims to estimate the probability of faults based on short-term failure rates. The concept of short-term failure rates is implemented, valuing the current risks that are actually present in each evaluation, in addition to the influencing factors also included in the probability calculation. The introduction of geographical location of risk gives the operators a more precise knowledge of which grid elements are exposed to a specific risk in a specific moment. This is achieved with the automatic update of current information (such as lightning and active forest fires), which is directly introduced in the method and, consequently, in the risk results. Beyond the accurate information of the influencing factors, operational experience was also needed to determine suitable weighting factors for each fault's cause.

The probabilistic method is fast and therefore compatible with the real-time operations environment. The computational time for the next hour takes less than 30 seconds, the probability and the severity functions calculation run in parallel and afterwards the risk indices (per impact and global) are calculated. It considers the different types of risks to which a component is exposed and also takes into account the difference between longer and shorter OHLs, where the longer ones are obviously more exposed to risks. Additionally, all the changes in procedures, practices and improving actions implemented in all the areas of the TSO are reflected in the faults. They affect their frequency and severity, which is certainly judged every time by incident analysis and integrated in the methodology including the considered influencing factors and failure rates. A good characterization of faults and consequent improvement actions is translated into improved reliability.

To consider only single contingencies in the risk assessment would limit the analysis by excluding double contingencies that are also frequent in the transmission system. Double contingencies caused by a common cause normally occur due to lightning or forest fires, affecting simultaneously OHLs that share the same towers during the whole or part of their path. The same forest fire can also affect a corridor composed by several OHLs, but the historical data show that entire corridors have not yet tripped simultaneously. Extreme wind is another cause that may be of concern regarding common cause faults, but it goes beyond the scope of this work. The β-factor model was used to calculate the common cause failure rate for N-2 contingencies and it has proven to be adequate to address the N-2 contingencies caused by lightning and by forest fires for parallel-running OHLs.

As already mentioned, for risk calculation, both probability and severity of each contingency are needed. These two parts are treated independently in the development of the methodology. The severity evaluation is composed of several functions, aiming to reflect the consequences of each contingency, based on the post-contingency values of the analysed State Estimator (SE) snapshot, in terms of thermal overload, voltage limit violations, voltage instability, loss of load, loss of generation and cascading sequences. The severity functions per type of impact are defined in such a way that their outcome is a normalized value, which is used in the calculation of a global severity index. To calculate severity for the next hour, current SE snapshots are used, including the expected changes in actual conditions such as programmed outages, wind generation forecast, load forecast and expected market-driven generation pattern. After calculating the probability and the severity functions for each contingency, risk is determined through one global index and another one per type of impact.

An algorithm was developed to evaluate cascading events, i.e. the sequence of line tripping caused by an initiating fault and followed by line overloading beyond a defined threshold. There are no dedicated overload protection systems in the Portuguese transmission system, although facing a severe overload, the distance protections can interpret it as remote short-circuit not cleared by the primary protections and, consequently, trip an overloaded grid element. First, the identification of the contingencies that may

lead to cascading is made and, afterwards, the iterative simulation of cascading outages due to consecutive opening of overloaded branches is performed. In the end, the subsequent severity is evaluated. This type of cascading events occurred for example in the Portuguese transmission system in the disturbances on 6th September 2001 and on 2nd August 2003, described in chapter 2.

The global severity index is based on a weighting concept, where the highest weight is given to the worst severity and the lowest weight to the least critical one. The assigned values can be changed according to experience after the methodology is in use. It is important to make this methodology flexible and easily updatable, i.e., to be valid for now and for the future. The risk indices must provide an insight to control room operators of the network state and of the constraints that operators face. They have to be simple and fully understood by those who operate the system. The transition from the deterministic to the probabilistic approach should happen progressively.

In addition to the severity calculation, the direct costs of a contingency for system operation are discussed, where the loss of load costs and the generation costs are addressed. Relevant issues as the wind generation behaviour when facing disturbance and the restoration time are also discussed.

In terms of risk assessment, the relevant parameters should be added, changed or removed of the probability of occurrence and of the severity function when needed and according to the evolution of the physical network, terrain conditions and system security requirements.

The methodology developed in this research work, is intended to evaluate operational risk for a short-period of time, but it can also be applied to evaluate the risk of operational scenarios in the operations planning phase, taking into account the probabilistic nature of contingencies and their severity under specific operating conditions. In order to evaluate the methodology, it was applied to the Portuguese transmission system, exemplifying short-term analysis for the next hour. The events that were evaluated include single contingencies of overhead lines, transformers, busbars and double common cause contingencies of OHLs.

Probabilities of fault were calculated from the beginning of June 2009 until the end of December 2009. The results show that the probability of fault increases with lightning and forest fires and also confirm the seasonality and the pattern that is expected for the four main causes. For this calculation, the fault historical data, from the beginning of 2001 until the end of 2008, was considered. Severity functions, risk indices and the cost of the loss of load were calculated from the beginning of July until the end of December 2009.

With this work the Portuguese TSO has an available tool to evaluate operational risk in the security analysis context. To define an acceptable level of risk is a management decision that has to be taken by the TSO. Once defined, this methodology will allow a more efficient use of the network capacity.

TSOs are not incentivized to adopt probabilistic methodologies in system operations; therefore this methodology is going to be used when:

- It is encouraged by the regulatory framework.
- There is lack of investment and the network conditions are more stressed.
- There is a need to maximize the usage of the network's capacity.
- The methodology has proven itself in successful pilot projects such as the one presented in this thesis.

Regulatory and political uncertainties are of paramount importance for power systems. The regulatory framework is always the basis for the changes and it has been continuously developed in the competitive market in order to cope with market design, which does not work with the same laws as physics. Political interference has also to be pointed out, because it is promoting specific aims through policies, such as greenhouse gas emission reduction and climate change mitigation, through various instruments, like tradable emission certificates and renewables over evaluated tariffs. The political decisions impose the

direction on how to operate and develop the electrical systems, but also introduce uncertainty in the electrical industry, although in a longer term.

To adopt a risk assessment methodology represents a transition from operating with an implicit defined risk management to an explicit effective risk assessment. The application of this methodology in other transmission systems has to be adapted to their intrinsic characteristics and data availability, although the used basic principles are exactly the same. The faults, their causes, the field characteristics and the operating conditions may vary greatly for each TSO. The system's performance is directly dependent on the factors to which it is exposed.

Finally, in this research work theory and practice are brought together as close as possible, in order to achieve the most realistic and useful results, giving a good indication of the system's risk in the system operations environment. One has to bear in mind that this research does not analyse all possible risks, but only the most significant ones to the Portuguese Transmission system in terms of contingencies. Moreover, engineering is an applied science, which means that only when applied it becomes truly useful.

9.2. Future work

In this work an operational risk assessment methodology was presented, which opens the opportunity to complement this research work and to develop some of the issues addressed in it. Therefore, the following topics that are considered relevant for future work are presented.

Hidden failures

A power system must be able to withstand the most likely contingencies, which basically are single, double common cause and double events caused by hidden failures in protection systems. Protection hidden failures are recognized as an important cause in spreading power system disturbances and therefore their impact in the system's performance should be included in the risk evaluation. Hidden failures are much more likely than double contingencies triggered by independent events. This was addressed in section 3.4.1 and its statistics shown in section in 5.7.1 of this work. The most common event, involving a hidden failure, is an N-2 contingency, because it occurs at the same time as the initiating short-circuit. The double contingencies caused by a hidden failure can always occur with any short-circuit, because they are not dependent on adverse weather or forest fires. However, their occurrence is limited to a vulnerability region, which is determined through an analysis of the installed protection systems. The grid elements in the vicinity of the faulted one are more vulnerable to hidden failures than all the other elements.

In order to integrate hidden failures in this methodology, the vulnerability region has to be defined and the combinations of two grid elements that can trip for an initiating fault plus a hidden failure needs to be determined. For each grid element, the grid elements inside its vulnerability region should be individually added to it, composing an N-2 contingency to be always considered in the operational risk assessment. In addition, the probability of double contingencies needs to be calculated.

Wind speed measurements

After the disturbance in Portugal, on 23rd December 2009, which was caused by extreme wind, as described in section 2.3.4, the awareness of the relevance of online available wind speed measurements has increased and common cause faults should be considered for measurements above 160 km/h.

Using the wind speed measurements made available by the wind farms connected to the transmission network, enough historical data needs to be collected and recorded, to perform a statistical analysis and to evaluate how often wind speeds above 160km/h occur. Afterwards, it is necessary to build up a mathematical model to calculate the probability of occurrence incorporating the online conditions, such as for lightning and forest fire.

In addition, the wind speed measurements can be used for dynamic rating calculation for OHLs, instead of using the standard 0.6 m/s value, which in many operating conditions causes constraints.

Dynamic simulations

To introduce dynamic simulations in the operational assessment will open many possibilities. It gives the opportunity to assess the response to disturbances, to model the under-frequency load shedding installed in the network and to evaluate its efficiency in case of islanding, to model the protection system installed in the network and the expected clearing times, and also to assess the system's stability. The evaluation of the stability limit becomes more relevant with the increasing stress in the operating conditions. It is important to assess if thermal limit is beneath or above the stability limit, for example for the N-1 security criterion.

Strategy for the definition of an acceptable risk level

The definition of an acceptable level of risk is mainly a management decision. However, having this methodology available in the control room, analysing many and different operating conditions, is the first step to quantify the acceptable risk level. There is a need of a learning process to gain experience with different numerical risk levels, which will take some time before determining what is acceptable. Therefore, it will be required to record the probability, severity and risk results to be associated with each incident.

Automatic processing of online lightning data

Up to now, the records of lightning have been manually downloaded from the Jobs software. The automation of these records is essential for the online assessment in the control room, as it was already made for forest fire information.

To automate the interaction with Jobs and to use its information online in the developed methodology, the coordinates, the lightning intensity and the error of the location need to be recorded and processed. The geographical information is crucial for the accuracy of the methodology.

Protection systems information

The failure rate implicit in the faults caused by protection systems is influenced by the technology and age. An updated and complete source of information is needed to be able to include this feature in the methodology.

The introduction of the location of each fault in the method will allow a better identification of the cause of faults, reducing the number of those classified as unknown, and the identification of the most critical areas, providing valuable data for risk reduction measures. This information can also be used to validate the regional influence of each cause, improving the quality of the results of the risk assessment methodology.

Control room interface

The two parts of this methodology, probability and severity, that are now independent, should be integrated in the same platform. The automatic download of online information needs to be synchronized with the time to run the risk analysis at the beginning of each period, e.g. at every hour. A common source of input data needs to be ensured and procedures to guarantee that it is always updated have to be created. Also visualization techniques to present the method to the control room operators need to be analysed and developed. The test of the methodology for some time in the control room is crucial to assess and fine-tune its results.

For information organization, it is recommended to organize all the relevant information in a geographical information system to be used in all company areas, such as operation, maintenance, design and planning. This information should be always updated with the possibility to be automatically accessed to provide the necessary inputs for the risk assessment methodology.

Equipment features

Up to now, there are no faults recorded on underground cables and therefore they were not included in the model. However, the number of kilometres of underground cables is increasing and, because these components are not exposed to weather or other external factors, a different analysis should be made. Exactly the same happens to indoor or gas insulated substations, whose number is also increasing in the Portuguese transmission network, requiring a different analysis.

While the numbers are still low, this equipment can be excluded from the methodology, given the low failure rates. However, it is recommended to also include these types of grid elements in the methodology when their numbers start to increase and when sufficient statistical fault data has become available.

Accuracy of lightning forecast

The current methodology uses an estimation of the accuracy of the lightning forecast, because no historical records of forecasts are available. The lightning forecasts are assumed to have a certain significance, as expressed in equation (7.35).

In order to determine the actual forecast accuracy, it is recommended to also store the lightning forecasts, in addition to the already stored observations. After having gained a sufficiently large database, typically several years, this accuracy assessment can be made and included in the methodology, making the methodology more precise.

Tower footing resistance

The tower footing resistance is an important parameter for the performance of an overhead line when exposed to lightning, which is one of the most important causes for faults. In this work, a large effort was made to gather and analyse all available data for the purpose of lightning performance prediction. The combination of the historical database of OHL faults due to lightning, the developed methodology and the tower footing resistance measurements database offers another unique opportunity: an effective and targeted approach to improve the PTS performance regarding lightning.

It is recommended to use the developed methodology and databases to identify how individual lines perform and whether this is in conformity with what would normally be expected. Subsequently, it can be pinpointed which are the limiting factors, possibly at the tower level, and analyze whether there is room for improvement.

Restoration time

At the moment, for security evaluation it is assumed that after a fault, the grid element cannot be restored within the period, which is the worst case. In section 8.11, it can be observed that a high percentage of grid elements are reconnected within 1 hour, especially in the case of OHLs. Approximately 80% of OHLs are reconnected in less than 10 minutes after a fault. The integration of the restoration time in the security analysis is expected to introduce added value to the methodology. This analysis should distinguish the grid element and the fault cause, which can influence if the fault is permanent or not.

REFERENCE LIST

[1] Ministério da Economia e da Inovação, "Política Energética - Março de 2005 a Março de 2007 em Portugal", 2007.

[2] UCTE - Union for the Coordination of Transmission of Electricity, "Final Report - System Disturbance on 4 November 2006", 30th of January, 2007.

[3] J. McCalley, S. Asgarpoor, L. Bertling, R. Billinton, H. Chao, J. Chen, J. Endrenyi, R. Fletcher, A. Ford, C. Grigg, G. Hamoud, D. Logan, A. P. Meliopoulos, M. Ni, N. Rau, L. Salvaderi, M. Schilling, Y. Schlumberger, A. Schneider, and C. Singh, "Probabilistic security assessment for power system operations," in *Proceedings of Power Engineering Society General Meeting, IEEE,* vol. 1, pp. 212-220, 2004.

[4] G. L. Doorman, K. Uhlen, G. H. Kjolle, and E. S. Huse, "Vulnerability analysis of the Nordic power system," *IEEE Transactions on Power Systems,* vol. 21, pp. 402-410, February, 2006.

[5] S. A. B. de Almeida, N. Machado, and R. Pestana, "Voltage Collapse: Real Time and Preventive Analysis in the Portuguese Transmission System," in *Proceedings of PowerTech2007*, Lausanne, Swizerland, 5-7 July, 2007.

[6] ENTSO-E, Operation Handbook, http://www.entsoe.eu/resources/publications/ce/oh/, 2009.

[7] M. H. J. Bollen, L. Wallin, T. Ohnstad, and L. Bertling, "On Operational Risk Assessment in Transmission Systems – Weather Impact and Illustrative Example," in *Proceedings of PMAPS 2008*, Puerto Rico, 14-17 June, 2008.

[8] J. D. McCalley, V. Vittal, and N. Abi-Samra, "Use of Probabilistic Risk in Security Assessment: A Natural Evolution," CIGRE Session 2000, Paris, France, August, 2000.

[9] W. Li and J. Zhou, "Probabilistic Reliability Assessment of Power System Operations," *in Electric Power Components and Systems,* pp. 1102-1114, 2008.

[10] NASA, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners", (in http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf), 2002.

[11] K. Morison, W. Lei, and P. Kundur, "Power system security assessment," *Power and Energy Magazine, IEEE,* vol. 2, pp. 30-39, 2004.

[12] CIGRE, "TF 38.03.12 - Power System Security Assessment: A position paper," in Electra, nº 175, pp. 49-78, December, 1997.

[13] CIGRE, "TF 38.02.24 Report - Defence Plan Against Extreme Contingencies", 2006.

[14] EPRI, "Transmission Reliability Evaluation for Large Scale System", 1998.

[15] EPRI, "Probabilistic Reliability Assessment Support and Maintenance", EPRI - Electric Power Research Institute, 2006.

[16] F. Xiao, J. D. McCalley, Y. Ou, J. Adams, and S. Myers, "Contingency Probability Estimation Using Weather and Geographical Data for On-Line Security Assessment," in *Proceedings of PMAPS 2006*, KTH, Stockholm, Sweden, June 11-15, 2006.

[17] N. Ming, J. D. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment," *IEEE Transactions on Power Systems,* vol. 18, pp. 258-265, 2003.

[18] Instituto Geográfico Português, Transcoord version 2.01 (http://www.igeo.pt/produtos/Geodesia/transcoord.htm), 2009.

[19] S. A. B. de Almeida, "Análise de Grandes Perturbações na Rede Eléctrica Nacional," M.Sc. Thesis, FEUP - Porto University, 2005.

[20] S. A. B. de Almeida, F. M. Barbosa, and R. Pestana, "Severe Contingencies Analysis in Portuguese Transmission System," UPEC2006 – 41st International Universities Power Engineering Conference, Northumbria University, Newcastle, UK, 5 - 8 September, 2006.

[21] W. Li, *Risk Assessment of Power Systems - Models, Methods, and Applications*: IEEE Press Series on Power Engineering, 2005.

[22] T. T. Soong, *Fundamentals of Probability and Statistics for Engineers*: John Wiley & Sons, Ltd, 2004.

[23] International Organization for Standardization, "ISO 14121-1:2007 Safety of machinery - Risk assessment - Part 1: Principles," 2007.

[24] U.S. - Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", 5th April, 2004.

[25] Svenska Kraftnät, "The blackout in southern Sweden and eastern Denmark on September 23, 2003", 10th of October, 2003.

[26] E. Ek, "The Blackout in southern Sweden and eastern Denmark, September 23, 2003," CIGRE Session 2004 - Large Disturbance Workshop, Paris, France, August, 2004.

[27] UCTE - Union for the Coordination of Transmission of Electricity, "Final Report of the Investigation Committee on the 28 September 2003 in Italy", 27th April, 2004.

[28] Hellenic Transmission System Operator, "Report on the 12 July 2004 Blackout in Greece", 2004.

[29] Hellenic Transmission System Operator, "Disturbance in the Greek Transmission System on the 27th of June 2007," UCTE, September, 2007.

[30] Operador Nacional do Sistema Eléctrico, "Perturbação no Sistema Interligado Nacional no dia 10/11/2009 às 22h13 (audiência pública), Brazil", 16th December, 2009.

[31] National Grid Transco, "Investigation Report into the Loss of Supply Incident affecting parts of South London at 18:20 on Thursday, 28 August 2003", National Grid Company, 10th September, 2003.

[32] RTE, "The French Power Transmission System confronted with the storms of 26-27-28 December 1999," August, 2000.

[33] PSE-Operator S.A., "Voltage Instability Incident in the Polish Power System on 26th June 2006," Large Disturbance Workshop - CIGRE Session, Paris, France, 28th August, 2006.

[34] E. O. Netz, "Report on the status of the investigations of the sequence of events and causes of the failure in the continental European electricity grid on Saturday, November 4, 2006, after 22:10 hours, Bayreuth, Germany", 14th of November, 2006.

[35] ERGEG, "ERGEG Interim Report on the lessons to be learned from the large disturbance in European power supply on 4 November 2006", 20th December, 2006.

[36] Rede Eléctrica Nacional, "Separação de redes na UCTE de 04 de Novembro 2006", November, 2006.

[37] ENERGINET/DK, "Island operation in Jutland-Funen on 29 May 2007", 12th July, 2007.

[38] Rede Eléctrica Nacional, "Falta de Energia na Zona Sul de Portugal no dia 9 de Maio de 2000", 19th May, 2000.

[39] Rede Eléctrica Nacional, "Falta de Energia Eléctrica no Alentejo e Algarve no dia 6 de Setembro de 2001", 9th October, 2001.

[40] Rede Eléctrica Nacional, "Falta de Energia Eléctrica no Alentejo e Algarve no dia 2 de Agosto de 2003", 13th August, 2003.

[41] J. Amarante dos Santos, "Revisiting the Blackout in Southern Portugal in 9th of May 2000," CIGRE Workshop on Large Disturbances, Paris, France, August, 2002.

[42] J. Amarante do Santos, "Storm in Portugal 23-12-2009, Presentation to ENTSO-E, Brussels," January, 2010.

[43] J. Endrenyi and W. H. Wellssow, "Power system reliability in terms of the system's operating states," in *Proceedings of PowerTech 2001, Porto,* vol. 2, 2001.

[44] Rede Eléctrica Nacional, "Manual de Procedimentos do Gestor do Sistema", June, 2007.

[45] U. G. Knight, *Power Systems in Emergencies: From Contingency Planning to Crisis Management*: Wiley, 2001.

[46] International Electrotechnical Commission, International electrotechnical vocabulary, www.electropedia.org, 2010.

[47] P. Kundur, J. Paserba, V. Ajjarapu, G. Anderson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, "IEEE/CIGRE Joint Task Force on stability terms and definitions. Definition and classification of power system stability," *IEEE Transactions on Power Systems,* vol. 19, pp. 1387-1401, August, 2004.

[48] D. S. Kirschen and D. Jayaweera, "Comparison of risk-based and deterministic security assessments," *Generation, Transmission & Distribution, IET,* vol. 1, pp. 527-533, 2007.

[49] D. S. Kirschen, K. R. W. Bell, D. P. Nedic, D. Jayaweera, and R. N. Allan, "Computing the value of security," *Generation, Transmission and Distribution, IEE Proceedings,* vol. 150, pp. 673-678, 2003.

[50] D. Kirschen, M. A. Ríos, K. R. W. Bell, and R. N. Allan, "Selection of Operating Scenarios based on the Value of Security," in *Proceedings of PMAPS 2000*, Funchal, Madeira, Portugal, 25-28 September, 2000.

[51] M. A. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan, "Value of security: modeling time-dependent phenomena and weather conditions," *IEEE Transactions on Power Systems, vol. 17, No. 3, August,* 2002.

[52] W. Li and J. K. Korczynski, "Risk evaluation of transmission system operation modes and its application at British Columbia Transmission Corporation," *Generation, Transmission and Distribution, IEE Proceedings,* vol. 151, pp. 658-664, 2004.

[53] W. Li and J. K. Korczynski, "Risk evaluation of transmission system operation modes: concept, method and application," in *Proceedings of Power Engineering Society Winter Meeting, IEEE,* vol. 2, pp. 1124-1129, 2002.

[54] Q. Chen, J. Chuanwen, Q. Wenzheng, and J. D. McCalley, "Probability models for estimating the probabilities of cascading outages in high-voltage transmission network," *IEEE Transactions on Power Systems,* vol. 21, pp. 1423-1431, 2006.

[55] Q. Chen, "The probability, identification, and prevention of rare events in power systems," PhD Thesis, Iowa State University, 2004.

[56] I. Dobson, "Where is the edge for cascading failure?: challenges and opportunities for quantifying blackout risk," in *Proceedings of Power Engineering Society General Meeting, IEEE,* pp. 1-8, 2007.

[57] Q. Chen and J. D. McCalley, "Identifying high risk N-k contingencies for online security assessment," *IEEE Transactions on Power Systems,* vol. 20, pp. 823-834, 2005.

[58] I. Dobson, J. Chen, J. S. Thorp, B. A. Carreras, and D. E. Newman, "Examining criticality of blackouts in power system models with cascading events," in *Proceedings of HICSS - 35th Annual Hawaii International Conference on System Sciences,* 2002.

[59] I. Dobson, K. R. Wierzbicki, B. A. Carreras, V. E. Lynch, and D. E. Newman, "An Estimator of Propagation of Cascading Failure," in *Proceedings of HICSS - 39th Annual Hawaii International Conference on System Sciences,* 2006.

[60] J. E. Afonso, "Protection of Transmission Lines & Co-ordination of Transmission System Protection," CIGRE SC B5 - Colloquium 2007, Madrid, 18-10-2007, 2007.

[61] J. D. McCalley, V. Vittal, and N. Abi-Samra, "An overview of risk based security assessment," in *Proceedings of Power Engineering Society Summer Meeting, IEEE,* pp. 173-178, vol.1, 1999.

[62] D. Jayaweera, "Value of Security Assessment - Extensions and Applications," PhD Thesis, UMIST, 2003.

[63] J. Chen and J. D. McCalley, "Comparison between Deterministic and Probabilistic Study Methods in Security Assessment for Operations," in *Proceedings of PMAPS 2000*, Funchal, Madeira, Portugal, 28-25 September, 2000.

[64] S. A. B. de Almeida and J. Lobo, "Gestinc-The Incidents Data Base: Purposes, Contents, Management And Automatic Indicators Calculation Future Developments," 1ere Conférence Internationale sur le Transport de l' Electricité en Algérie, Alger, Algeria, 19-20 September, 2005.

[65] N. Maruejouls, V. Sermanson, S. T. Lee, and P. Zhang, "A practical probabilistic reliability assessment using contingency simulation," in *Proceedings of Power Systems Conference and Exposition, IEEE,* vol. 3, pp. 1312-1318, 2004.

[66] S. Tamronglak, "Analysis of power system disturbances due to relay hidden failures," PhD Thesis, Virginia Polytechnic Institute State University, Blacksburg, 1994.

[67] D. S. Kirschen and D. P. Nedic, "Consideration of hidden failures in security analysis," Power System Computation Conference, Sevilla, 2002, 2002.

[68] Q. Qiu, "Risk Assessment of Power System Catastrophic Failures and Hidden Failure Monitoring & Control System," PhD thesis, Virginia Polytechnic Institute and State University, 2003.

[69] D. C. Elizondo, J. de La Ree, A. G. Phadke, and S. A. H. S. Horowitz, "Hidden failures in protection systems and their impact on wide-area disturbances," in *Proceedings of Power Engineering Society Winter Meeting, IEEE,* vol. 2, pp. 710-714, 2001.

[70] J. De La Ree, L. Yilu, L. Mili, A. G. Phadke, and L. DaSilva, "Catastrophic failures in power systems: causes, analyses, and countermeasures," *Proceedings of the IEEE,* vol. 93, pp. 956-964, 2005.

[71] C. N. Ning, C. A. Hsieh, T. Y. Hsiao, and C. N. Lu, "Two application examples of probabilistic risk assessment in power system operations," in *Proceedings of PMAPS 2006*, KTH, Stockholm, Sweden, June 11-15, pp. 1-5, 2006.

[72] L. Pottonen, "A Method for the Probabilistic Security Analysis of Transmission Grids," PhD Thesis, Helsinki University of Technology, 2005.

[73] S. Kaplan and B. J. Garrick, "On the Quantitative Definition of Risk," in Risk Analysis, vol. 1, pp. 11-37, nº 1, 1981.

[74] Y. Dai, J. D. McCalley, N. Abi-Samra, and V. Vittal, "Annual risk assessment for overload security," *IEEE Transactions on Power Systems,* vol. 16, pp. 616-623, 2001.

[75] H. Wan, J. D. McCalley, and V. Vittal, "Risk based voltage security assessment," *IEEE Transactions on Power Systems,* vol. 15, pp. 1247-1254, 2000.

[76] J. D. McCalley, A. A. Fouad, V. Vittal, A. A. Irizarry-Rivera, B. L. Agrawal, and R. G. Farmer, "A risk-based security index for determining operating limits in stability-limited electric power systems," *IEEE Transactions on Power Systems,* vol. 12, pp. 1210-1219, 1997.

[77] H. Wan, J. D. McCalley, and V. Vittal, "Increasing thermal rating by risk analysis," *IEEE Transactions on Power Systems,* vol. 14, pp. 815-828, 1999.

[78] F. Weihui, J. D. McCalley, and V. Vittal, "Risk assessment for transformer loading," *IEEE Transactions on Power Systems,* vol. 16, pp. 346-353, 2001.

[79] V. Vittal, J. D. McCalley, V. Van Acker, W. Fu, and N. Abi-Samra, "Transient instability risk assessment," in *Proceedings of Power Engineering Society Summer Meeting, IEEE,* vol. 1, pp. 206-211, 1999.

[80] D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan, "A probabilistic indicator of system stress," *IEEE Transactions on Power Systems,* vol. 19, pp. 1650-1657, 2004.

[81] S. Jeong, J. Kwon, B. Shi, J. Park, J. Choi, J. Cha, H. Choi, T. Song, and H. Yeo, "A Study on Probabilistic Reliability Evaluation of Korea Power System in Operation Mode," Security and Reliability of Electric Power Systems - CIGRE Regional Meeting, Tallinn, Estonia, June 18-20, 2007, 2007.

[82] J. Kwon, S. Jeong, B. Shi, T. Tran, J. Choi, J. Cha, Y. Yoon, H. Choi, and D. Jeon, "Probabilistic Reliability Evaluation of Korea Power System in Operation Mode," in *Proceedings of Power Engineering Society General Meeting, IEEE,* pp. 1-5, 2007.

[83] Y. V. Makarov and R. C. Hardiman, "Risk, reliability, cascading, and restructuring," in *Proceedings of Power Engineering Society General Meeting, IEEE,* vol. 3, pp. 1417-1429, 2003.

[84] Y. V. Makarov and R. C. Hardiman, "On risk-based indices for transmission systems," in *Proceedings of Power Engineering Society General Meeting, IEEE,* vol. 2, p. 678, 2003.

[85] J. K. T. Tran, S. Jeong, B. Shi, J. Choi, B. Jang, S. Moon, D. Jeon, J. Choo, K. Han, "Transmission System Reliability Management Decision – Based on Probability Reliability Evaluation," Security and Reliability of Electric Power Systems - CIGRE Regional Meeting, Tallinn, Estonia, June 18-20, 2007.

[86] T. Tran, K. Jungji, C. Jaeseok, J. Donghun, H. Gyoungnam, and R. Billinton, "Sensitivity analysis of probabilistic reliability evaluation of Korea power system," in *Proceedings of Power Engineering Society General Meeting, IEEE,* 2006.

[87] Redes Energéticas Nacionais, "2006 Sustainability Report - Trustworthy Networks", 2007.

[88] European Parliament, "Directive of the European Parliament and of the council nº 2001/77/CE on the promotion of the use of renewable energy sources, 27th September," 2001.

[89] Rede Eléctrica Nacional, Dados Técnicos 2009, http://www.centrodeinformacao.ren.pt/PT/InformacaoTecnica/Paginas/DadosTecnicos.aspx, 2010.

[90] A. A. Marques, "Increasing the performance in the Portuguese Transmission Network," 4th Transmission and Distribution Forum, Berlin, 29th - 30th September, 2008.

[91] INEGI, "Wind Farms in Portugal, in http://www.inegi.pt/publicacoes/outras/Wind_Farms_in_Portugal_Dec08.pdf, December", 2008.

[92] Rede Eléctrica Nacional, "RL PRPR 10/2006: Reavaliação da temperatura ambiente de Verão de referência para planeamento da RNT - Lista actualizada da capacidade térmica das linhas da RNT", November, 2006.

[93] R. Pestana, N. Machado, and S. A. B. de Almeida, "Melhoria do desempenho dos Operadores na avaliação da Segurança da Rede: Treino e Análise," X CLEEE - 10º Congresso Luso Espanhol de Engenharia Electrotécnica, Funchal, Madeira, Portugal, 5 - 7 July 2007, 2007.

[94] H. Valente, "Soluções para o Uprating de linhas aéreas de muito alta tensão," M.Sc. thesis, IST - Lisbon University, October, 2008.

[95] R. Pestana, "Interchange Capacity between Portugal and Spain - Methodology, Evolution and its use in the MIBEL environment," CEE07 - 2nd International Conference on Electrical Engineering, Coimbra, Portugal, 28 November, 2007.

[96] R. J. A. Mestre, "Curvas Teóricas de Radiação solar diárias", Universidade do Algarve, Faro, 2001.

[97] Fibersensing, http://www.fibersensing.com/PageGen.aspx, 2010.

[98] UCTE - Union for the Coordination of Transmission of Electricity, www.ucte.org, 2008.

[99] P. Kundur, *Power System Stability and Control*, New York, London: McGraw-Hill Inc, 1994.

[100] Y. Rebours and D. S. Kirschen, "What is spinning reserve?, University of Manchester", 19th of September, 2005.

[101] R. V. Fernandes, S. A. B. de Almeida, F. P. Maciel Barbosa, and R. Pestana, "Load Shedding - Coordination between the Portuguese Transmission Grid and the Distribution Grid with Minimization of Loss of Distributed Generation," Proceedings of PowerTech 2009, Bucharest - Romania, 28 June - 2 July, 2009.

[102] Rede Eléctrica Nacional, http://www.ren.pt, 2009.

[103] Redes Energéticas Nacionais, "Caracterização da utilização da potência eólica instalada desde Janeiro de 2005 até Outubro de 2008", 2009.

[104] M. Cremenescu, N. Cukalevski, C. Fontaine, O. Gjerde, V. Isoard, D. Kaller, L. Karlström, M. Markovic, A. Mendonca De Souza Oliveira, O. Molstad, U. Spanel, and K. Walve, "Joint and coordinated development of operators in control centres from different companies and nationalities (WG C2.21)," CIGRE session 2008, Paris, France, August 2008.

[105] S. Almeida, M. Cremenescu, N. Cukalevski, C. Fontaine, O. Gjerde, V. Isoard, D. Kaller, L. Karlström, M. Markovic, A. Mendonca De Souza Oliveira, O. Molstad, U. Spanel, and K. Walve, "Joint and Coordinated Development of Operators in Control Centres from Different Companies and Nationalities," poster session in CIGRE Session, Paris, France, 24-29 August, 2008.

[106] J. Hoogveld, G. Siffels, D. Rumpel, G. Krost, and U. Spanel, "Power System Restoration - Strategies and Operator Training in the Netherlands," CIGRE SC 39 Session, Paris, France, 1998.

[107] U. Spanel and M. Markovic, "Combined Simulator based Operator Training for restoring the Austrian Power Grid (APG)," CIGRE Regional Meeting, Tallinn, Estonia, 2007.

[108] A. R. Hileman, *Insulation coordination for power systems*: CRC Press, 1999.

[109] Autoridade Nacional de Protecção Civil - Portugal, http://www.proteccaocivil.pt/PrevencaoProteccao/RiscosNaturais/IncendiosFlorestais/Pages/Oquesao.aspx, May 2009.

[110] Diário da República - I Série A, "Decreto-Lei nº 124/2006 de 28 de Junho (http://www.proder.pt/ResourcesUser/Legisla%C3%A7%C3%A3o/Nacional/Decreto-Lein%C2%BA124-2006.pdf)," 2009.

[111] CIGRE WG C4.303, "Outdoor Insulation in polluted conditions: Guidelines for selection and dimensioning; Part 1: General principles and the AC case", June, 2008.

[112] All You Need To Know About Lightning, All You Need To Know About Lightning, http://www.2dog.com/cat/pg4.html, 2008.

[113] L. L. Grigsby, *The Electric Power Engineering Handbook*: CRC Press and IEEE Press, 2001.

[114] Rede Eléctrica Nacional, "Relatório da Qualidade de Serviço 2008", 2008.

[115] Rede Eléctrica Nacional, "Relatório da Qualidade de Serviço 2007", 2007.

[116] Rede Eléctrica Nacional, "Relatório da Qualidade de Serviço 2006 ", 2006.

[117] Rede Eléctrica Nacional, "Relatório da Qualidade de Serviço 2005 ", 2005.

[118] RWE, "Distrubance in the region Osnabrück and Münsterland in Germany - 25-11-2005," Large Disturbances Session 2006 - CIGRE, Paris, France, August 2006.

[119] E. Brostrom, J. Ahlberg, and L. Soder, "Modelling of Ice Storms and their Impact Applied to a Part of the Swedish Transmission Network," Proceedings of PowerTech 2007, Lausanne, Switzerland, 5-7 July, 2007.

[120] CENELEC, "EN 50341-1:2001 Overhead electrical lines exceeding AC 45 kV -- Part 1: General requirements - Common specifications 6060," 2001.

[121] Rede Eléctrica Nacional, "Relatório da Qualidade de Serviço 2001", 2001.

[122] Rede Eléctrica Nacional, "Relatório da Qualidade de Serviço 2002", 2002.

[123] Rede Eléctrica Nacional, "Relatório da Qualidade de Serviço 2003", 2003.

[124] Rede Eléctrica Nacional, "Relatório da Qualidade de Serviço 2004", 2004.

[125] Autoridade Nacional de Protecção Civil - Portugal, Lista de Incêndios Florestais (active forest fires list), http://www.proteccaocivil.pt/CNOS/Pages/ListaFogos.aspx, 2009.

[126] Instituto de Meteorologia, www.meteo.pt, 2009.

[127] Instituto Geográfico Português, Carta Administrativa Oficial de Portugal (Official Administrative Map of Portugal), http://www.igeo.pt/produtos/cadastro/caop/versao2008_0.htm, 2008.

[128] Labelec S.A., "Mapa das resistividades do solo de Portugal Continental - Caracterização geoeléctrica das principais formações geológicas", 2008.

[129] Rede Eléctrica Nacional, "Reformulação da Metodologia de Previsão da Procura Mensal de Electricidade", July, 2008.

[130] K. L. Cummins, E. P. Krider, and M. D. Malone, "The U.S. National Lightning Detection Network and application of cloud to ground lightning data by electric power utility," *IEEE Trans. Electromag. Compat.,* vol. 40, pp. 465-480, 1998.

[131] S. A. Melin, "Lightning location system increases personnel safety in Swedish power transmission network," in *Proceedings of AFRICON,* pp. 497-500, 1992.

[132] M. I. Lees, "Lightning strike location for overhead lines," in *Proceedings of IEE Colloquium on Operational Monitoring of Distribution and Transmission Systems (Digest No. 1997/050)* 1997.

[133] M. J. G. Janssen, "The LPATS III system in The Netherlands; critical evaluation of the results," in *Proceedings of International Conference on Lightning and Static Electricity*, Bath (UK) 1989.

[134] G. Diendorfer, W. Schulz, and V. A. Rakov, "Lightning characteristics based on data from the Austrian lightning location system," *IEEE Trans. Electromagn. Compat., vol. 40, pp. 465-480,* 1998.

[135] R. Evert and G. Schulze, "Impact of a new lightning detection and location system in South Africa," in *Proceedings of Power Engeneering Society Inaugural Conference and Exposition in Africa*, 11-15 July, pp. 356-363, 2005

[136] E. Katz and A. Segev, "The lightning position and tracking system (LPATS) in Israel: first results," in *Proceedings of 18th Convention of Electrical and Electronic Engineers*, Israel, 1995.

[137] S. M. Chen, Y. Du, L. M. Fan, H. M. He, and D. Z. Zhong, "A lightning location system in China: its performances and applications," *IEEE Trans. Electromag. Compat.,* vol. 44, pp. 555-560, November, 2002.

[138] R. B. Rodrigues, V. M. F. Mendes, J. P. S. Catalao, S. Correia, V. Prior, and M. Aguado, "An investigation over the lightning location system in Portugal for wind turbine protection development," in *Proceedings of Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century,* pp. 1-8, 2008.

[139] P. Tavaria, "Monitorização da capacidade de transporte em tempo real em linhas aéreas," Licenciatura (final graduation project), ISEL, 2006.

[140] Natural Resources Canada, Canadian Forest Fire Weather Index (FWI) System, http://fire.nofc.cfs.nrcan.gc.ca/en/background/bi_FWI_summary_e.php, 2009.

[141] Direcção Geral dos Recursos Florestais, "Defesa da floresta contra incêndios - relatório 2007", March, 2008.

[142] C. E. Wagner, "Conversion of Williams' severity rating for use with the fire weather index, Petawa forest experiment station Chalk River, Ontario, Information report PS-X-21, Canadian forestry service, Department of fisheries and forestry", November, 1970.

[143] R. M. Durão, A. Soares, J. M. C. Pereira, J. A. Corte-Real, and M. F. E. S. Coelho, "Bayesian Classification of a Meteorological Risk Index for Forest Fires: DSR," in geoENV VI - Geostatistics for Environmental Applications, pp. 283-294, 2008.

[144] IEEE, "Guide for improving the Lightning performance of Transmission Lines," in *IEEE Std. 1243*, 1997.

[145] CIGRE WG 01 of Study Committee 33, "Guide to procedures for estimating the lightning performance of transmission lines", 1991.

[146] CENELEC, "EN 50341-3-17 Overhead electrical lines exceeding AC 45 kV -- Part 3: Set of National Normative Aspects," 2001.

[147] CIGRE WG C4.404, "Cloud-to-ground lightning parameters derived from lightning location systems - the effects of system performance", April, 2009.

[148] IEEE Working Group Report, "Estimating Lightning Performance of Transmission Lines II -Updates to Analytical Models"," in IEEE Trans. Power Delivery, Vol. 8, No.3, July 1993.

[149] IEEE, IEEE FLASH v1.9, http://ewh.ieee.org/soc/pes/lpdl/, 2009.

[150] B. Gao, G. K. Morison, and P. Kundur, "Toward the development for voltage stability assessment of a large-scale power systems," *IEEE Trans. Power System,* vol. 1, pp. 1314-1319, August, 1996.

[151] S. Maslennikov and E. Litvinov, "Adaptive Emergency Transmission Rates in Power System and Market Operation," *IEEE Transactions on Power Systems,* vol. 24, pp. 923-929, 2009.

[152] R. Pestana, "Despachabilidade da Eólica - Parte IV - Impacto da Eólica na gestão técnica do SEN: Comportamento da Eólica perante Incidentes na Rede," 2009.

[153] ETSO - European Transmission System Operators, "Definitions of Transfer Capacities in liberalised Electricity Markets", April, 2001.

LIST OF PUBLICATIONS

S. A. B. de Almeida, R. Pestana and F. P. Maciel Barbosa, N. Machado, “Operational Risk Assessment Methodology for the Portuguese Transmission System”, CIGRE ELECTRA, accepted to be published in October 2010.

S. A. B. de Almeida, R. Pestana and F. P. Maciel Barbosa, “Risk Assessment Methodology for Operations applied to the Portuguese Transmission System - the Probabilistic Model”, in CIGRE SESSION 2010, Paris, France, 22 – 27 August, 2010 (accepted to be presented).

S. A. B. de Almeida, R. Pestana and F. P. Maciel Barbosa, “Integration of common cause faults in the operational probabilistic approach”, in PMAPS 2010, Singapore, 14-17 June, 2010.

S. A. B. de Almeida, R. Pestana and F. P. Maciel Barbosa,, “Risk Assessment for Operations in the Portuguese Transmission System – The key issues for the probability of contingencies”, in Operation and Development of Power Systems in the New Context - Guilin Symposium, CIGRE, Guilin City, Guangxi Province, China, 18 - 30 October, 2009.

S. A. B. de Almeida, C. Loureiro, R. Pestana, F. P. Maciel Barbosa, “Historical Data Analysis of Lightning and its Relation with the Portuguese Transmission System Outages”, in PowerTech 2009 – Bucharest – Romania, 28 June - 2 July, 2009.

S. A. B. de Almeida, R. Pestana, F. P. Maciel Barbosa,“The main causes of incidents in the Portuguese Transmission System - Their characterization and how they can be used for risk assessment”, in EEM09 – Leuven – Belgium, 27 - 29 May, 2009.

S. A. B. de Almeida, R. Pestana, F. P. Maciel Barbosa, “Principais Causas dos Incidentes na Rede Nacional de Transporte – Caracterização e forma de utilização numa metodologia de análise de risco”, in XIII ERIAC, Puerto Iguassu – Argentina, 24 – 28 May, 2009.

GLOSSARY

Already Allocated Capacity (AAC) — is the total amount of allocated transmission rights, whether they are capacity or exchange programs depending on the allocation method [153].

Area Control Error (ACE) — is the instantaneous difference between the actual and the reference value of the power interchange between to neighbouring systems (control areas), taking into account the effect of frequency bias for that control area according to the network power frequency characteristic of that control area and the overall frequency deviation (see section 4.9.2) [6].

Available Transfer Capacity (ATC) — is a measure of the transfer capability remaining in the physical transmission network for further commercial activity over and above already committed uses. ATC is the part of NTC that remains available after each phase of the allocation procedure for further commercial activity [153].
ATC=NTC-AAC.

Cause — what leads to a fault. Incident's cause is the cause of the initiating fault.

Contingency — is the unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element. A contingency also may include multiple components, which are related by situations leading to simultaneous component outages.

Control Area — is a coherent part of an Interconnected System (usually coincident with the territory of a company, a country or a geographical area, physically demarcated by the position of points for measurement of the interchanged power and energy to the remaining interconnected network), operated by a single TSO, with physical loads and controllable generation units connected within the control area. a control area may be a coherent part of a control block that has its own subordinate control in the hierarchy of secondary control [6].

DACF Data Sets — AC load flow calculation input data sets given in the UCTE format and corresponding to the forecast state of the transmission grid (topology, loads and generation pattern) at a determined timestamp of the day-ahead.

Fault — is the inability of a component to perform its required function. It can be permanent – it implies damage and it cannot be restored before repair. It can be fugitive – it is restored at first attempt because there is no damage.

Fault Clearing Time — corresponds to the short-circuit current duration, since the beginning of the short-circuit until the circuit-breakers that isolate the fault are open.

Incident — an event that leads to disconnection (not planned) of one or more grid elements – incident elements, which may lead to demand not supplied (see chapter 5).

Interruption — failure to supply electrical energy to one or more delivery points, totally or partially.

Net Transfer Capacity (NTC)	is the maximum total exchange program between two adjacent control areas compatible with security standards applicable in all control areas of the interconnected system, and taking into account the technical uncertainties on future network conditions [153]. NTC=TTC-TRM
Operating Security Limits	the acceptable operating boundaries (thermal, voltage and stability limits).
SE snapshots	AC load flow calculation input data sets given in a specific format (such as IEEE, UCTE or PSS/E) and corresponding to the state of the transmission grid (topology, loads and generation pattern) at a determined timestamp of the present day.
Severe Incidents	are contingencies that far exceed all the security principles used for planning and system operation. These major disturbances are usually a conjunction of several events.
Total Transfer Capacity (TTC)	is the maximum exchange program between two adjacent control areas that is compatible with operational security standards applied in each system (if future network conditions, generation and load patterns are perfectly known in advance) [153].
Tower	or Pylon
Transmission Reliability Margin (TRM)	is a security margin that copes with uncertainties on the computed TTC values arising from: [153] – unintentional deviations of physical flows during operation due to the physical functioning of secondary control – emergency exchanges between TSOs to cope with unexpected unbalanced situations in real-time – inaccuracies, e. g. in data collection and measurements

Appendix A

Network map

Figure A.1: The Portuguese transmission network (2009).

Appendix B

Overhead line corridors

Definition The definition of a line corridor is based on the following criteria:

- The width is smaller than 200 meters.
- The number of circuits is higher than or equal to 2.
- The lines' equal pathway is longer than 1000 meters.

The following list was updated last in November 2009.

Corridor	Lines in corridor	Voltage level
1	LPDVRA + LALRA2 + LRARR2	400
2	LALRA2 + LAFRA	150 / 400
3	LCDPDV1 + LCDPDV2 + LALPDV	150 / 400
4	LMDRPDV1 + LMDRPDV2 + LALPDV	150 / 400
5	LALRA2 + LVNRA/OR	150 / 400
6	LMDRPDV1 + LMDRPDV2	150
7	LCDPDV1 + LCDPDV2 + LCDVI1/VF	150
8	LCDPDV1 + LCDPDV2 + LMDRPDV1 + LMDRPDV2	150
9	LCDVI1/VF + LORVI + LPDVVI	150
10	LORPDV + LORVI + LPDVVI	150
11	LVNRA/OR + PDVVI + LORPDV	150
12	LVNRA/OR + LVNSD + LCDRA1/FRD + LCDFRD/PDV	150
13	LVNRA/OR + LSDCD + LCDRA1/FRD + LCDFRD/PDV	150
14	LVNRA/OR + LCDRA1/FRD + LCDFRD/PDV + LCDRA2/GR	150
15	LRAED1 + LRAED2 + LRAED3 + LRAED4	150
16	LRAED1 + LRAED2 + LRAED3 + LVMED1	150
17	LVMED1 + LVMED2 + LVMED3/MAA	150
18	LRRCT + LVMCT1	220
19	LRRVM1 + LRRVM2 + LRRVM3 + LRRCT + LVGVM4	220
20	LVGRR1 + LRRUR + LVGVM4	220
21	LVGRR1 + LRRUR + LRARR1	200 / 400
22	LVGRR1 + LRRUR	220
23	LVGRR1 + LVGUR	220
24	LRRCN3/TG + LTGRR	220
25	LTGCN/EJ + LRRCN3/TG	220
26	LVGRR1 + LVGUR + LVGVM4	220
27	LVGCL1 + LVGCL2 + LVGCL3	220
28	LCLMC + LCLEJ2	220
29	LCLMC + LCLEJ1 + LCLEJ2	220
30	LTGCN/EJ + LCLEJ1 + LCLEJ2	220
31	LCTRTR1 + LCTRTR2	220
32	LVRVG1 + LVRVG2 + LPNVG1	220
33	LPNVG2 + LTCRG	150 / 220
34	LPNVG2 + LBAVG	220

Continued on next page

Corridor	Lines in corridor	Voltage level
35	LPNVG1 + LPNVG2	220
36	LPTBT + LPTLGC1 + LPTMG	220
37	LPTLGC1+LBTLGC1+LBTLGC2	220
38	LPNLGC1+LPNLGC2	220
39	LLGCAAV2 + LLGCAAV3	220
40	LMDPT1 + LMDPT2	220
41	LPNCF1 + LPNCF2	220
42	LCLMC + LRRPI	220 / 400
43	LEJMC+ LRRLV	220 / 400
44	LEJMC + LCLMC + LRRPI	220 / 400
45	LMCPI + LMCPR1 + LRRPI	220 / 400
46	LMCPI + LMCPR1	220
47	LMCPR1 + LPIPR/MR	220
48	LPIPR/MR + LMCPI + LBAPI	220
49	LPIPR/MR + LMCPR1 + LPRTBA1/MRT	220
50	LVCTBA1+LVCTBA2	220
51	LPRTBA1/MRT+LPRTBA2	220
52	LAGPR1 + LAGPR2/MRT + LPRTBA1/MRT	220
53	LCFVC1/GVA + CFVC2/GVA	220
54	LCFFE1/SSE + LCFFE2/SSE	220
55	LCCFE1/FTL + LCCFE2/FTL	220
56	LCCFE1/FTL + LCCFE2/FTL + LGUCC	150 / 220
57	LFRCC1/RDA + LFRCC2/RDA + LCOSFR	150
58	LZRFR + LFTFR	150
59	LZRFR + LBLPG	150 / 400
60	LBCZR1 + LBCZR2	150
61	LCBZR1 + LCBZR2 + LCBZR3	220
62	LPRBL1 + PRBL2/PB	220
62	LPRBL1 + LBLPI	220 / 400
63	LPRBL2/PB + LLVRM	220 / 400
64	LPRBL2/PB + LBLRM2	220
65	LBLRM2 + LLVRM	220 / 400
66	LBLRM1 + LBLRM2	220
67	LBLRM1 + LBLRJ	220 / 400
68	LLRSLV1 + LLRSLV2	400
69	LRRLV + LLRSLV1 + LLRSLV2	400
70	LRRLV + LLVRM	400
71	LCGRM2 + LCGRM3 + LBLRJ	220 / 400
72	LCGRM1 + LRMCVR	220
73	LRMCVR + LCVRTJ	220
74	LPMRJ + LBLRJ	400
75	LCVRTJ + LFNTJ + LRMAM	220 / 400
76	LFNTJ + LRMAM + LFNAM4 + LAMRJ	220 / 400
77	LCVRTJ + LAMCH/TJ	220
78	LCGFN2 + LPMFN	220 / 400
79	LSVPA + LCGSV + LCGCH/SV	150 / 220
80	LSVPA + LCGSXL	150 / 220
81	LSVPA + LPMFN	150 / 400
82	LPAPM1 + LPAPM2 + LCGSXL + LPMFN + LPMRJ	150 / 220 / 400
83	LFNSV1 + LSVPA + LCGSV + LFNSV2 + LCGCH/SV	150 / 220
84	LCGSV + LFNSV2	220
85	LFNSV1 + LFNAM3/CH	150 / 220
86	LFNCH + LFNSV2	220
87	LFNCH + LCGCH/SV	220
88	LFNCH + LFNAM3/CH	220
89	LFNCH + LAMCH/TJ	220
90	LFNAM3/CH + LCGCH/SV	220
91	LFNAM3/CH + LAMCH/TJ + LAMSS	220

Continued on next page

Corridor	Lines in corridor	Voltage level
92	LPAQGD1 + LPAQGD2	150
93	LFFTFR1 + LFFTFR2	150
94	LFFFGT1 + LFFFGT2	150
95	LPMFF1 + LPMFF2	150
96	LPMFF4/SXS/SXR + LPMQAJ	150
97	LPMFF4/SXS/SXR + LFFQAJ	150
98	LPMMP/PGS + LPMER/PGS	150
99	LPMER/PGS + LFAER	150
100	LPMMP/PGS + LPMSN2 + LPMSN3	150 / 400
101	LPMSB1 + LPMSB2 + LPMSB3	150
102	LCSBPM1 + LCSBPM2 + LCSBPM3 + LCSBPM4	400
103	LSNES + LPMSN2 + LPMSN3	150 / 400
104	LCSNSN1 + LCSNSN2	150 / 400
105	LCSNSN3 + LCSNSN4	400
106	LSNOQ1 + LSNOQ2	150
107	LSNES + LFASN	150 / 400
108	LFAER + LAVFA	150 / 400
109	LSNSI + LSNPO2 + LSNPO3	150
110	LSIPO + LSNPO2 + LSNPO3	150 / 400
111	LPOTN1 + LPOTN2	150
112	LSIPO + LSNPO2 + LSNPO3 + LPOTN1 + LPOTN2	150
113	LSILZN1+ LSILZN2	150
114	LOQET1 + LOQET2	150

Appendix C

Summer temperature

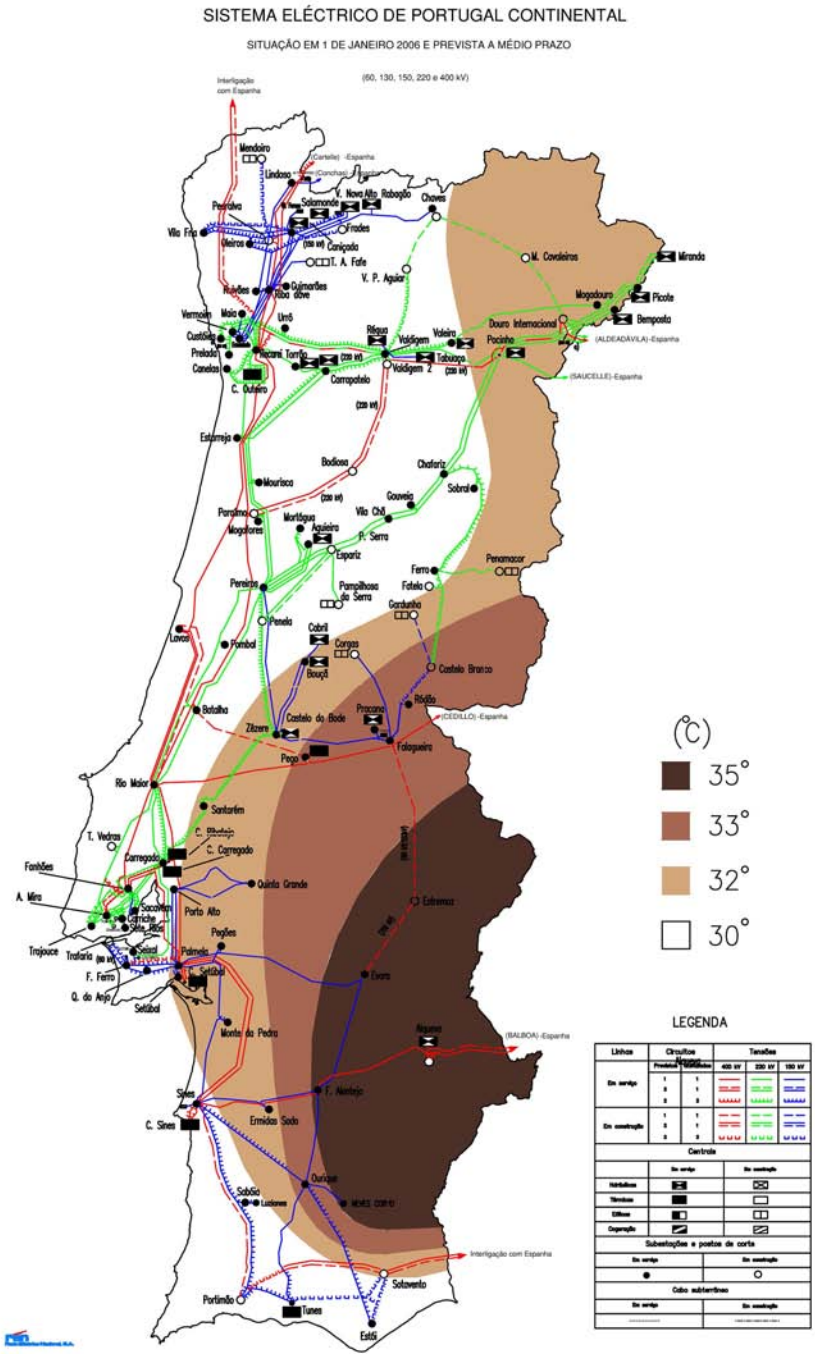


Figure C.1: Summer temperature map (2006).

Appendix D

Overview of faults in PTS

Including all grid elements:

Cause		Voltage Level	Period of Analysis								
			2001	2002	2003	2004	2005	2006	2007	2008	2009
Atmospheric	Lightning	150 kV	43	38	55	38	5	26	33	43	41
		220 kV	34	60	8	20	6	25	30	18	26
		400 kV	7	14	9	13	1	8	12	3	5
		Total	84	112	72	71	12	59	75	64	72
	Fog + Pollution	150 kV	7	11	4	11	1	0	8	5	0
		220 kV	8	46	0	7	17	5	0	4	0
		400 kV	12	34	9	15	44	1	3	3	0
		Total	27	91	13	33	62	6	11	12	0
	Other	150 kV	0	0	0	0	0	0	0	0	4
		220 kV	1	0	0	0	0	2	0	0	7
		400 kV	0	0	6	0	0	0	0	0	2
		Total	1	0	6	0	0	2	0	0	13
Environmental	Storks	150 kV	45	34	63	48	19	49	39	18	20
		220 kV	4	0	1	3	4	14	3	3	3
		400 kV	9	4	6	3	5	10	14	18	18
		Total	58	38	70	54	28	73	56	39	41
	Forest Fires	150 kV	4	8	46	15	25	7	4	0	0
		220 kV	60	27	38	12	128	11	0	1	31
		400 kV	2	24	48	11	79	34	1	2	3
		Total	66	59	132	38	232	52	5	3	34
	Trees	150 kV	0	1	0	0	0	0	0	0	0
		220 kV	0	0	2	0	2	0	0	0	0
		400 kV	0	1	2	1	1	3	0	0	0
		Total	0	2	4	1	3	3	0	0	0
	Other	150 kV	0	0	0	0	0	0	0	0	1
		220 kV	2	1	3	0	0	1	0	3	2
		400 kV	0	0	0	0	0	0	0	0	0
		Total	2	1	3	0	0	1	0	3	3
Internal Origin		150 kV	14	18	16	13	21	19	10	13	6
		220 kV	16	32	20	16	24	14	8	10	15
		400 kV	6	11	6	11	2	8	6	8	14
		Total	36	61	42	40	47	41	24	31	35
External		150 kV	0	0	0	4	0	1	0	2	0
		220 kV	0	0	4	0	3	1	0	0	0
		400 kV	0	0	2	0	0	1	0	2	0
External		Total	0	0	6	4	3	3	0	4	0
Unknown		150 kV	16	13	6	1	5	5	10	3	5
		220 kV	4	3	7	3	8	7	7	18	16
		400 kV	3	8	8	7	2	2	4	6	16
		Total	23	24	21	11	15	14	21	27	37
Total		150 kV	129	123	190	130	76	107	104	84	77
		220 kV	129	169	83	61	192	80	48	57	100
		400 kV	39	96	96	61	134	67	40	42	58
		Total	297	388	369	252	402	254	192	183	235

Including only overhead lines:

Cause		Voltage Level	Period of Analysis								
			2001	2002	2003	2004	2005	2006	2007	2008	2009
Atmospheric	Lightning	150 kV	43	38	55	38	5	26	33	43	41
		220 kV	34	58	8	20	6	22	29	17	26
		400 kV	7	14	9	13	1	8	11	3	5
		Total	84	110	72	71	12	56	73	63	72
	Fog + Pollution	150 kV	7	11	4	11	1	0	8	5	0
		220 kV	8	43	0	7	17	5	0	4	0
		400 kV	12	34	9	14	39	1	3	3	0
		Total	27	88	13	32	57	6	11	12	0
	Other	150 kV	0	0	0	0	0	0	0	0	4
		220 kV	1	0	0	0	0	2	0	0	7
		400 kV	0	0	6	0	0	0	0	0	2
		Total	1	0	6	0	0	2	0	0	13
Environmental	Storks	150 kV	45	34	63	48	19	49	39	18	19
		220 kV	4	0	1	3	4	14	3	3	3
		400 kV	9	4	6	3	5	10	14	18	18
		Total	58	38	70	54	28	73	56	39	40
	Forest Fires	150 kV	4	8	46	15	25	7	4	0	0
		220 kV	60	27	38	12	128	11	0	1	31
		400 kV	2	24	48	11	79	34	1	2	3
		Total	66	59	132	38	232	52	5	3	34
	Trees	150 kV	0	1	0	0	0	0	0	0	0
		220 kV	0	0	2	0	2	0	0	0	0
		400 kV	0	1	2	1	1	3	0	0	0
		Total	0	2	4	1	3	3	0	0	0
	Other	150 kV	0	0	0	0	0	0	0	0	0
		220 kV	0	0	0	0	0	0	0	1	2
		400 kV	0	0	0	0	0	0	0	0	0
		Total	0	0	0	0	0	0	0	1	2
Internal Origin		150 kV	10	11	9	7	14	11	3	6	2
		220 kV	8	15	11	10	11	8	3	6	5
		400 kV	5	8	3	8	0	3	4	2	8
		Total	23	34	23	25	25	22	10	14	15
External External		150 kV	0	0	0	4	0	0	0	2	0
		220 kV	0	0	4	0	3	1	0	0	0
		400 kV	0	0	2	0	0	1	0	2	0
		Total	0	0	6	4	3	2	0	4	0
Unknown		150 kV	16	12	6	1	5	5	9	3	5
		220 kV	4	2	4	2	8	7	7	18	16
		400 kV	3	8	8	7	2	2	4	6	16
		Total	23	22	18	10	15	14	20	27	37
Total		150 kV	125	115	183	124	69	98	96	77	71
		220 kV	119	145	68	54	179	70	42	50	90
		400 kV	38	93	93	57	127	62	37	36	52
		Total	282	353	344	235	375	230	175	163	213

Appendix E

Stork nests density

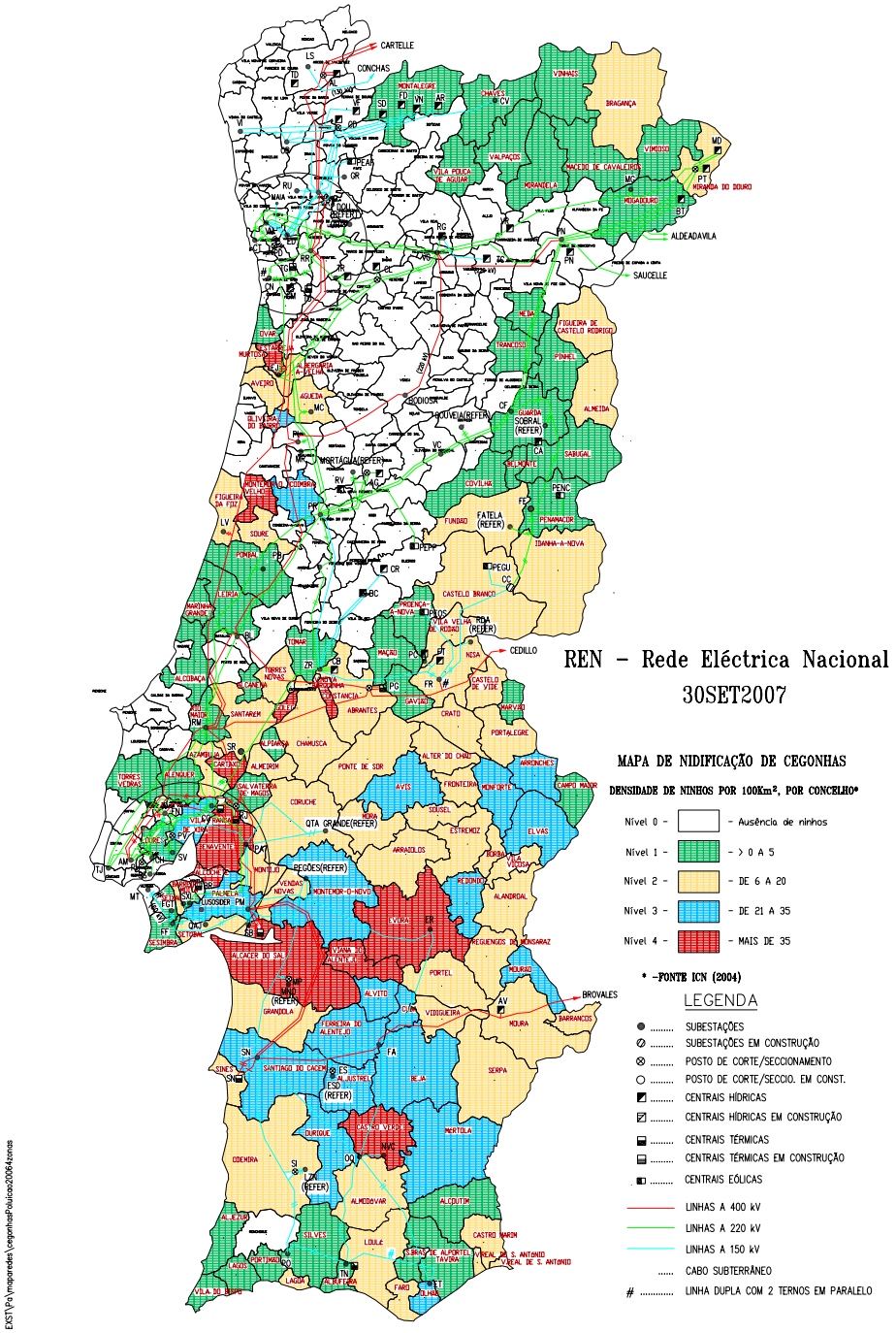


Figure E.1: Number of stork nests per 100 km^2 (2007).

Appendix F

Pollution

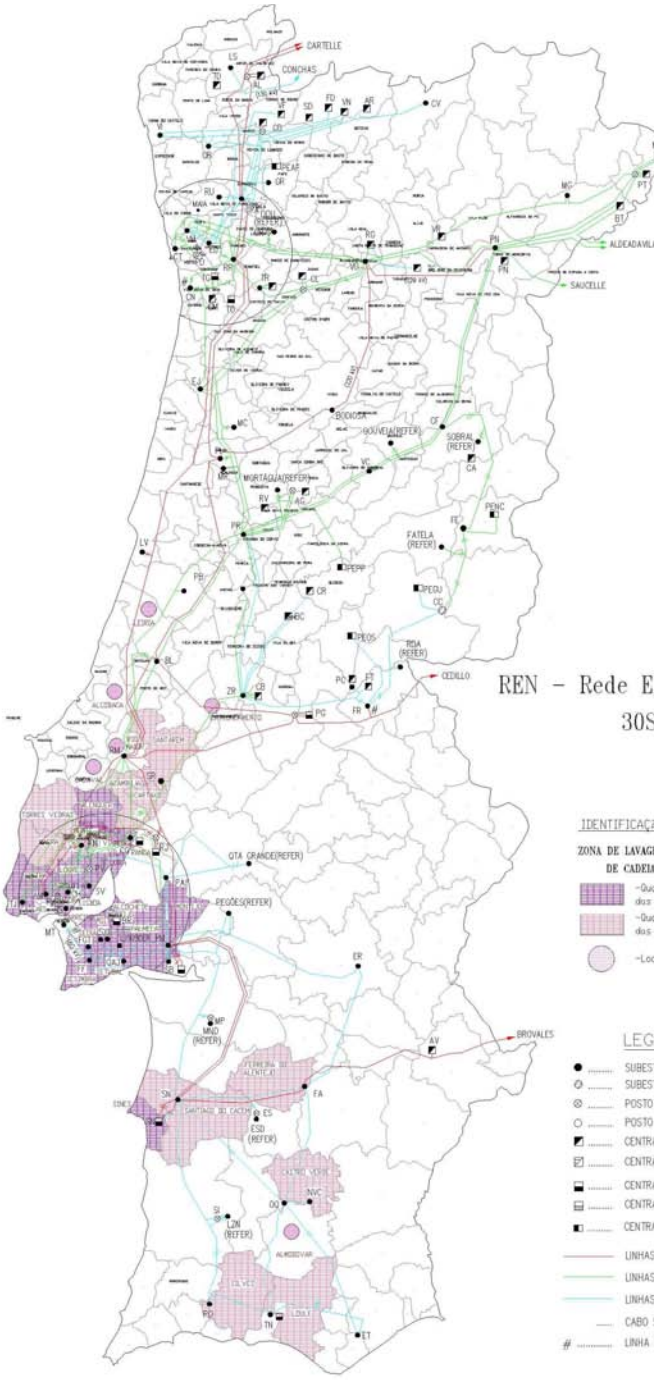


Figure F.1: Pollution map (2007).

Appendix G

Lightning density

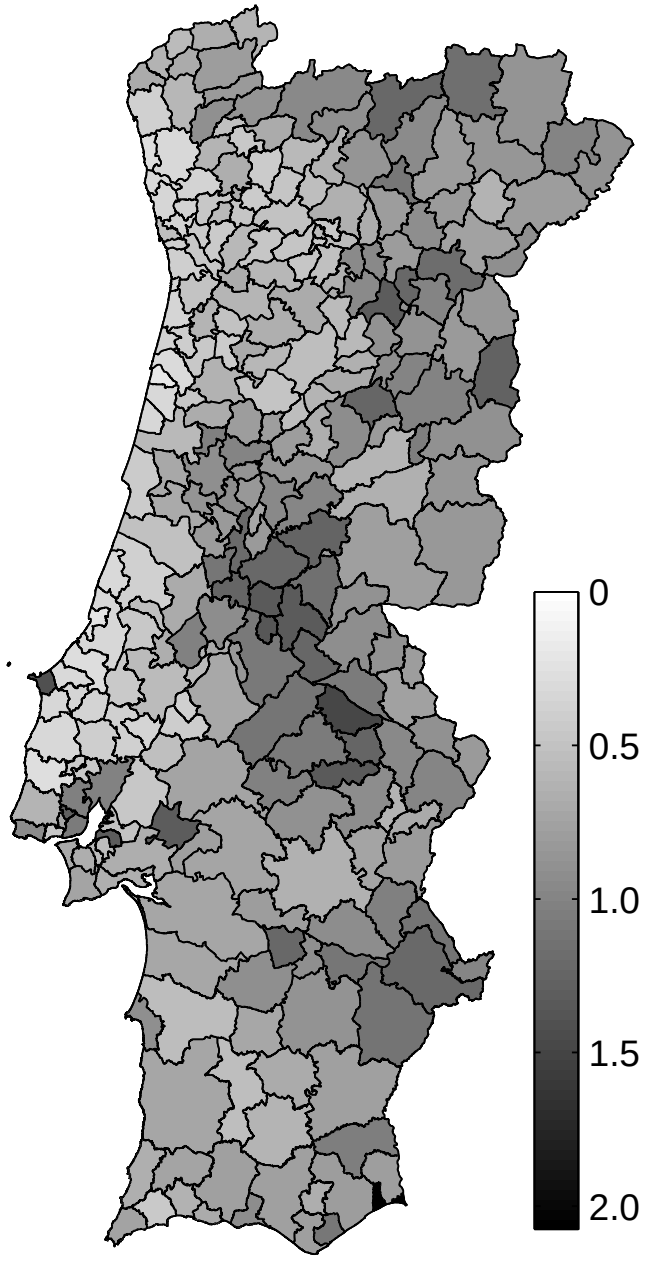


Figure G.1: Average lightning density per municipality from 2003 until 2009.

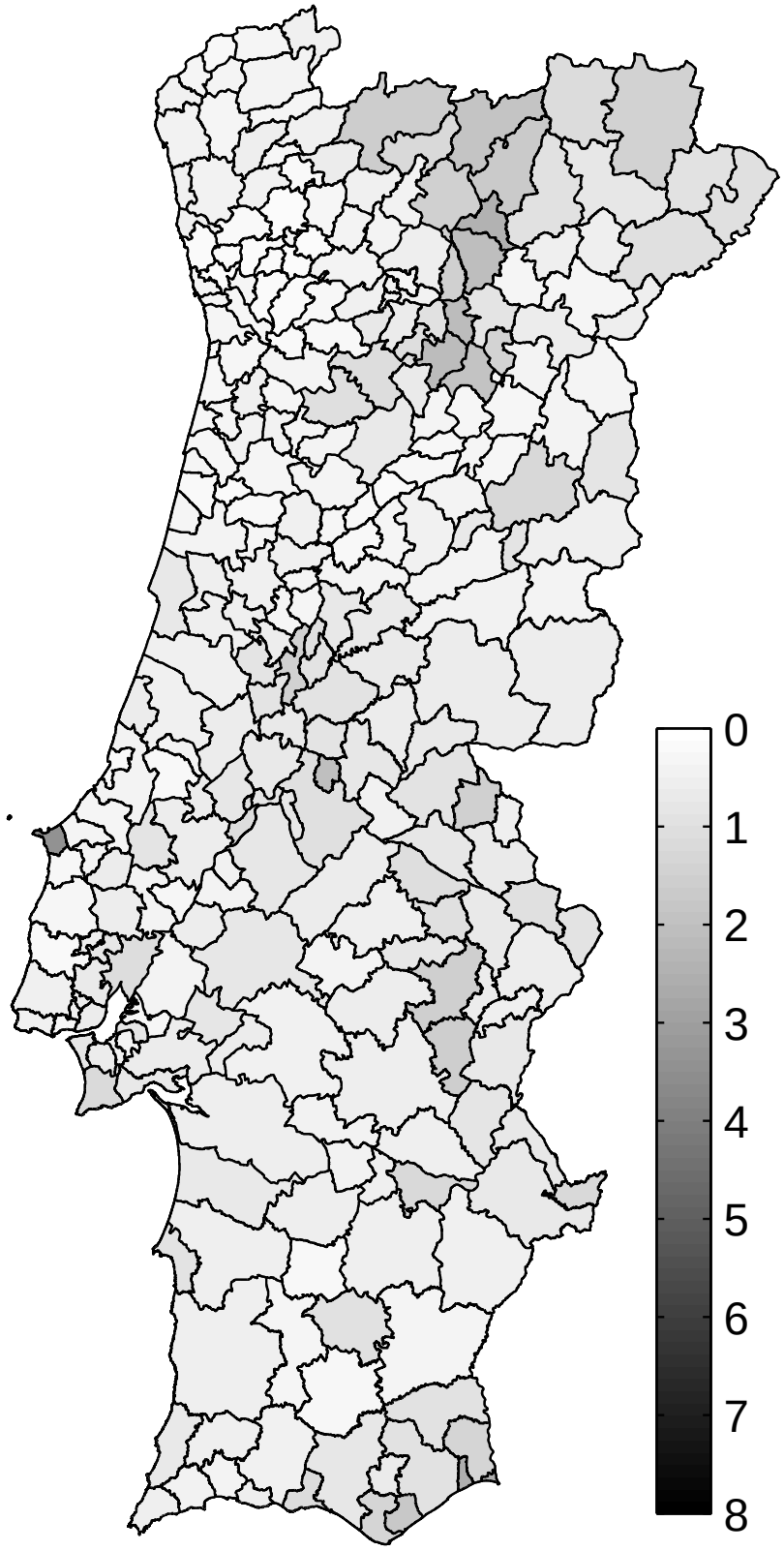


Figure G.2: Average lightning density per municipality in 2003.

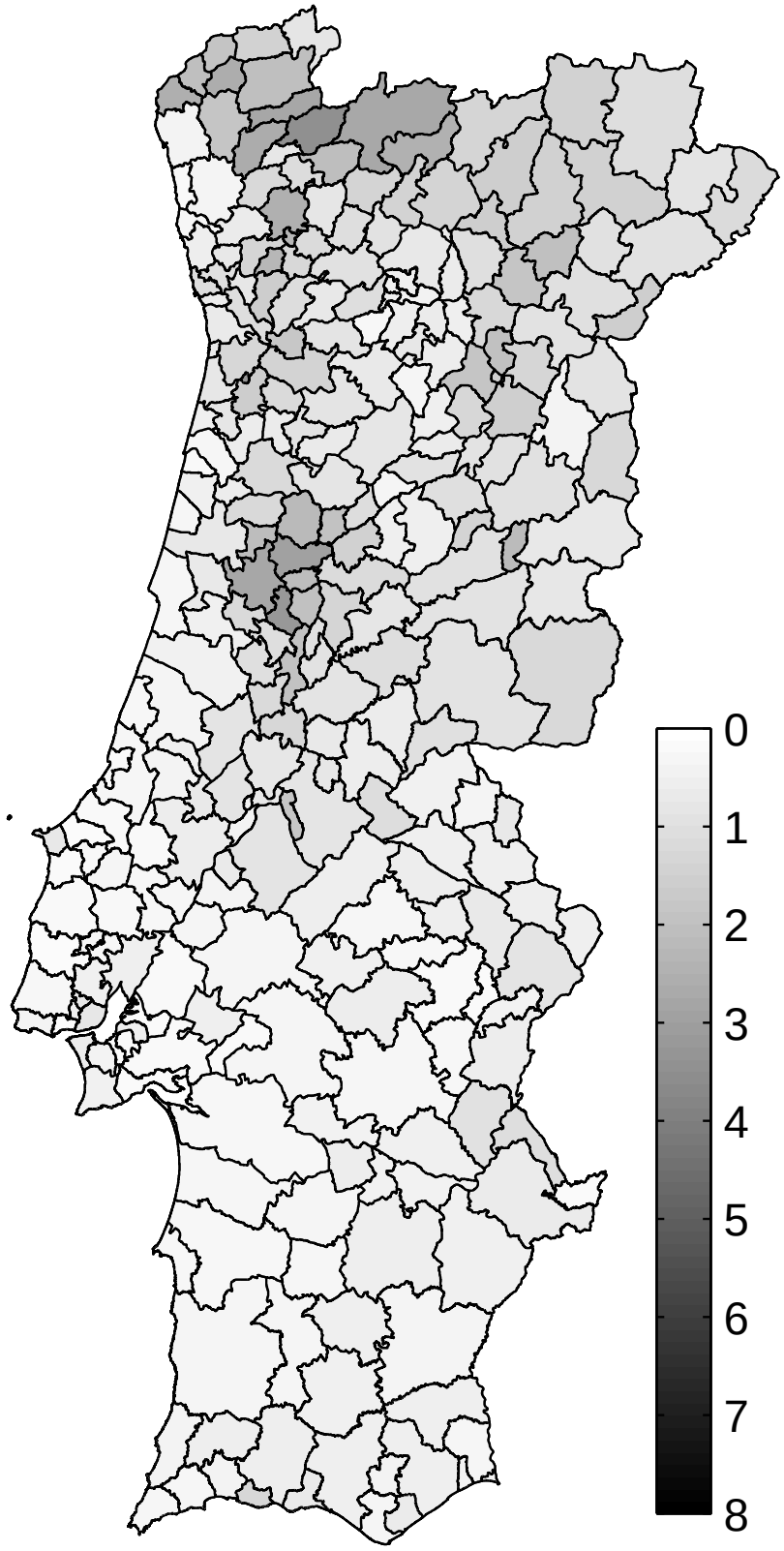


Figure G.3: Average lightning density per municipality in 2004.

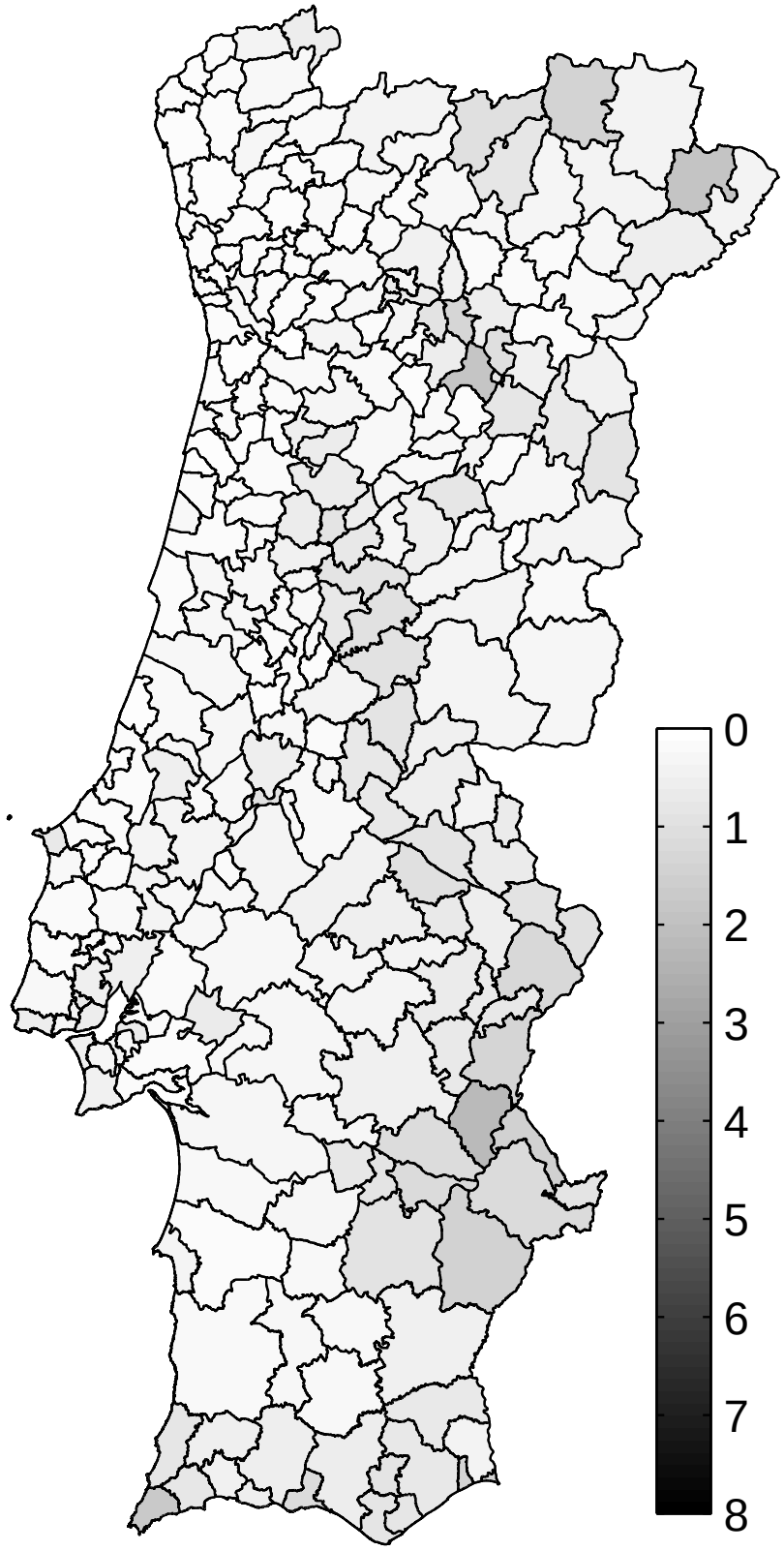


Figure G.4: Average lightning density per municipality in 2005.

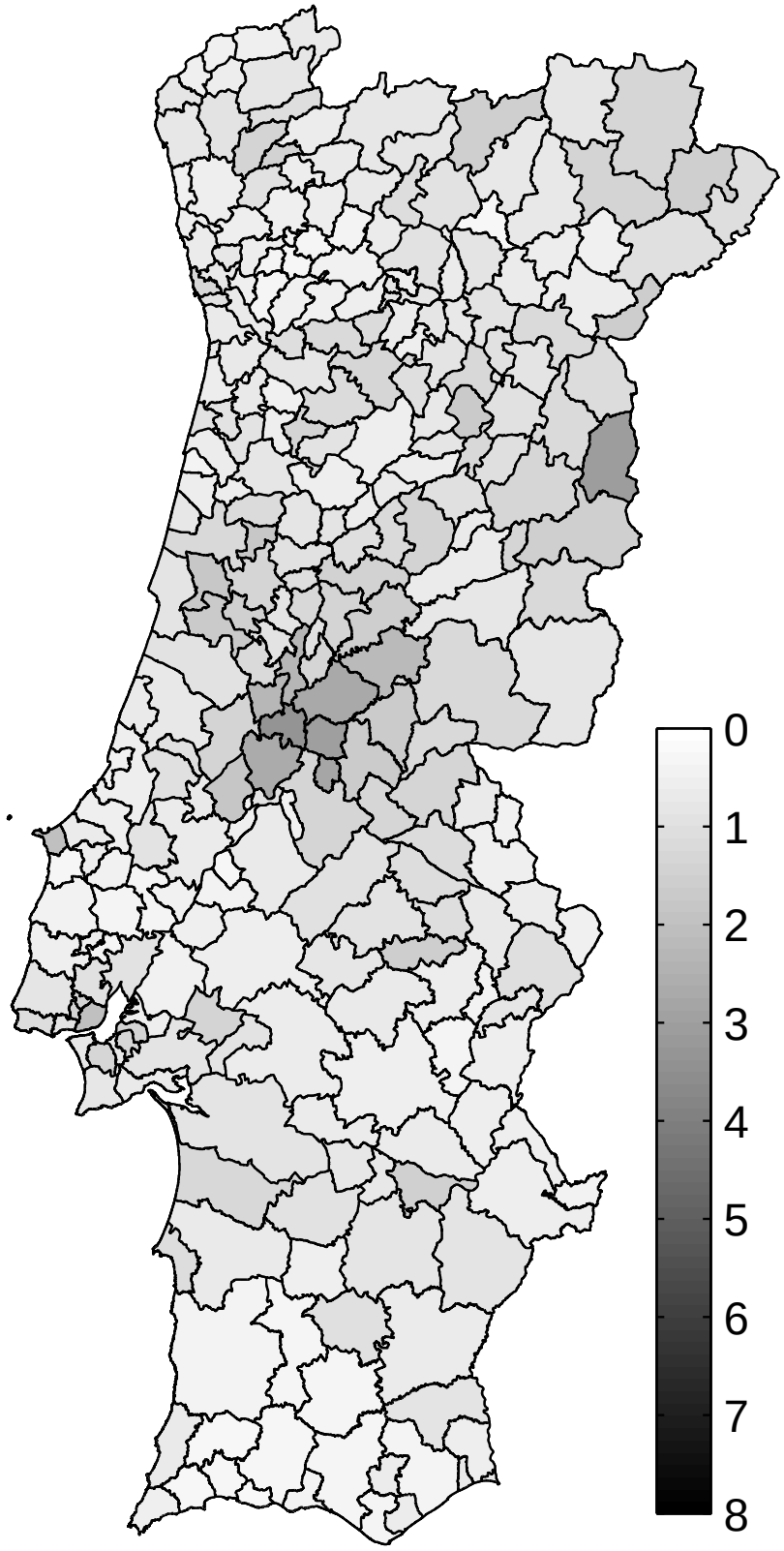


Figure G.5: Average lightning density per municipality in 2006.

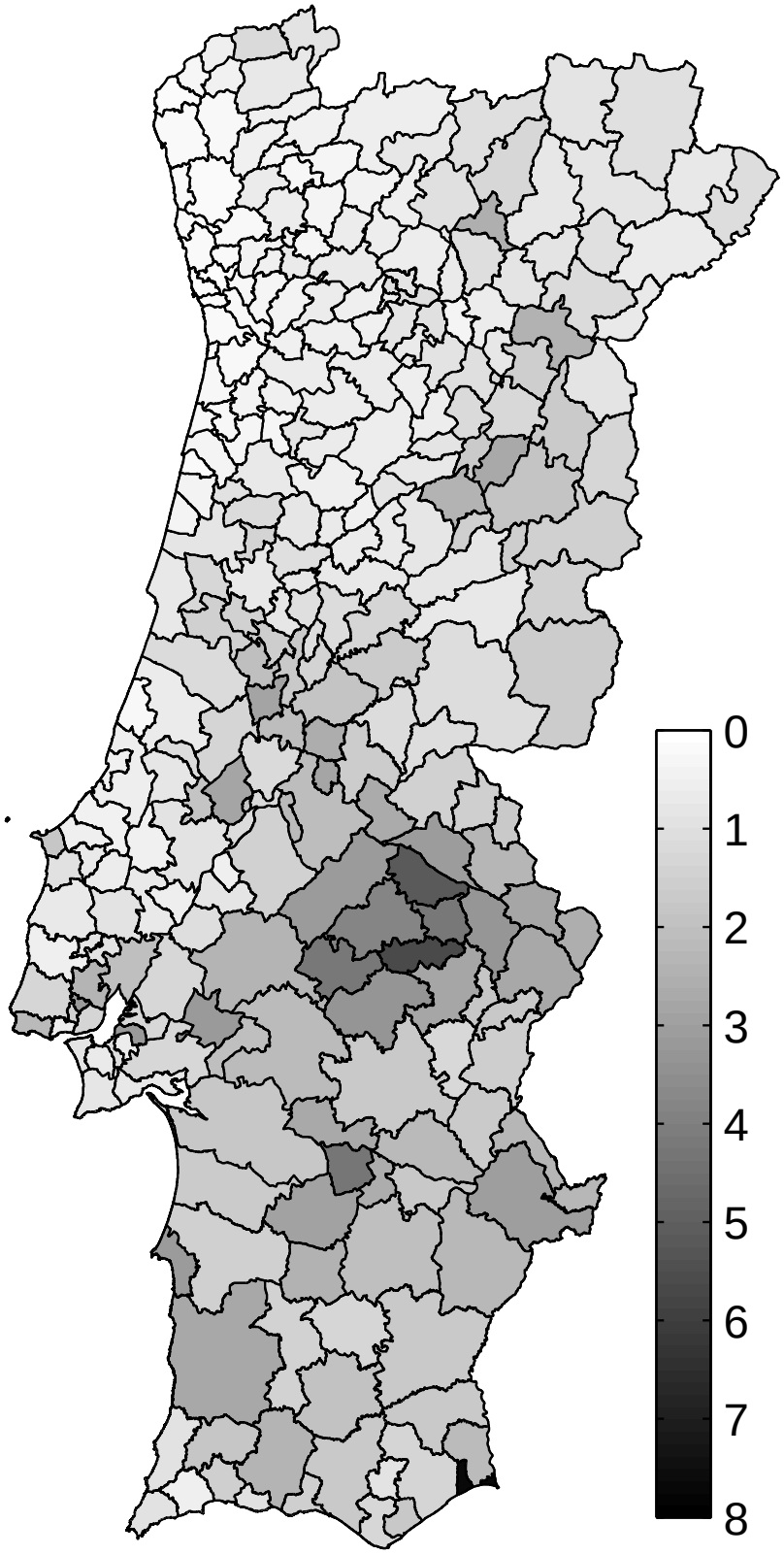


Figure G.6: Average lightning density per municipality in 2007.

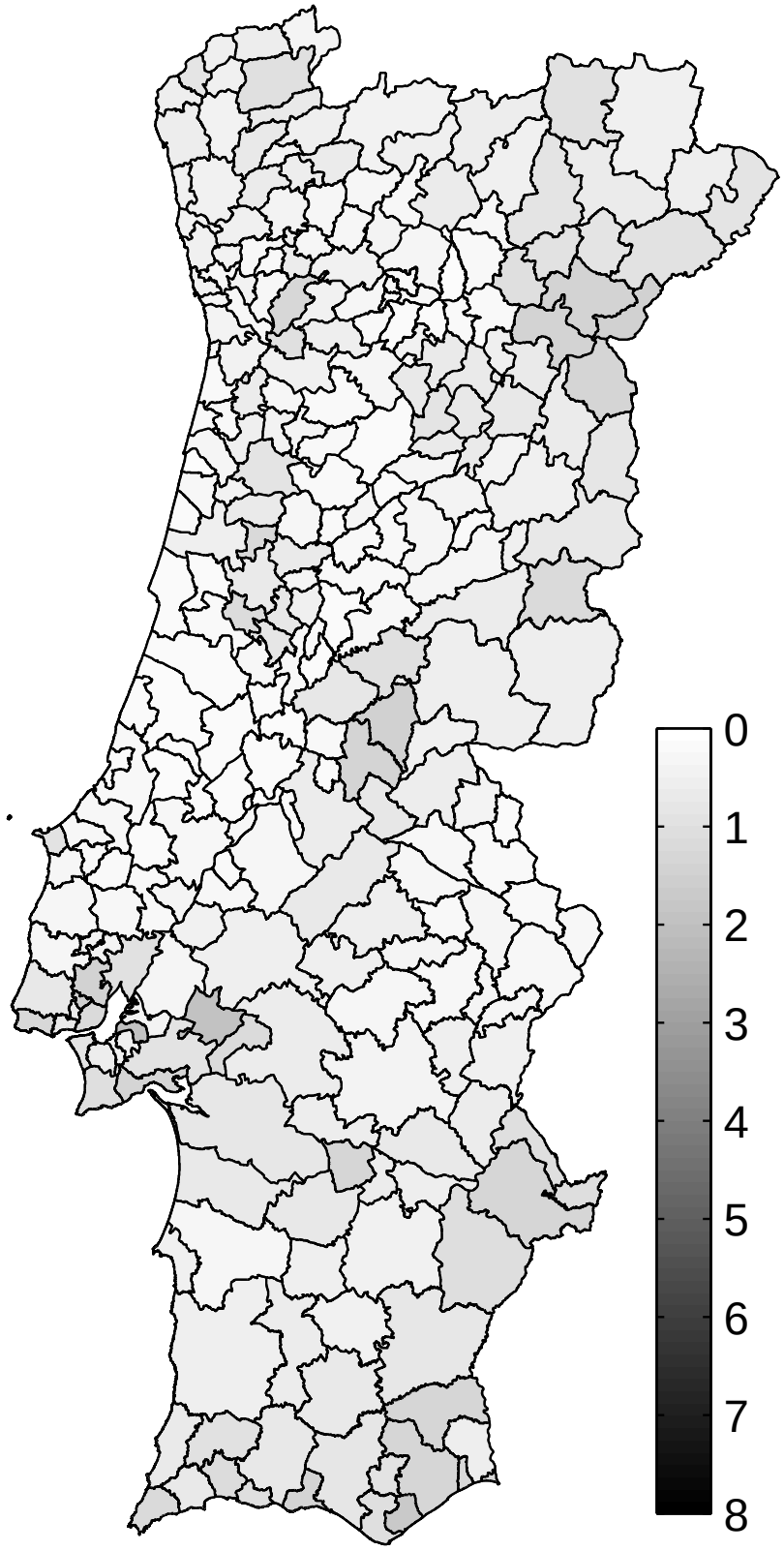


Figure G.7: Average lightning density per municipality in 2008.

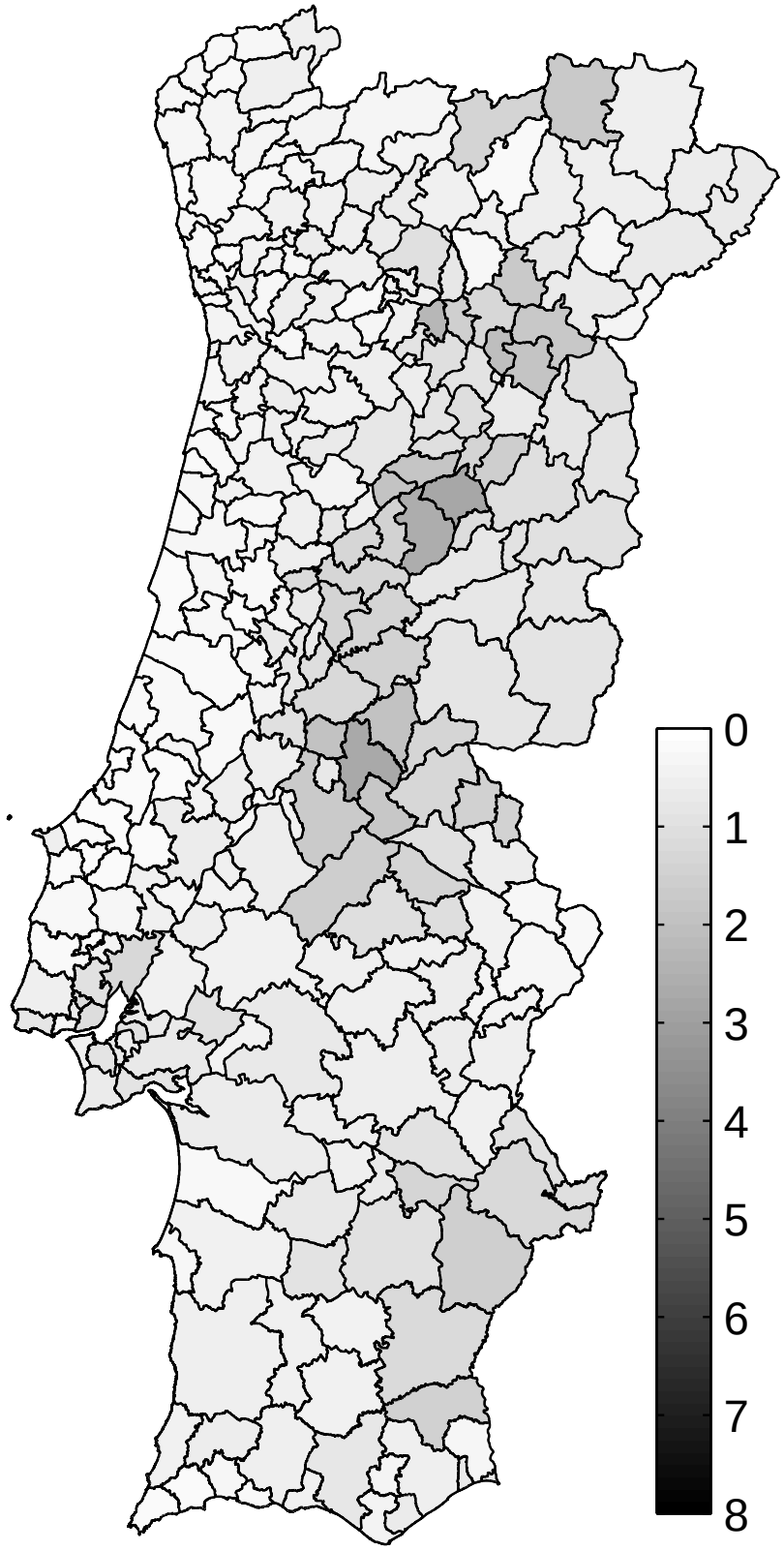


Figure G.8: Average lightning density per municipality in 2009.

Appendix H

Faults caused by fog and pollution and composite insulators

OHL name	2001	2002	2003	2004	2005	2006	2007	2008	2009	Composite Installation	Faults after Installation	Faults before Installation
LAMRJ				5	5		1	1		Partially	2	10
LFNRJ							2	2		Partially		4
LCCFE2/FTL								4				4
LCGCH/SV		2			4					Totally		6
LCGRM2					13					Partially		13
LCGSV	4	11								Totally		15
LCGSXL		15								Almost all		15
LCSBPM1				1						Totally		1
LCSBPM4	1									Totally		1
LFAAV/BVL					1							1
LFFFGT1				1								1
LFNAM3/CH		1								Totally		1
LFNAM4				5	8					Partially		13
LFNCH		4								Totally		4
LFNSV2	4	10		7						Totally		21
LLVRM		8										8
LOQET2			1				1					2
LPAPM2					1		2			Totally		3
LPAQGD1				1								1
LPAQGD2	3	1		1				5				10
LPGRM	1	7										8
LPMER/PGS							5					5
LPMFF1		3								Totally		3
LPMFF2		1								Totally		1
LPMFN		9	1	1	6					Totally		17
LPMRJ	7	4	7	1	2					Totally		21
LRMPM												
LPMSB1	2											2
LPMSN1/PGS		1										1
LPMMP/PGS										Partially		
LPMSN2	2			1	2					Partially		5
LPMSN3		2			5					Partially		7
LPRBL2/PB						5						5
LRMFN			1		2	1						4
LRMAM										Partially		
LRRRM2	1	4			8							13
LBLRJ										Partially		
LSNSI			2	2								4
LSNTN1												
LSITN												
LSNTN2				2								2
LSVPA	1	1		1						Partially		3
LZRPR1		1										1
LZRPA1	1	1		1								3
LZRSV2		2	1	2								5
Total	27	88	13	32	57	6	11	12	0		2	244
		Partially equipped										
		Totally equipped										

Appendix I

Backflash rates overhead lines

OHL name	Voltage level	BFR per year
LSVPA	150kV	0.029950
LCRBC	150kV	0.145396
LBCZR1	150kV	0.713844
LVNSD	150kV	0.259874
LSDCD	150kV	0.465817
LBCZR2	150kV	0.704565
LVMED1	150kV	0.050735
LTCRG	150kV	0.113594
LVMED2	150kV	0.069364
LPMSB1	150kV	0.020125
LPMFF1	150kV	0.197810
LPMFF2	150kV	0.197810
LPAPM1	150kV	0.108791
LPAPM2	150kV	0.432680
LPMSB2	150kV	0.009702
LPMSB3	150kV	0.011567
LSNPO2	150kV	0.261310
LPOTN2	150kV	0.083707
LVMED3/MAA	150kV	0.084287
LVNRA/OR	150kV	2.153970
LRAED1	150kV	0.412530
LCDRA1/FRD	150kV	1.301268
LRAED2	150kV	0.258904
LCDRA2/GR	150kV	0.685018
LRAED3	150kV	0.267845
LRARU	150kV	0.052592
LPMFF4/SXS/SXR	150kV	0.234949
LCSNSN1	150kV	0.136565
LPMER/PGS	150kV	0.411280
LRAED4	150kV	0.317519
LFNSV1	150kV	0.028141
LOQET1	150kV	0.483625
LCDVI1/VF	150kV	1.045273
LFAER	150kV	0.194356
LSNOQ1	150kV	0.995797
LSNOQ2	150kV	0.995791
LTNET	150kV	0.229520
LFAOQ	150kV	0.078159
LOQTN	150kV	0.233098
LOQNVC	150kV	0.095872
LFTFR	150kV	0.148283
LZRFR	150kV	0.721375
LORVI	150kV	0.398610

Continued on next page

OHL name	Voltage level	BFR per year
LPMQAJ	150kV	0.121055
LFFQAJ	150kV	0.101103
LRAOR	150kV	0.831400
LPAQGD1	150kV	0.050198
LPAQGD2	150kV	0.074493
LFFTFR1	150kV	0.017334
LFFFGT1	150kV	0.048898
LFFFGT2	150kV	0.048929
LPMMP/PGS	150kV	0.386273
LMPSN	150kV	1.081852
LSNES	150kV	0.100125
LESFA	150kV	0.027919
LOQET2	150kV	0.483632
LFRCC1/RDA	150kV	0.138761
LFRCC2/RDA	150kV	0.136231
LSILZN1	150kV	0.029417
LSILZN2	150kV	0.029427
LAFRA	150kV	0.438007
LSNSI	150kV	0.314264
LCOSFR	150kV	0.262702
LGUCC	150kV	0.175177
LMDRPDV1	150kV	0.650457
LCDPDV1	150kV	0.042566
LCDPDV2	150kV	0.085143
LORPDV	150kV	0.199854
LPDVVI	150kV	0.150720
LSIPO	150kV	0.069551
LPOTN1	150kV	0.055807
LFFTFR2	150kV	0.017334
LCDFRD/PDV	150kV	0.082744
LARFRD/CV	150kV	1.663013
LCFDFRD	150kV	0.004015
LMDRPDV2	150kV	0.325227
LSNPO3	150kV	0.079150
LSNGP	150kV	0.002625
LCGSR	220kV	0.048084
LPTBT	220kV	0.132992
LPNSLL	220kV	0.090811
LMDPT1	220kV	0.137295
LVCPR1/MRT	220kV	0.617545
LVGCL1	220kV	0.266993
LRGVG	220kV	0.002171
LVGCL2	220kV	0.297524
LVGCL3	220kV	0.297536
LPTPN	220kV	0.287718
LPNVG1	220kV	0.733351
LBTPN	220kV	0.542836
LPRBL1	220kV	0.052715
LCGRM1	220kV	0.047246
LCGRM2	220kV	0.075783
LCGRM3	220kV	0.076697
LBLRM1	220kV	0.029897
LVRVG1	220kV	0.161180
LVRVG2	220kV	0.161180
LPRBL2/PB	220kV	0.148639
LBLRM2	220kV	0.050488
LVCPR2/PP	220kV	0.611264
LAGPR1	220kV	0.154129

Continued on next page

OHL name	Voltage level	BFR per year
LAGPR2/MRT	220kV	0.275221
LCPNPN	220kV	0.001388
LPNVG2	220kV	0.478199
LCLMC	220kV	0.628168
LMCPR1	220kV	0.211915
LCLEJ1	220kV	0.370433
LCLEJ2	220kV	0.503084
LBTAAV	220kV	0.124168
LPNAAV	220kV	0.210439
LMGVR/MCC	220kV	0.587139
LPTMG	220kV	0.136141
LFNAM3/CH	220kV	0.020153
LCGFN2	220kV	0.005068
LCGCH/SV	220kV	0.004778
LCLTR	220kV	0.064733
LTRRR	220kV	0.099908
LVGRR1	220kV	0.509735
LCGSXL	220kV	0.011090
LVGUR	220kV	0.424552
LRRUR	220kV	0.085297
LMDPT2	220kV	0.065847
LRRVM2	220kV	0.063084
LRRVM3	220kV	0.063521
LRRCN1	220kV	0.059695
LCPTPT1	220kV	0.001328
LCPTPT2	220kV	0.000600
LCPTPT3	220kV	0.000420
LRRCT	220kV	0.101372
LVMCT1	220kV	0.015597
LRRCN3/TG	220kV	0.037849
LTGCN/EJ	220kV	0.117112
LTGRR	220kV	0.015112
LCFFE1/SSE	220kV	0.923809
LCFFE2/SSE	220kV	0.923816
LFNCH	220kV	0.005958
LAMCH/TJ	220kV	0.003513
LPNCF1	220kV	0.383132
LPNCF2	220kV	0.388424
LCFVC1/GVA	220kV	0.509185
LCFVC2/GVA	220kV	0.544865
LCGSV	220kV	0.056705
LFNSV2	220kV	0.002826
LVMCT2	220kV	0.020601
LEJPI	220kV	0.158001
LPIPR/MR	220kV	0.172797
LSRZR	220kV	0.074147
LAMSS	220kV	0.001250
LNCFE	220kV	0.045189
LCCFE1/FTL	220kV	0.131880
LCCFE2/FTL	220kV	0.131888
LFNTJ	220kV	0.002401
LVGVM4	220kV	0.082826
LPRPNL	220kV	0.008732
LPNLZR	220kV	0.127650
LRMCVR	220kV	0.020197
LCVRTJ	220kV	0.016935
LVPAVG	220kV	0.038982
LBAVG	220kV	0.088374

Continued on next page

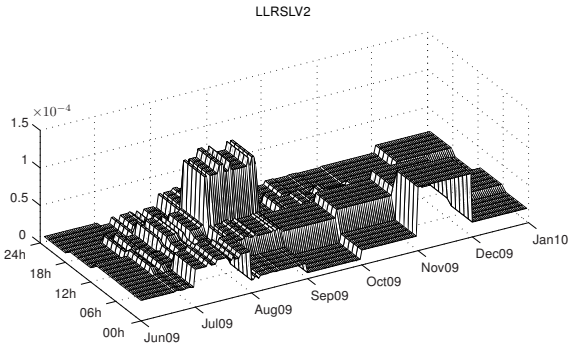
OHL name	Voltage level	BFR per year
LBAPI	220kV	0.051152
LRRVM1	220kV	0.085739
LCTRTR2	220kV	0.000091
LCTRTR1	220kV	0.000120
LCBZR1	220kV	0.004952
LCBZR2	220kV	0.004977
LCBZR3	220kV	0.005003
LCSBPM1	400kV	0.005779
LCSBPM2	400kV	0.005779
LCSBPM3	400kV	0.000789
LCSBPM4	400kV	0.000789
LPMFN	400kV	0.033355
LCSNSN2	400kV	0.041007
LPMSN2	400kV	0.237356
LALRA2	400kV	1.611212
LRARR1	400kV	0.401955
LCSNSN3	400kV	0.041814
LCSNSN4	400kV	0.041810
LPMSN3	400kV	0.084303
LRARR2	400kV	0.160386
LALCTL1	400kV	0.020568
LALCTL2	400kV	0.015404
LCALAL1	400kV	0.002650
LCALAL2	400kV	0.001919
LPGRM	400kV	0.272155
LFNAM4	400kV	0.002116
LAVBVL	400kV	0.017697
LPMRJ	400kV	0.017798
LAMRJ	400kV	0.003318
LFNRJ	400kV	0.001745
LCRJRJ2	400kV	0.000003
LCRJRJ3	400kV	0.000002
LRRPI	400kV	0.076295
LALPDV	400kV	0.274143
LPDVRA	400kV	0.136657
LPGFR	400kV	0.453940
LFRCLL	400kV	0.306509
LBLPI	400kV	0.393878
LBLRJ	400kV	0.050624
LFASN	400kV	0.026909
LAVFA	400kV	0.020639
LRMAM	400kV	0.001042
LBLPG	400kV	0.142947
LCAVAV	400kV	0.000212
LRRLV	400kV	0.254285
LLVRM	400kV	0.044972
LCPGPG1	400kV	0.000125
LCPGPG2	400kV	0.000116
LLRSLV1	400kV	0.000332
LLRSLV2	400kV	0.000332

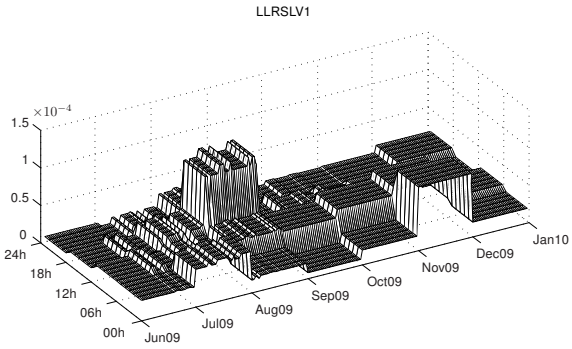
Appendix J

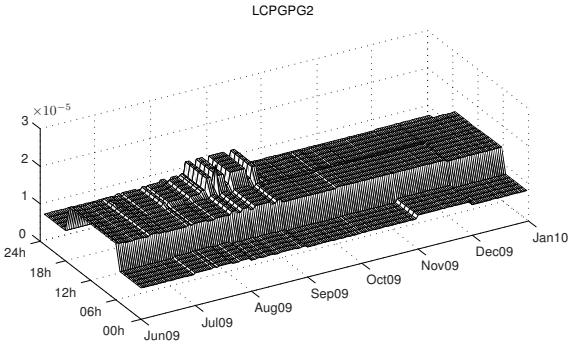
Contingency probability results

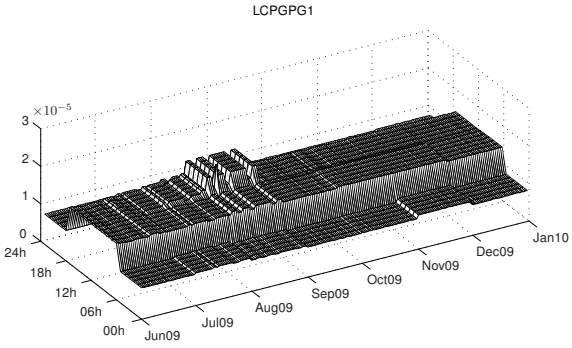
In the following pages, the results are given of the contingency probability calculation for overhead lines, busbars, transformers and N-2 contingencies. For overhead lines, an overview is given of maximum, minimum and average contingency probabilities.

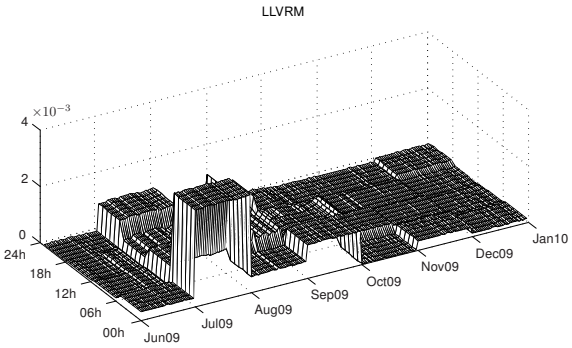
J.1 Overhead lines

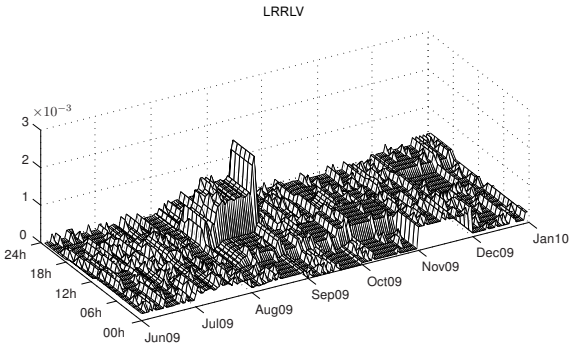




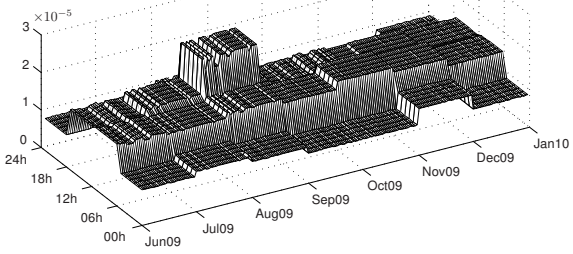




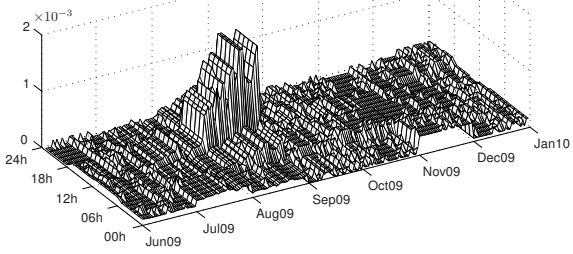




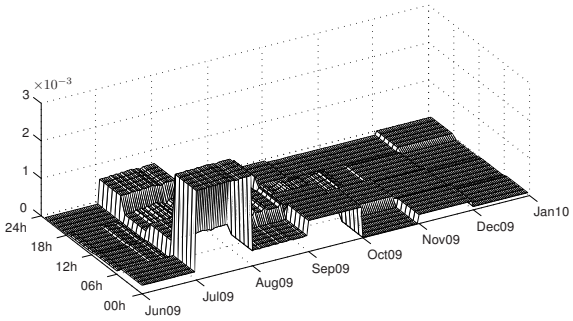
LCAVAV



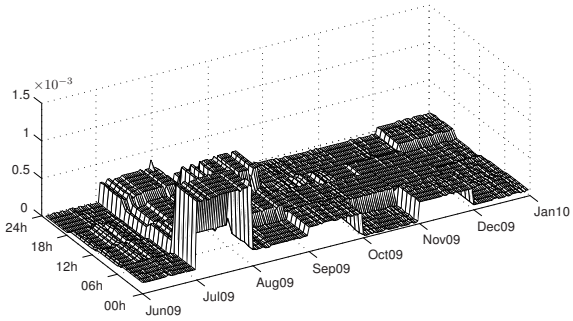
LBLPG



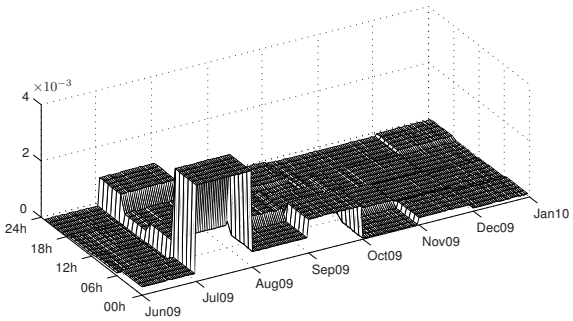
LRMAM



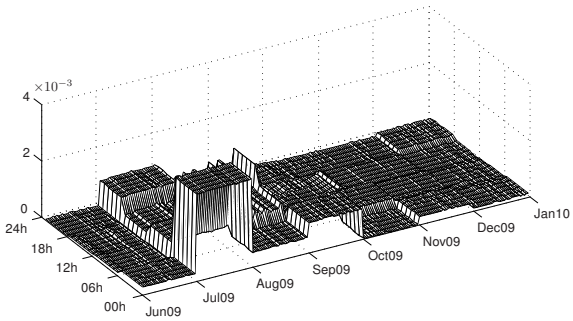
LAVFA



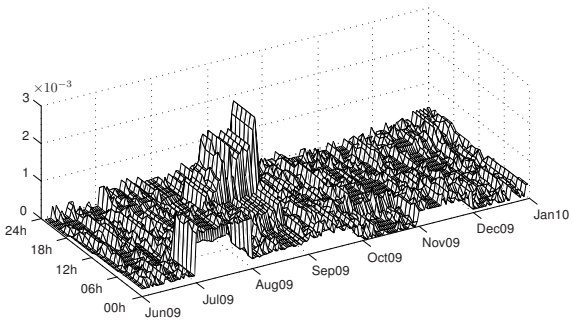
LFASN



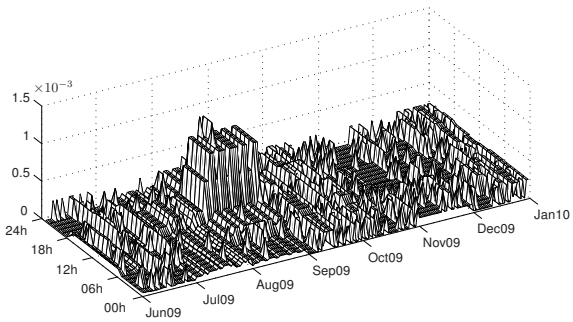
LBLRJ



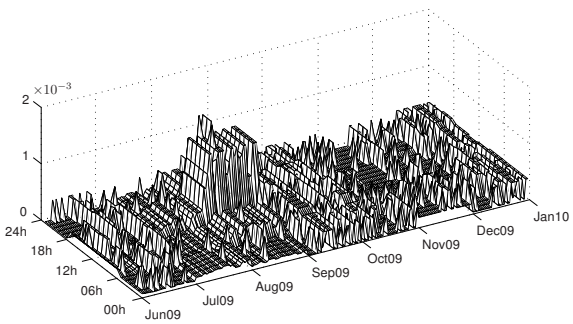
LBLPI



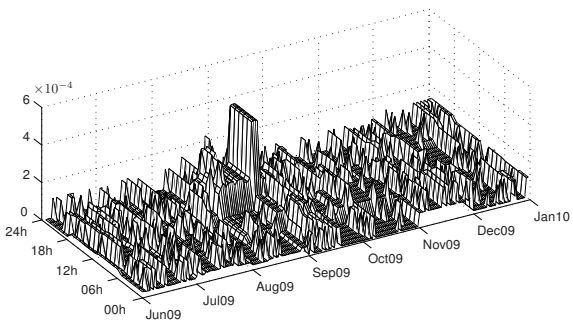
LFRCLL



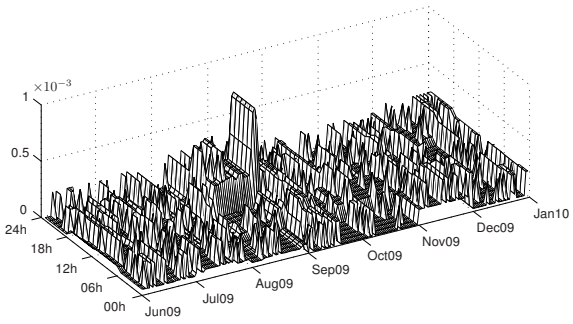
LPGFR



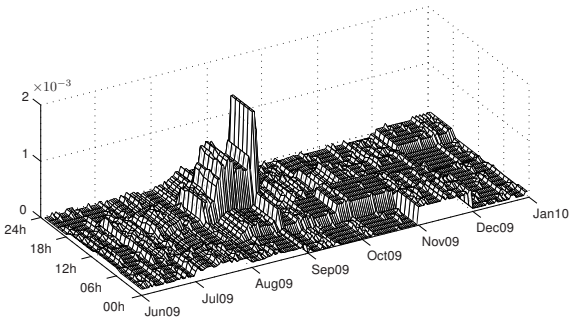
LPDVRA



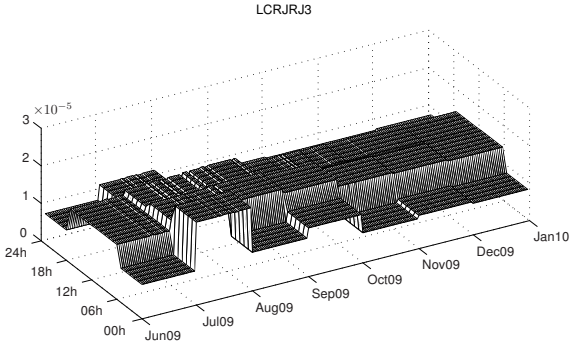
LALPDV



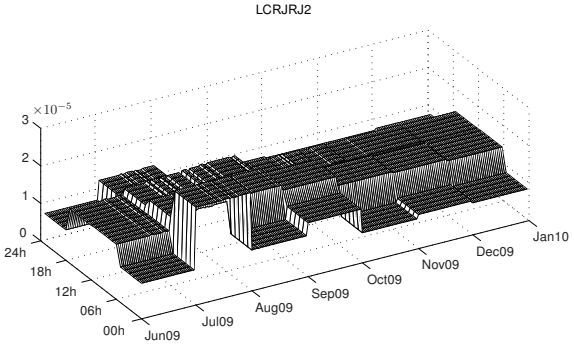
LRRPI



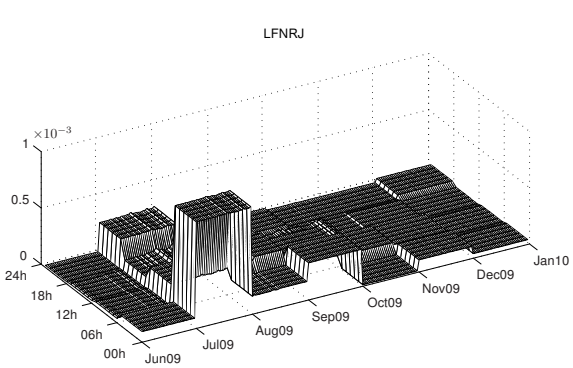
LCRJRJ3



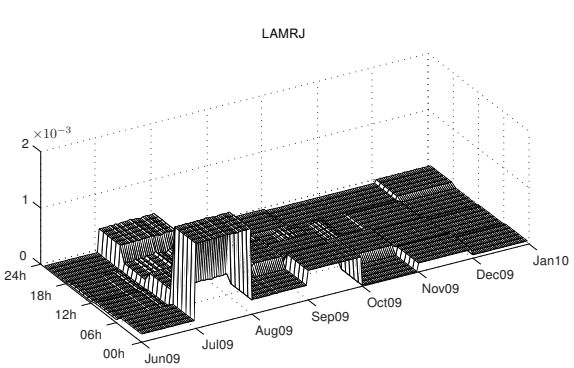
LCRJRJ2



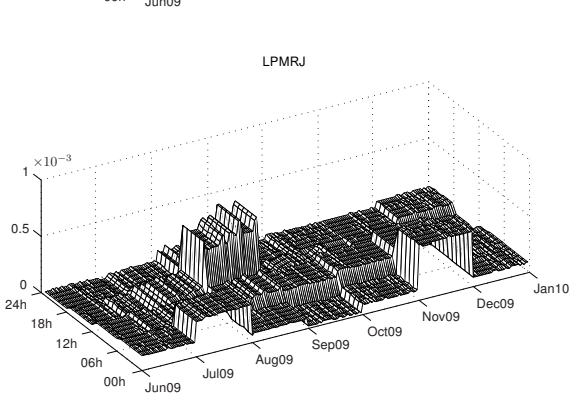
LFNRJ



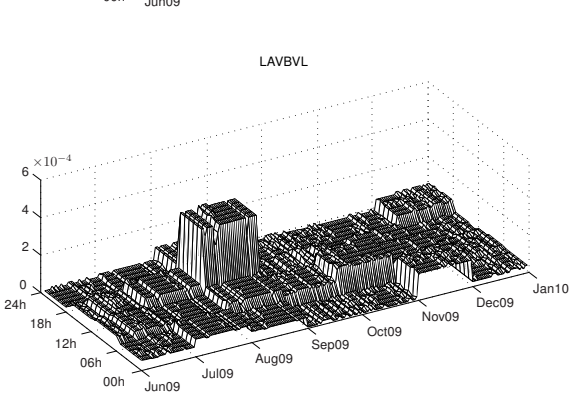
LAMRJ



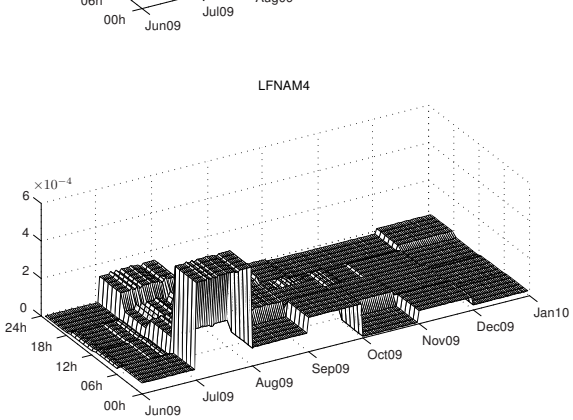
LPMRJ



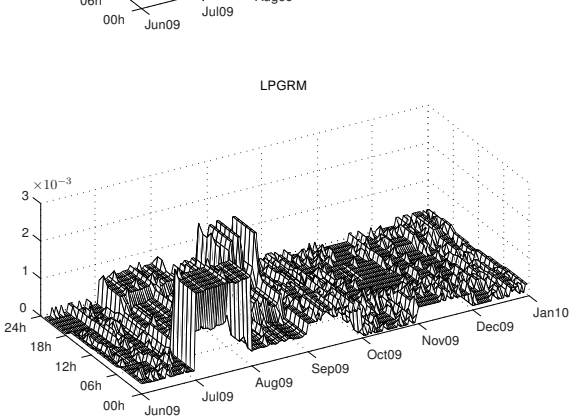
LAVBVL



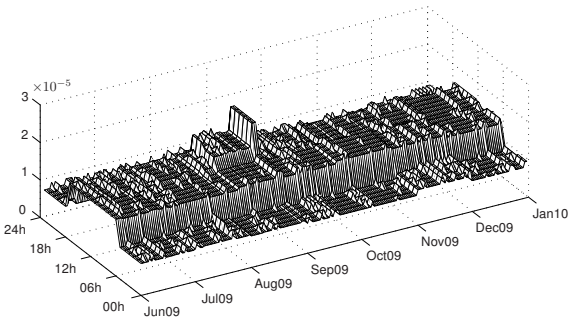
LFNAM4



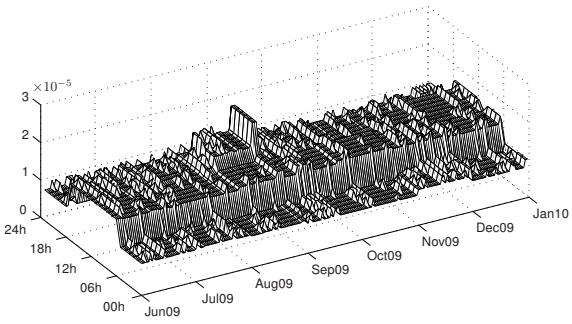
LPGRM



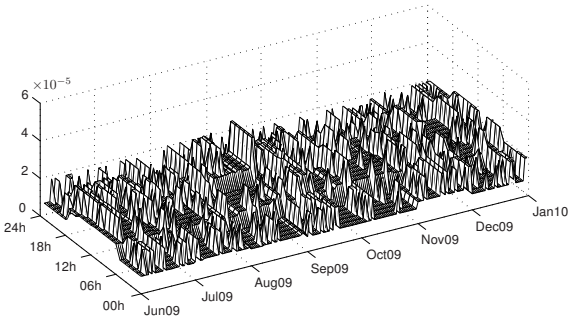
LCALAL2



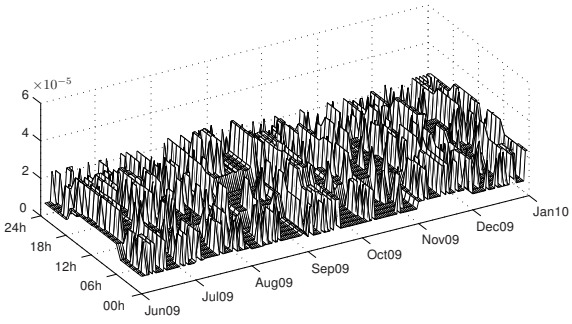
LCALAL1



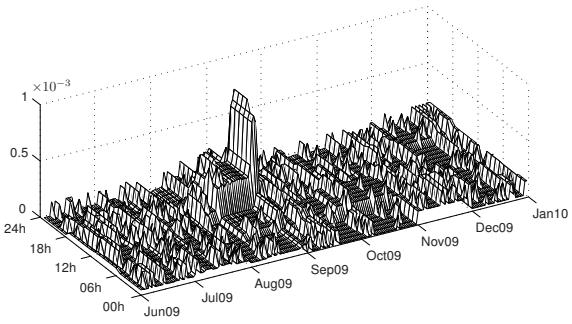
LALCTL2



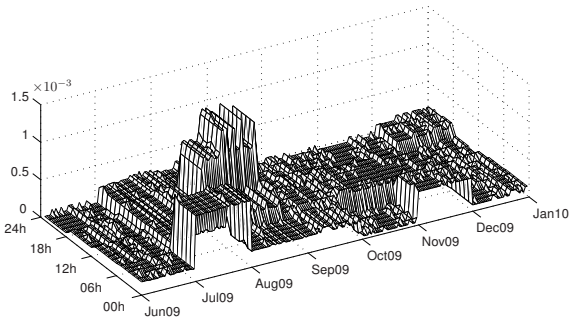
LALCTL1



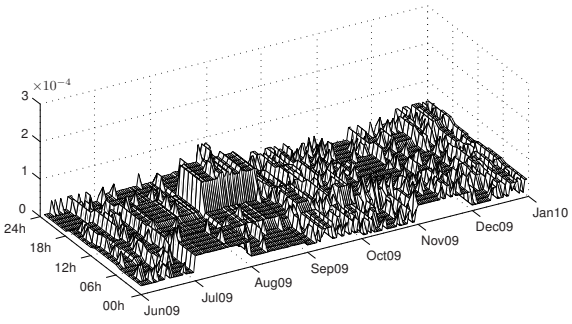
LRARR2



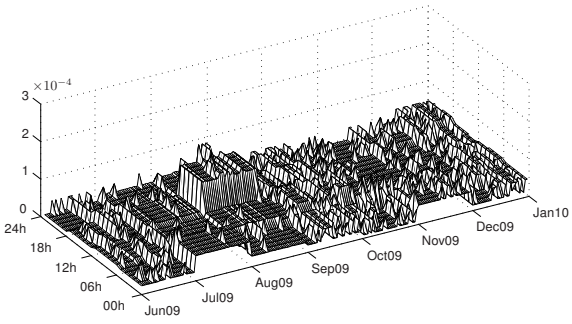
LPMSN3



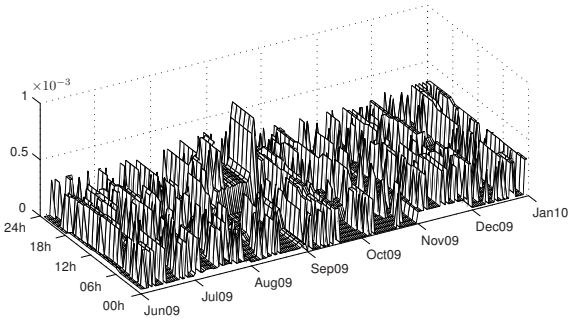
LCSNSN4



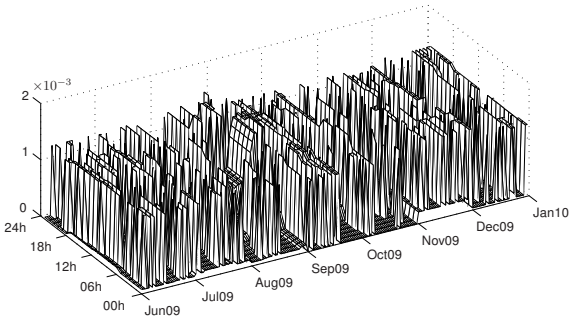
LCSNSN3



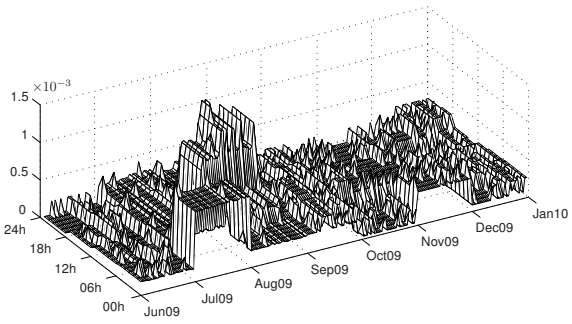
LRARR1



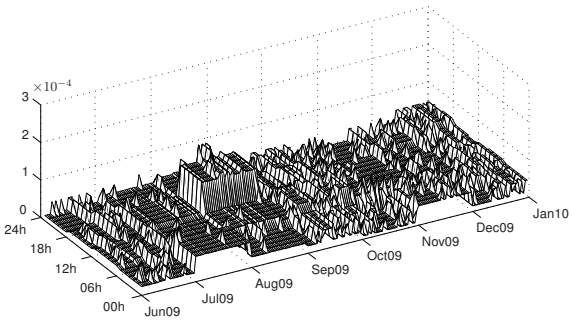
LALRA2



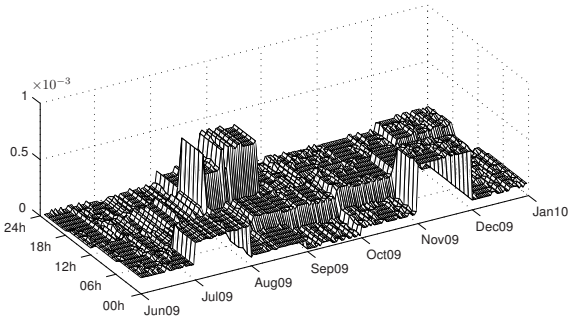
LPMSN2



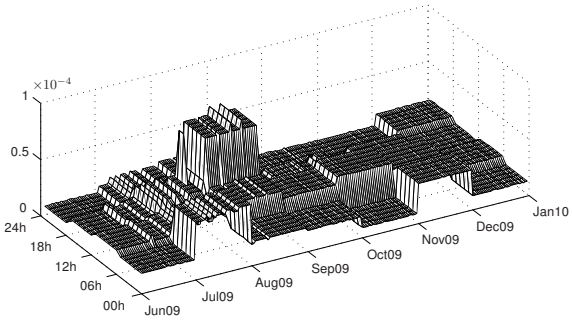
LCSNSN2



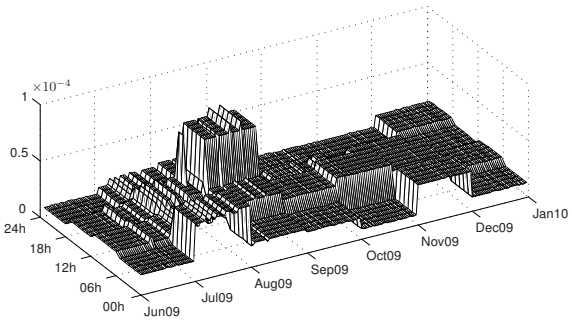
LPMFN



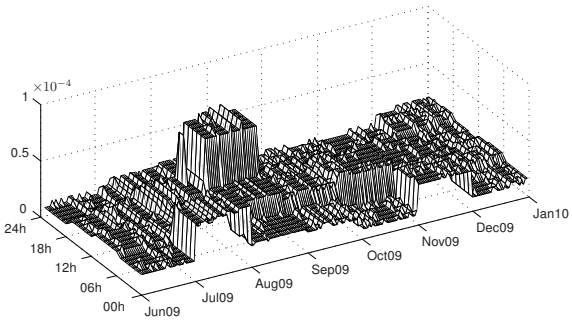
LCSBPM4



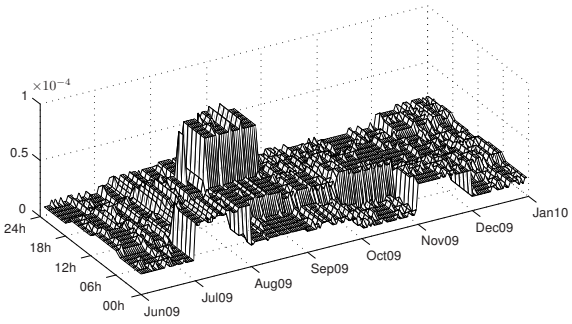
LCSBPM3



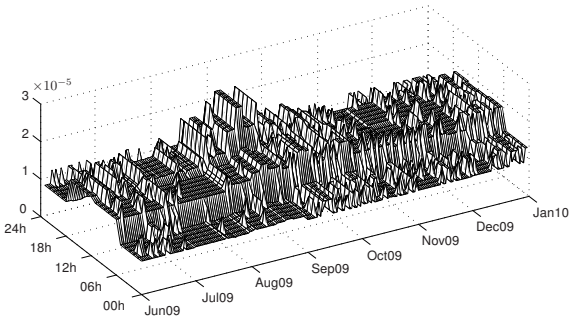
LCSBPM2



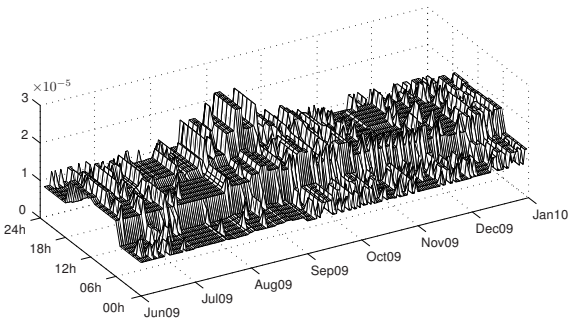
LCSBPM1



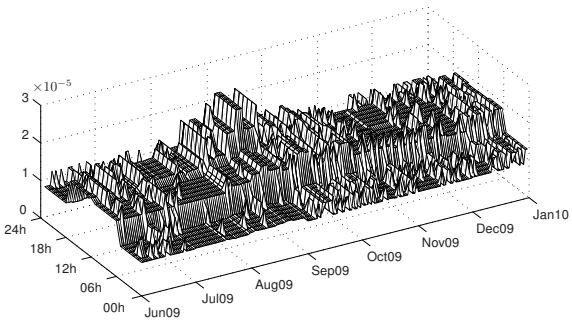
LCBZR3



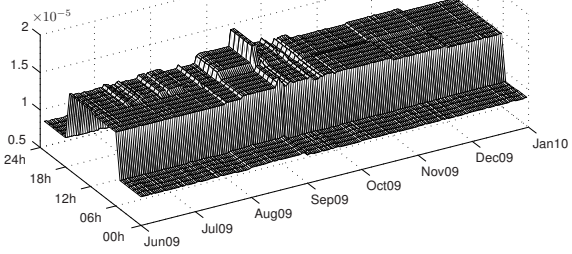
LCBZR2



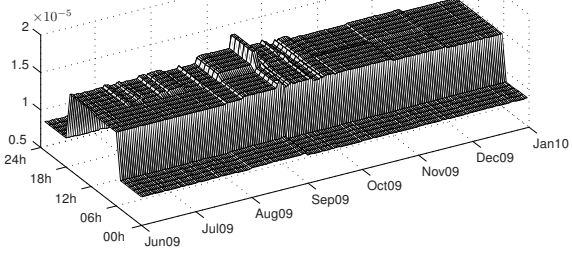
LCBZR1



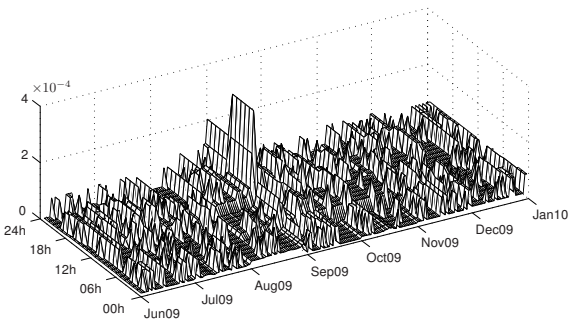
LCTRTR1



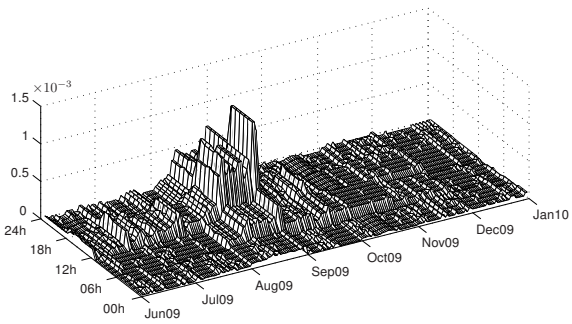
LCTRTR2



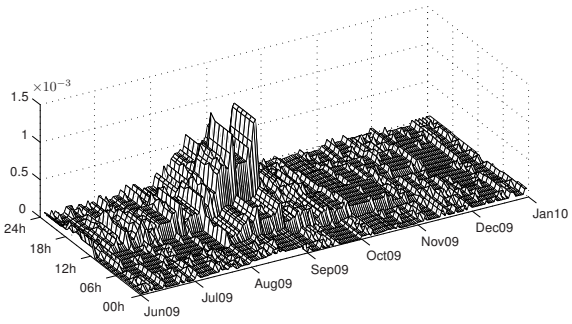
LRRVM1



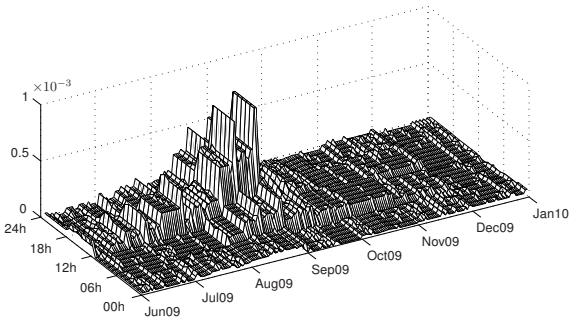
LBAPI



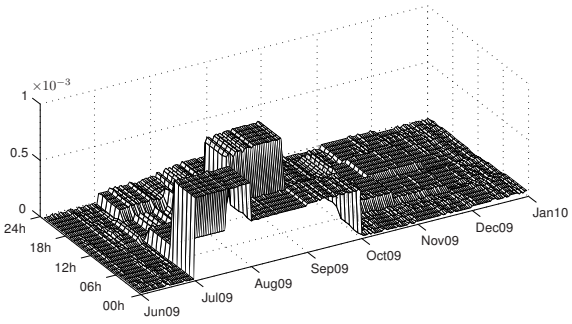
LBAVG



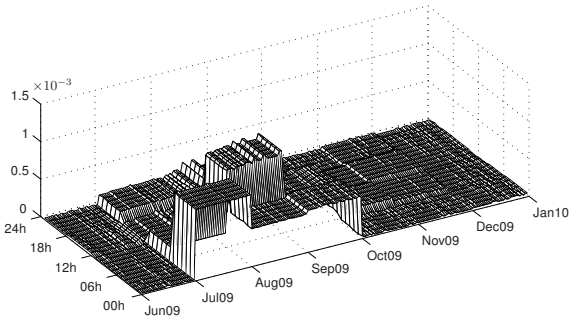
LVPAVG



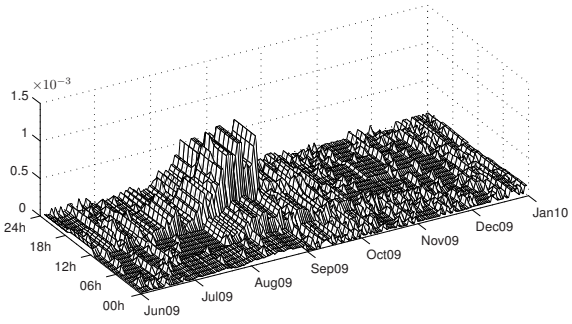
LCVRTJ



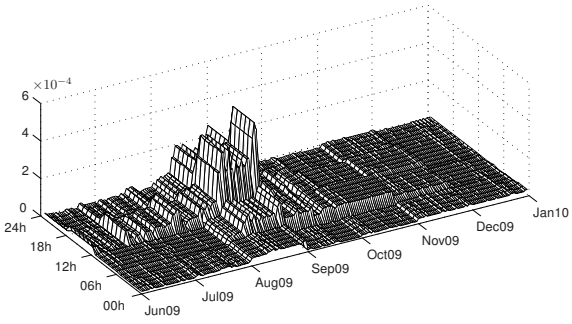
LRMCVR



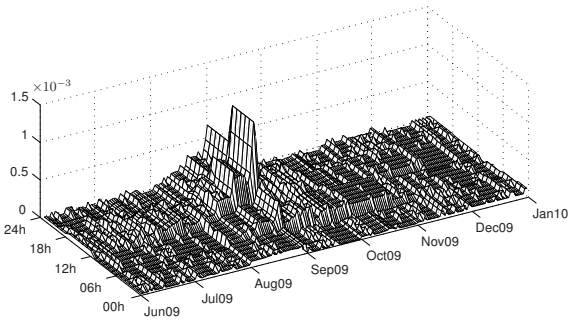
LPNLZR



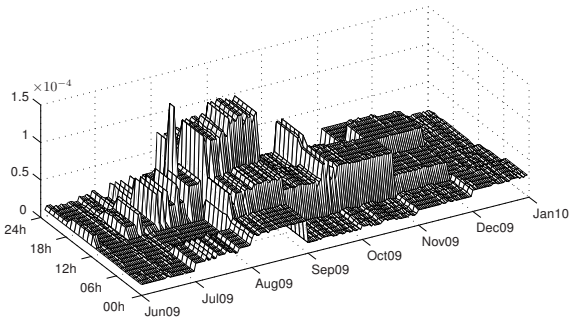
LPRPNL



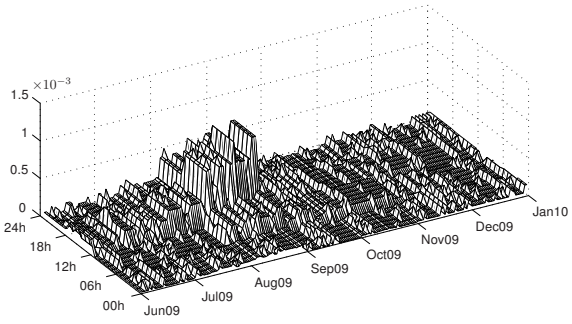
LVGVM4



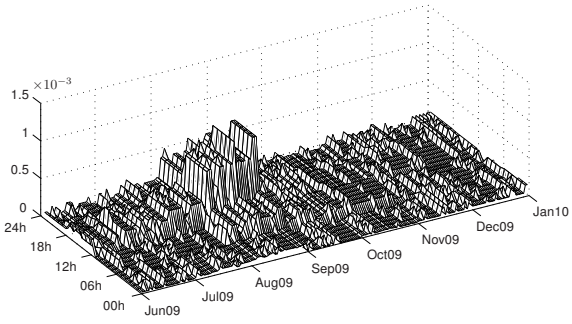
LFNTJ



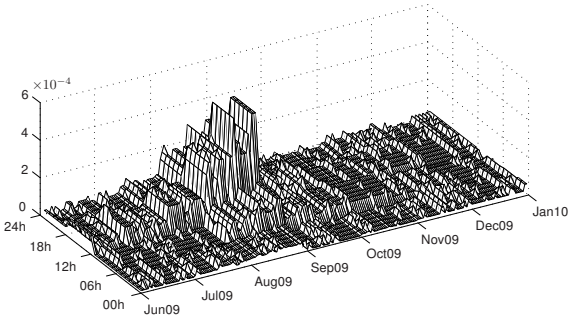
LCCFE2/FTL



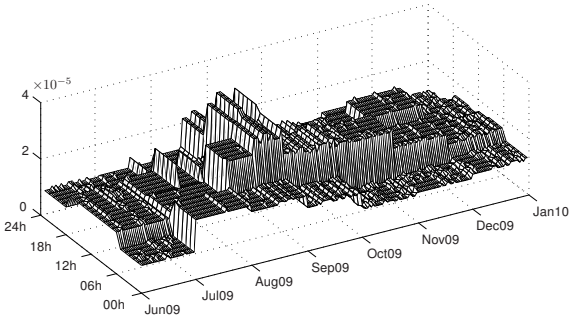
LCCFE1/FTL



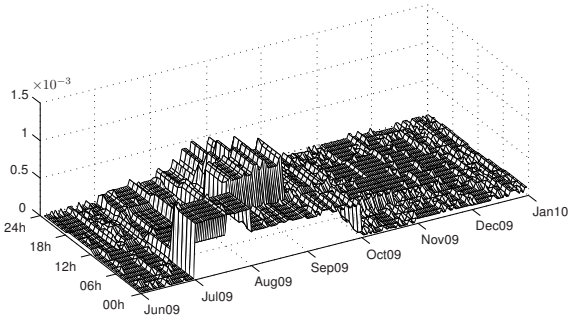
LNCFE



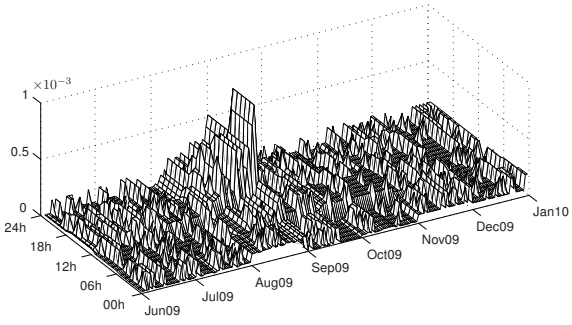
LAMSS



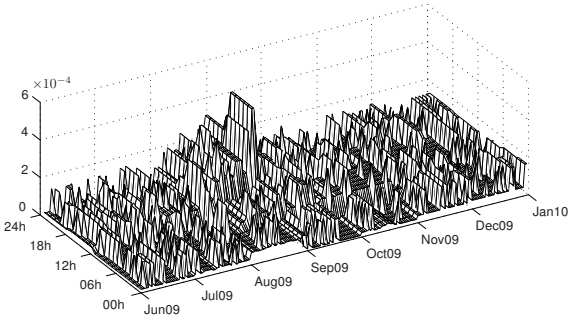
LSRZR



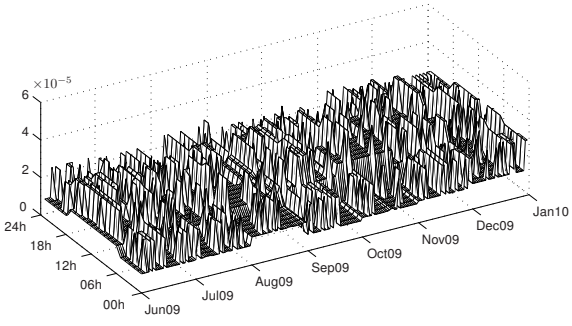
LPIPR/MR



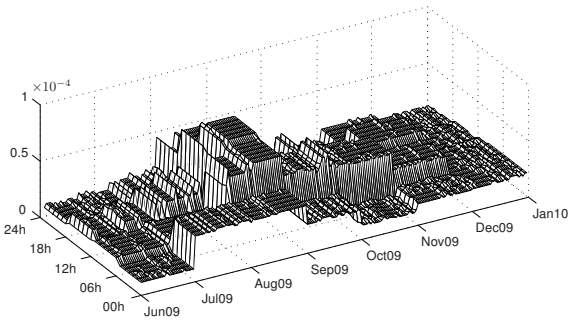
LEJPI



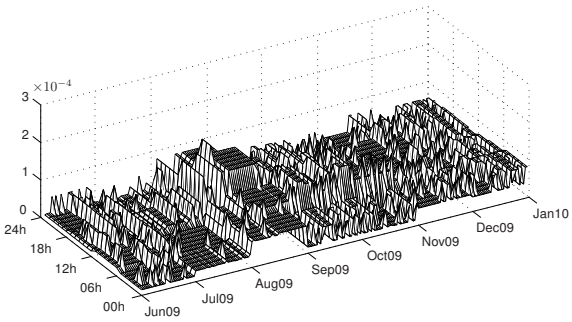
LVMCT2



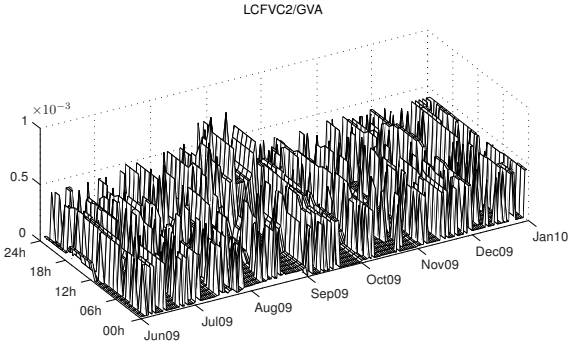
LFNSV2



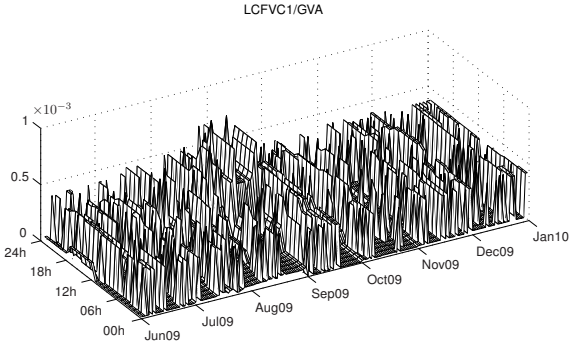
LCGSV



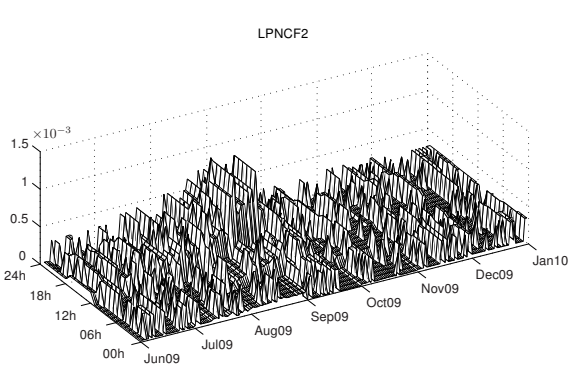
LCFVC2/GVA



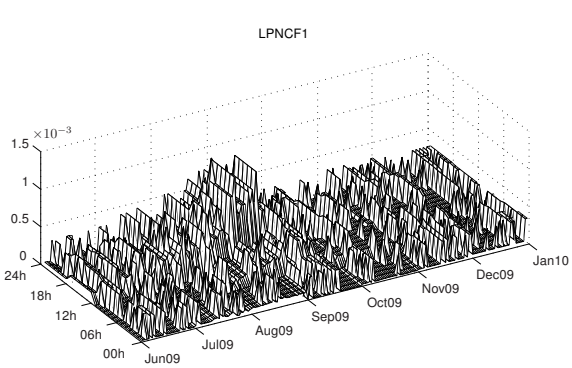
LCFVC1/GVA



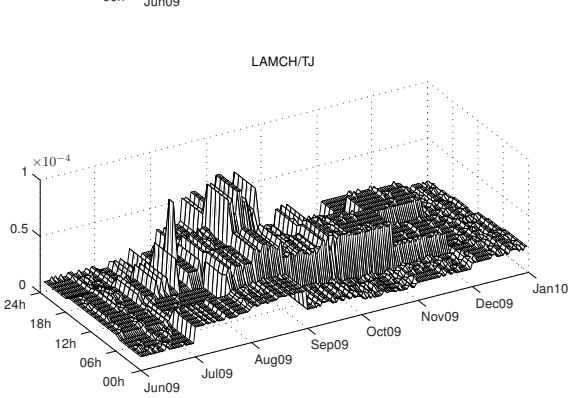
LPNCF2



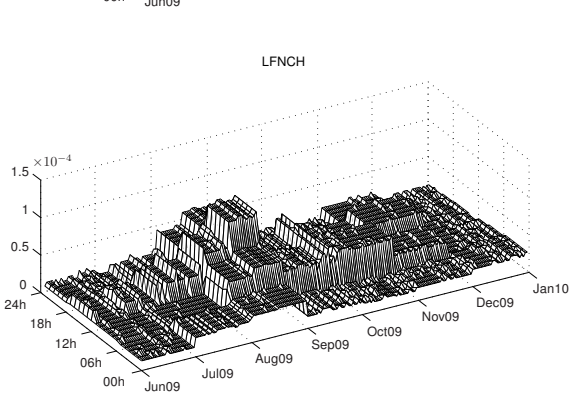
LPNCF1



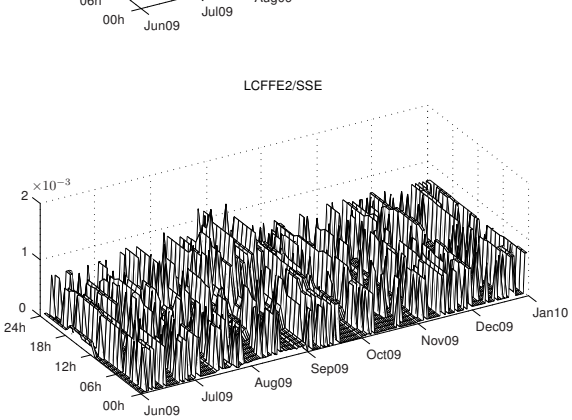
LAMCH/TJ



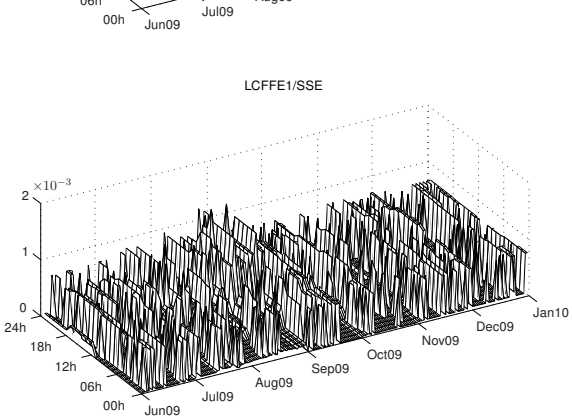
LFNCH



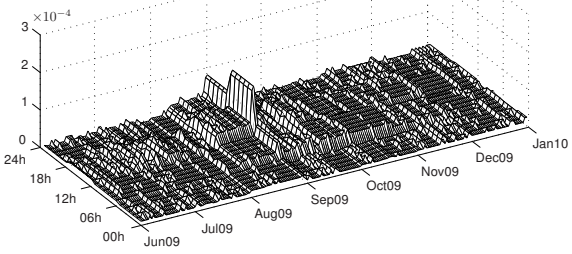
LCFFE2/SSE



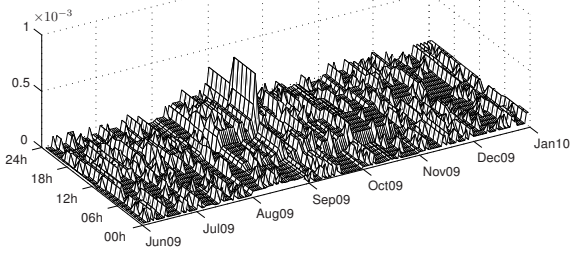
LCFFE1/SSE



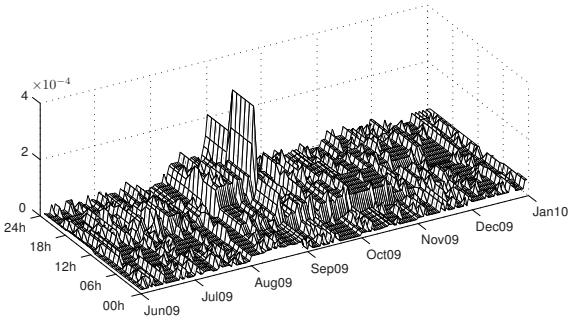
LTGRR



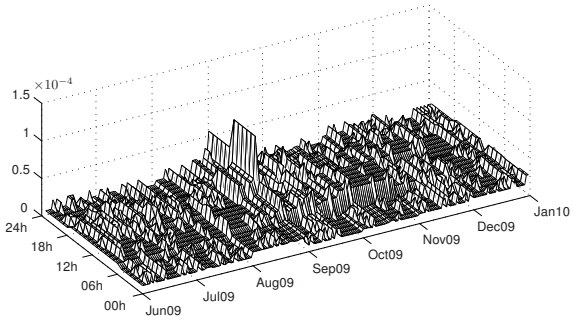
LTGCN/EJ



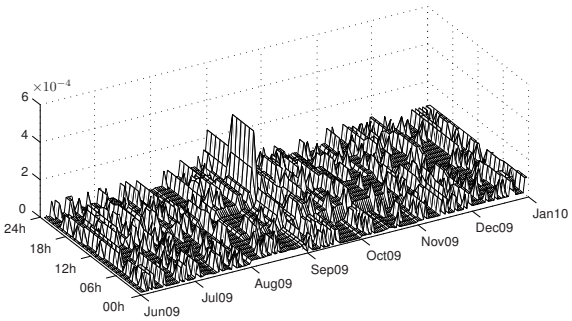
LRRCN3/TG



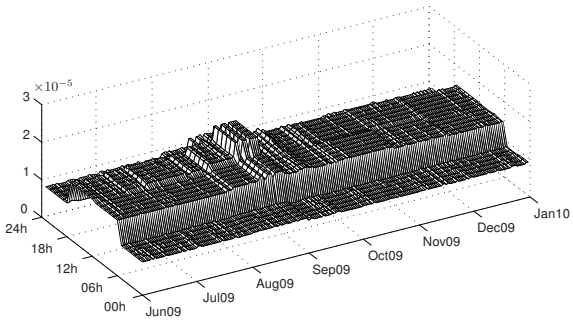
LVMCT1



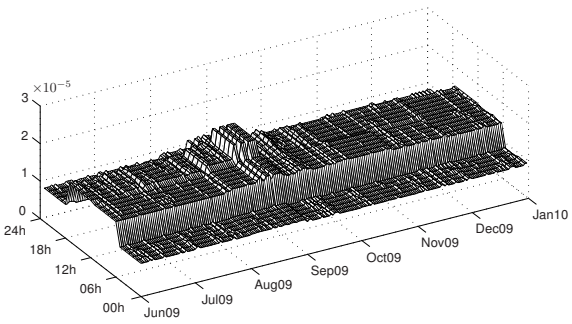
LRRCT



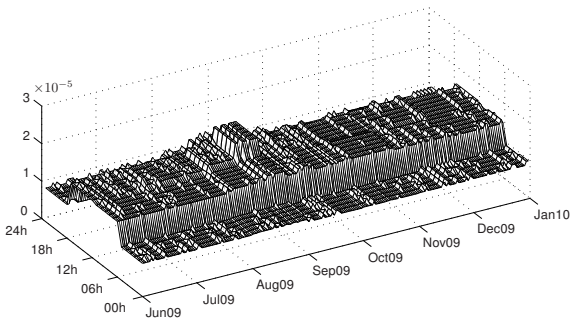
LCPTPT3



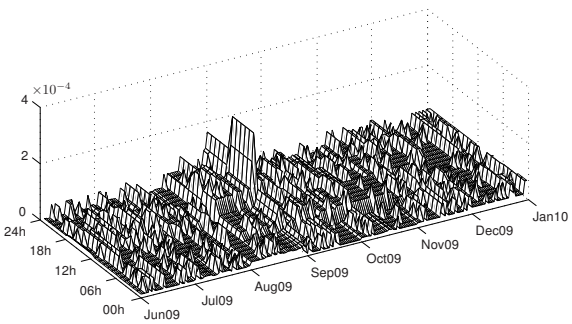
LCPTPT2



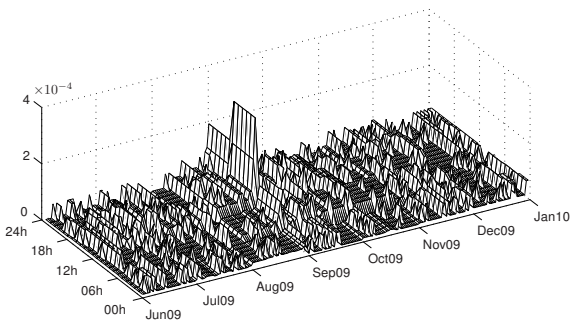
LCPTPT1



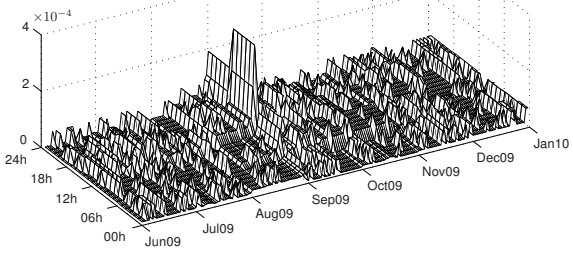
LRRCN1



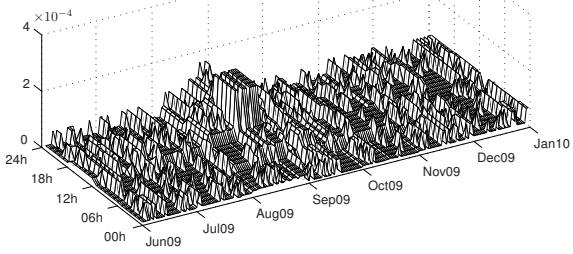
LRRVM3



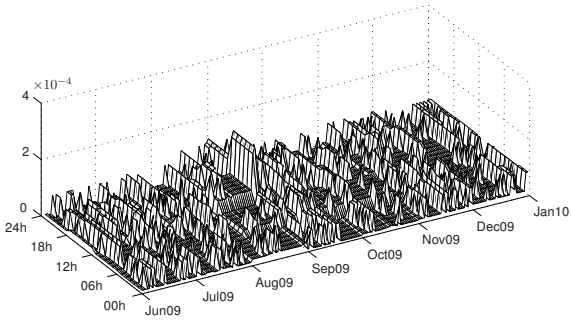
LRRVM2



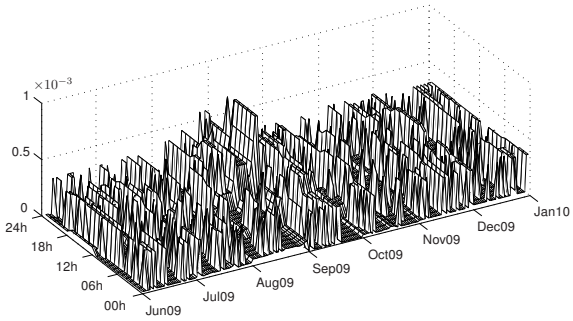
LMDPT2



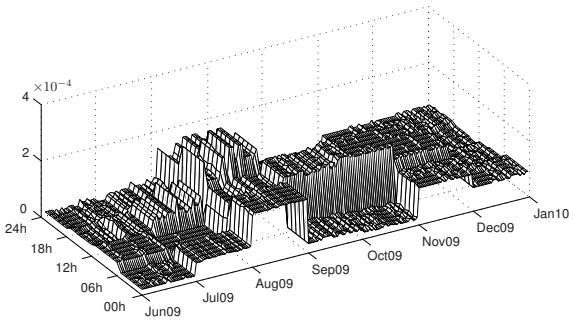
LRRUR



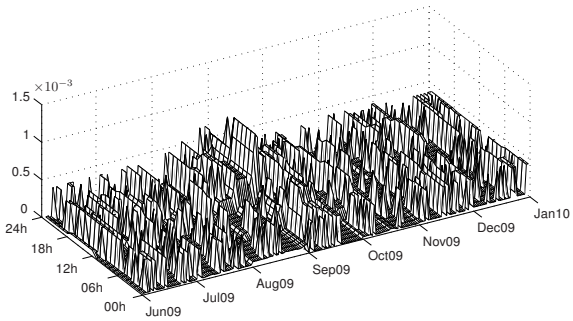
LVGUR



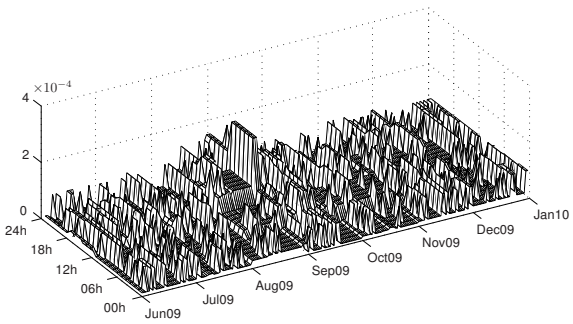
LCGSXL



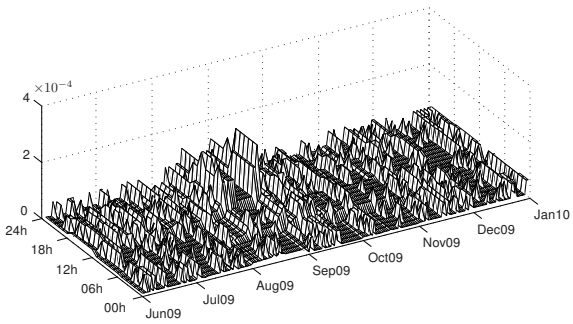
LVGRR1



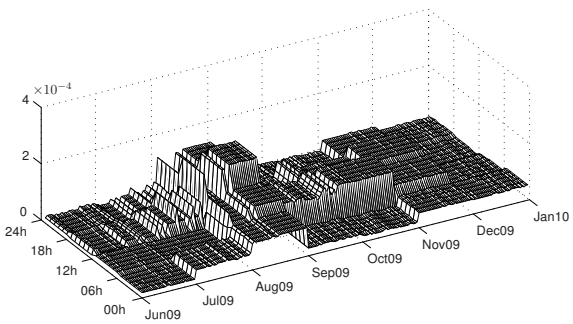
LTRRR



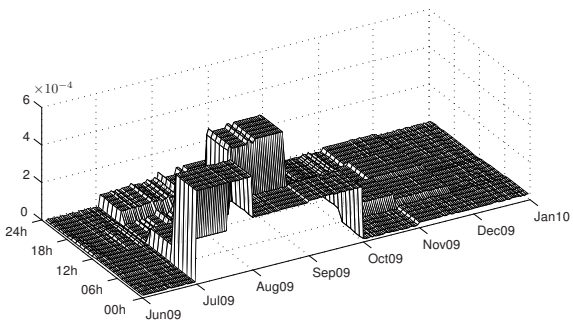
LCLTR



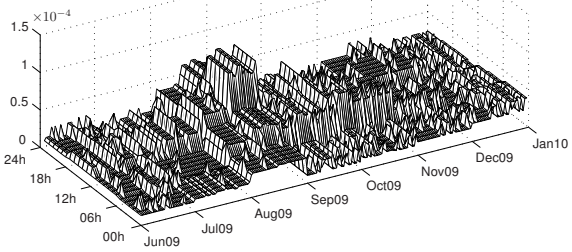
LCGCH/SV



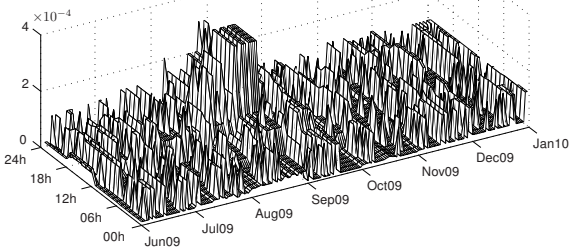
LCGFN2



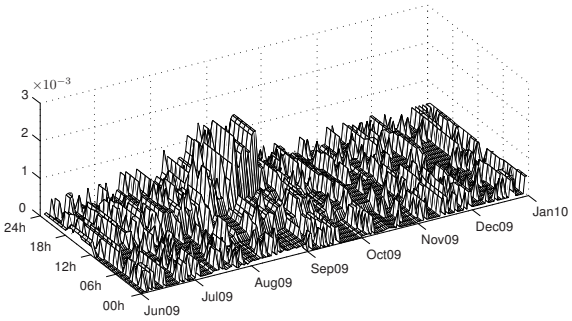
LFNAM3/CH



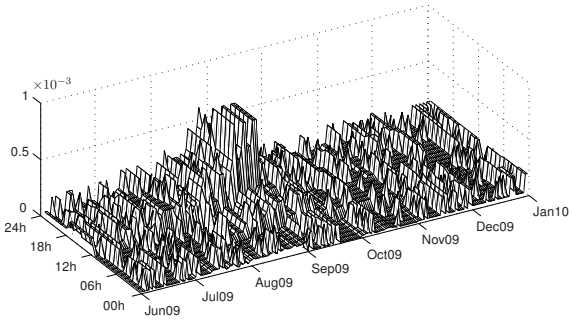
LPTMG



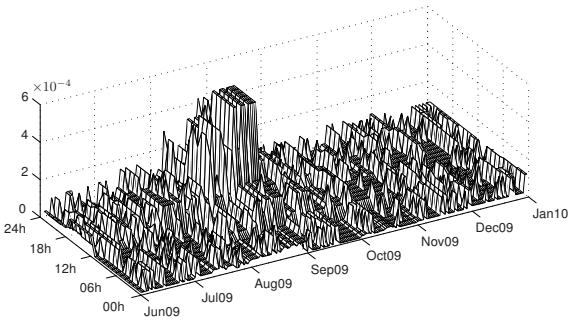
LMGVR/MCC



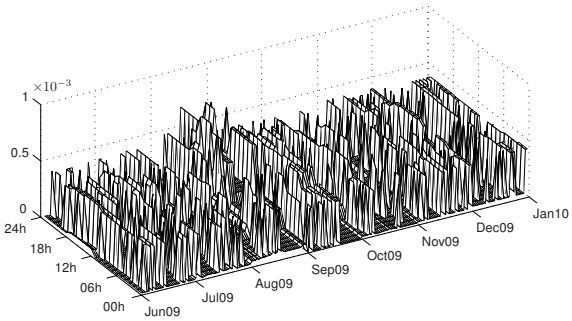
LPNAAV



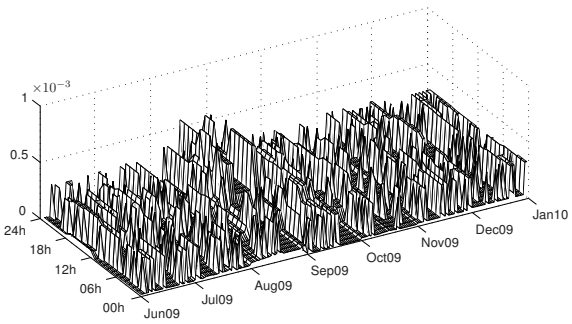
LBTAAV



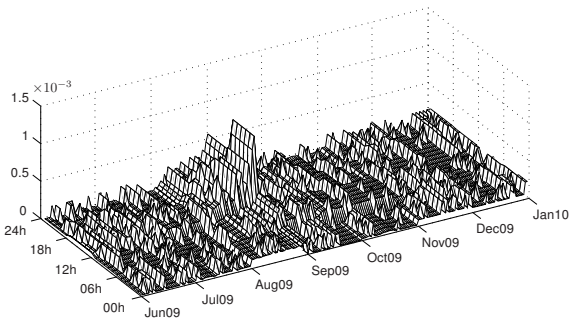
LCLEJ2



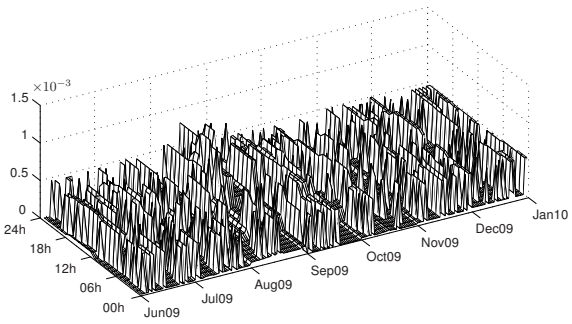
LCLEJ1



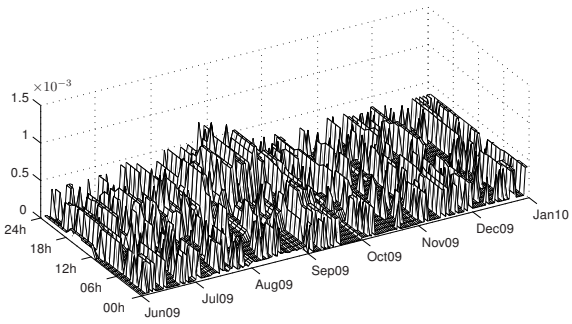
LMCPR1



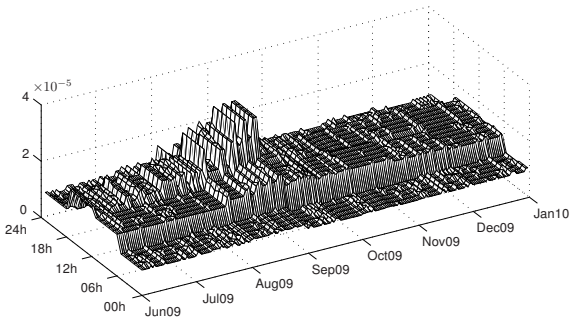
LCLMC



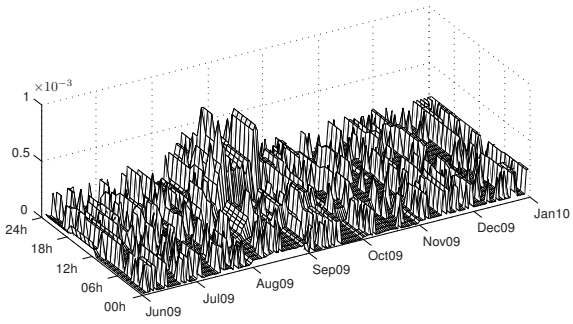
LPNVG2



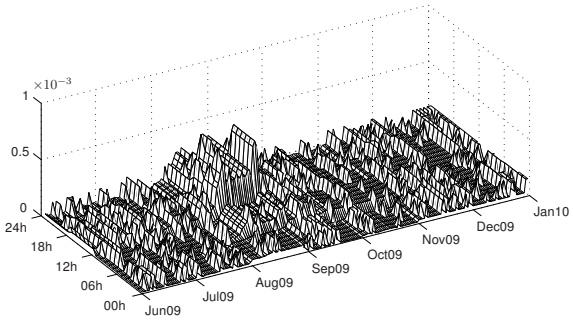
LCPNPN



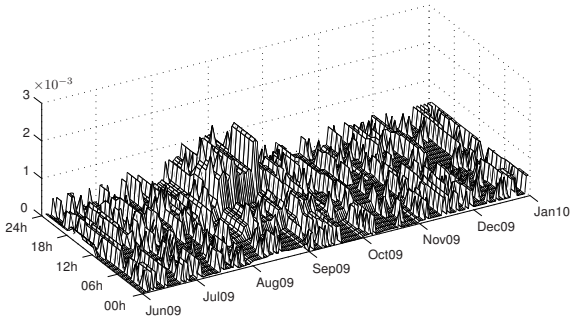
LAGPR2/MRT



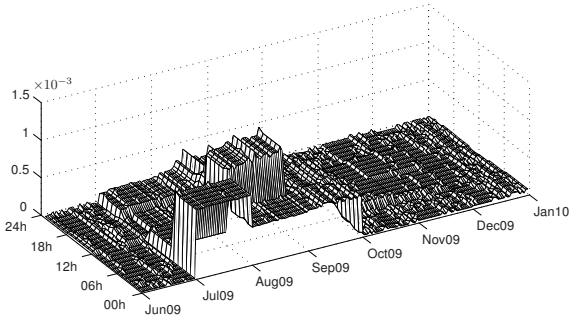
LAGPR1



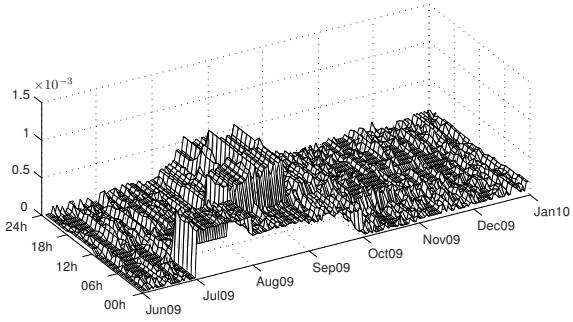
LVCPR2/PP



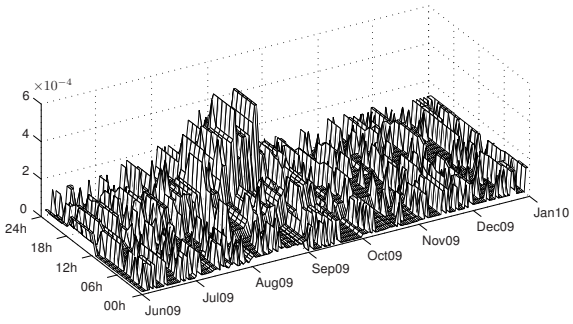
LBLRM2



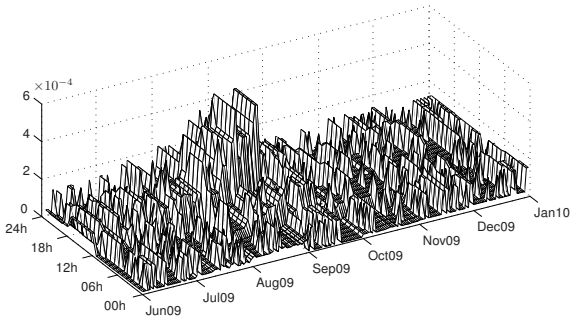
LPRBL2/PB



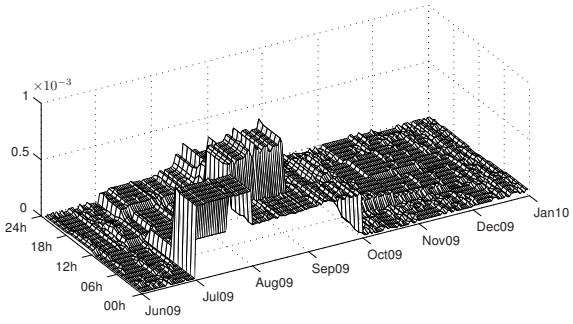
LVRVG2



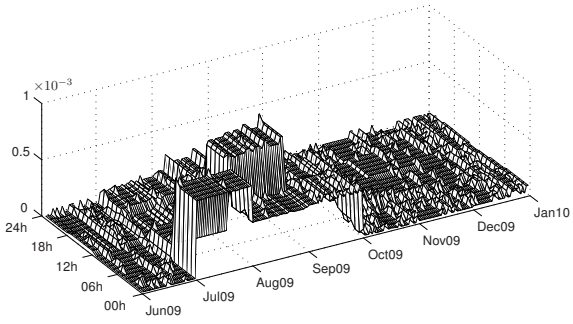
LVRVG1



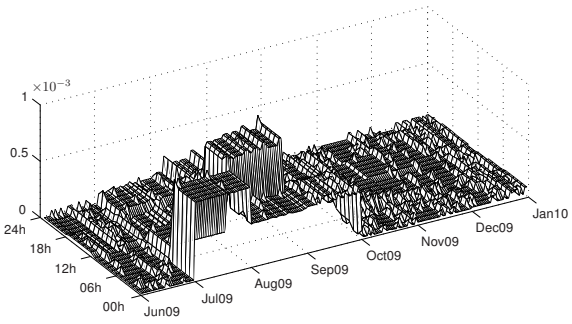
LBLRM1



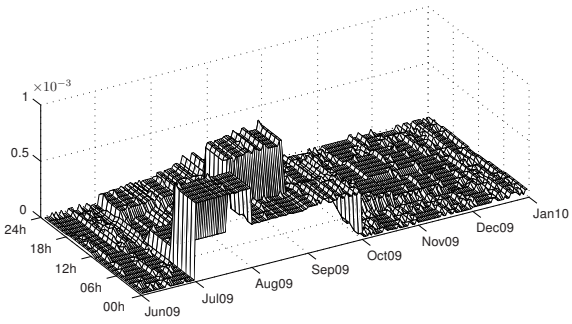
LCGRM3



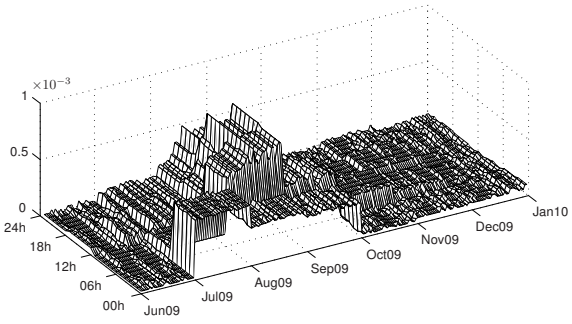
LCGRM2



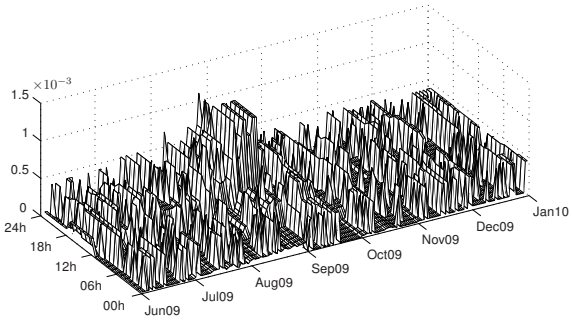
LCGRM1



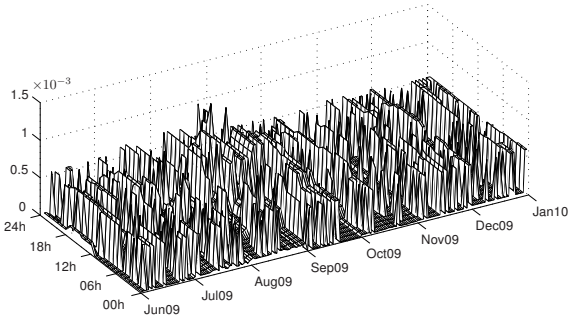
LPRBL1



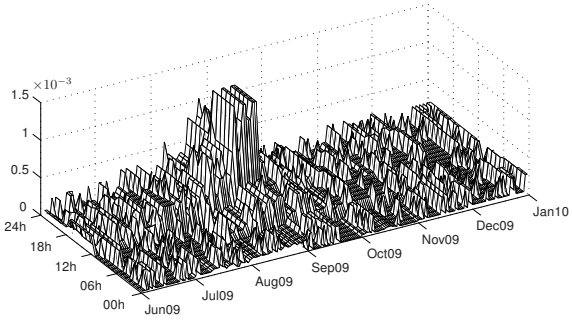
LBTPN



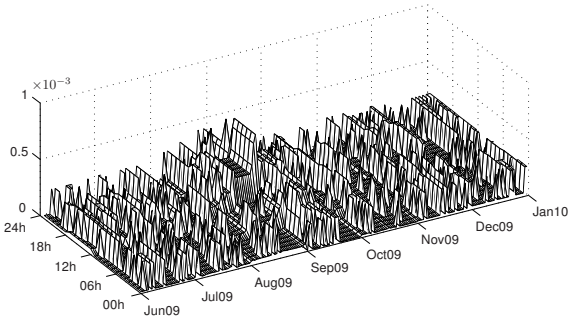
LPNVG1



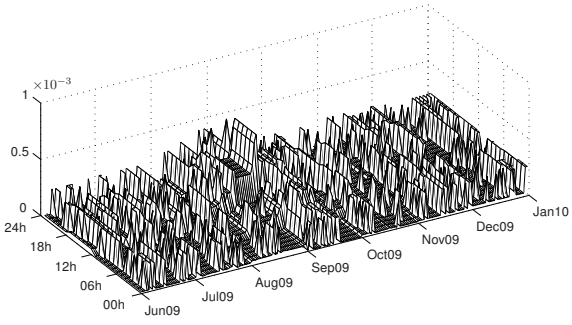
LPTPN



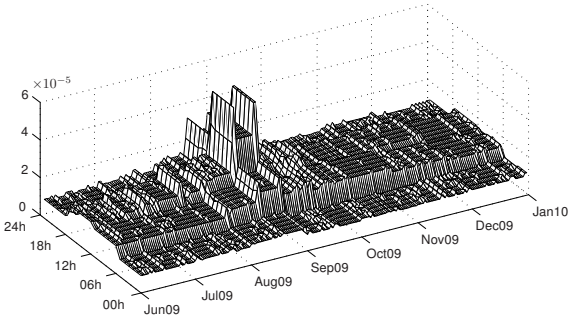
LVGCL3



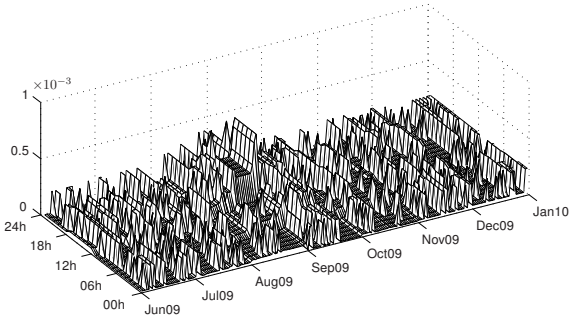
LVGCL2



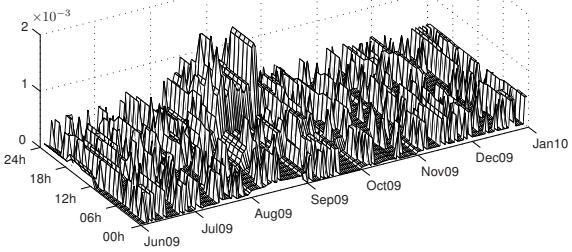
LRGVG



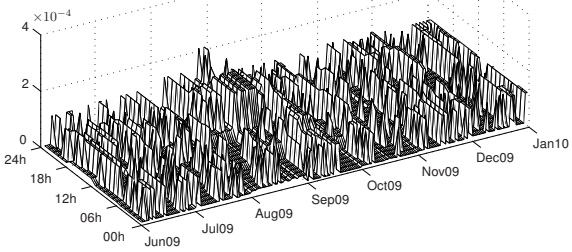
LVGCL1



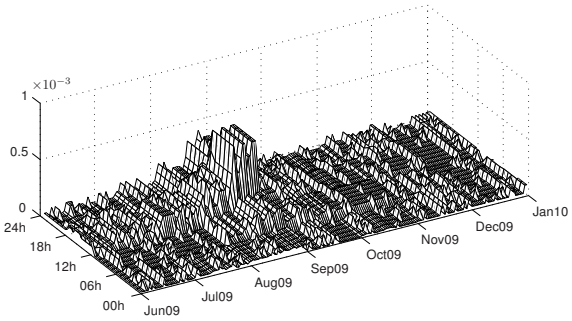
LVCPR1/MRT



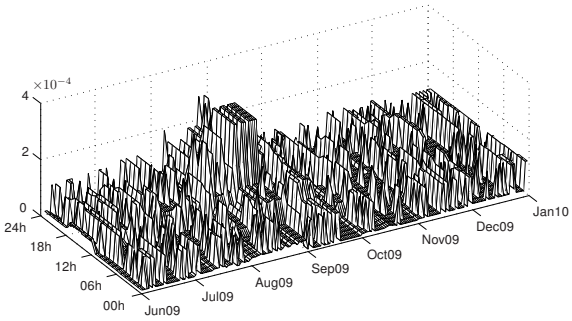
LMDPT1



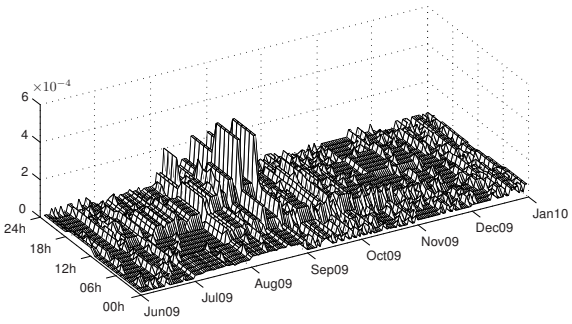
LPNSLL



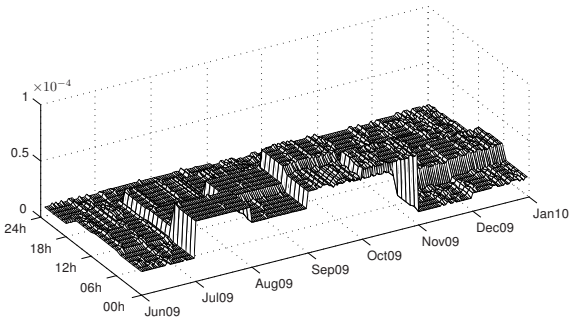
LPTBT



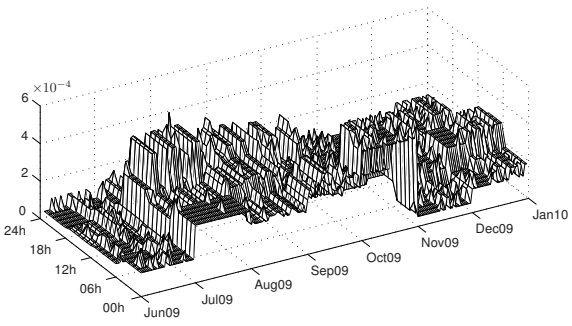
LCGSR



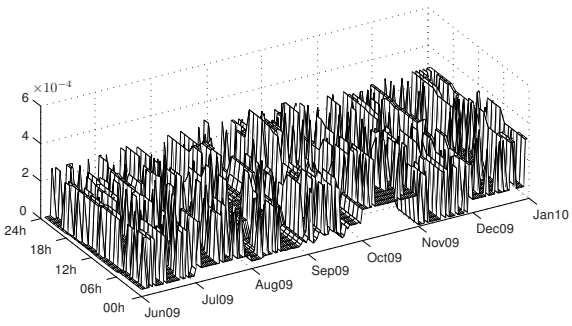
LSNGP



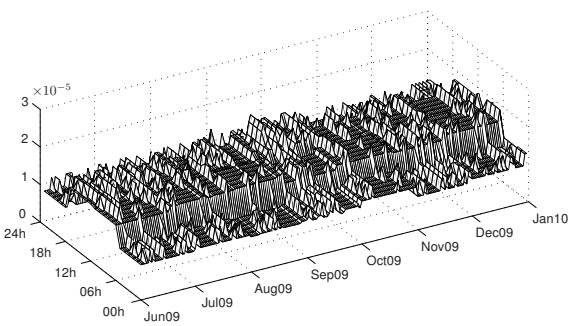
LSNPO3



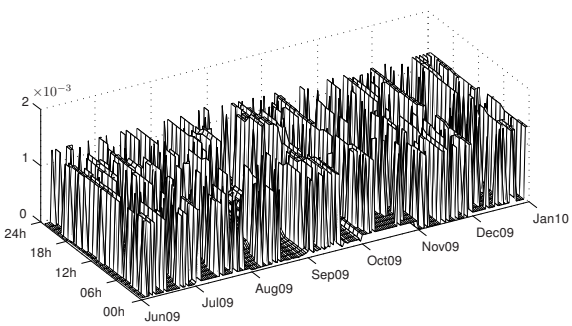
LMDRPDV2



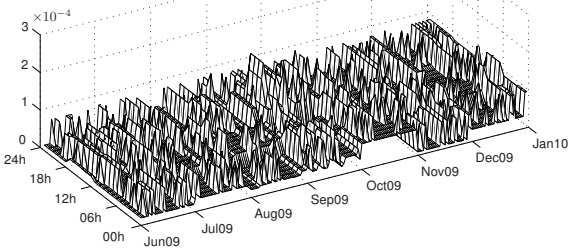
LCFDFRD



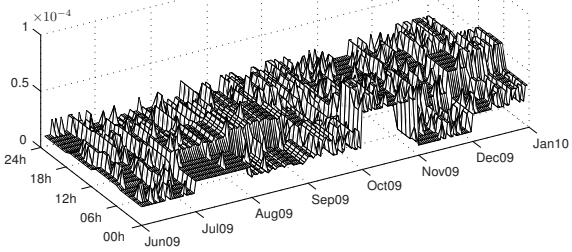
LARFRD/CV



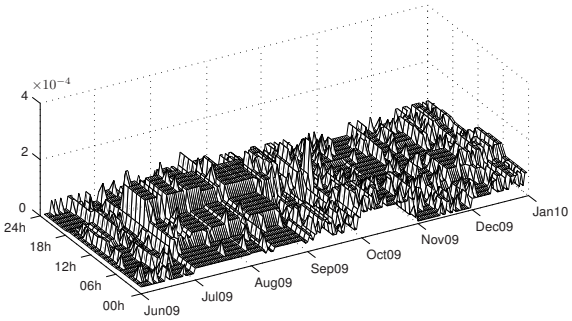
LCDFRD/PDV



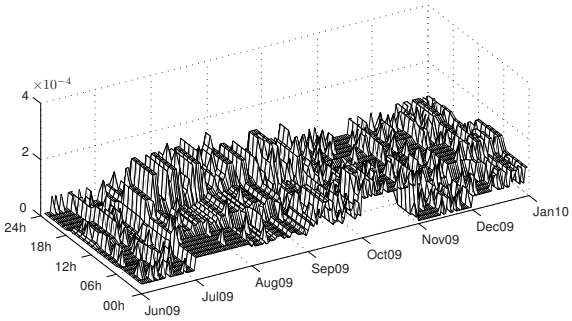
LFFTFR2



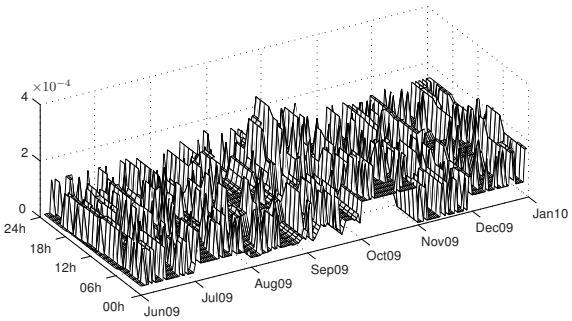
LPOTN1



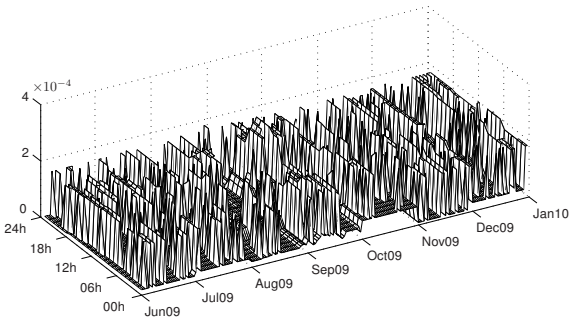
LSIPO



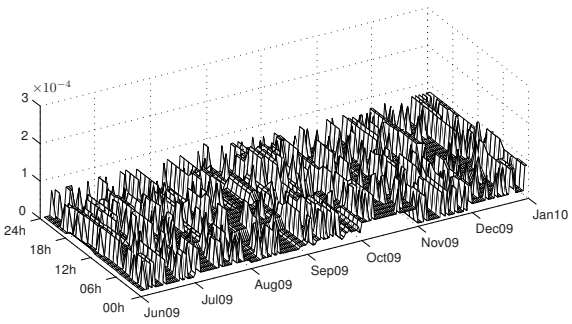
LPDVVI



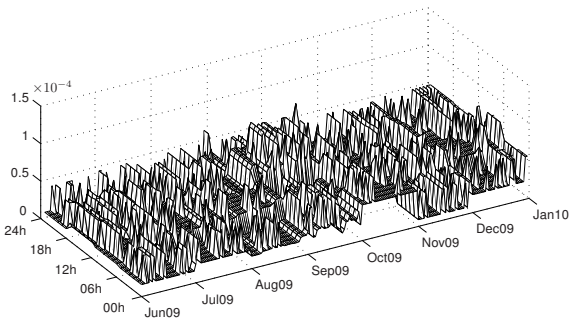
LORPDV



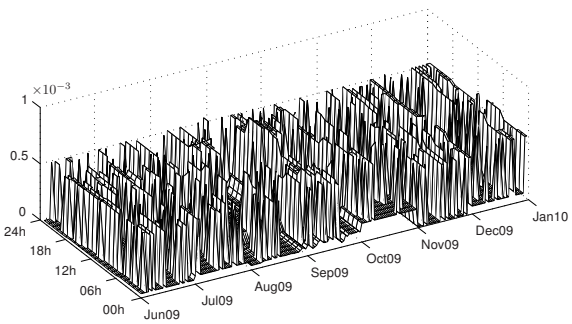
LCDPDV2



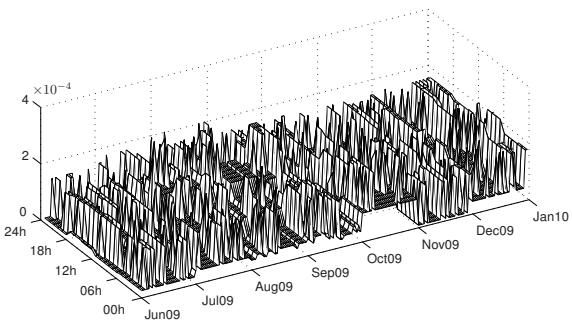
LCDPDV1



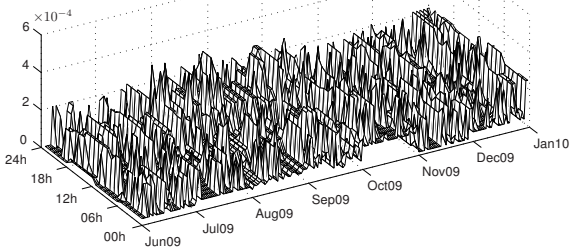
LMDRPDV1



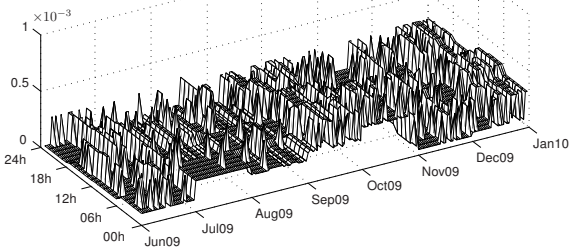
LGUCC



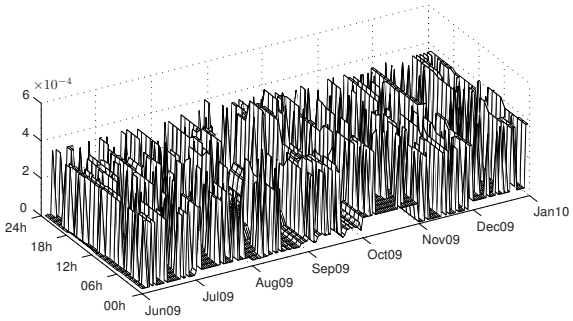
LCOSFR



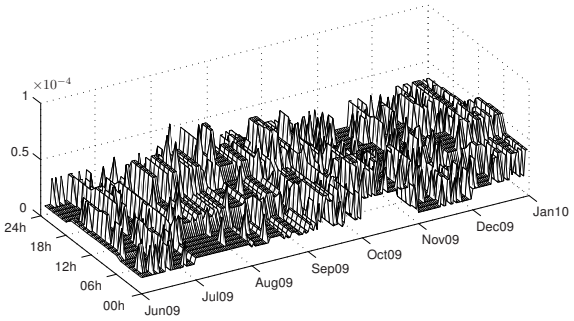
LSNSI



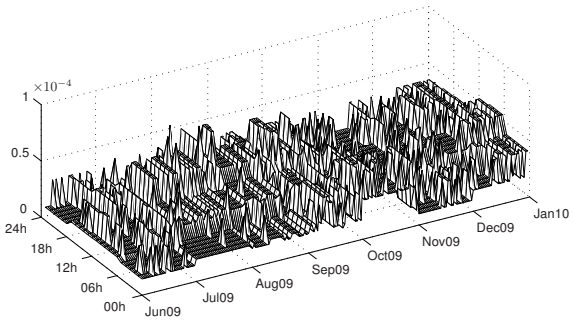
LAFRA



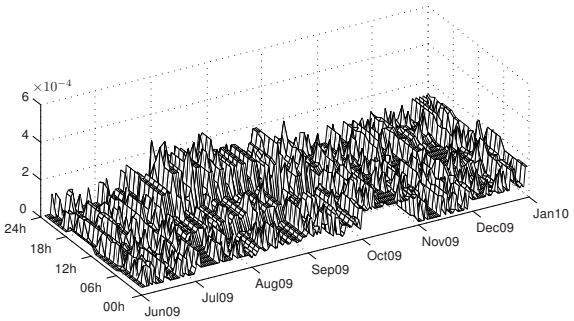
LSILZN2



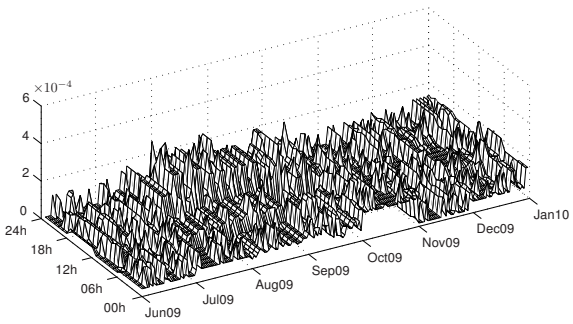
LSILZN1



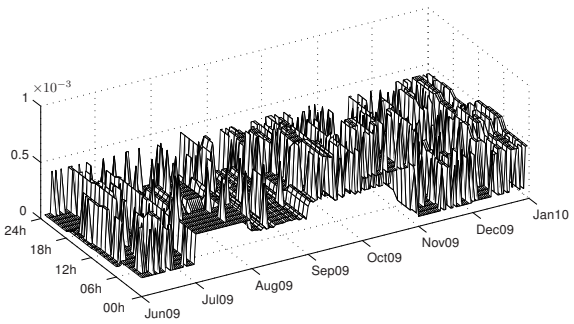
LFRCC2/RDA



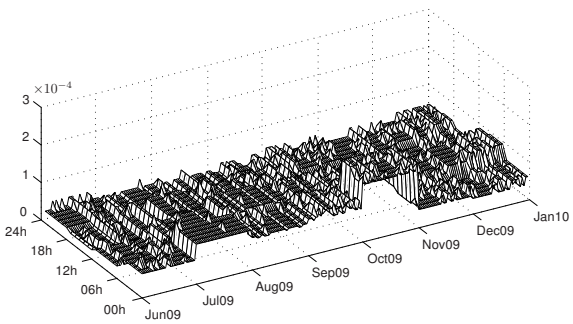
LFRCC1/RDA



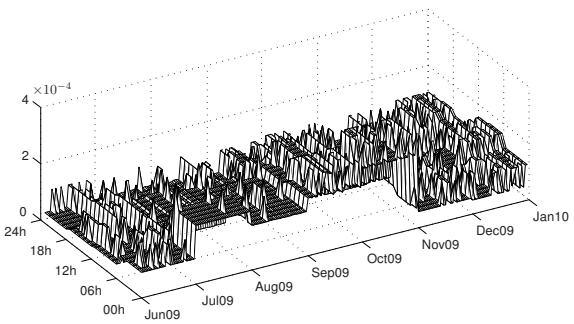
LOQET2



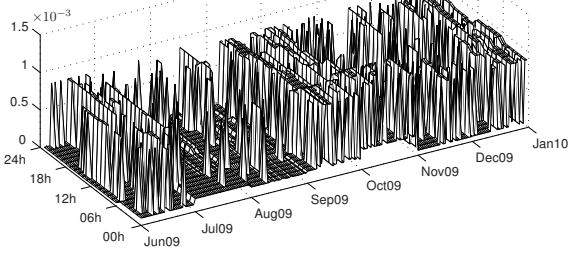
LESFA



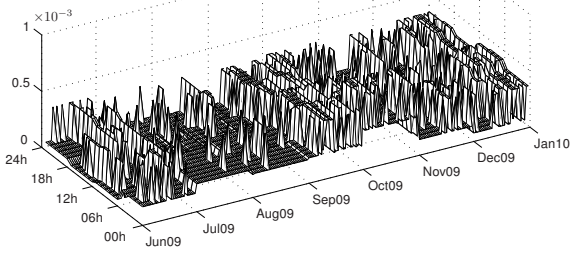
LSNES



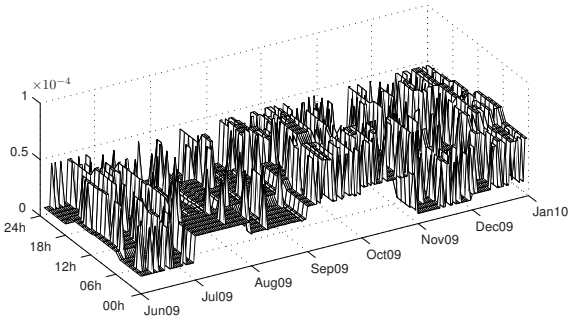
LMPSN



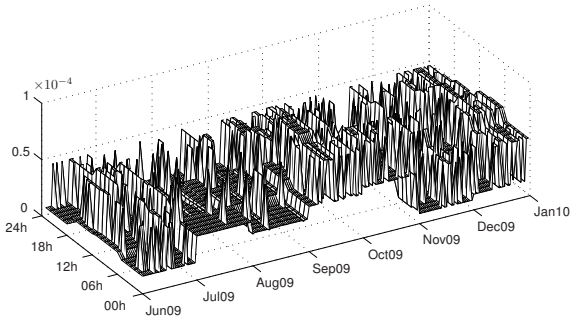
LPMMP/PGS



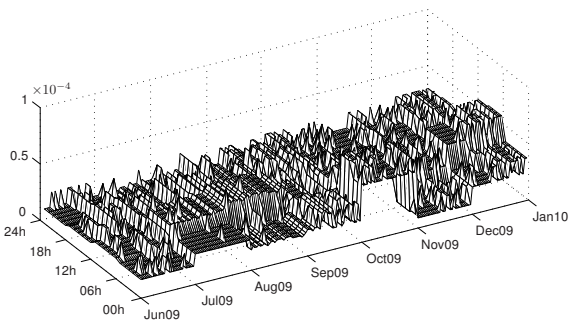
LFFFGT2



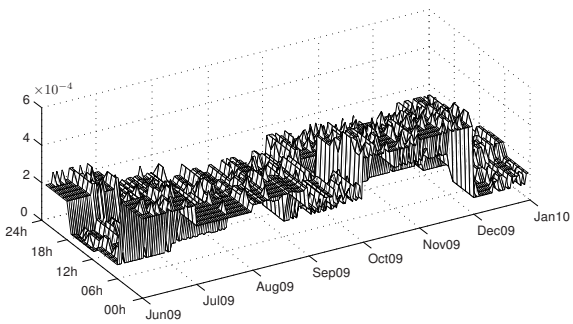
LFFFGT1



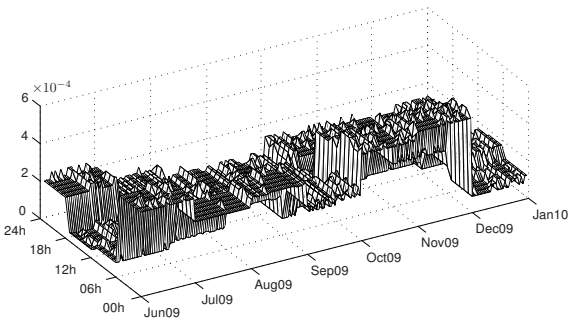
LFFTFR1



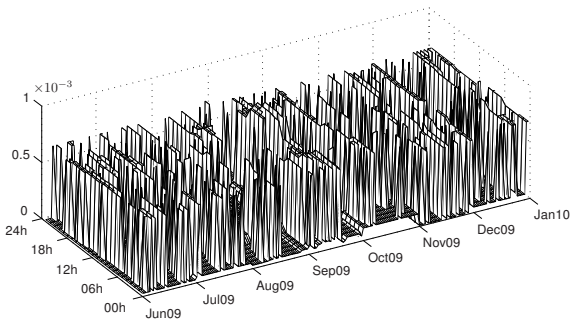
LPAQGD2



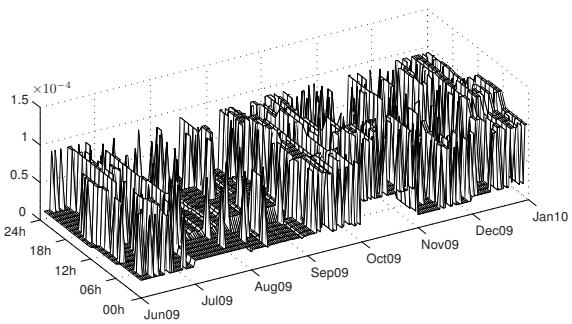
LPAQGD1



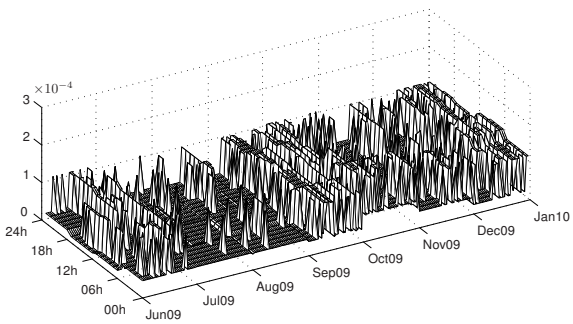
LRAOR



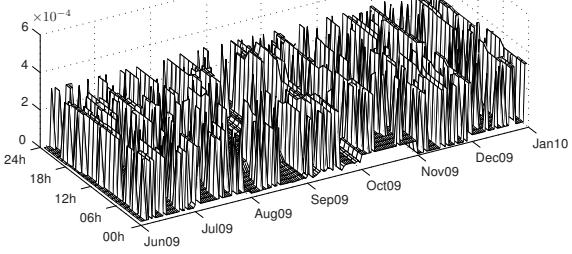
LFFQAJ



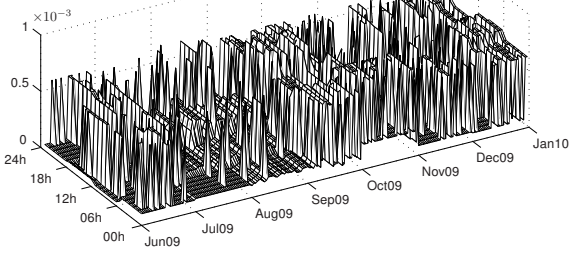
LPMQAJ



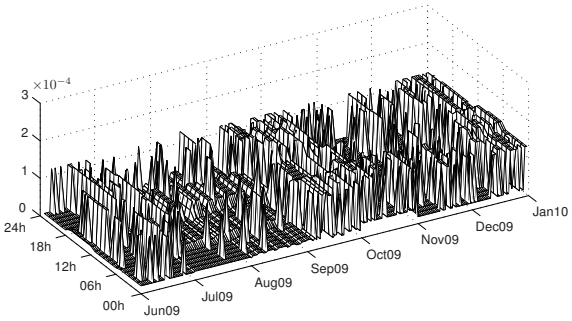
LORVI



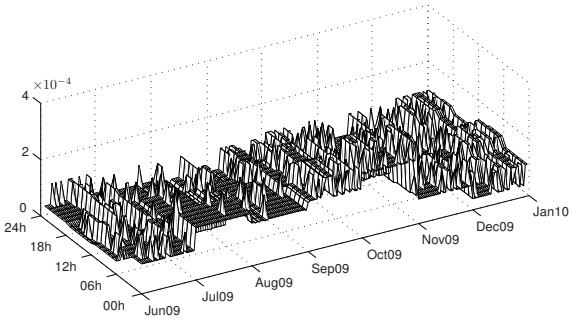
LZRFR



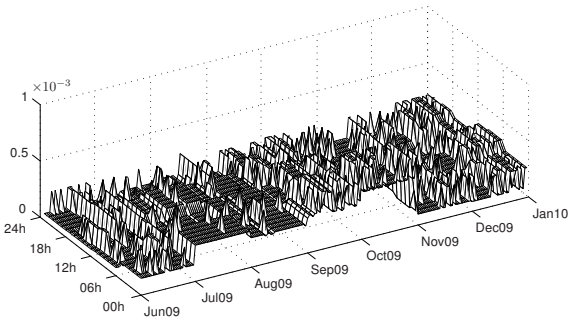
LFTFR



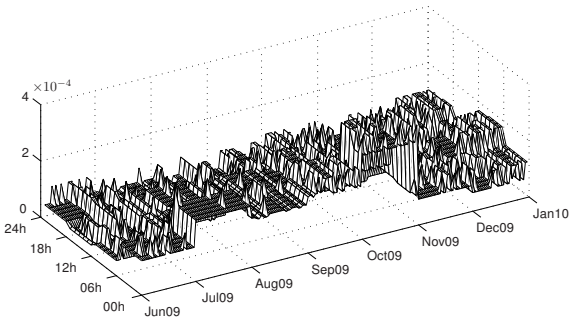
LOQNVC



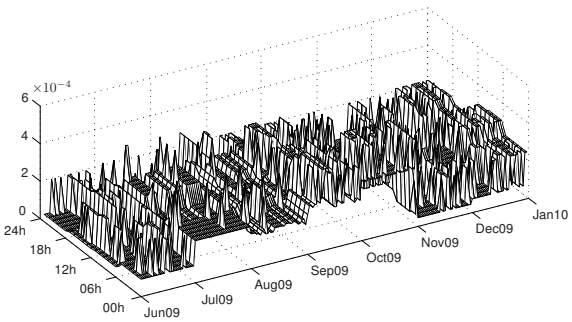
LOQTN



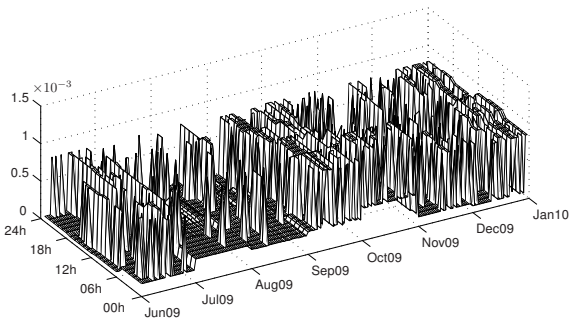
LFAOQ



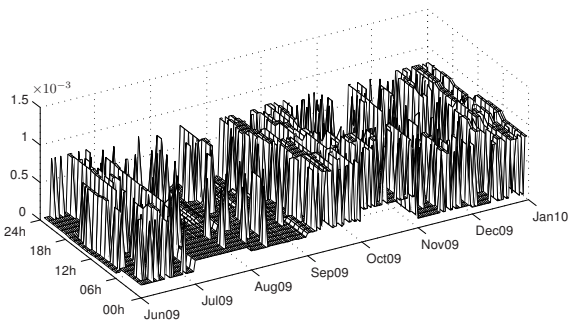
LTNET



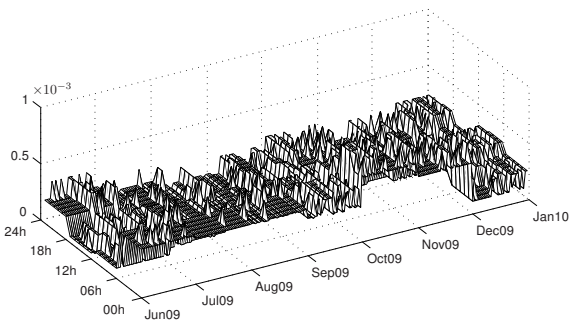
LSNOQ2



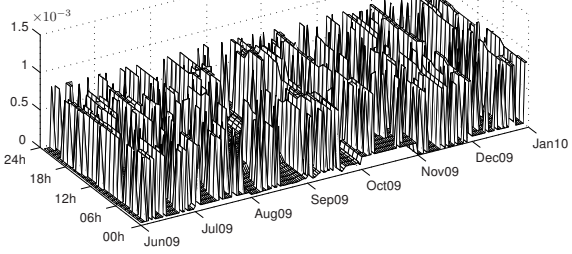
LSNOQ1



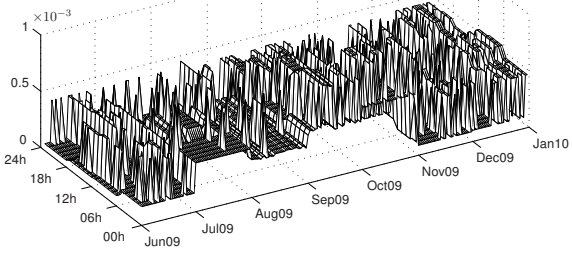
LFAER



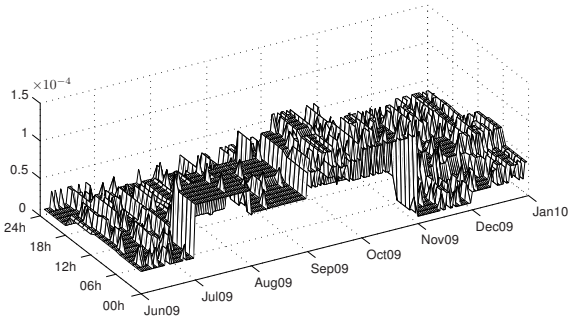
LCDVI1/VF



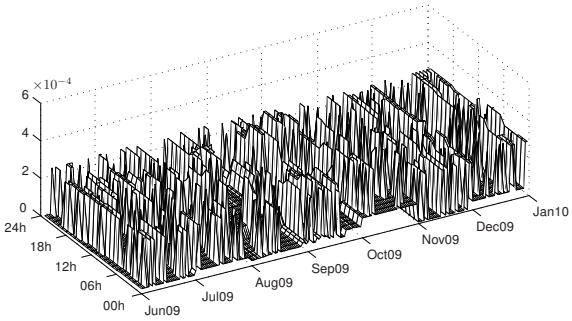
LOQET1



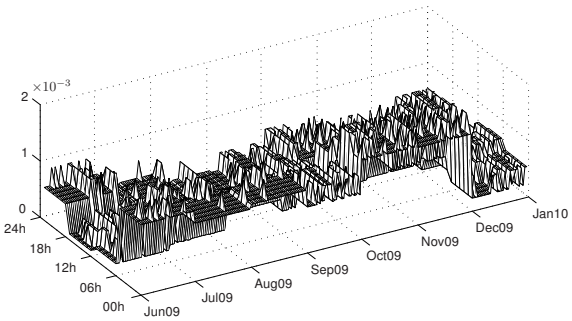
LFNSV1



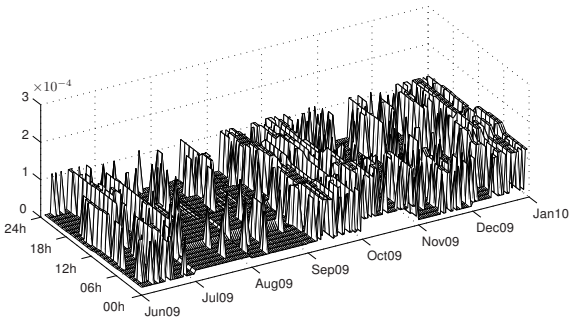
LRAED4



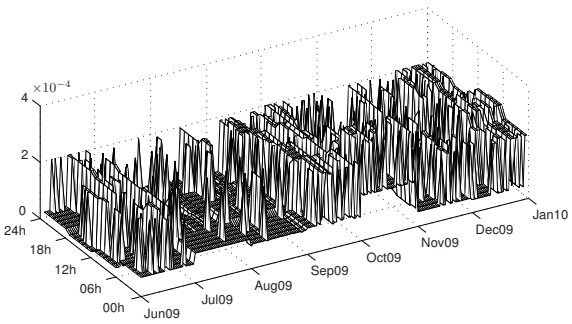
LPMER/PGS



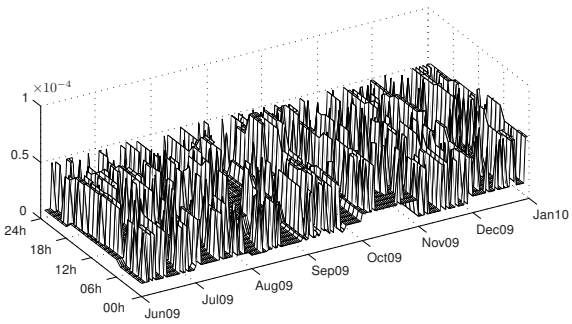
LCSNSN1



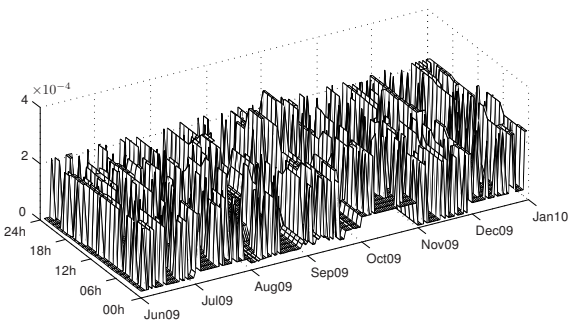
LPMFF4/SXS/SXR



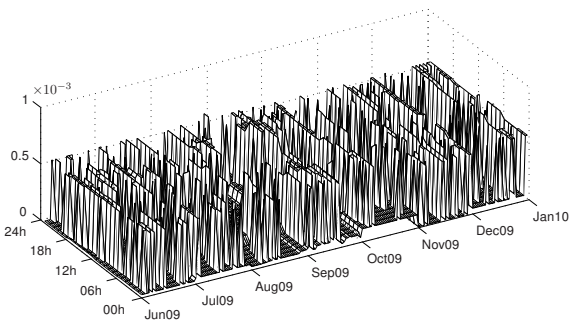
LRARU



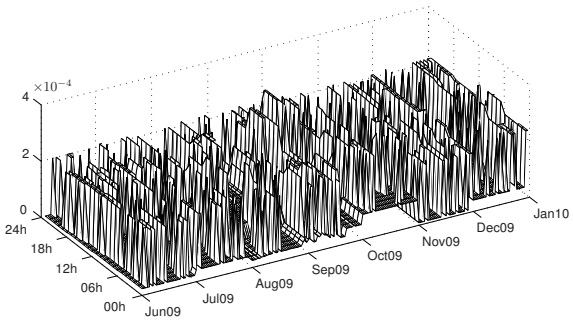
LRAED3



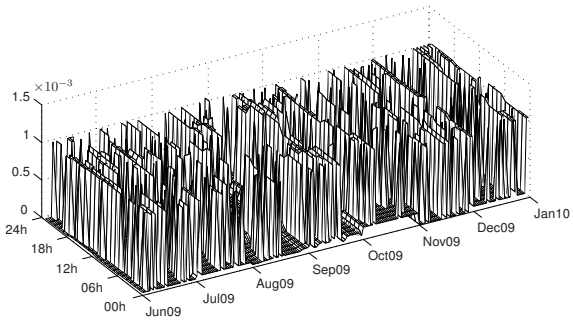
LCDRA2/GR



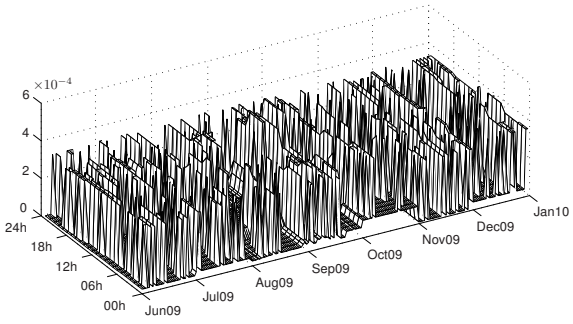
LRAED2



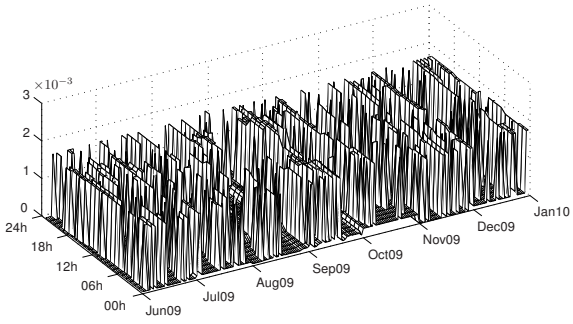
LCDRA1/FRD



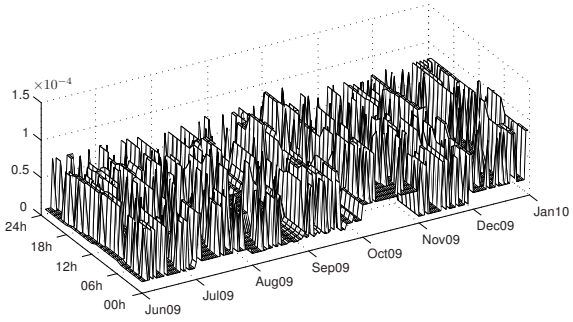
LRAED1



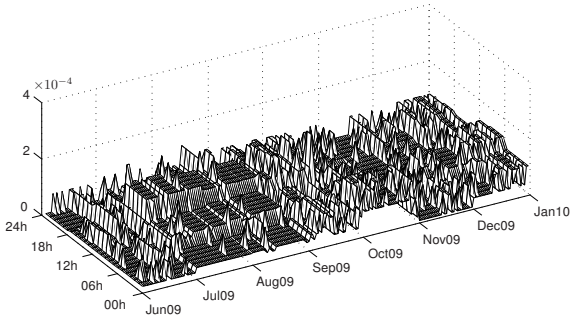
LVNRA/OR



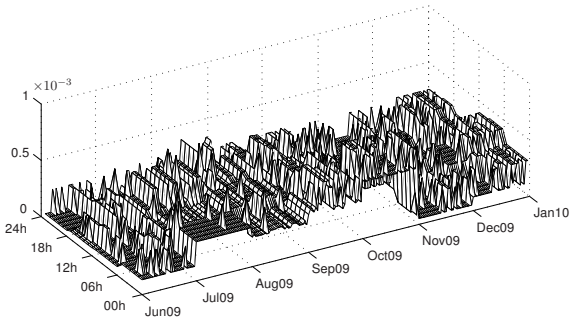
LVMED3/MAA



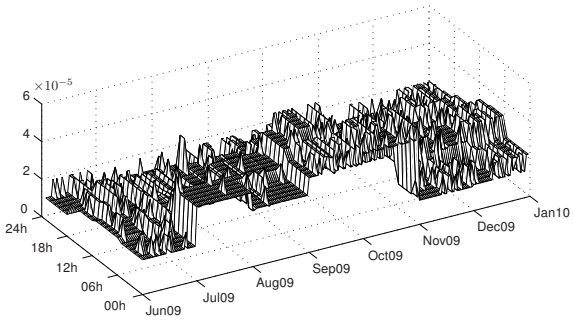
LPOTN2



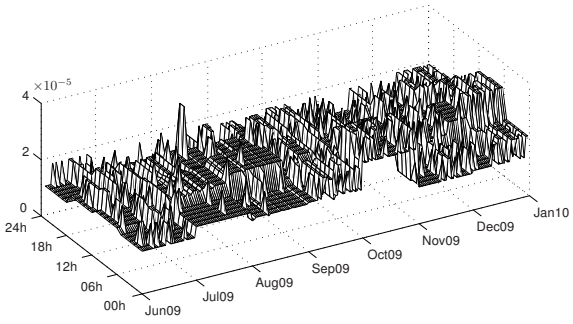
LSNPO2



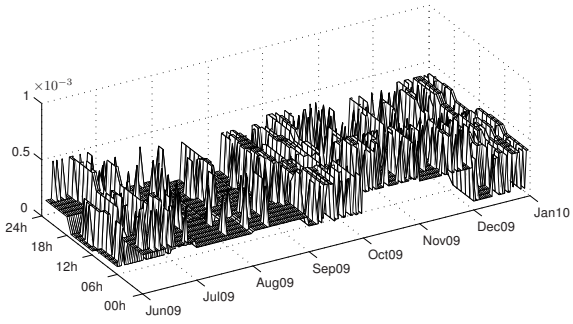
LPMSB3



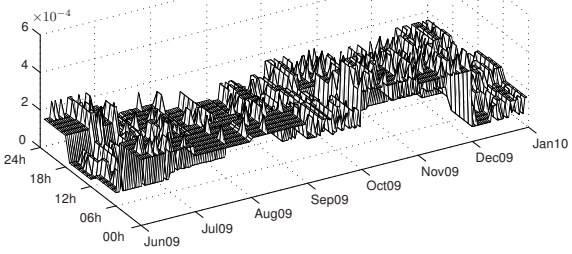
LPMSB2



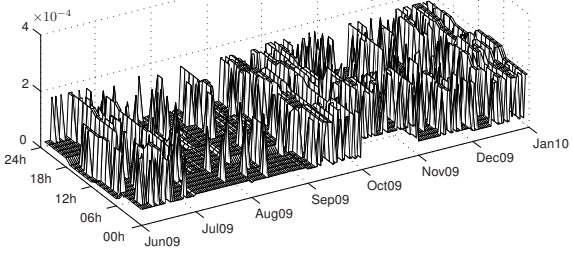
LPAPM2



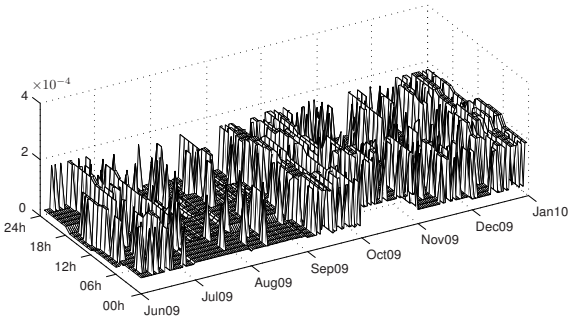
LPAPM1



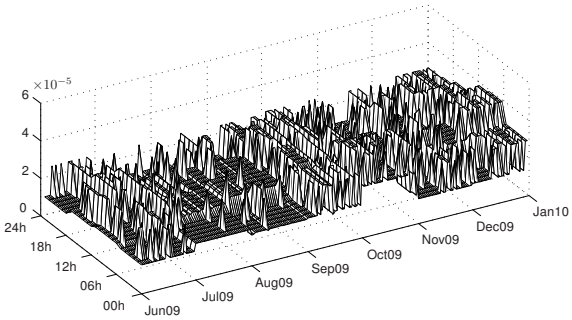
LPMFF2



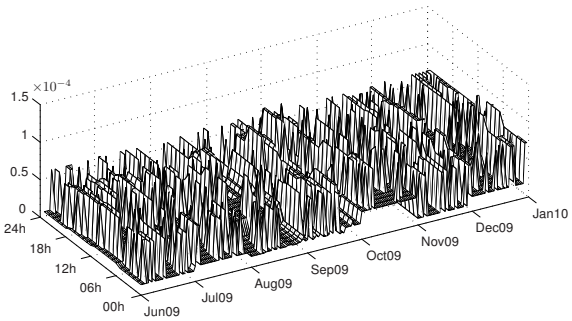
LPMFF1



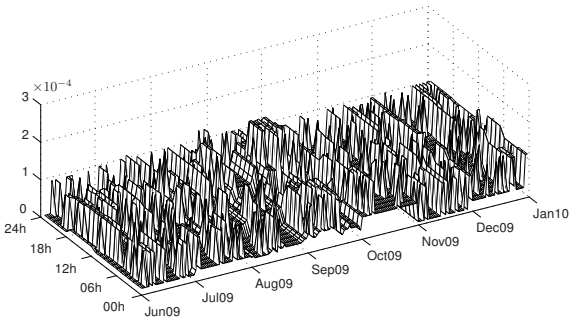
LPMSB1



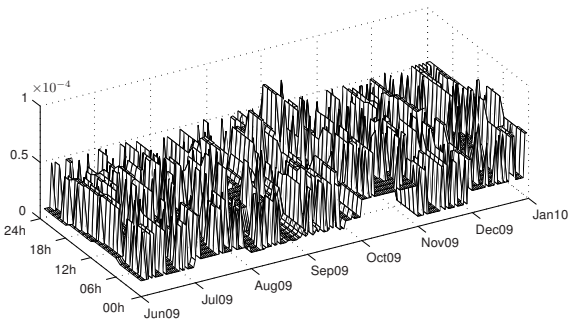
LVMED2



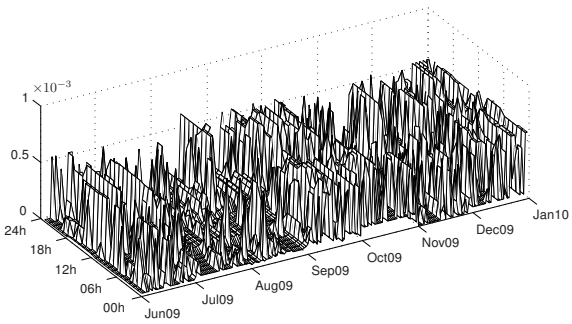
LTCRG



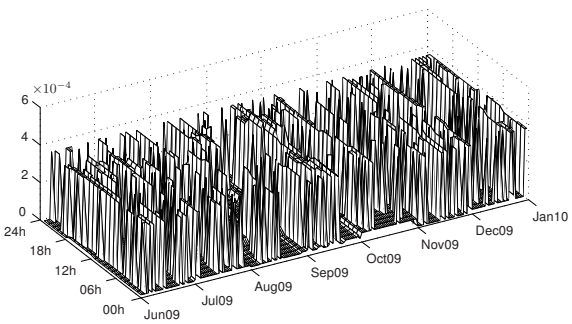
LVMED1



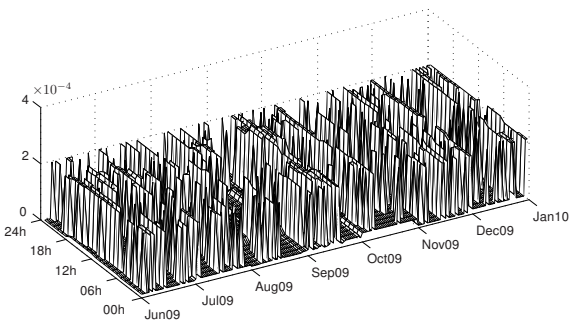
LBCZR2



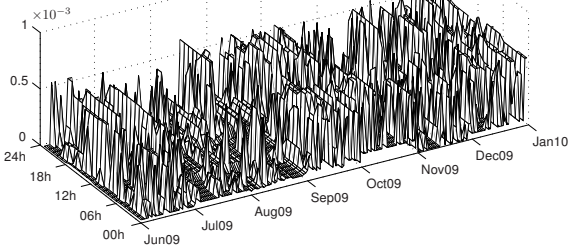
LSDCD



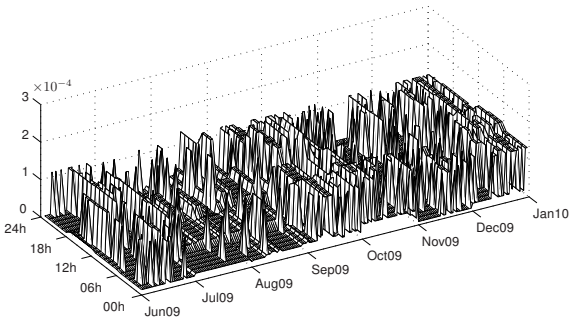
LVNSD



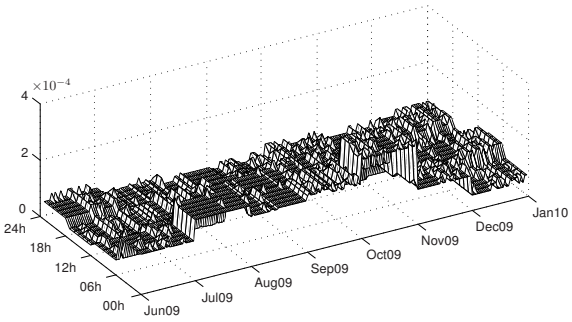
LBCZR1



LCRBC

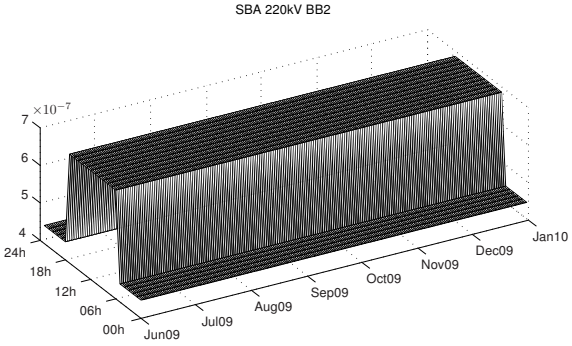


LSVPA

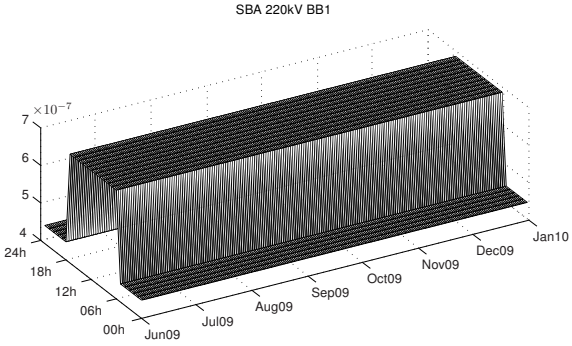


J.2 Busbars

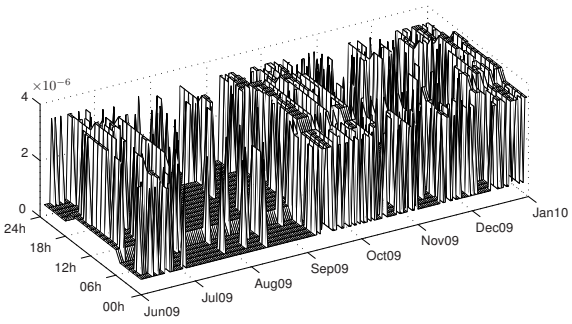
SBA 220kV BB2



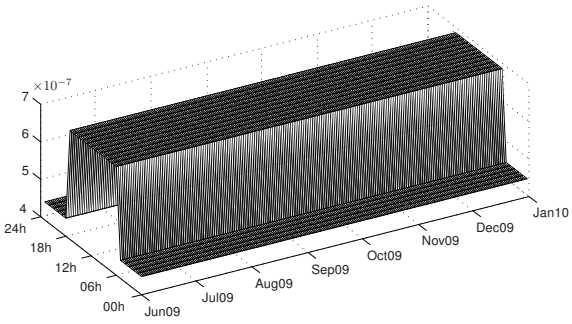
SBA 220kV BB1



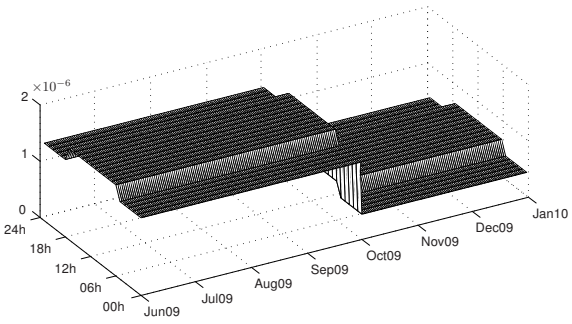
SFR 400kV BB2



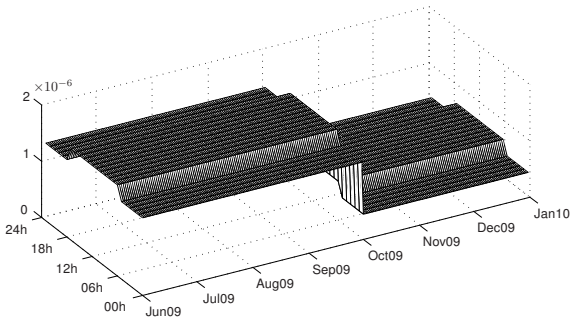
SVC 220kV BB1C



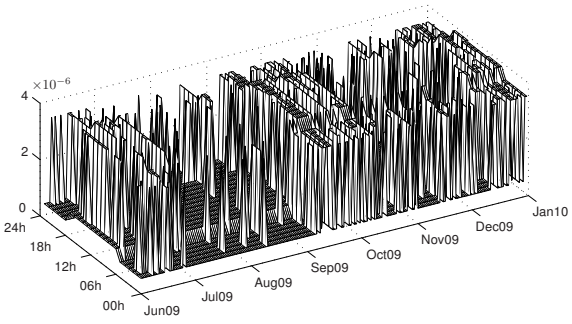
SSR 220kV BB2



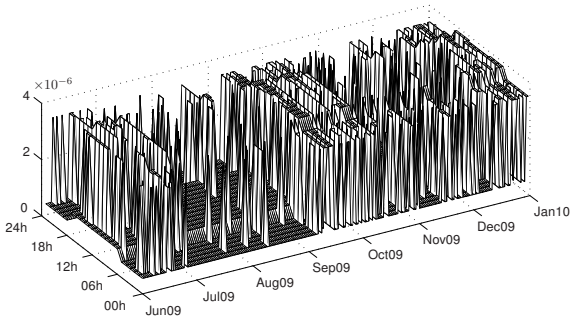
SSR 220kV BB1



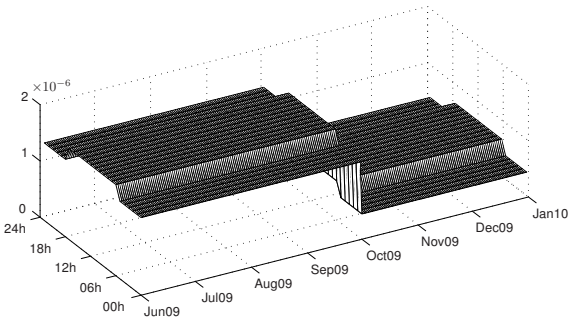
SFR 400kV BB1



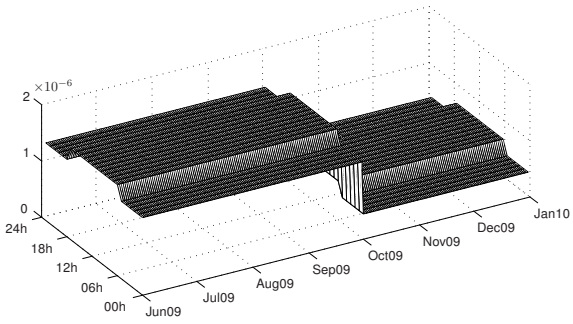
SFA 400kV BB2



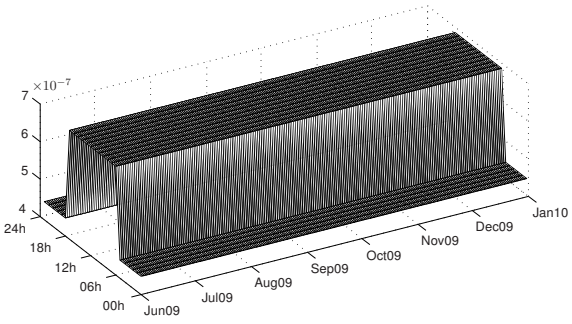
SSS 220kV BB2



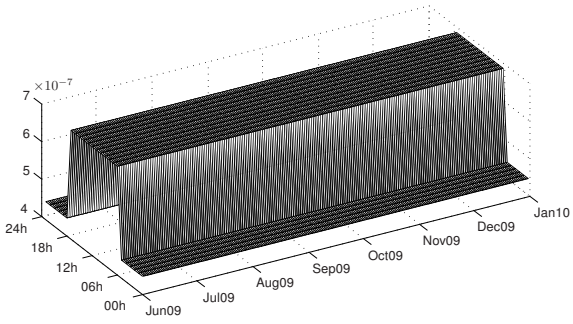
SSS 220kV BB1



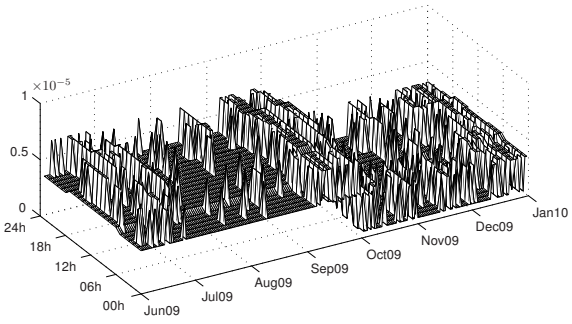
SZR 220kV BB2



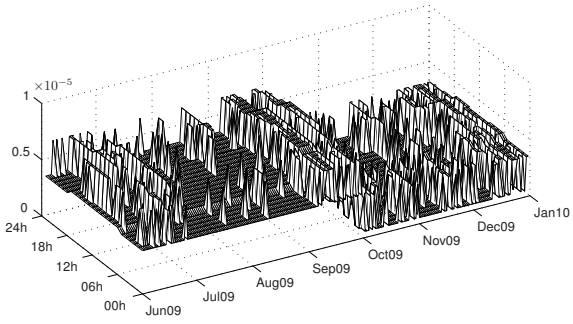
SZR 220kV BB1



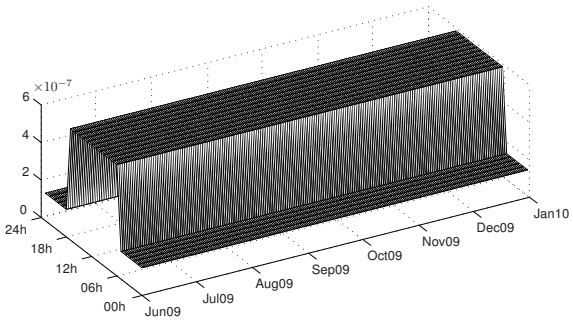
SRJ 400kV BB2



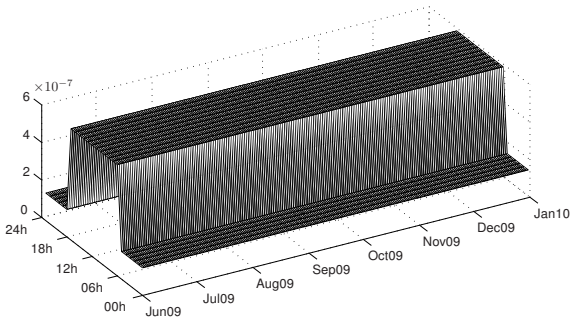
SRJ 400kV BB1



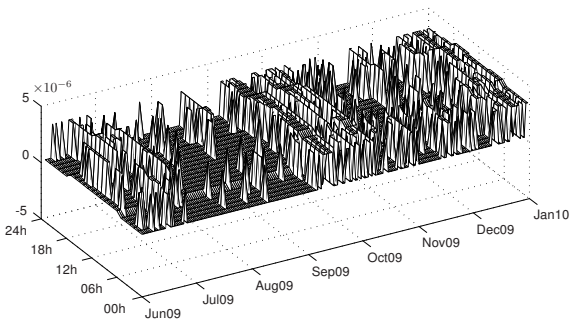
SZR 150kV BB2



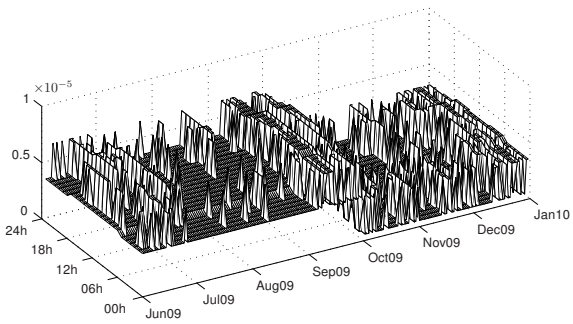
SZR 150kV BB1



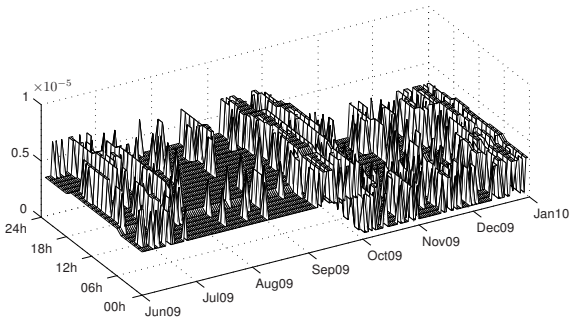
SFA 400kV BB1



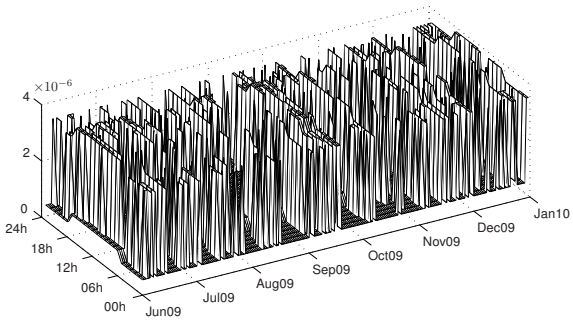
SAM 400kV BB2



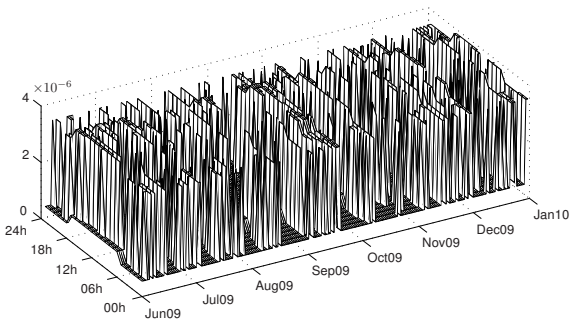
SAM 400kV BB1



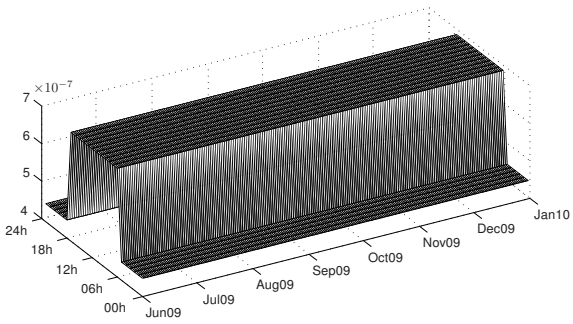
SLV 400kV BB2



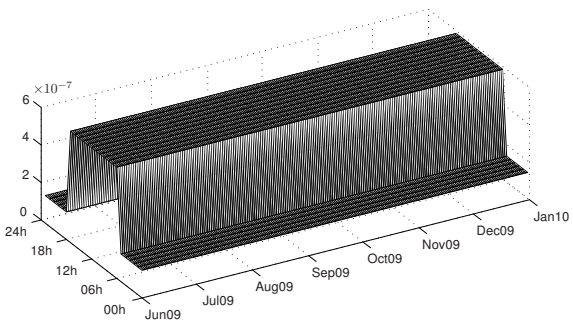
SLV 400kV BB1



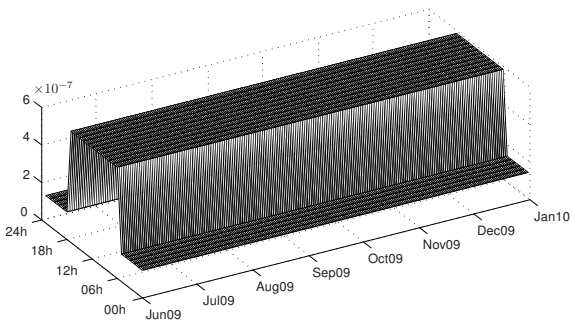
SFE 220kV BB2



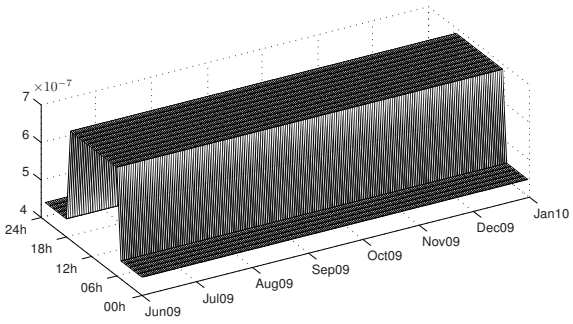
SVM 150kV BB1A



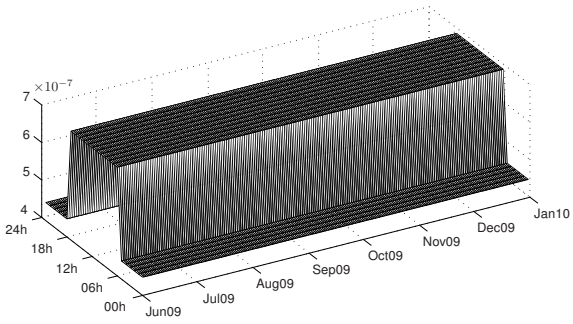
SVM 150kV BB1B



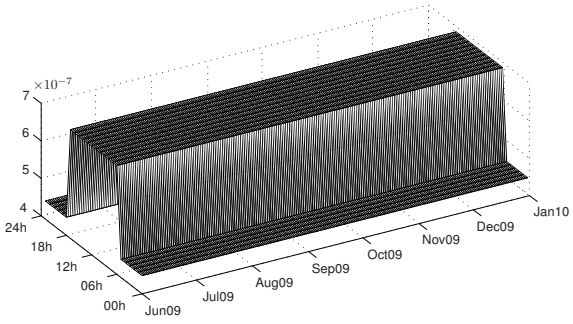
SVG 220kV BB2B



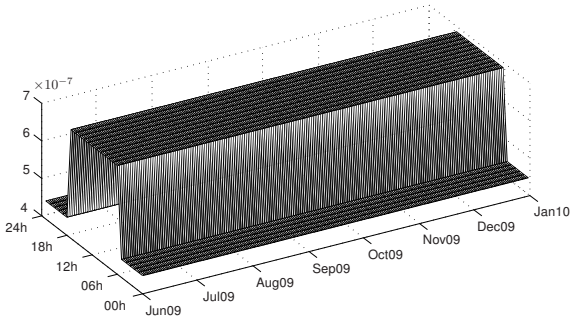
SVG 220kV BB1B



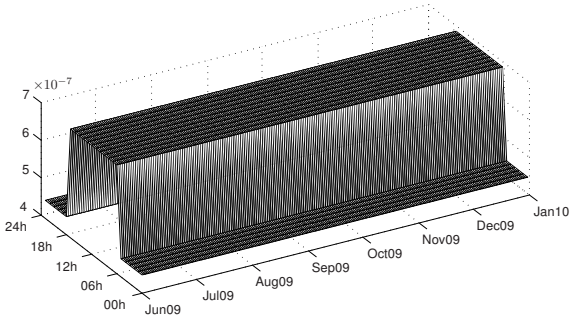
SVG 220kV BB2A



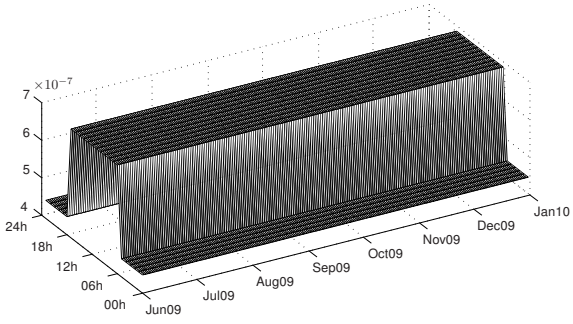
SVG 220kV BB1A



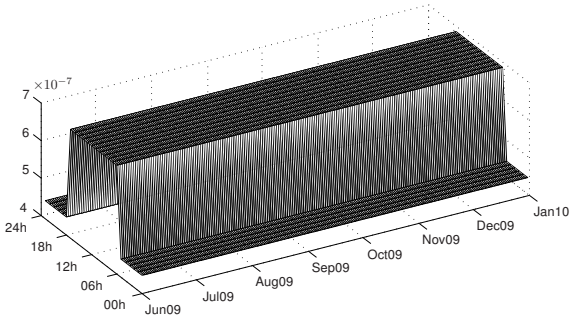
SVM 220kV BB2



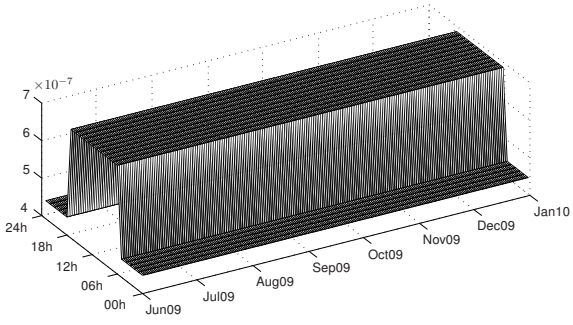
SVM 220kV BB1



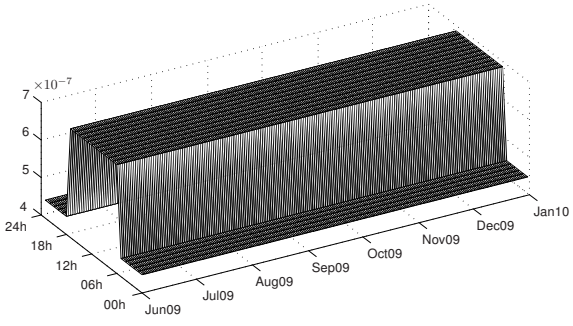
SCL 220kV BB2A



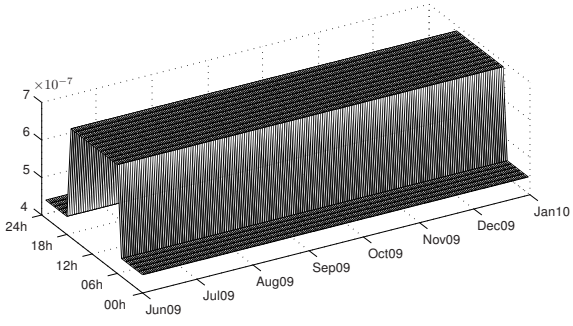
SCL 220kV BB1B



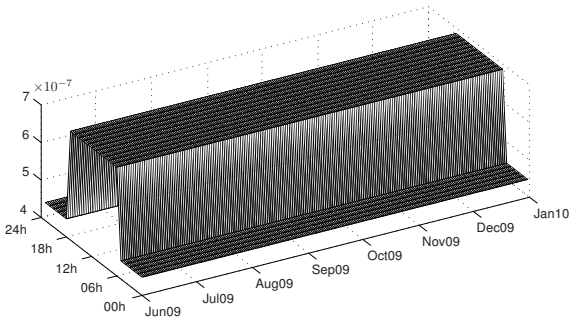
SVC 220kV BB1B



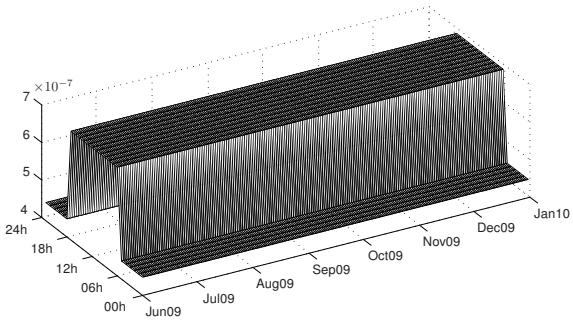
SVC 220kV BB1A



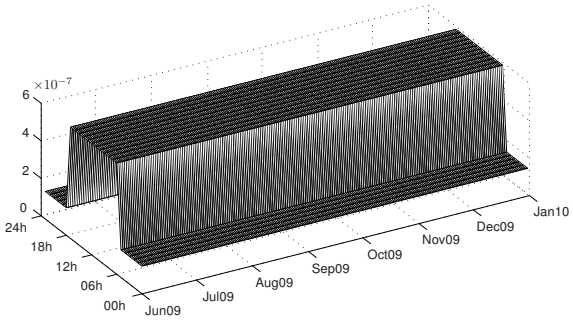
SCL 220kV BB2B



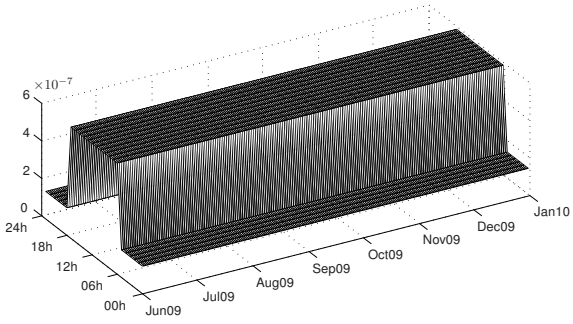
SCL 220kV BB1A



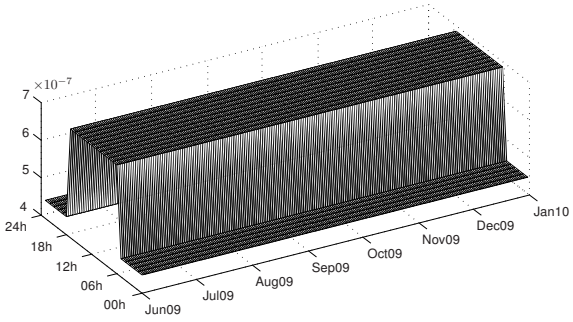
SED 150kV BB2



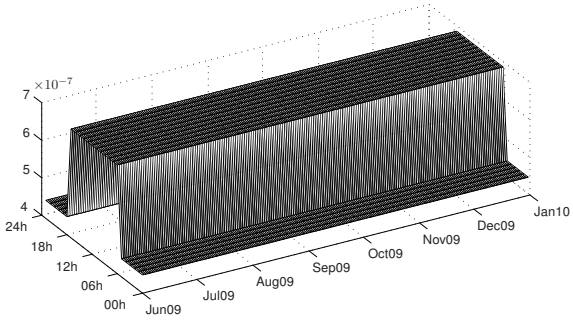
SED 150kV BB1



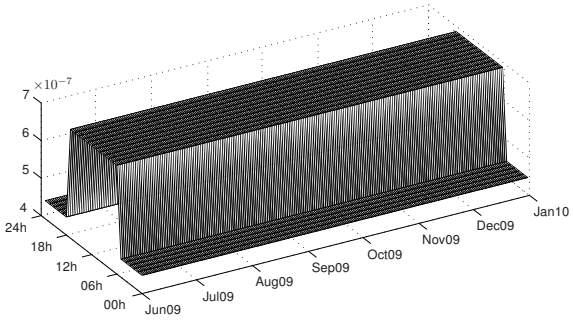
SCT 220kV BB2



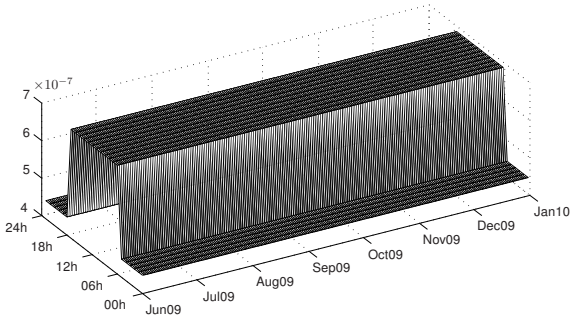
SCT 220kV BB1



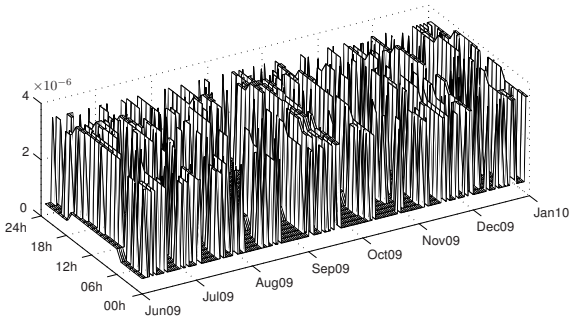
SRR 220kV BB2



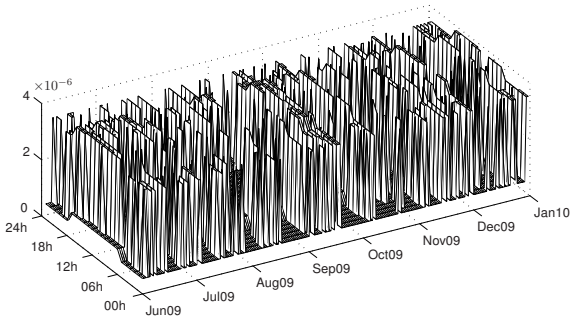
SRR 220kV BB1



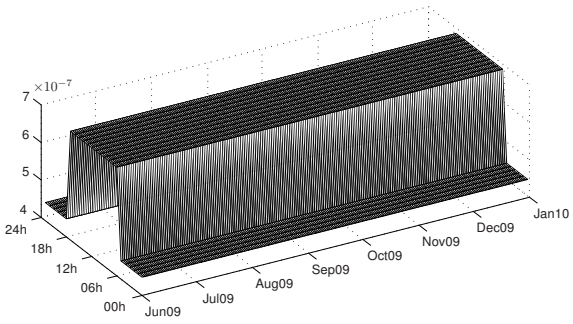
SRR 400kV BB2



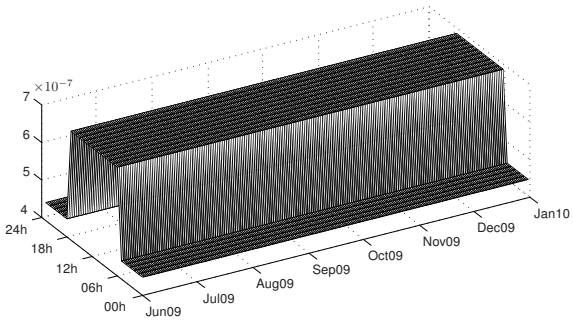
SRR 400kV BB1



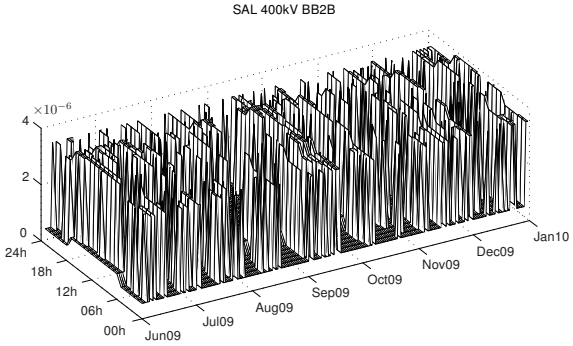
SCN 220kV BB2



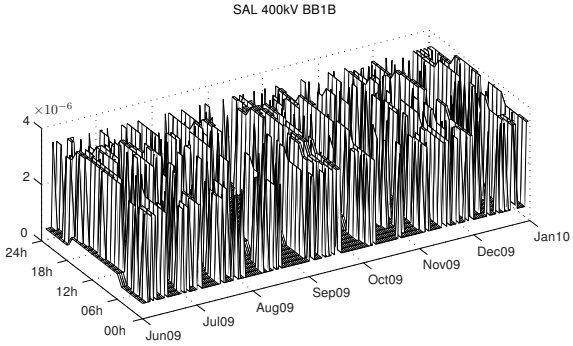
SCN 220kV BB1



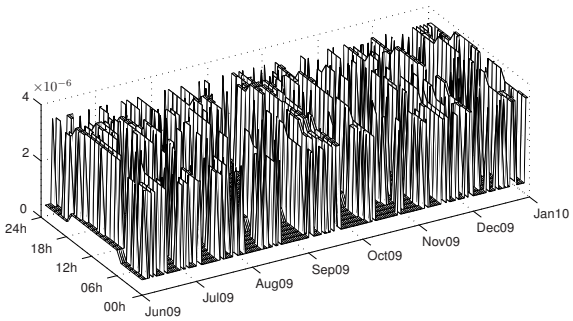
SAL 400kV BB2B



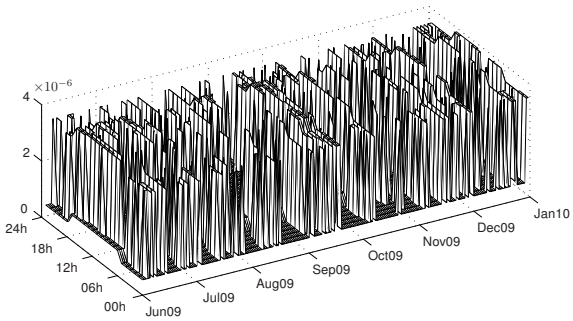
SAL 400kV BB1B



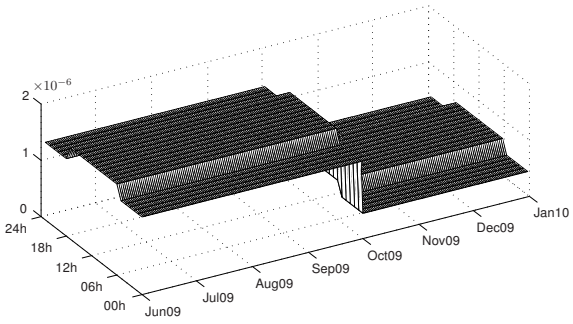
SAL 400kV BB2A



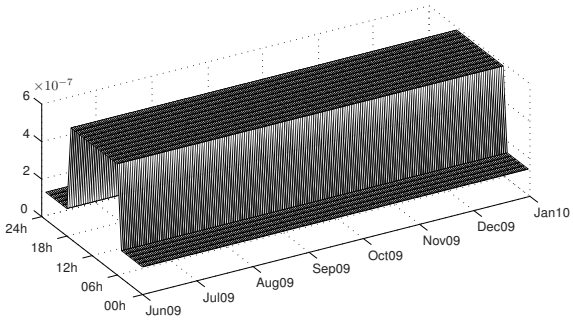
SAL 400kV BB1A



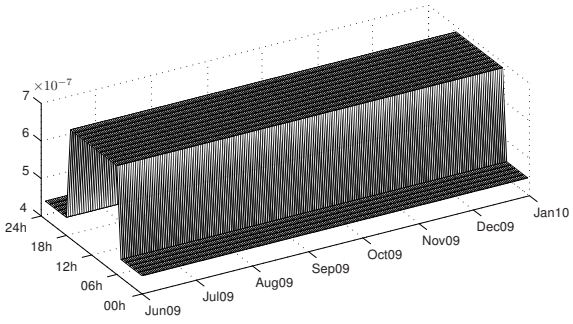
SFN 220kV BB2



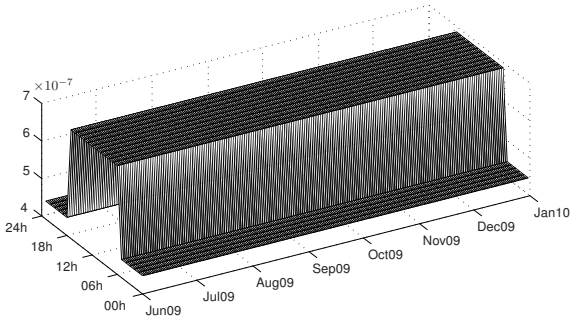
SPR 150kV BB2



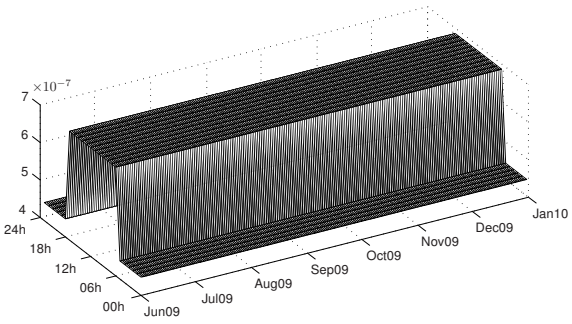
SMCC 220kV BB2



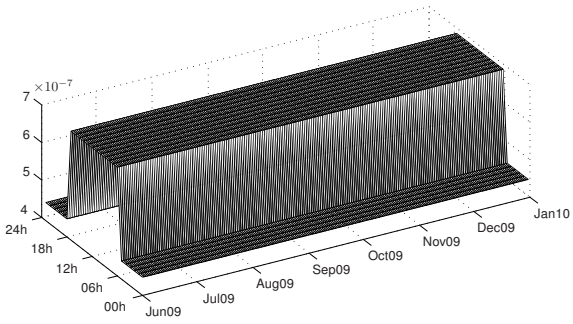
SMCC 220kV BB1



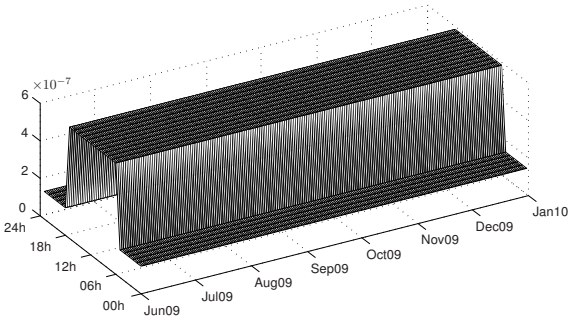
SVPA 220kV BB2



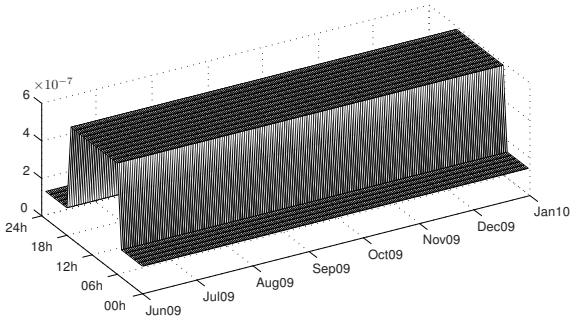
SVPA 220kV BB1



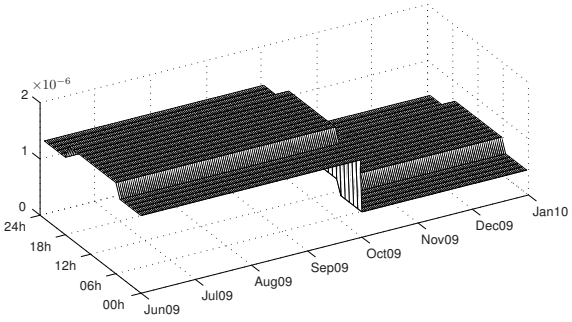
SFRD 150kV BB2



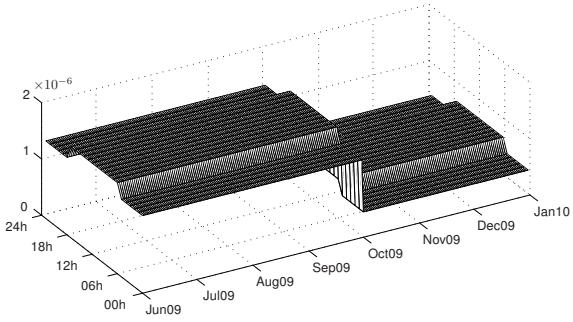
SFRD 150kV BB1



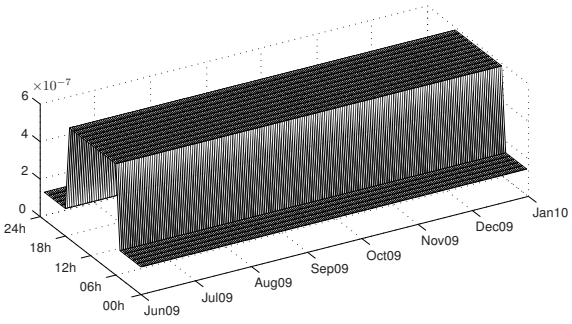
SCVR 220kV BB2



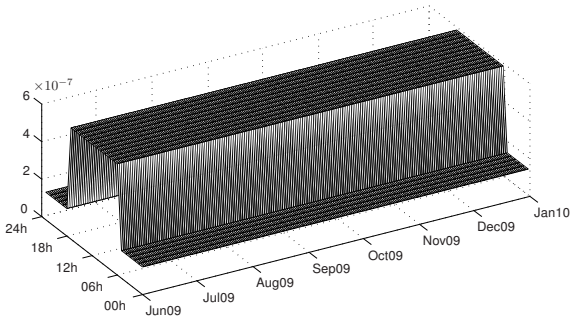
SCVR 220kV BB1



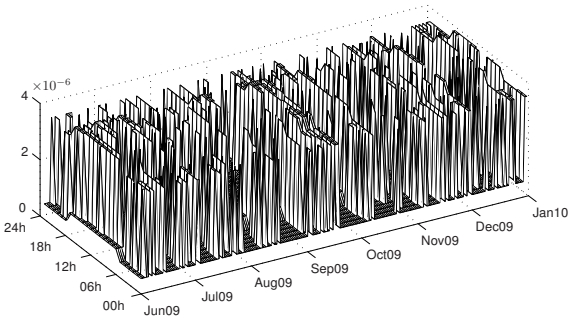
SPDV 150kV BB2



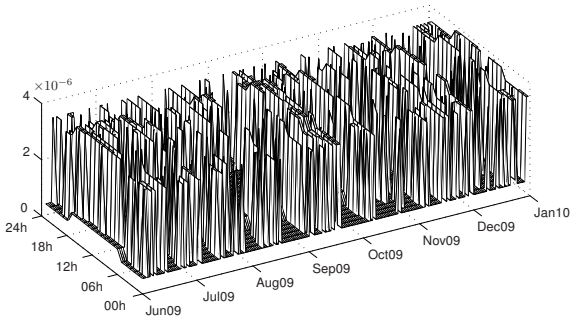
SPDV 150kV BB1



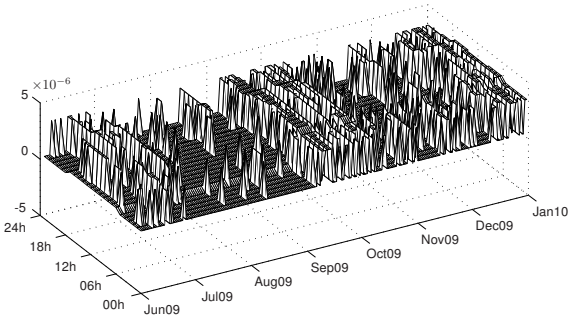
SPDV 400kV BB2



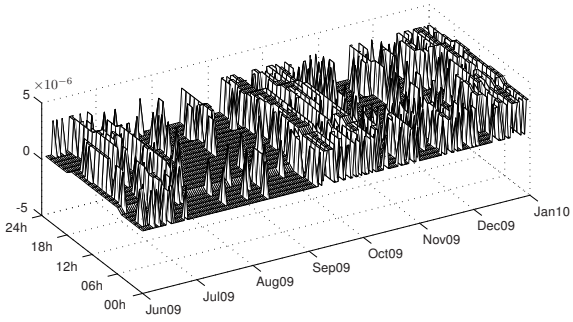
SPDV 400kV BB1



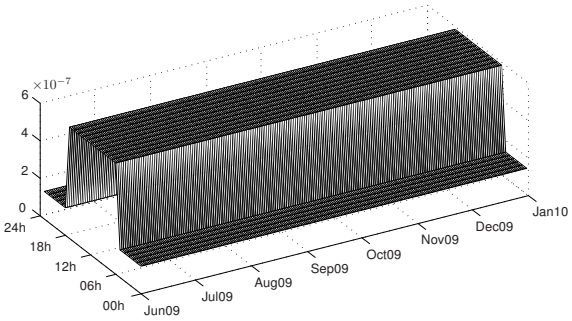
SAV 400kV BB2



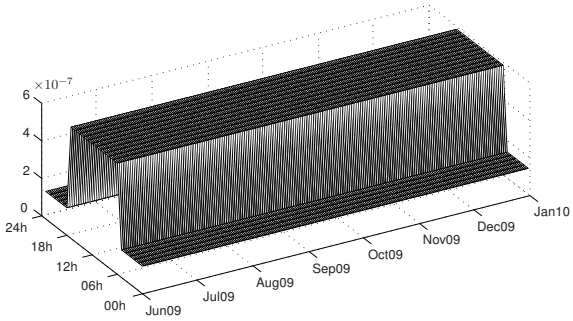
SAV 400kV BB1



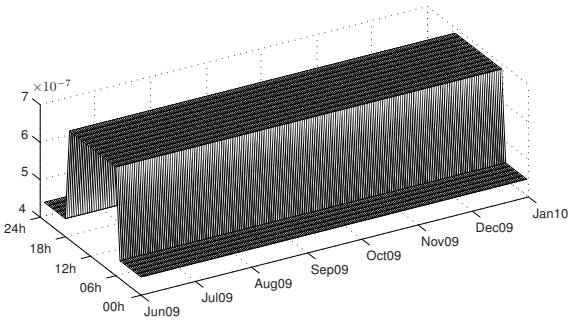
STFR 150kV BB2



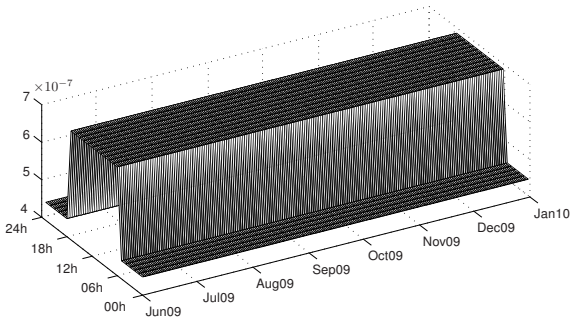
STFR 150kV BB1



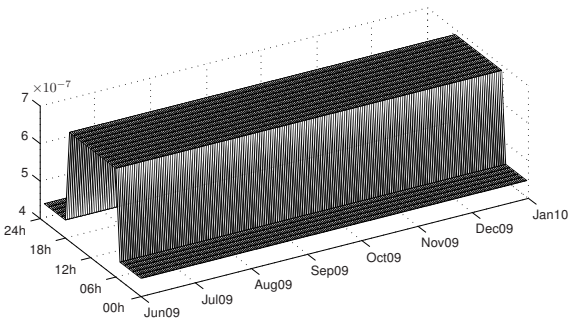
SPNL 220kV BB2



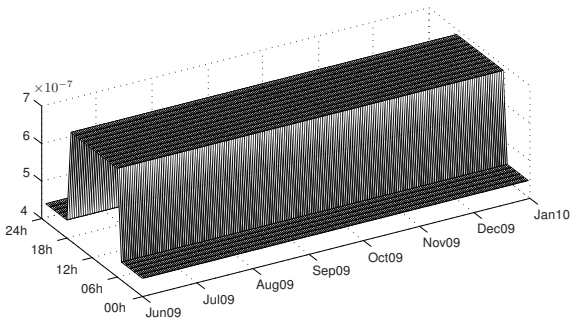
SPNL 220kV BB1



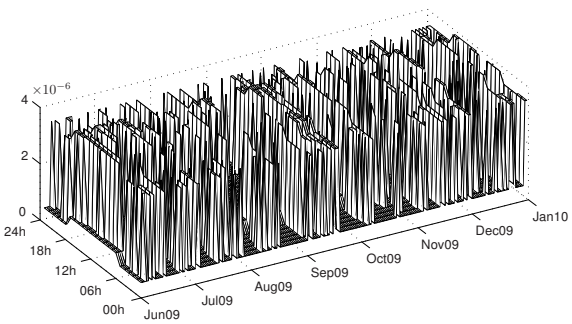
SPI 220kV BB2



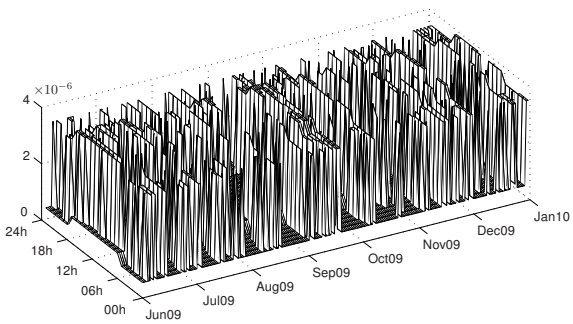
SPI 220kV BB1



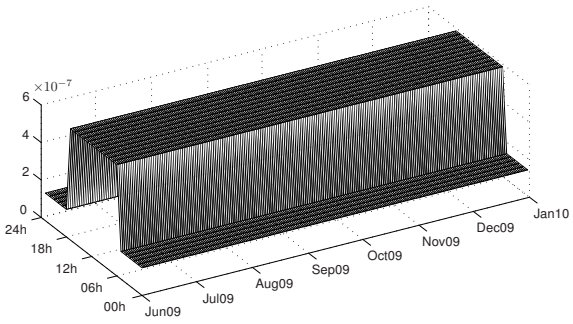
SPI 400kV BB2



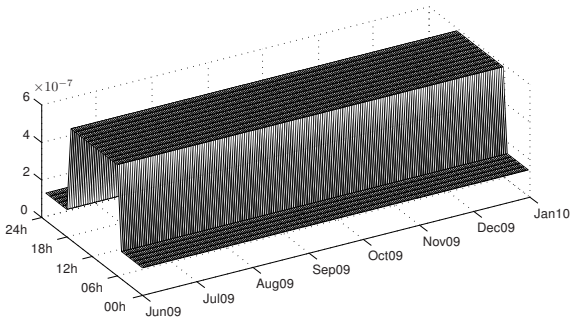
SPI 400kV BB1



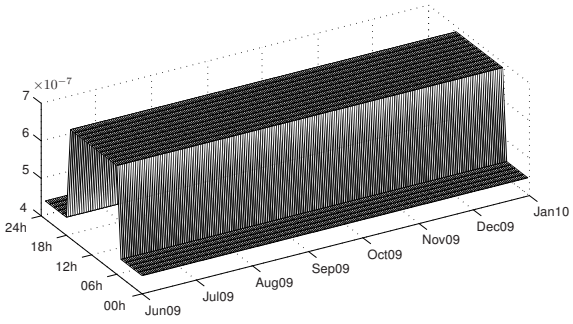
SCC 150kV BB2



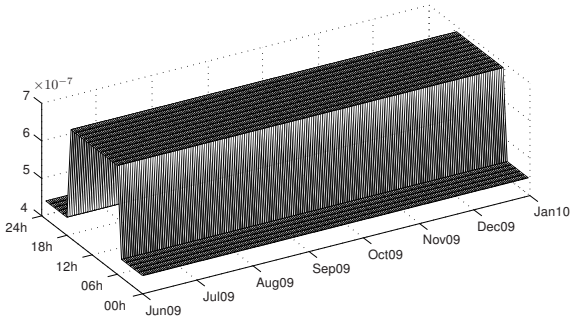
SCC 150kV BB1



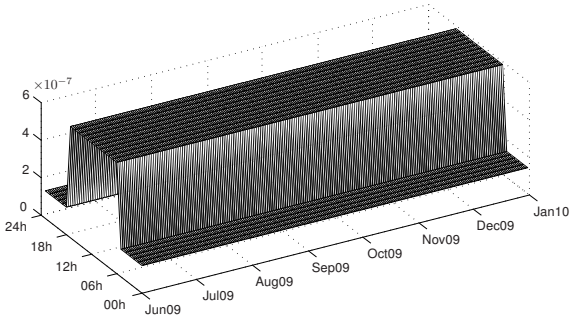
SCC 220kV BB2



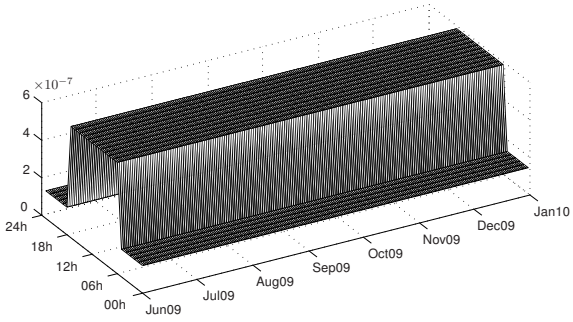
SCC 220kV BB1



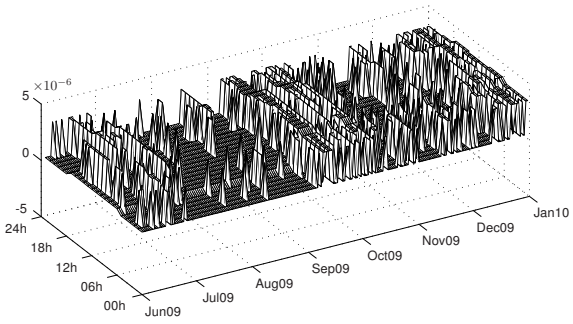
SPO 150kV BB2



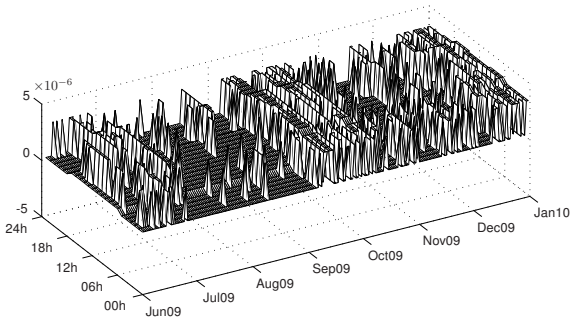
SPO 150kV BB1



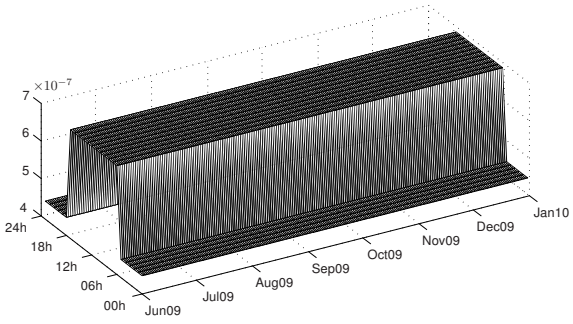
SBL 400kV BB2



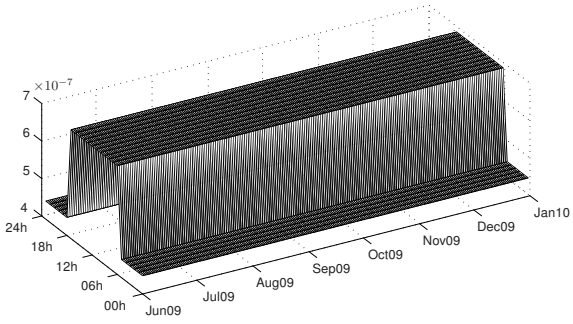
SBL 400kV BB1



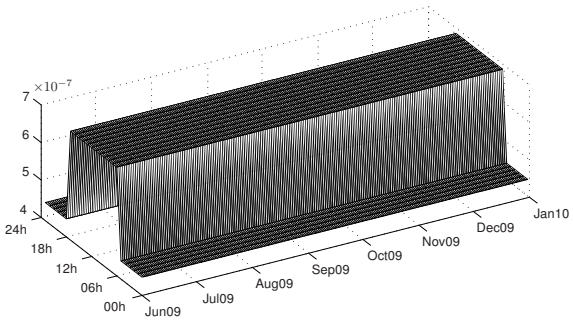
SFE 220kV BB1



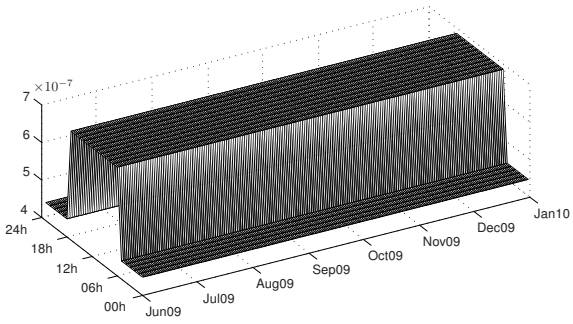
SCF 220kV BB2



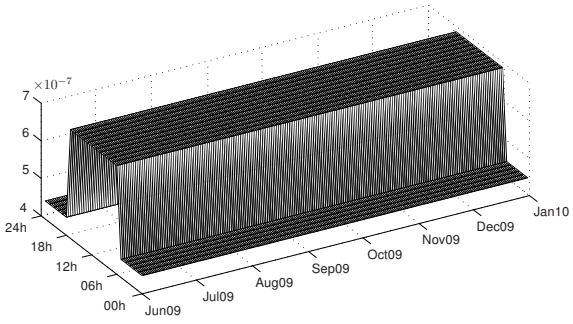
SCF 220kV BB1



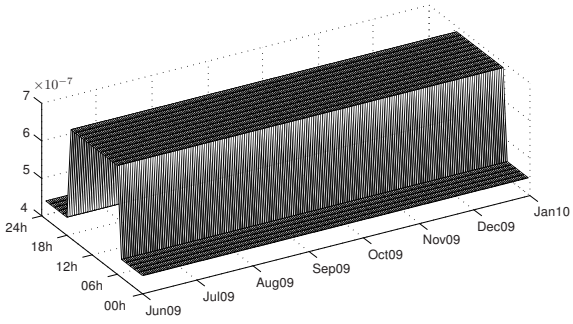
SEJ 220kV BB2



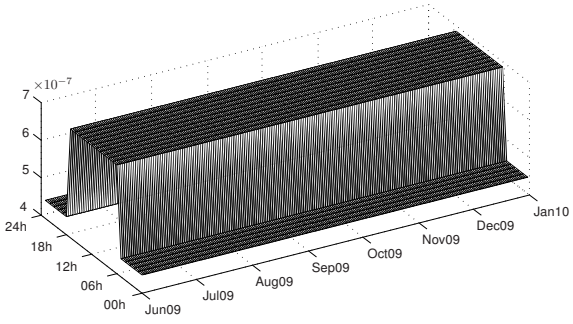
SEJ 220kV BB1



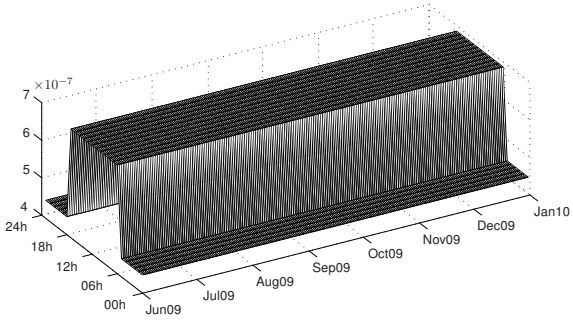
SMG 220kV BB1



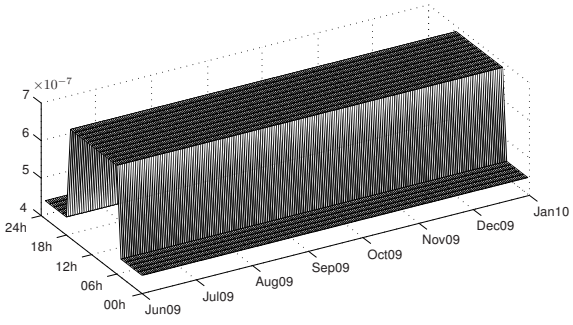
SPN 220kV BB2



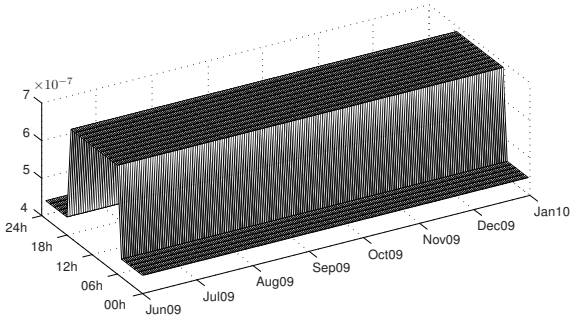
SPN 220kV BB1



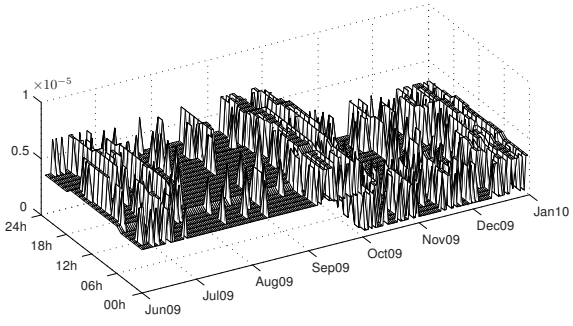
SPR 220kV BB2



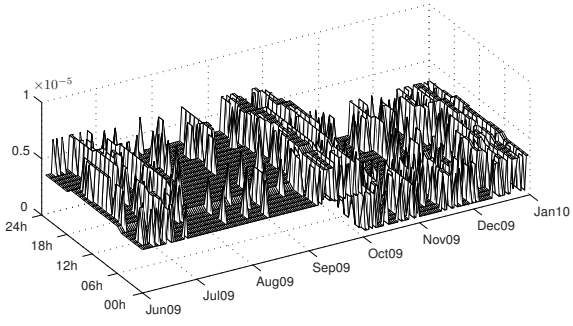
SPR 220kV BB1



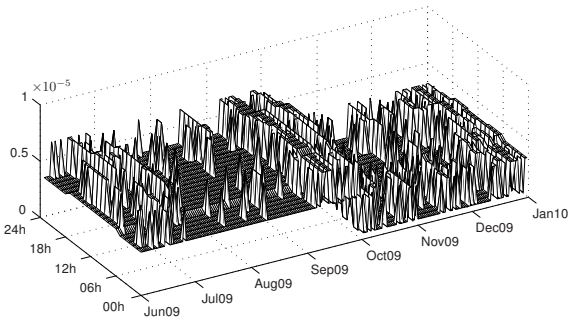
SPM 400kV BB2B



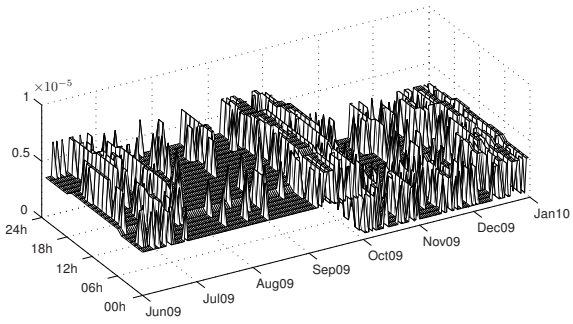
SPM 400kV BB2A



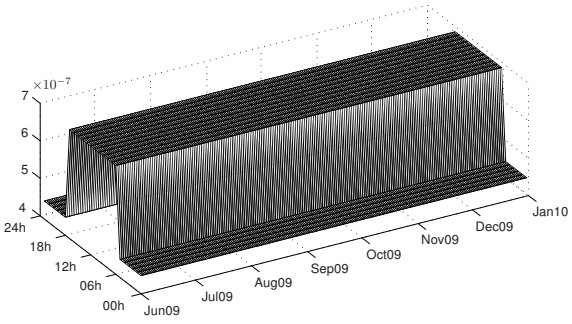
SPM 400kV BB1B



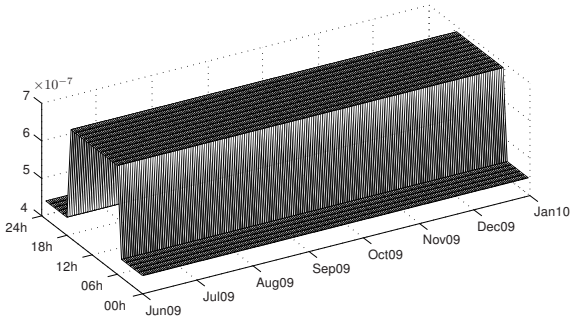
SPM 400kV BB1A



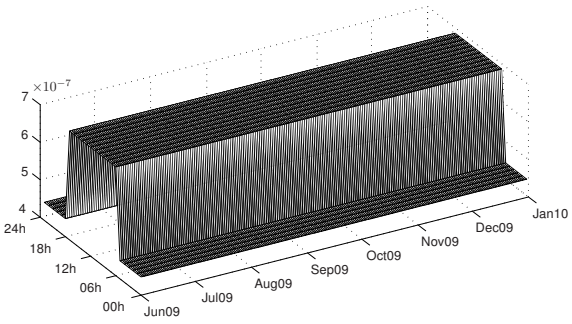
SRM 220kV BB2B



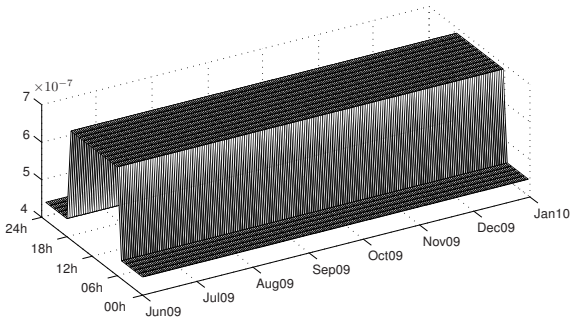
SRM 220kV BB2A



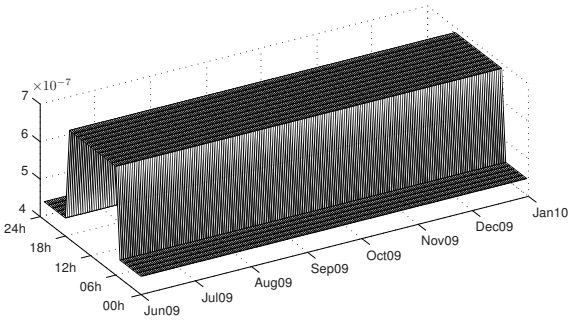
SRM 220kV BB1B



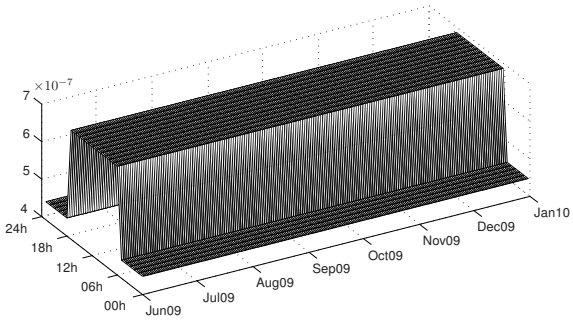
SRM 220kV BB1A



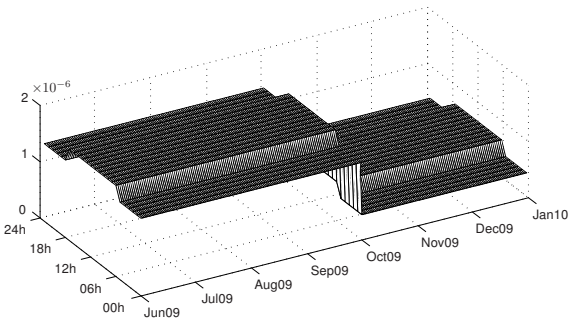
STR 220kV BB2



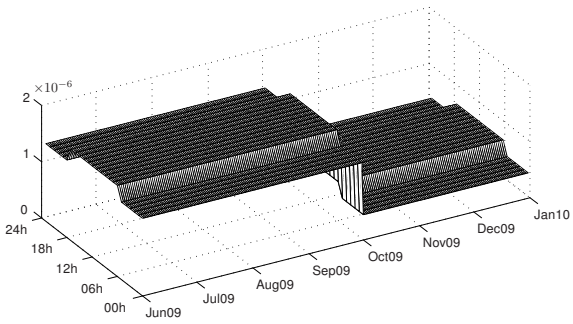
STR 220kV BB1



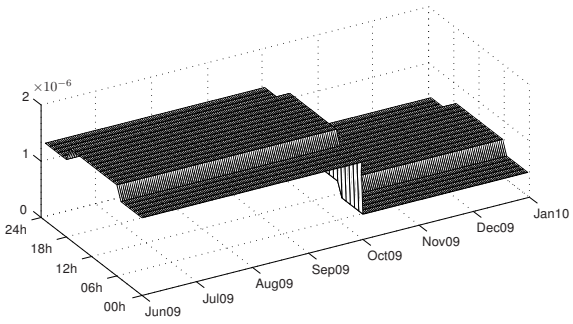
SCG 220kV BB2C



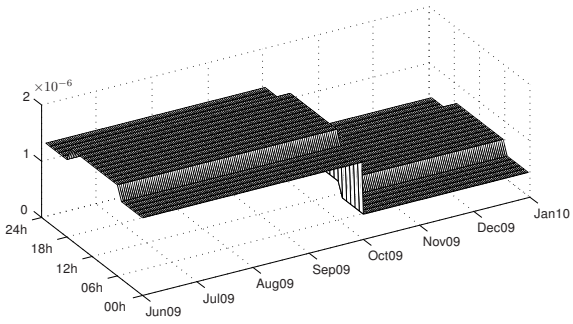
SCG 220kV BB1C



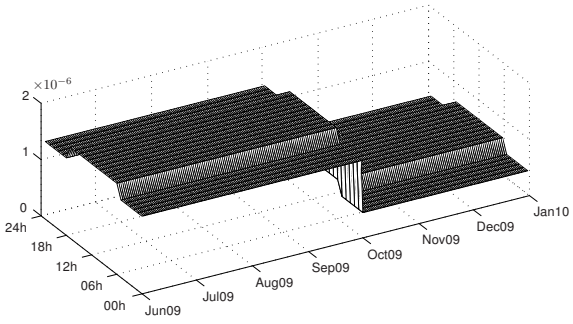
SCG 220kV BB2B



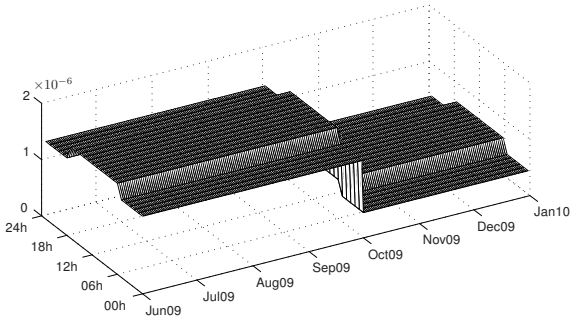
SCG 220kV BB1B



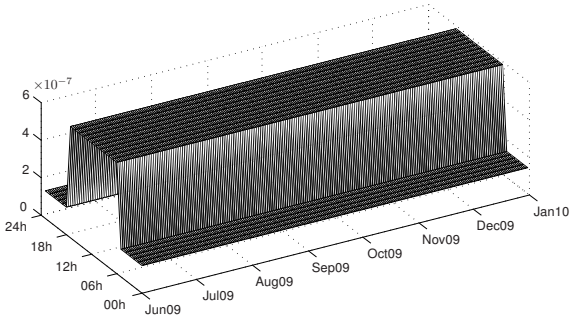
SCG 220kV BB2A



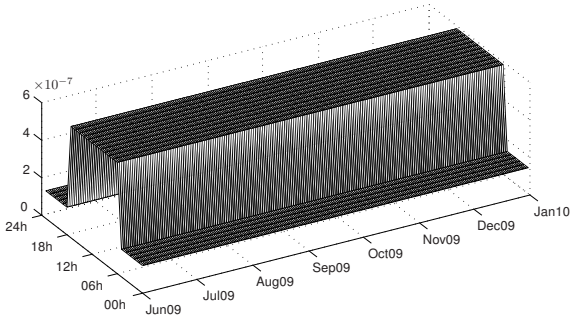
SCG 220kV BB1A



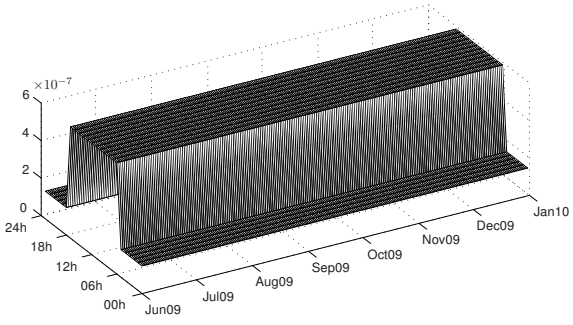
SOR 150kV BB2



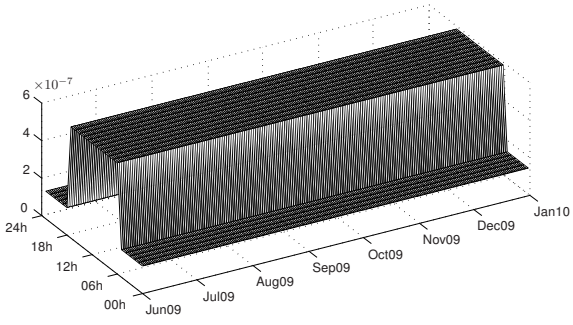
SOR 150kV BB1



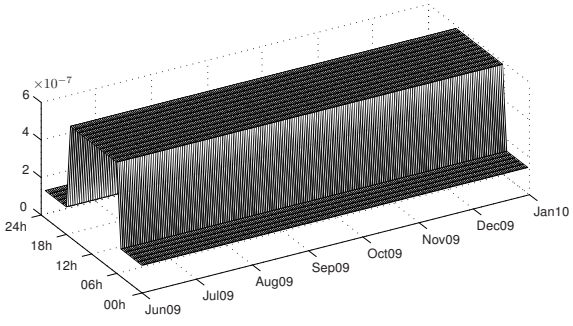
SOQ 150kV BB2



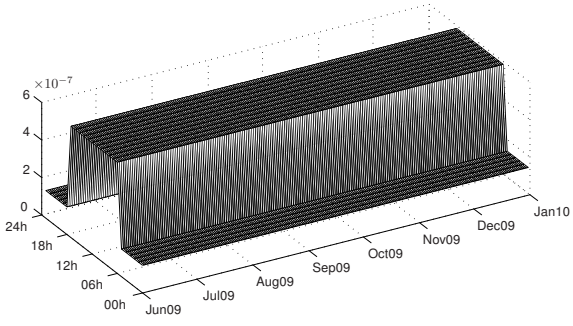
SVI 150kV BB2



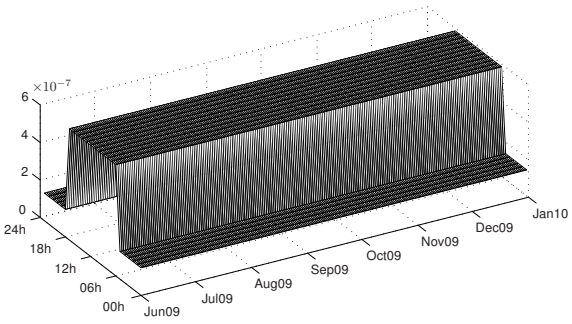
SVI 150kV BB1



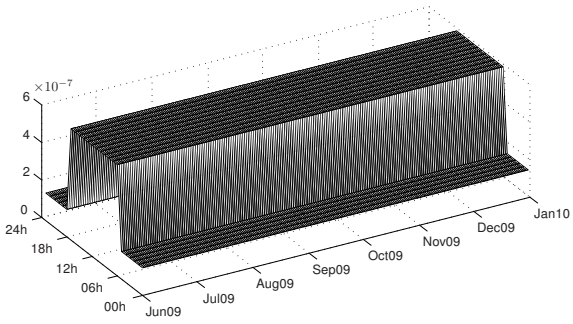
SOQ 150kV BB1



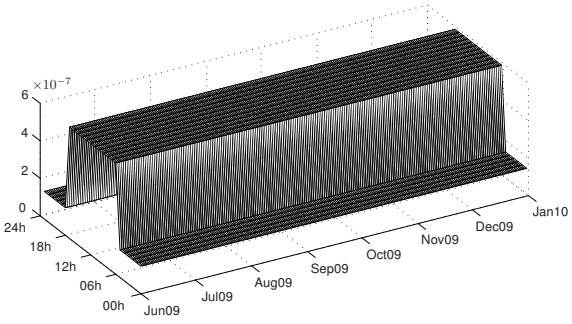
SRA 150kV BB2B



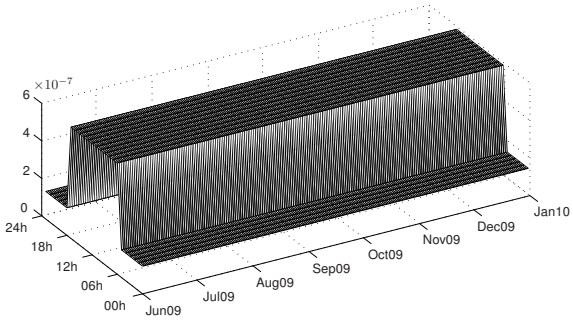
SRA 150kV BB1B



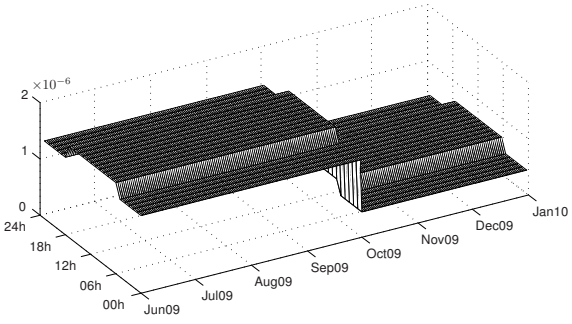
SRA 150kV BB2A



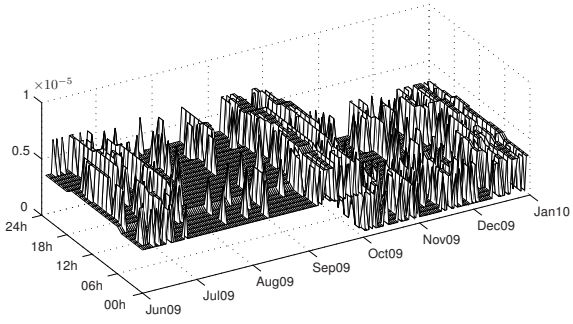
SRA 150kV BB1A



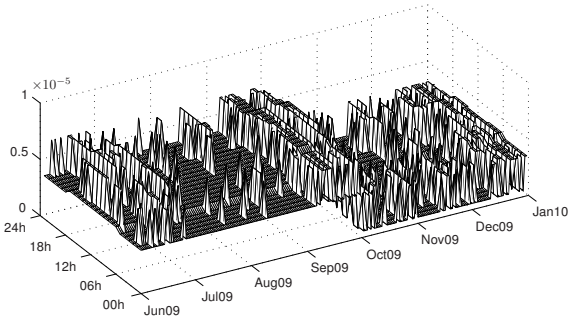
SFN 220kV BB1



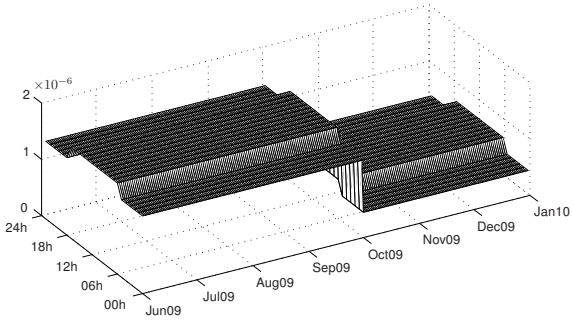
SFN 400kV BB2



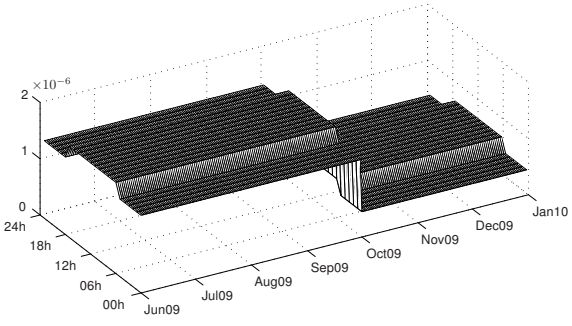
SFN 400kV BB1



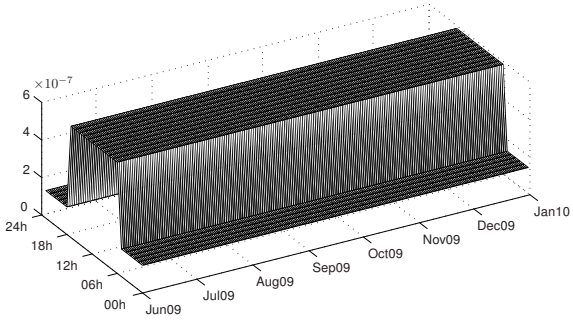
SCH 220kV BB2



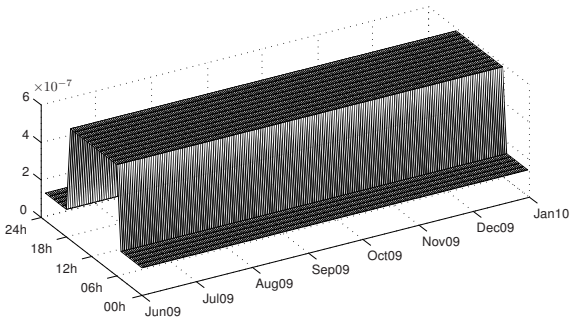
SCH 220kV BB1



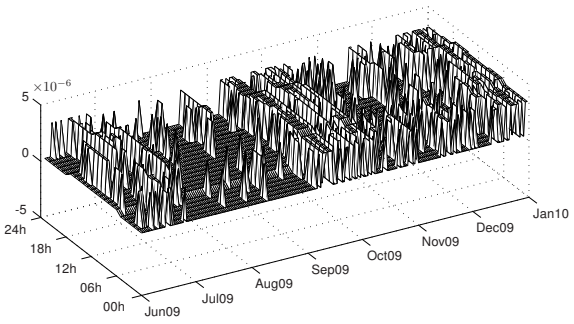
SPM 150kV BB2



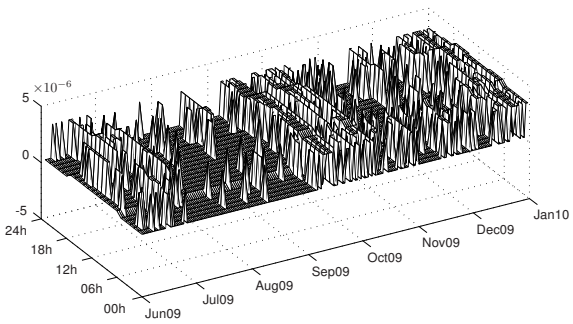
SPM 150kV BB1



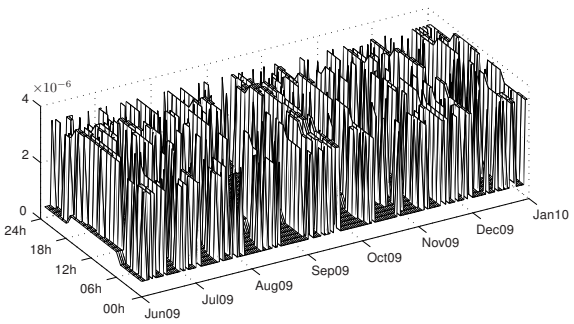
SPG 400kV BB2



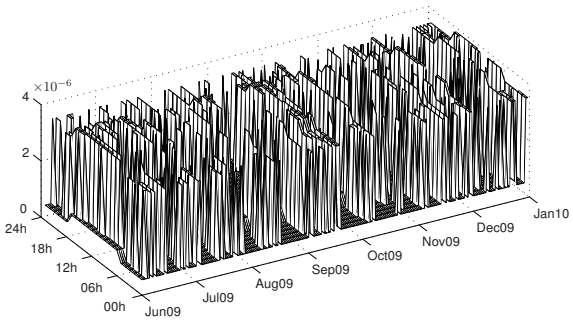
SPG 400kV BB1



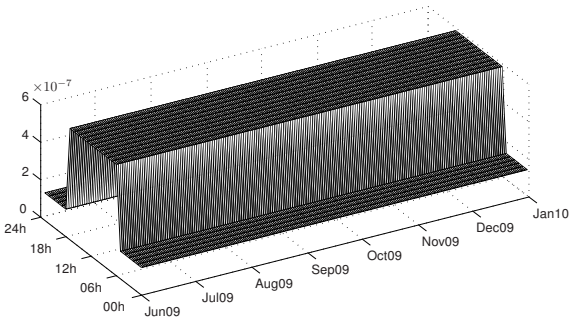
SRA 400kV BB2



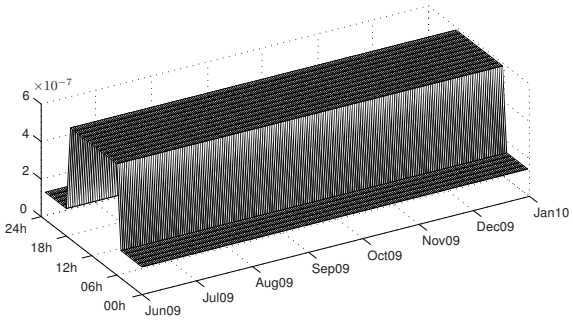
SRA 400kV BB1



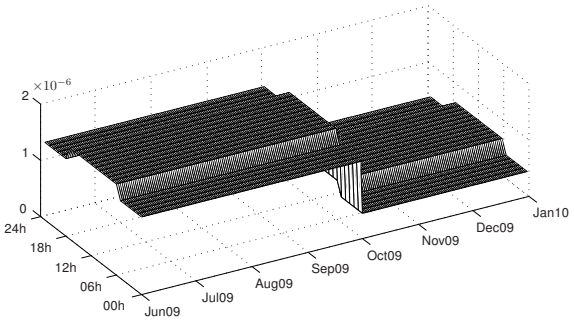
SET 150kV BB2



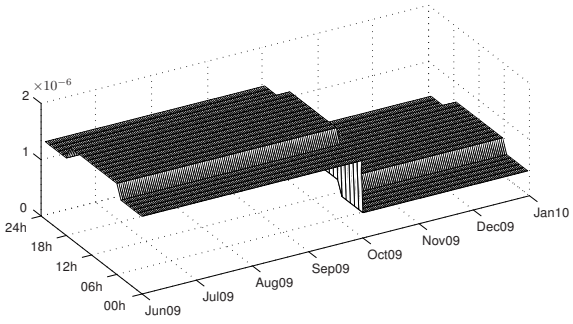
SET 150kV BB1



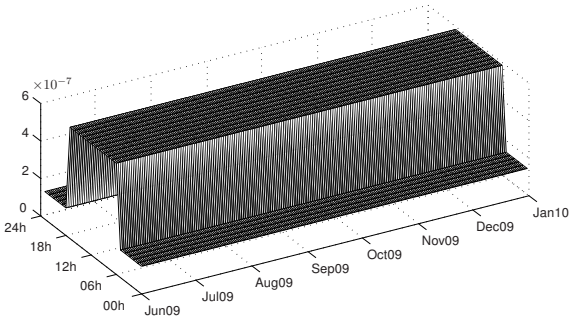
SSV2 220kV BB2



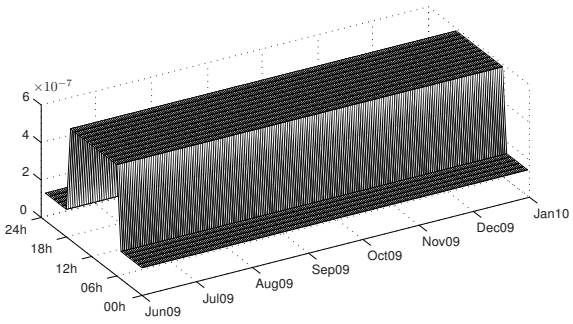
SSV2 220kV BB1



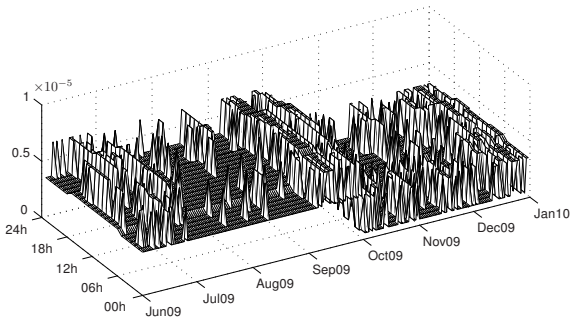
SSN 150kV BB2



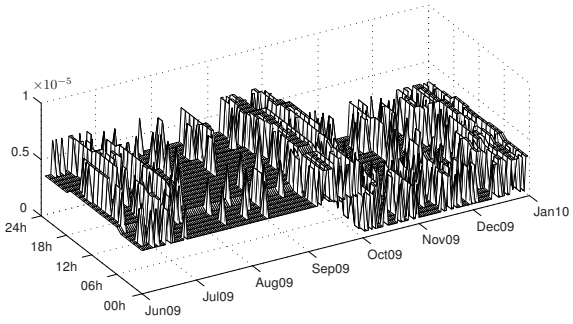
SSN 150kV BB1



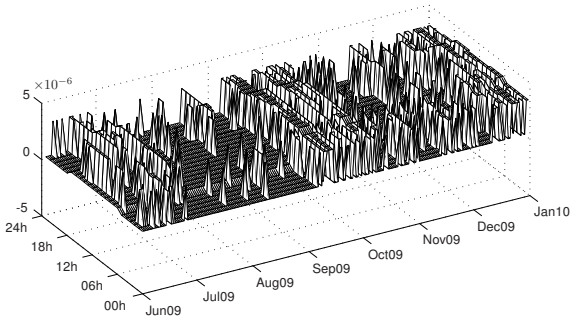
SSN 400kV BB3



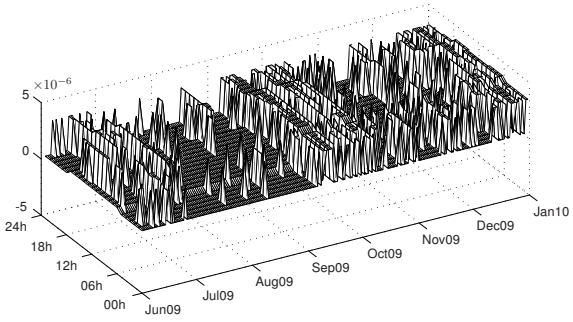
SSN 400kV BB2



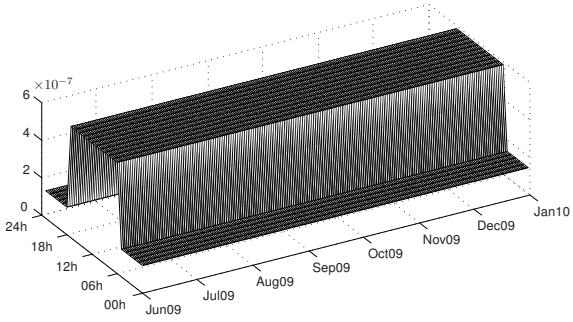
SRM 400kV BB2



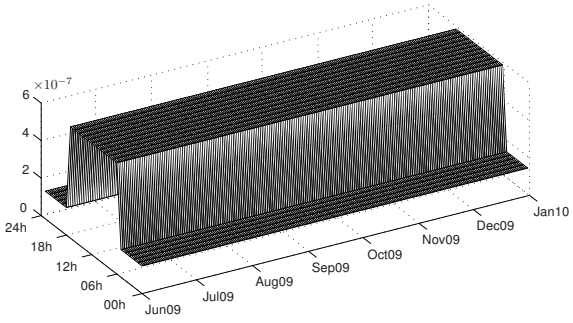
SRM 400kV BB1



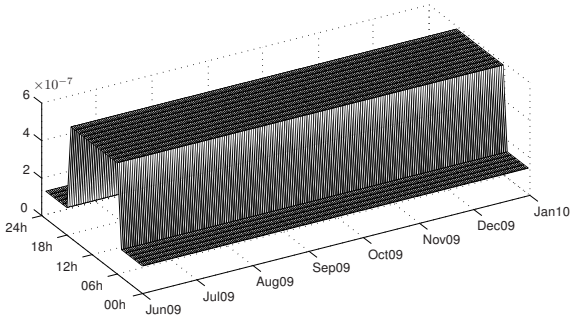
SFR 150kV BB2



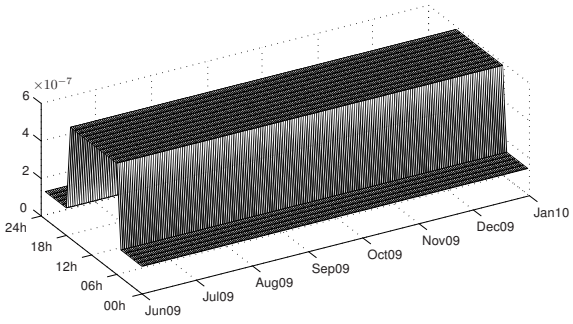
SFR 150kV BB1



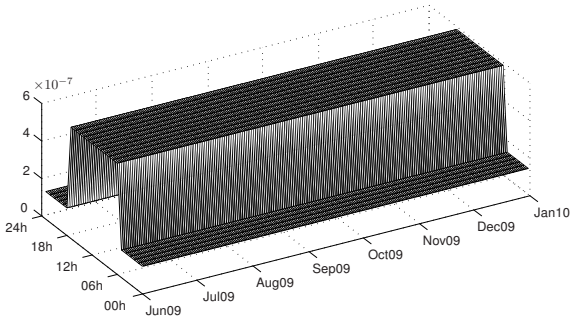
SER 150kV BB2



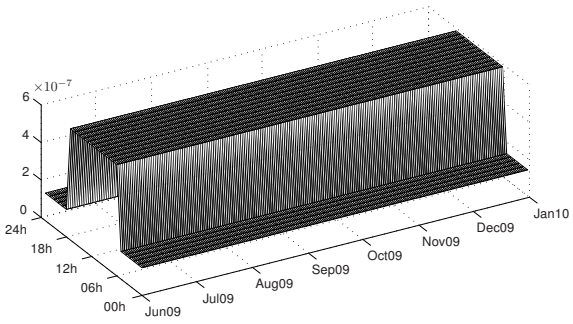
SER 150kV BB1



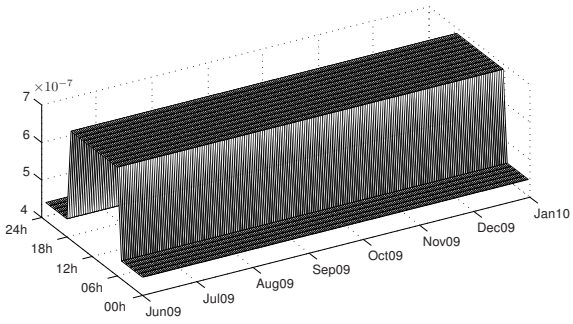
SFF 150kV BB2



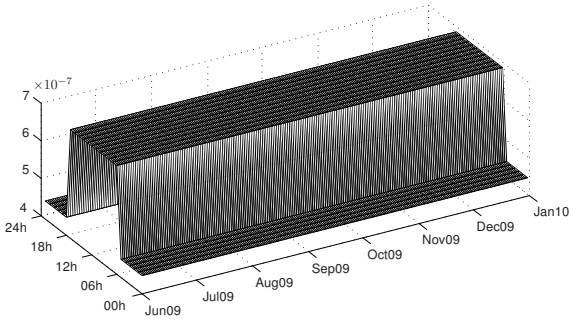
SFF 150kV BB1



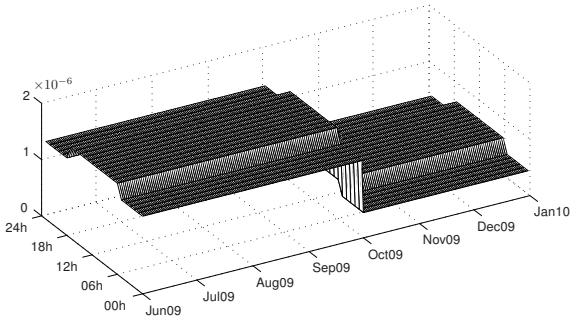
SMC 220kV BB2



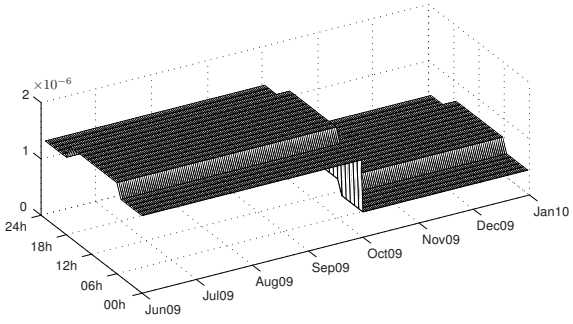
SMC 220kV BB1



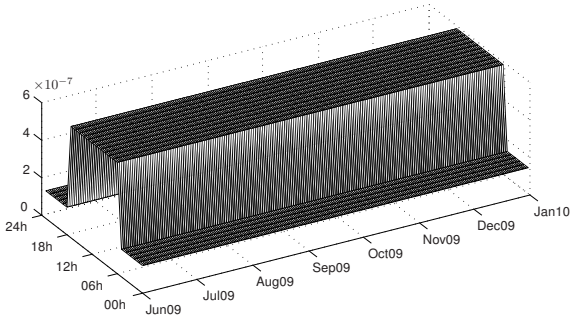
STJ 220kV BB2



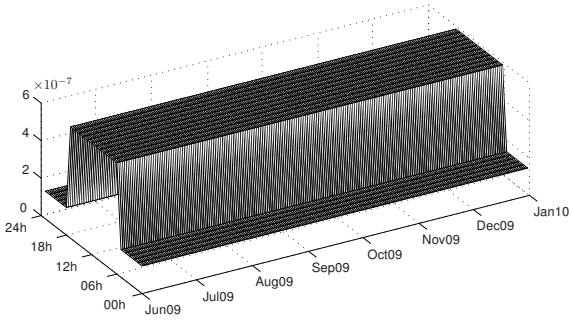
STJ 220kV BB1



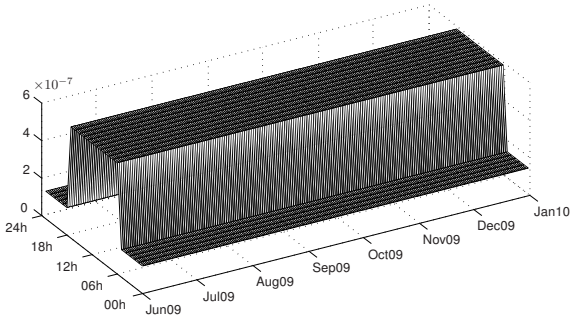
SPA 150kV BB2



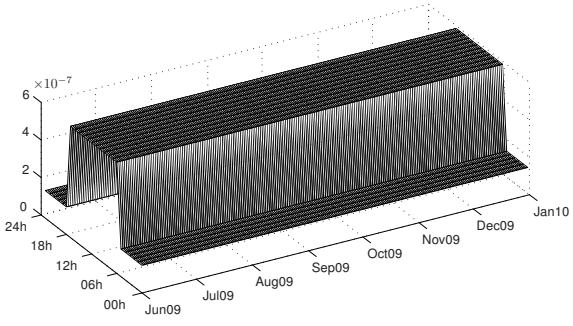
SPA 150kV BB1



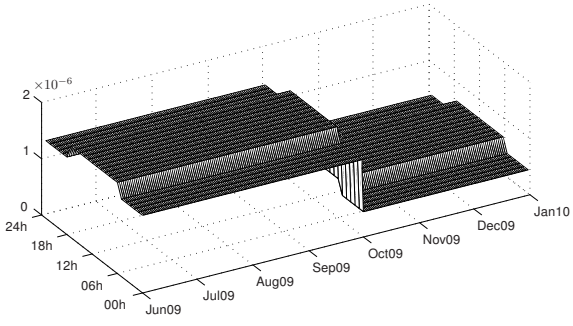
STN 150kV BB2



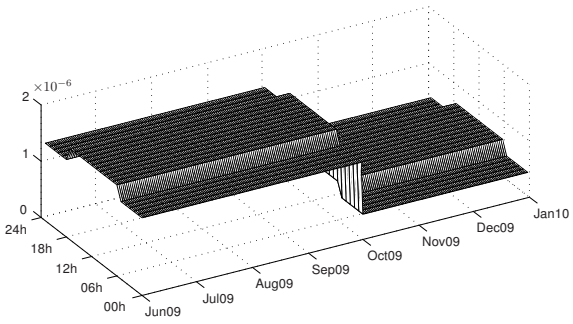
STN 150kV BB1



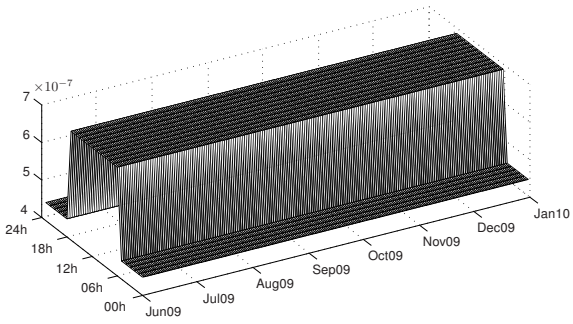
SAM 220kV BB2



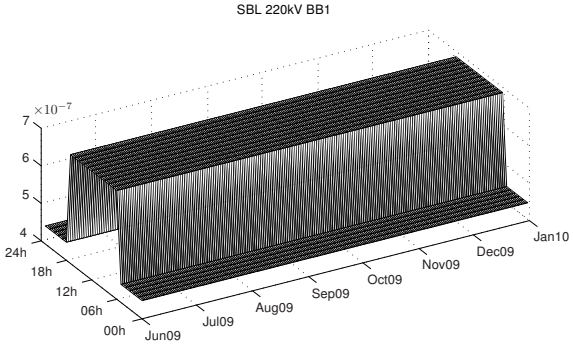
SAM 220kV BB1



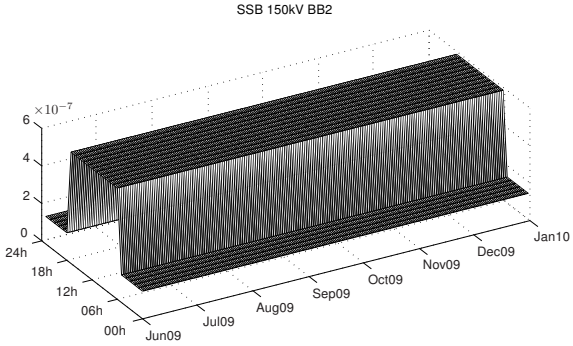
SBL 220kV BB2



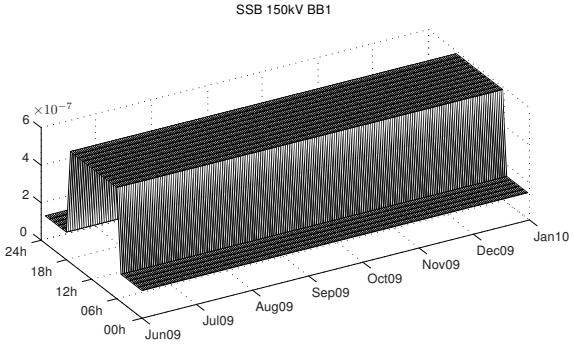
SBL 220kV BB1



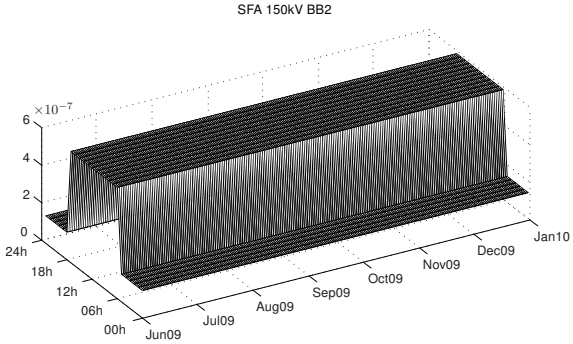
SSB 150kV BB2



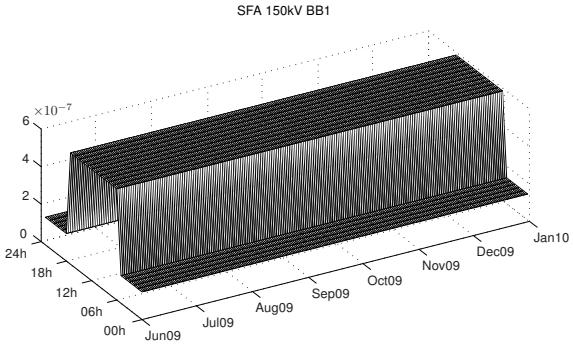
SSB 150kV BB1



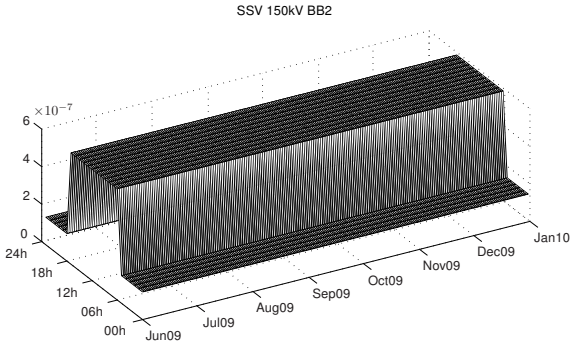
SFA 150kV BB2



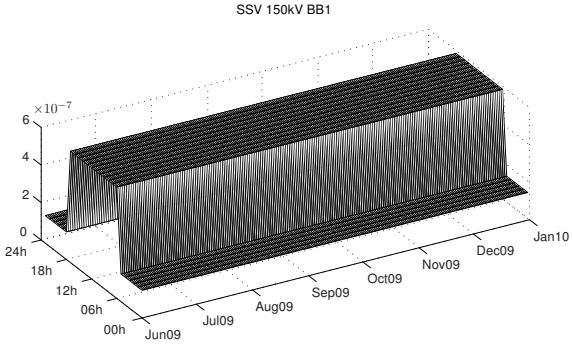
SFA 150kV BB1



SSV 150kV BB2

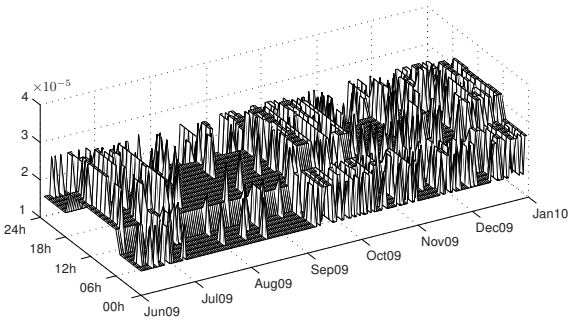


SSV 150kV BB1

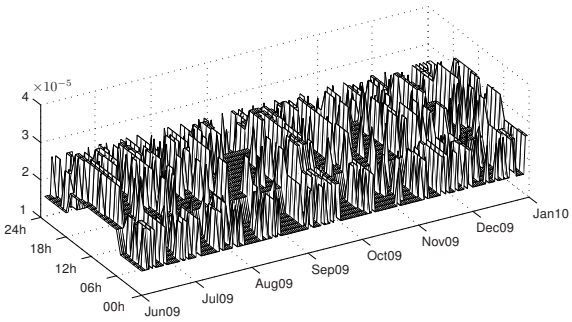


J.3 Transformers

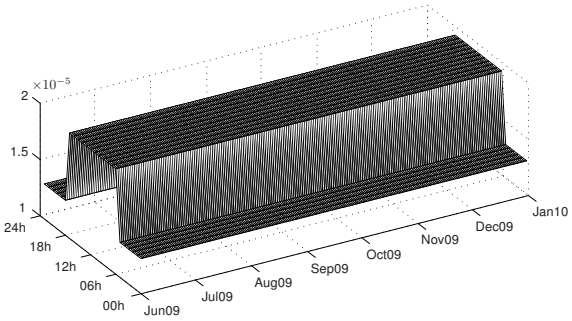
TR 220kV-150kV S



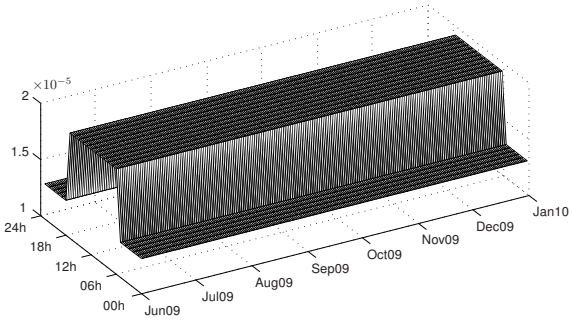
TR 220kV-150kV N



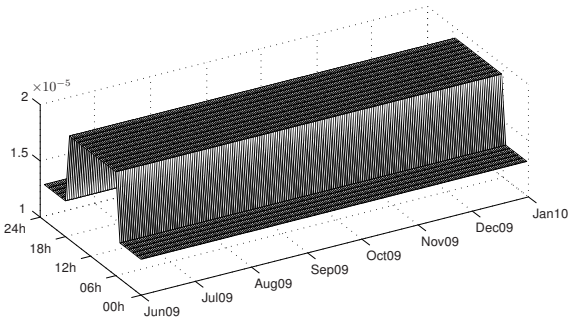
TR 400kV-220kV S



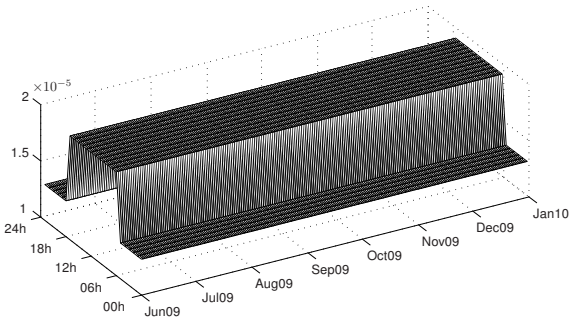
TR 400kV-220kV N



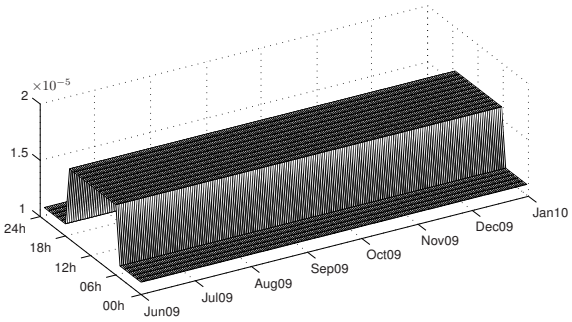
TR 400kV-150kV S



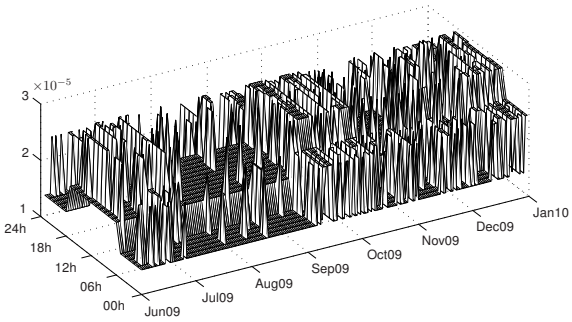
TR 400kV-150kV N

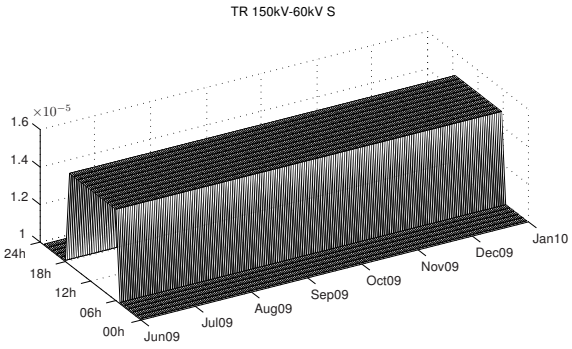


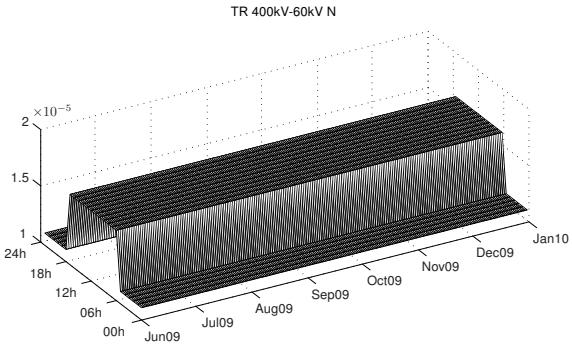
TR 400kV-60kV S

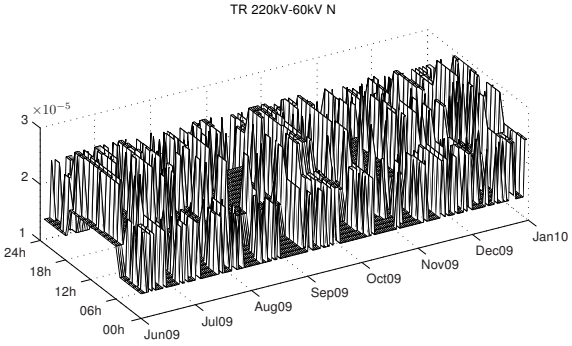


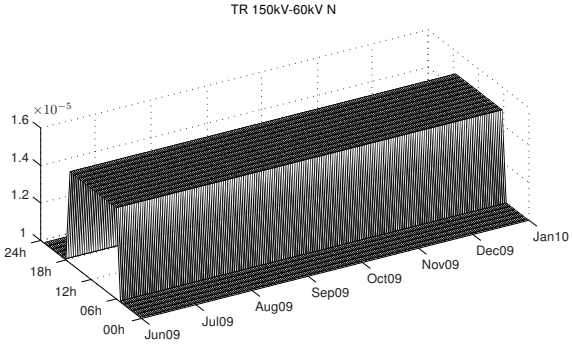
TR 220kV-60kV S



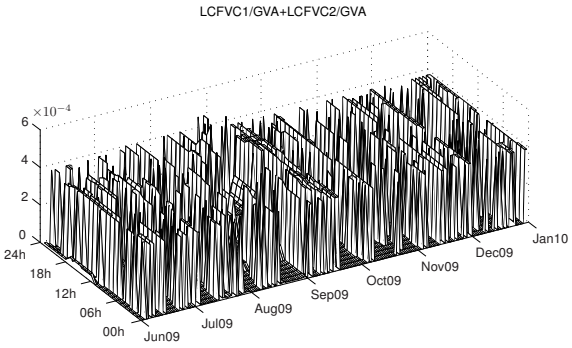


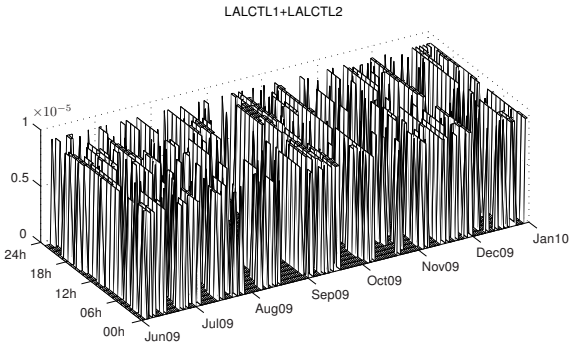


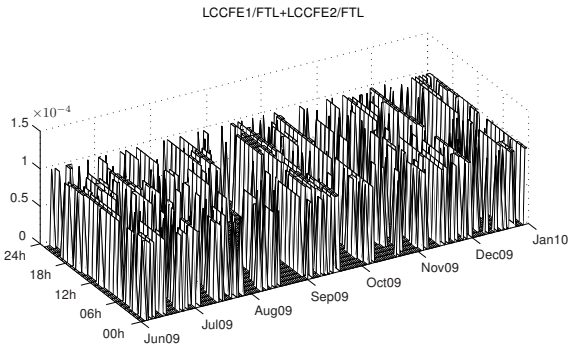


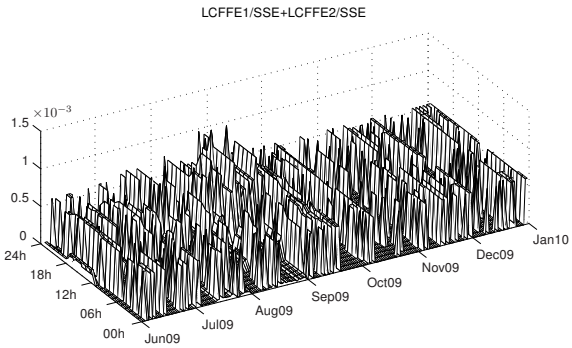


J.4 Overhead lines N-2

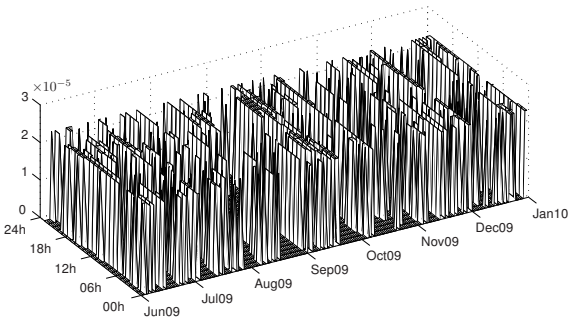




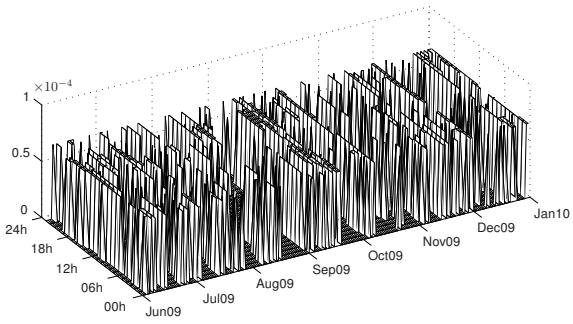




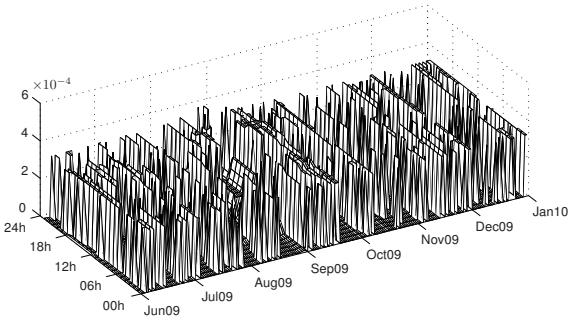
LRRCN3/TG+LTGRR



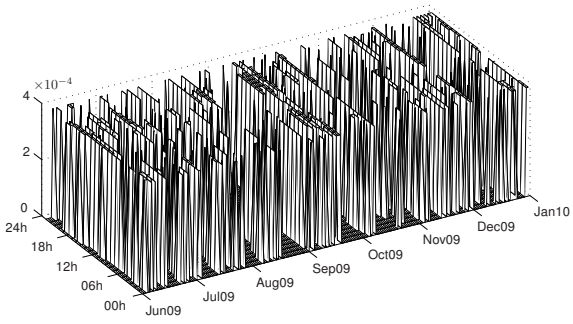
LRRVM1+LRRCT



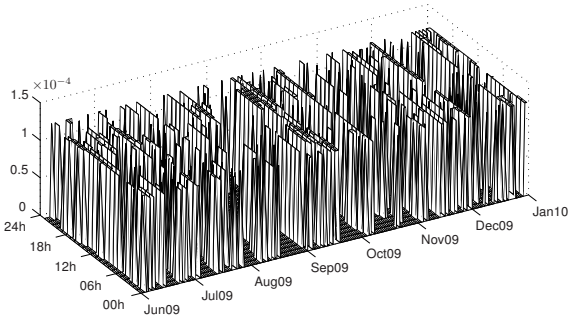
LVGRR1+LVGUR



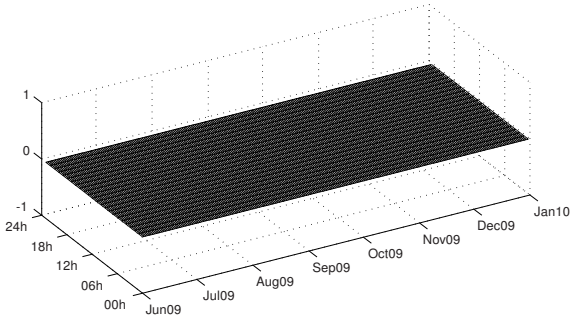
LCLMC+LCLEJ2



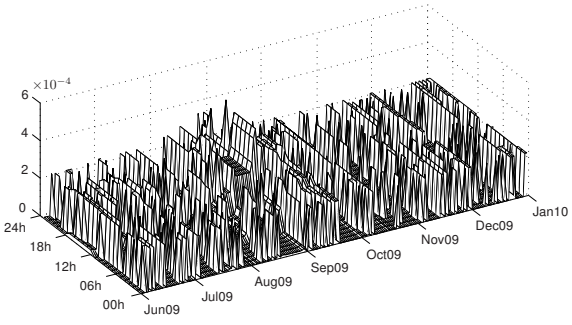
LVRVG1+LVRVG2



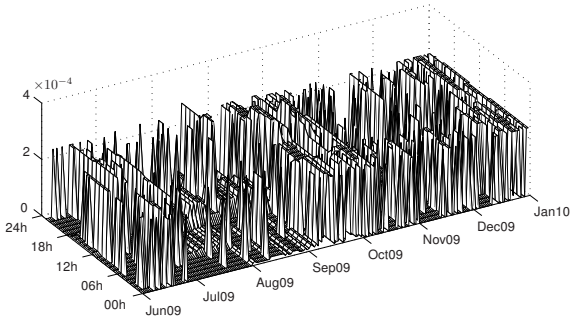
LCGRM2+LCGRM3



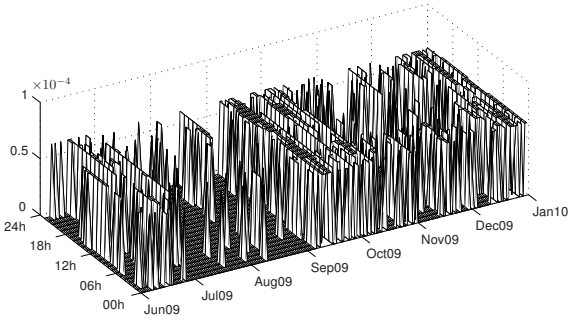
LVGCL2+LVGCL3



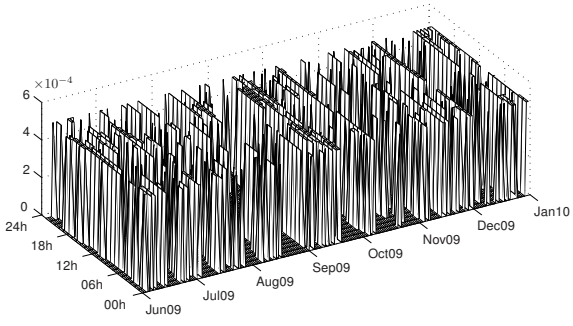
LSNPO2+LSNSI



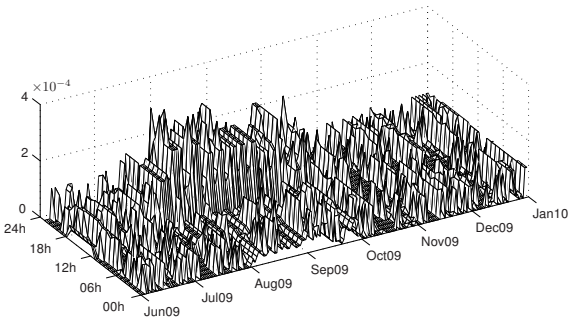
LPOTN1+LPOTN2



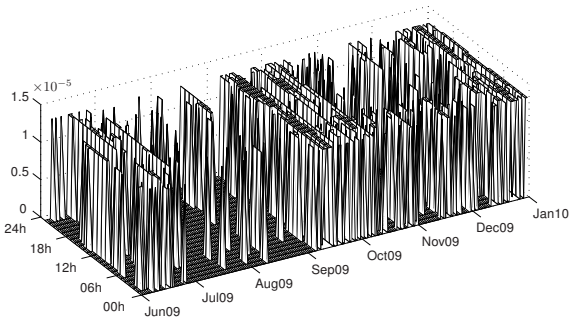
LMDRPDV1+LMDRPDV2



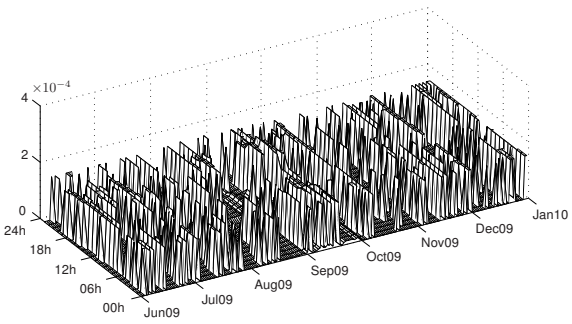
LFRCC1/RDA+LFRCC2/RDA



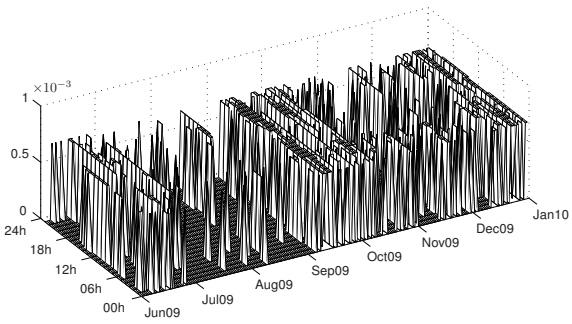
LFFTFR1+LFFTFR2



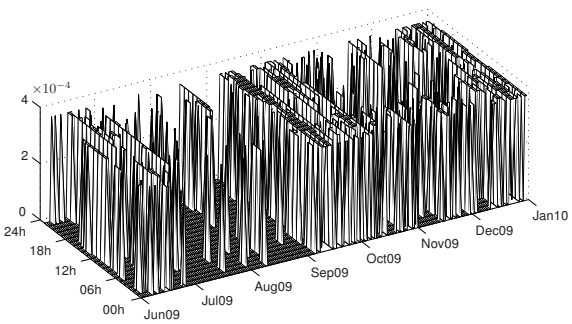
LORVI+LPDVVI



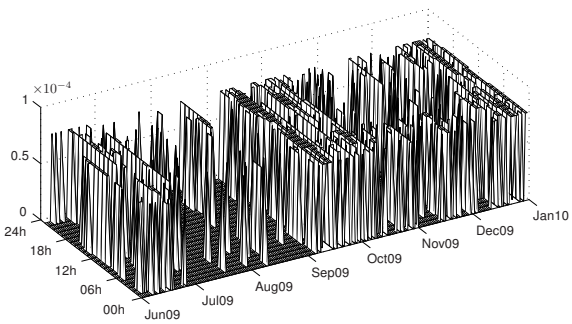
LSNOQ1+LSNOQ2



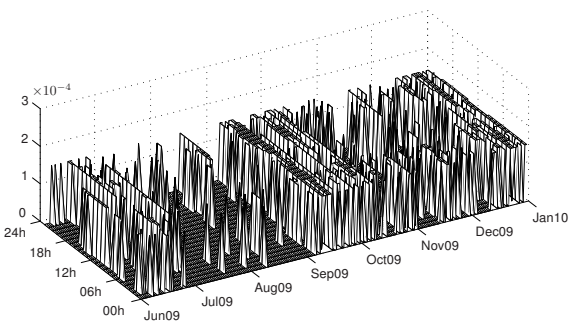
LOQET1+LOQET2



LPMFF4+LFFQAJ



LPMFF1+LPMFF2



J.5 Overhead lines contingency probability results: maximum, minimum and average

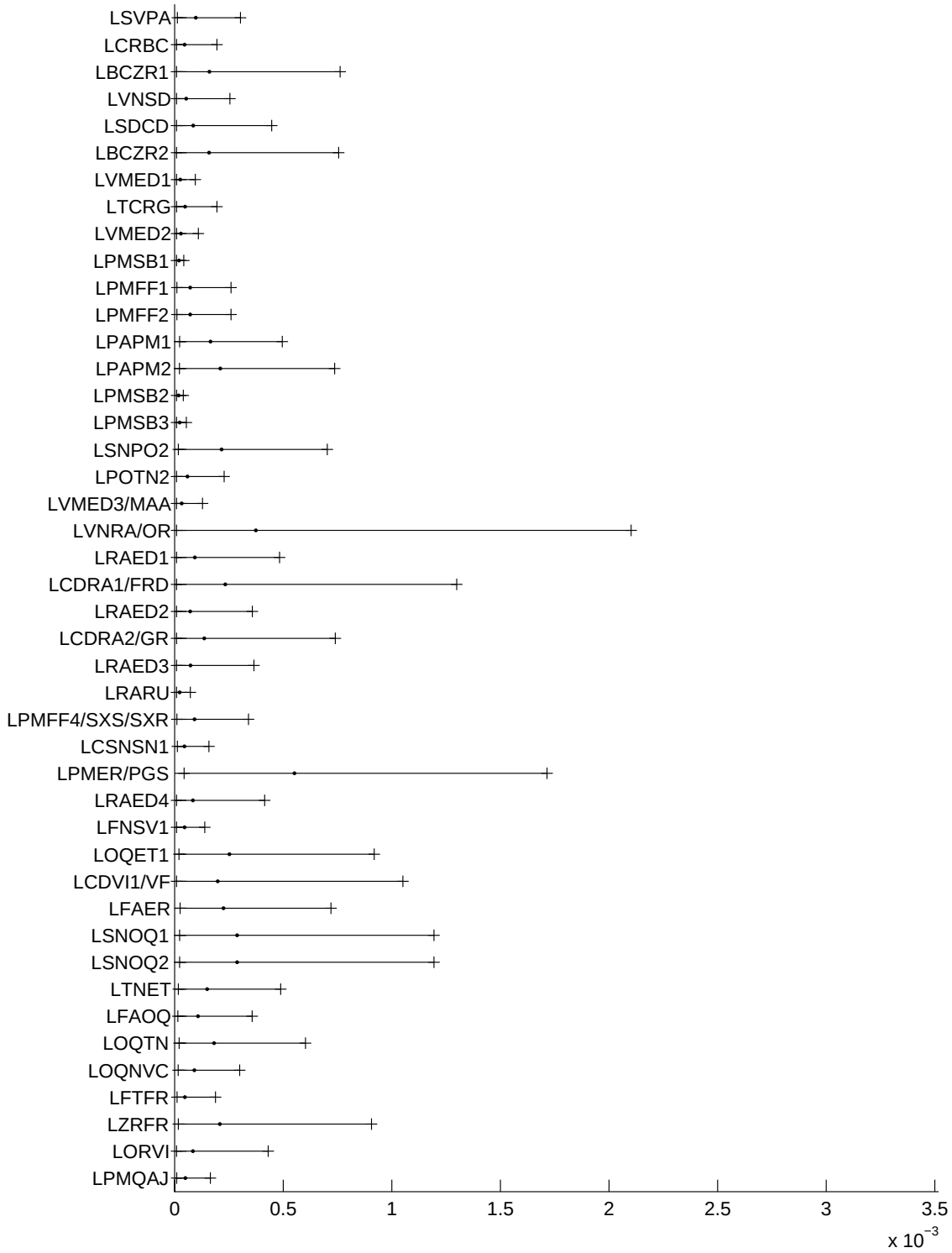


Figure J.1: 150kV overhead line contingency probability results, maximum, minimum and average (1/2).

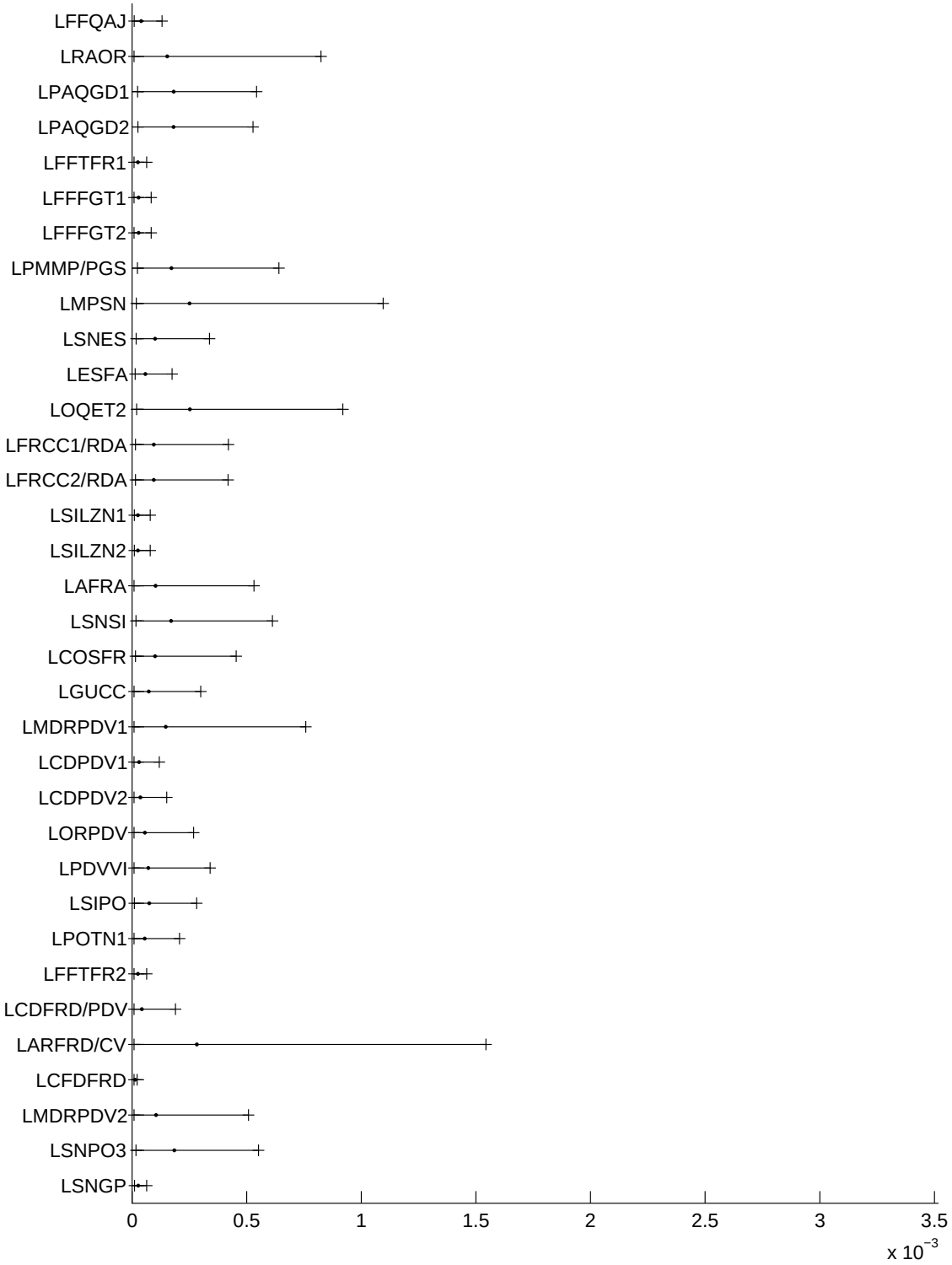


Figure J.2: 150kV overhead line contingency probability results, maximum, minimum and average (2/2).

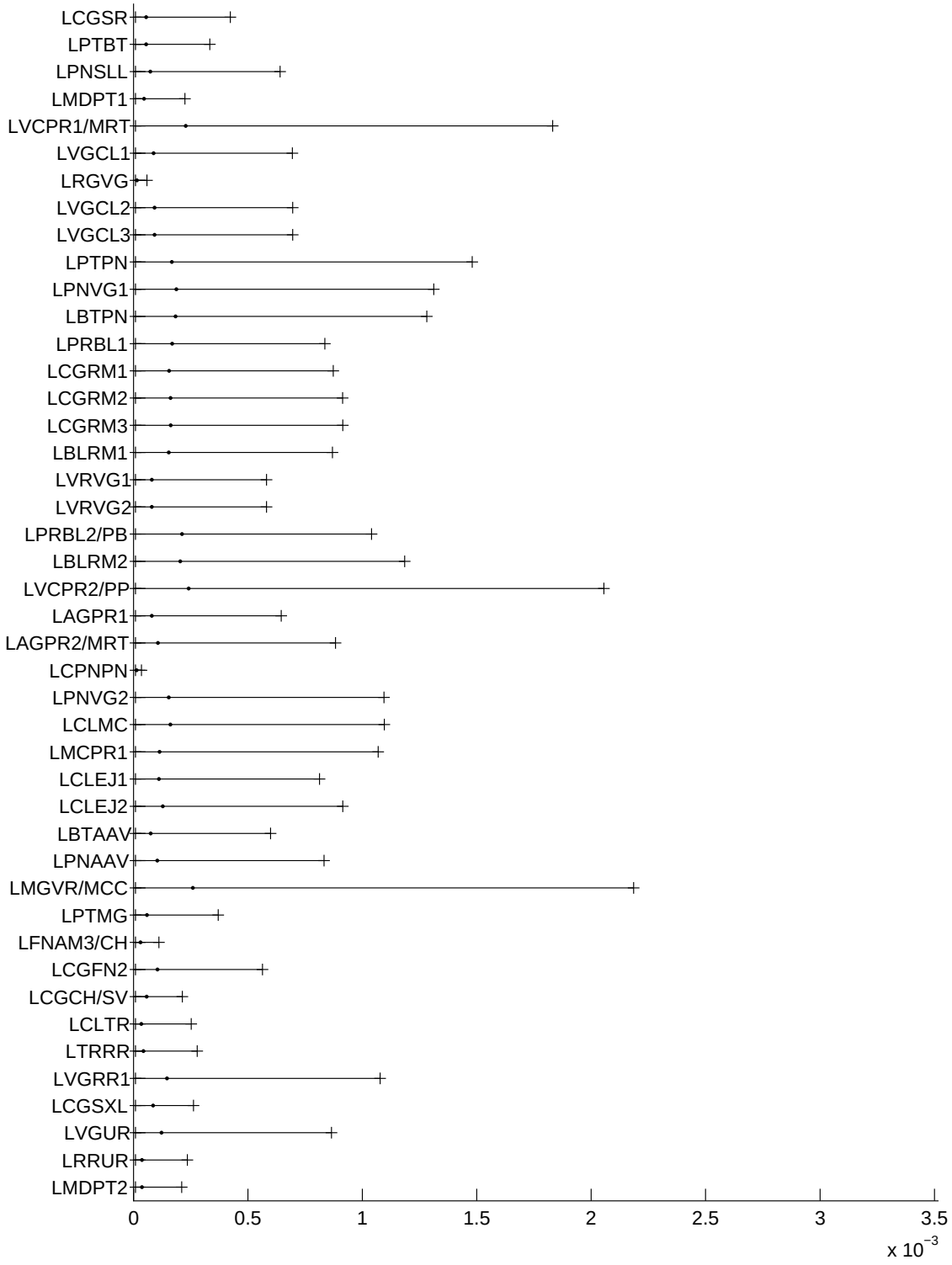


Figure J.3: 220kV overhead line contingency probability results, maximum, minimum and average (1/2).

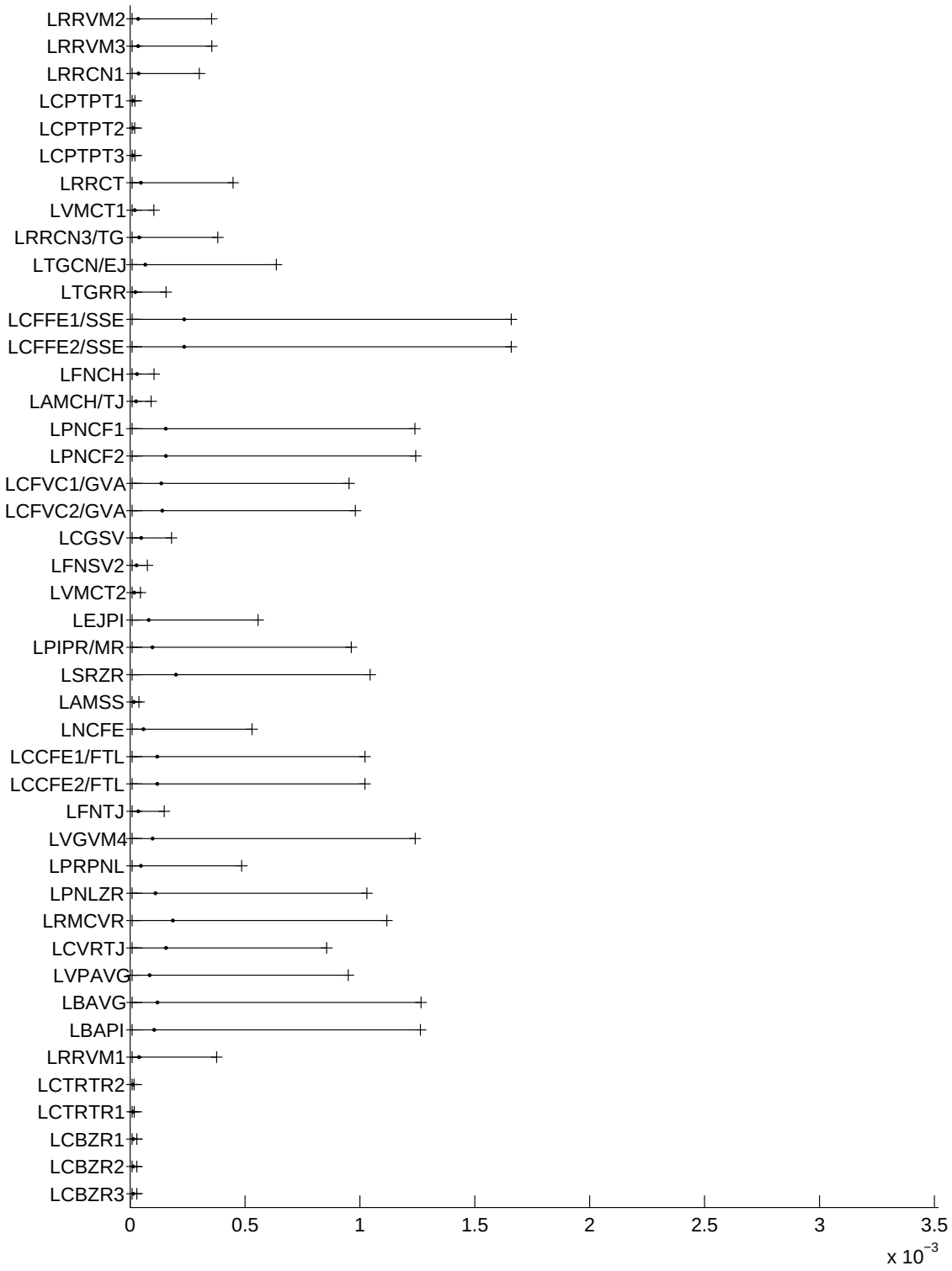


Figure J.4: 220kV overhead line contingency probability results, maximum, minimum and average (2/2).

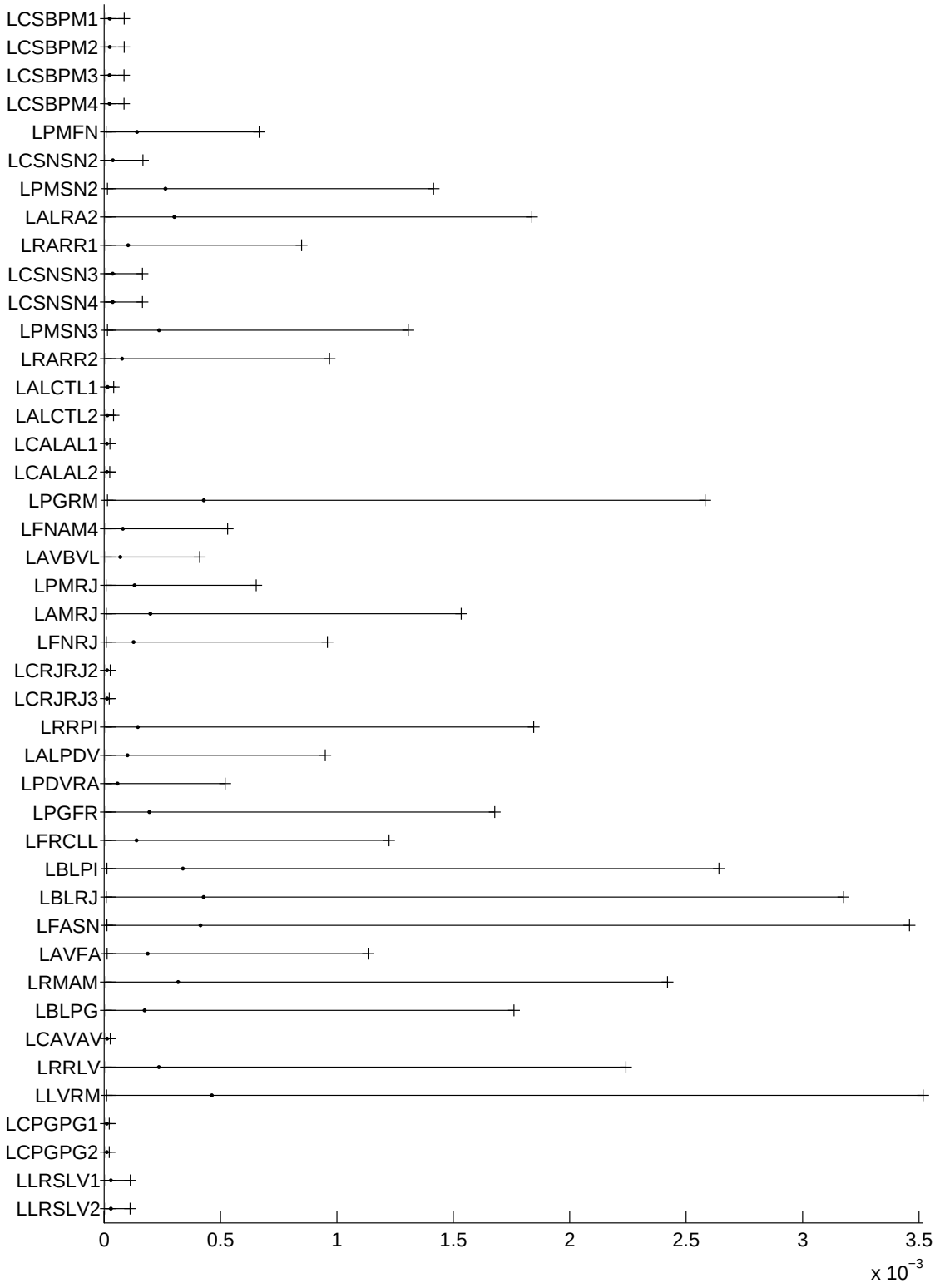


Figure J.5: 400kV overhead line contingency probability results, maximum, minimum and average.