

Integration of Common Cause Faults in the Operational Probabilistic Approach

S. A. B. de Almeida and R. Pestana

System Operator Division
Rede Eléctrica Nacional, S.A. (REN)
Portugal
susana.almeida@ren.pt, rui.pestana@ren.pt

F. P. Maciel Barbosa

Electrical Engineering and Computers
FEUP, INESC Porto
Portugal
fmb@fe.up.pt

Abstract—Transmission system operators have to consider multiple contingencies in the security analysis whenever lightning or active forest fires exist or are expected, in order to be prepared and prevent harmful situations. This paper presents a method to integrate multiple contingencies in the security analysis.

Keywords— β -factor model; common cause faults; failure rates; multiple contingencies; risk assessment; system operation; system security

I. INTRODUCTION

The increasing competitiveness of the power systems' environment has created new challenges regarding security assessment that call for 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 free 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.

References [1-4] present some examples of severe disturbances, which occurred in the recent past. These disturbances have increased the awareness of TSOs for multiple events. During periods of adverse weather or forest fires multiple contingencies have a high likelihood of occurrence. Despite all the efforts being done regarding supervisory practices, operation strategies and protection 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, making incident analysis a crucial activity.

The risk of single and multiple contingencies cannot be neglected and the analysis needs to include local conditions, such as environmental, geographical and geological, e.g. the presence of pollution or storks' population, but also current

conditions, such as adverse weather or risk of forest fires. For on-line risk assessment short-term failure rates are crucial when the security for the next hour is evaluated. Reference [5] gives a very good insight on the operational risk assessment and discusses the external influencing factors and the concept of short-term failure rate developed in this work.

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.

This paper describes an analysis of the occurrence of common cause faults and its integration in the integral risk assessment methodology, presented in Fig. 1.

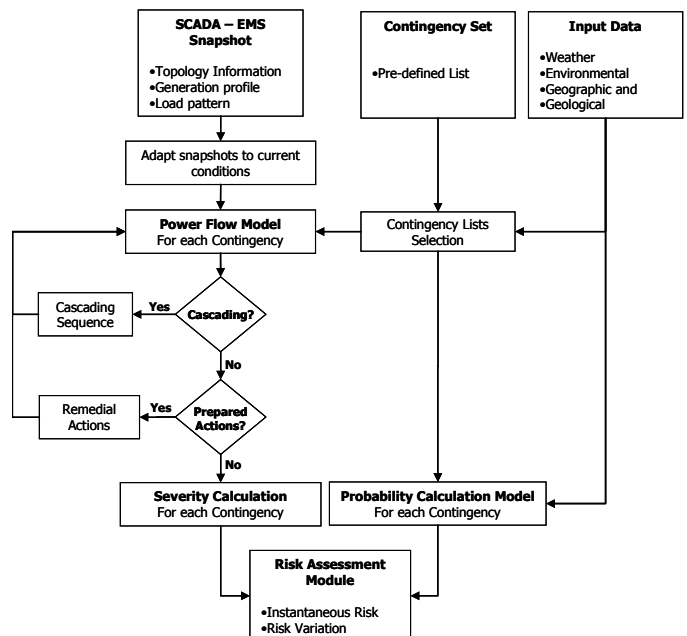


Figure 1. Risk Assessment Methodology Flowchart

II. FAULT HISTORY

The incidents' set of data under analysis is composed by 2337 faults over 8 years, where 2157 are overhead line (OHL)

faults, representing 92% of the total number of faults in the Portuguese Transmission system (PTS). The faults in transformers represent about 7% and in busbars 1% of the total. The most frequent causes for faults in the PTS are storks, forest fires, fog in combination with pollution and lightning, as shown in Table I.

TABLE I. PERCENTAGE OF FAULTS 2001-2008

Incident's cause	% of faults (2001-2008)
Storks	18%
Lightning	24%
Forest Fires	25%
Fog + Pollution	11%
Unknown	7%
Others	15%

These causes affect mainly the circuit part of an overhead line. In addition to these causes, OHL faults can also be caused due to OHL equipment failure or a small group classified in this work as others, which includes trees, other animals, and proximity with external objects (like cranes). For transformers, as well as faults caused by the transformer components, e.g. trip caused by Buchholz relay, also the intrinsic characteristics of the location and the current conditions influence their performance, such as local fauna. Regarding busbar, the main causes of faults are fog associated with pollution within an identified area and internal origin, like equipment, human errors and protection or control system anomalies, which are causes that affect equally the bays associated with other grid elements.

Reference [6] presents an accurate characterization of the incidents' main causes, an analysis of their occurrence and of the intrinsic characteristics of the Portuguese territory, including the mentioned input data, which are crucial for the risk assessment methodology. Due to the fact that several causes are dependent on length and on the intrinsic characteristics across the Portuguese territory, this methodology needs accurate network topology and physical characteristics data, geographical and environmental information, which makes it mainly possible within a TSO structure, where the asset owner and system operator are the same entity.

Faults are mainly independent contingencies, but dependent contingencies may also occur. Thus, we can define two types of faults, namely:

- Independent – faults resulting from different causes and which are not related to each other; they can be single (the majority of faults) or multiple.
- Dependent – faults triggered by the same event, such as common cause contingencies (normally OHL sharing the same tower and path) or 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.

TABLE II. TYPE OF CONTINGENCIES IN THE PTS FROM 2001 TO 2008

Type of contingency	2001	2002	2003	2004	2005	2006	2007	2008
Independent	249	303	288	222	334	222	170	140
Dependent	32	42	42	33	40	36	29	36
Total	281	345	330	255	374	258	199	176

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 shown in Table II, from the 290 dependent contingencies (about 13% of the total), 137 are common cause, which represents about 47%. About 98.5% of the faults caused by lightning affect OHLs and 30% of those are common cause faults. The length of OHL sharing the same tower represents on average 15% of the OHL total length. Table III presents the distribution of dependent contingencies.

TABLE III. TYPE OF CONTINGENCIES IN THE PTS FROM 2001 TO 2008

Type of dependency	2001	2002	2003	2004	2005	2006	2007	2008
Common cause	16	20	27	13	16	15	11	19
Different causes	14	17	6	13	10	8	8	11
Functional dependence	2	5	9	7	14	13	10	6

The increase of the functional dependence of faults is justified with 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 enter in this category.

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 2008, forest fires have only affect simultaneously two OHL, which are normally parallel sharing the same towers and path. 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.

III. RISK OF CONTINGENCIES

The probabilistic assessment has become an important topic for researchers and engineers, because by combining severity and probability it is possible to evaluate the risk of contingencies, as in (1).

$$Risk_i = probability_i \times severity_i \quad (1)$$

where i represents the i^{th} contingency under analysis.

A. Probability of contingencies

The probability of fault occurrence on a line can be modelled using the Poisson distribution with a constant fault rate [7]. Therefore, the probability of fault in the time period t is calculated as in (2).

$$Pr obability\ fault = 1 - e^{-\lambda \cdot t} \quad (2)$$

Where λ is the average failure rate for the considered period and t the duration. If $\lambda t \ll 1$, (2) can be approximately defined 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 [7].

The probability of occurrence of a contingency has to consider the actual and current conditions, identifying which are the areas more expose to failures. The analysis must also include network characteristics, geographical, geological, and environmental and weather data in the calculation, as well as historical fault data. Due to this fact, short-term failure rates are calculated based on location and current conditions, considering lightning real-time data, forest fire risk and meteorological information. This will prevent that the simple use of the historical average failure rate for operational risk assessment will overestimate the risk during periods of normal weather and strongly underestimate the risk during periods of adverse weather. Additional details about the probability of fault calculation for OHL are presented in [8].

B. Severity of Contingencies

The severity of contingencies is assessed in terms of thermal loading, voltage violations and loss of load, considering the pre-defined contingency lists for analysis. Although severity calculations are beyond the scope of this paper, it is worth to mention that multiple contingencies will be included in the analysis under specific circumstances.

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 a credible set of contingencies, the aim is to analyse and evaluate them off-line (some on-line, depending on current conditions), in order to identify suitable preventive and corrective actions to mitigate their consequences in the PTS. The existing lists that are used in the security evaluation are the following:

- List A – The “must run” on-line 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 UCTE 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 35km, and some lines of the neighbouring network that affect the system security (because of interconnection transmission capacity).
- List B – Busbar faults.
- 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 [9].

- List D – Distribution failures (includes closed rings through the distribution 60 kV network and the EHV/60kV transformers, excluding single feeders).
- List E – Extreme (extreme situations were selected that 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).
- 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 groups. The first group is the “must run” list, automatically run on-line for security assessment by the EMS. The second group 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 on-line. The third (“Extreme”) group contains E and F lists, which represent less likely but more severe contingencies, also available for periodical analysis.

For instance, facing an adverse weather situation, such as lightning occurrence, there are several TSOs that also include specific N-2 events in their “must-run” contingencies list, because in these circumstances the likelihood of common cause faults increases. As shown in Table IV, the amount of common cause faults is significant, considering the total amount of faults caused by lightning in the Portuguese Transmission System.

TABLE IV. NUMBER AND TYPES OF FAULTS CAUSED BY LIGHTNING FROM 2001 TO 2008

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

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 IV results strengthen the additional security measures taken by the control room operators, which are influenced by weather conditions and its forecast, where a closer look is taken at N-2 selected contingencies, especially when two lines share the same towers over a long distance (so called double line by UCTE) and permissions to start or continue planned outages are re-evaluated. In addition, special security measures are activated, such as the cancelation of planned outages and the implementation of remedial actions identified as necessary (for instance the implementation of a special topological scheme).

In case of forest fires, the C list is extremely useful when combined with the real-time information of active forest fires in the country and their exact location, because the operator can select only the specific OHL corridors that are actually at risk, making a selective analysis.

C. 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 2008, 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 the 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, because it is assumed that in a time period shorter than one hour the control room operators are normally able to restore n-1 security criteria, independently of the disturbance dimension and extent of the damage.

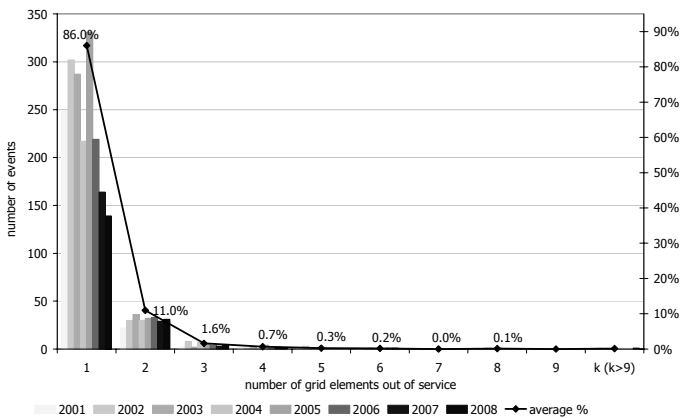


Figure 2. N-k characterization in the PTS incidents from 2001 to 2008

As presented in Fig. 2, N-1 and N-2 contingencies are dominant in the Portuguese transmission grid. The

consideration of N-k where $k > 2$ is mainly relevant in the forest fire season. These situations are included in the contingency lists presented and will be taken into account for severity calculation.

IV. COMMON CAUSE FAULTS

Common cause failures are dependent events; two events A and B are said to be dependent if

$$P(A \cap B) \neq P(A)P(B) \quad (3)$$

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, such as a transformer being single fed by one overhead line or cascading failure caused by over-current after an initiating fault. Extrinsic dependencies refer to an external common cause, such as lightning flash causing a simultaneous fault in two OHL that share the same tower [10]. 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.

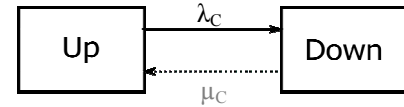


Figure 3. Model for common cause forced outages [7]

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 with the same timeframe. Otherwise, with human intervention the OHLs are reconnected independently and with different response times.

A. 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 Fig. 4.

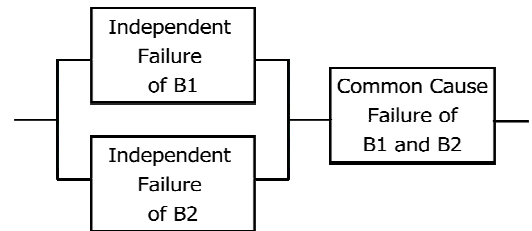


Figure 4. Reliability block diagram for CCF events

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 (4) and λ_C and λ_I are calculated as in (5) and (6), respectively.

$$\beta = \lambda_C / \lambda_T \quad (4)$$

$$\lambda_C = \beta \lambda_T \quad (5)$$

$$\lambda_I = (1 - \beta) \lambda_T \quad (6)$$

The failure probability of the two parallel components B1 and B2, considering both independent and common cause faults, is calculated as in (7).

$$Q_s = (\lambda_I t)^2 + (\lambda_C t) \quad (7)$$

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.

A point estimate for β presented in (4) is given by (8) [10].

$$\beta = 2n_1 / (n_1 + 2n_2) \quad (8)$$

where: n_1 = number of independent failures and n_2 = number of common cause failures.

For only common cause faults that affect two identical grid elements, $\lambda_C t$ is used to calculate the probability of occurrence which will be multiplied by the respective severity to obtain the risk of the specific contingency.

V. COMMON CAUSE PROBABILITY 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 fault to 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 path, which can be considered identical components having the same failure rate, which is true for the OHL that mainly trip because of faults caused by lightning. For OHLs that only share part of the total path, 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 developed by CIGRE [11]. This method uses a large amount of information to calculate the BFR, such as tower geometry, tower footing resistance, insulation level, conductor diameter, geographical and geological information, among others. Hence, parallel OHLs have exactly the same BFR value.

TABLE V. COMMON CAUSE FAILURE RATE RESULTS PER YEAR

OHL Codes	U(kV)	λ_T (BFR) per year	N° of CCF per year	β	λ_C per year
1041+1042	150	0.1978	0.33	1	0.1978
1079+1105	150	0.9958	0.67	0.89	0.8851
1116+1134	150	0.6505	2	1	0.6505
2021+2022	220	0.2975	0.5	1	0.2975
2044+2045	220	0.1612	0.33	1	0.1612
2124+2125	220	0.9238	0.5	0.86	0.7918

Table V presents some results for the common cause failure rate; from them it is possible to conclude that there are some

OHLs for which the only common cause contingencies are due to lightning. In the 400 kV voltage level there are no OHLs sharing the same towers and, consequently, no common cause faults due to lightning.

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 a probability of lightning. In case of one of the parallel OHLs with more independent faults than the other, but the same number of common cause faults, the maximum of the λ_C is used. Assuming that for N-2 only common cause faults occur, the probability of the common cause occurrence will be $\lambda_C t$.

In 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) [8]. Corridors can be affected quasi-simultaneously by forest fires, causing N-k 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 do 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.

However, often within an interval of a few minutes, more than 3 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. 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 SCADA snapshots where OHLs of corridors were already disconnected by previous faults with the same cause.

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.

VI. CONCLUSIONS

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 path. Another possible origin of common cause faults is forest fires affecting a corridor composed by several OHLs [9].

The β -factor model has proven to be adequate to address the N-2 contingencies caused by lightning, because most of the

OHLs, which share the same towers within the same path, mainly 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, one or two OHLs are normally affected at the same time. After analysing the characteristics of the N-2 contingencies, it was possible to conclude that it mainly affects parallel OHLs, making the β -factor model suitable. For faults caused by forest fires that affect simultaneously entire corridors (N-k with k=3 or 4), the number of faults per year (or per hour for short-term analysis) in each corridor is calculated, although in the period under analysis they have never occurred.

Within an interval of a few minutes, the same forest fire can affect more than 3 OHLs and typically 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 but without any defined sequence and the best approach for analysis is to use the probability of N-1 and N-2 events caused by forest fires and to simulate severity every few minutes, using SCADA snapshots, where OHLs of corridors were already disconnected by previous faults with the same cause. Thus, the severity will reflect the consequences of an N-k event.

Common cause failure rates are needed when assessing the risk of multiple contingencies, in order to calculate the probability of occurrence.

This paper presents a small part of an integral risk assessment methodology that aims to provide control room operators with risk-based security indices for the subsequent time period (such as 1 hour), allowing them to react in advance and to be aware of inherent risks, preventing harmful situations. These indices combine probability and severity for each contingency. The probabilistic part of the developed methodology takes into account the effect of frequency of faults, local conditions and current conditions, such as 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. 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. Using (1), it is possible to calculate for each contingency the risk per type of impact.

In risk assessment methodology, single and double contingencies are analysed, because they occur frequently in the transmission system. The β -factor model is used to calculate the common cause failure rate for N-2 contingencies that are often caused by lightning and forest fires in parallel-running OHLs.

REFERENCES

- [1] UCTE - Union for the Coordination of Transmission of Electricity, "Final Report - System Disturbance on 4 November 2006," 30th of January 2007.
- [2] 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.
- [3] J. Amarante dos Santos, "Revisiting the Blackout in Southern Portugal in 9th of May 2000," in Cigré Workshop on Large Disturbances Paris, 2002.
- [4] 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.
- [5] 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, 2008.
- [6] S. A. B. de Almeida, R. Pestana, and 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 *Proceedings of EEM09*, Leuven - Belgium, 2009.
- [7] W. Li, *Risk Assessment of Power Systems - Models, Methods, and Applications*: IEEE Press Series on Power Engineering, 2005.
- [8] De Almeida, S. A. B., Pestana, R., Maciel Barbosa, F.P., "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.
- [9] S. A. B. de Almeida, F. M. Barbosa, and R. Pestana, "Severe Contingencies Analysis In Portuguese Transmission System," in *UPEC2006 - 41st International Universities Power Engineering Conference* Northumbria University - Newcastle - UK, 2006.
- [10] NASA, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, version 1.1, pp. 166-171, August, 2002.
- [11] CIGRE WG 01 of Study Committee 33, "Guide to procedures for estimating the lightning performance of transmission lines," CIGRE, 1991.