XI SEPOPE
17 a 20 de Março 2009
March – 17th to 20th – 2009
BELÉM (PA) - BRASIL

XI SIMPÓSIO DE ESPECIALISTAS EM PLANEJAMENTO DA OPERAÇÃO E EXPANSÃO ELÉTRICA

XI SYMPOSIUM OF SPECIALISTS IN ELECTRIC OPERATIONAL AND EXPANSION PLANNING

Probabilistic Risk Assessment of Large Electric Power Plants: A Case Study

Iony Patriota de Siqueira[1]

CHESF

Brazil

SUMMARY

This paper presents a probabilistic methodology to assess risks of major accidents on large electric power plants. Major accidents are those resulting on complete loss or impediment of any high voltage unit, with consequent operational and/or economic hazards, or human injuries to operating personnel or customers. A top-down, systematic approach is proposed, so that It can be applied to any high voltage installation. The method was tested on a large substation owned by CHESF (Companhia Hidro Elétrica do São Francisco), supplier of electricity to a major metropolitan area in the Northeast of Brazil. With minor changes, the method can be applied to many other process industries.

KEYWORDS

Probabilistic Risk Assessment, Accidents.

1. Introduction

Risk assessment of large electrical installations traditionally has been a difficult task due to its complexity, and inadequacy or lack of statistical data on the behaviour of electrical equipment. Lack of maintenance history forces risk managers to adopt ad-hoc methods such as intuition and empirical criteria, personal judgment, technical agreement among utilities, manufacturer advice or insurance company policies. Although many risk indexes may be regularly gauged, few of them are statistically correlated to managerial risk decisions, making adequacy of these methods difficult dto assess. Moreover, it is impossible to objectively evaluate, with current practices, the influence of risk on company mission and more important, to appraise its cost and worth for utility customers.

2. Definitions

The following definition will be used in this paper: Risk is a measure of the extent of danger, evaluated by correlating the frequency or probability of undesirable events to their effects or

[1] Iony Patriota de Siqueira, E-mail: iony@tecnix.com.br, Tel: +55 81 32294145

consequences. If the consequences can be expressed numerically, and the events are statistically independent, risk can be evaluated by the expression:

$$R = \sum_{i \in S} F_i x C_i$$

where F_i is the frequency of event i, C_i its consequence, and the sum is taken over the set of relevant events S. If C_i is measured in monetary term, then R will be the expected cost flow from accidents on the plant. If the events do not occur individually, but are statistically correlated or dependent, more elaborate expressions must be considered, derived from a fault tree of the process. The choice of undesirable events and their effects is strongly dependent on the concern of the risk analyst. Usually, relevant events are chosen from those that cause relevant changes on the consequences of interest. These can be a human (injury, illness, deaths), economic (revenue losses, capital expenditures) or environmental (on flora, fauna and ecosystems), etc.

3. Methodology

A methodology is proposed in this paper, to assess risks in electric power plants, comprising the following steps: (1) definitions of risk levels and failure modes of electric substations; (2) plant partitioning and zoning of large stations for risk analysis; (3) identification of automated protection systems; (4) probabilistic modelling of equipment and protection schemes; (5) estimation of consequences for each failure mode; (6) calculation and identification of risky areas for a real substation; (7) recommendations of maintenance and protective policies to reduce risk. These steps are summarized on Figure 1, making explicit the role played by protective apparatus.

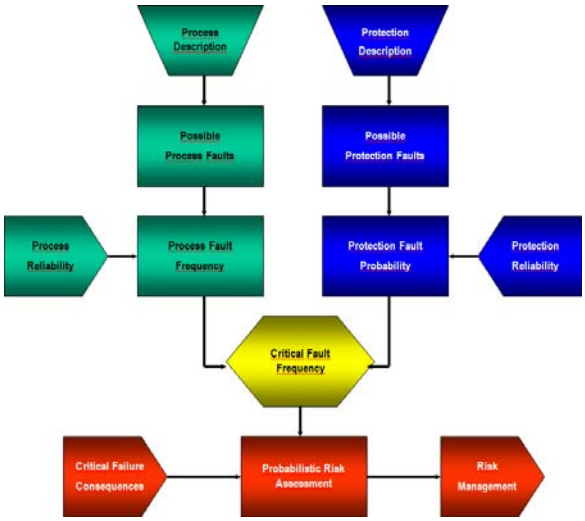

Figure 1 – Probabilistic Risk Assessment

4. Plant Description

Large electric power plants have evolved, dictated mainly by economic and technological factors. Huge installations, with large capacity transformers, generators and transmission lines are built and interconnected by Very High and Ultra High Voltage networks, spanning extensive geographical areas. This trend has increased the chances and consequences of major accidents, with large impacts on the economy, environment and human beings. Figure 2 shows a one-line diagram of Recife II power Plant, a large transmission station owned by Companhia Hidro Elétrica do são Francisco (CHESF), located on the metropolitan area of Recife, the state capital of Pernambuco, Brazil. It will be used to illustrate the approach of this paper. A short-circuit capacity of 7 GVA on its 500kV bus is a measure of the destructive power liberated by this plant during a primary fault.

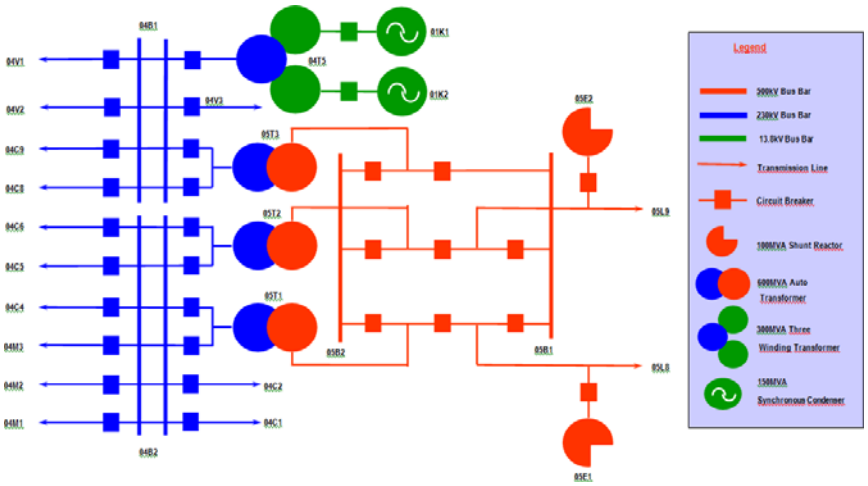

Figure 2 – Recife II Power Plant

5. Partitioning and Risk Zoning

To avail the risk in a station, it is necessary to identify the parts subject to failure or damage. In this respect, it is instructive to partition the plant into zones amenable to isolation in case of accident. Isolation is achieved by circuit breakers, shown as small squares on Figure 2. This criteria corresponds roughly to the range and setting of primary protective apparatus, with tripping acting on the delimiting breakers. These zones are shown on Figure 3.

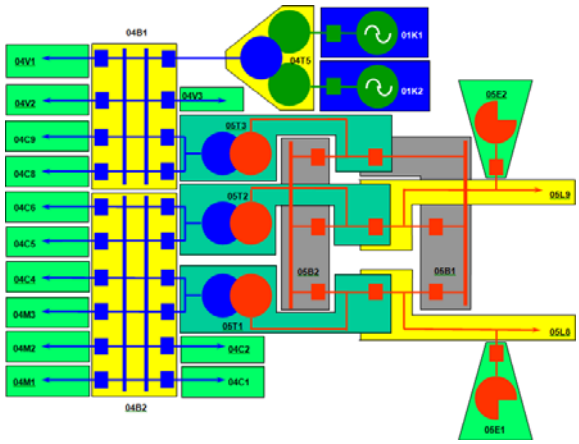

Figure 3 – Recife II Protection Zones

Note the intentional overlapping of some zones to protect also the circuit breakers. Each major unit or protected zone is monitored by a set of relays and instrument transformers that act on its breakers. Ideally, each zone should be delimited by its own breakers, to allow isolation from others in case of defect. Cost reduction may dictate a topology different from this criterion. As shown on Figure 3, it is a good practice to overlap adjacent zones in order to avoid dead spaces, or zones not monitored by at least a primary protection. Figure 4 is an engineering drawing of the protection systems of Recife II station. Note the instrument transformers and protective apparatus, and how they are connected. Note also how zone overlapping is achieved by crossing current transformers of adjacent units. Although not shown, most protective devices are duplicated on the 500kV units, to increase their reliability. Trip paths from the relays to each breaker are omitted to avoid cluttering the figure.

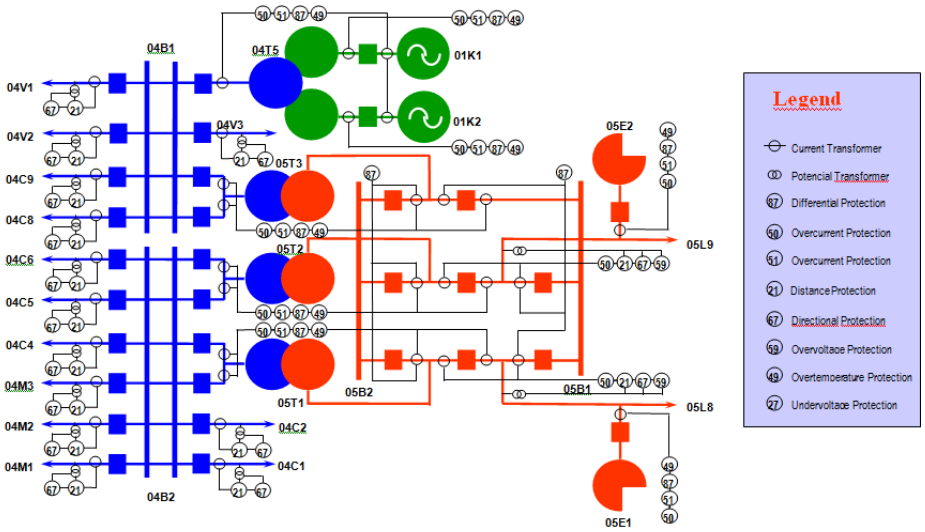

Figure 4 – Recife II Protection System

6. Risk Levels and Failure Modes

Two main sources of failures may originate in a power station: primary faults on the high voltage equipment or secondary faults on auxiliary, control and protection equipment. High voltage systems may fail due to natural loss of isolation or accidental (human or natural) events, conducting, mainly, to short-circuits. Due to the high voltage used, these faults may spark large short-circuit capacities, resulting on the uncontrolled liberation of huge amounts of energy (7 GVA in this case). This liberation, besides their intrinsic destructive power, may act as the ignition or source of heat for fires or explosions. On the other side, automatic protection systems may fail due to internal defects in relays, instrument transformers, circuit breakers, power and auxiliary circuits. To minimize risk, it is an industry practice to protect each equipment by a second set of relays, known as secondary protection, usually used also as primary protection of adjacent equipment and near stations. To increase security, normally they act on different circuit breakers then the primary protection. Each unit has as many backup protections as there are adjacent units or substations, from which there is an electric path to a source of power. These concepts allow us to draw the main event tree for a critical failure in a power station (Figure 5). Starting from the inception of a primary fault, defined as the first level of failure, it is possible to limit the danger and risk to a unit failure, by the action of its primary protection, isolating just the faulted unit. Upon refusal of primary protection, consequences may evolve to a plant failure, with disconnection of the complete plant or a large part of it, tripped by backup protection. Simultaneous failure of primary and backup protection will result on a critical failure, probably with complete loss of the faulted equipment, and interruption of electricity to a larger regional area. Remote protection or manual intervention will be necessary to interrupt the source of short-circuit power to the faulted station. Lacking of automatic interruption will submit many units to stress, during the time taken by human actions to isolate the fault. Usually, these events are followed by a disruption of the entire power system, with serious social consequences.

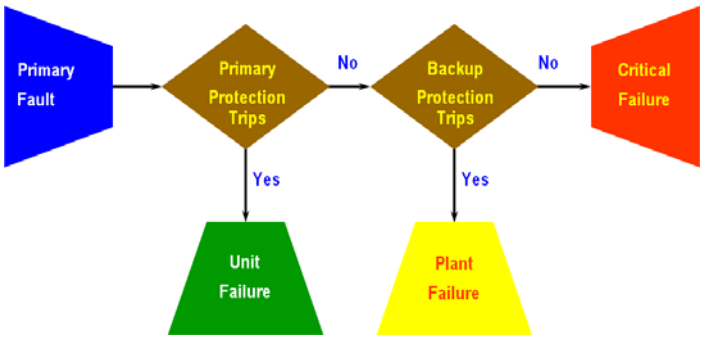

Figure 5 – Plant Failure Levels and Event Tree

7. Plant Failure Tree

Having defined the concept of critical failure, it is possible to start the construction of the failure tree for the whole station. To this end, this paper proposes a top down approach, where the main event, identified as a catastrophic plant failure, is defined as the occurrence of any critical failure on any of its units. This definition is coherent with the concept of a catastrophe, as the energy and station will be out of control, by automatic means, according to the definition of critical failures. To illustrate this method, Figure 6 shows just the top of Recife II failure tree. Note that the topmost event, a catastrophic plant failure, is composed in the next level by all possible critical failures in the station. There are as many critical failure modes as there are units on the station, that is, 27 high voltage units on this example. These events are identified by the operating code of each unit, as shown on previous pictures.

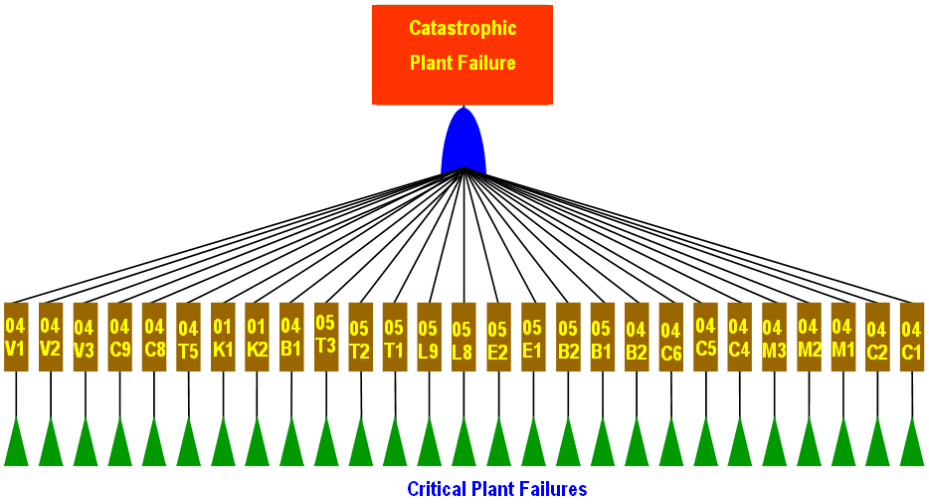

Figure 6 – Recife II Failure Tree

To further detail the plant failure tree, it is necessary to expand each critical failure into its constituent failure modes. This resumes to the elicitation of a sub tree for each critical failure, that is, 27 small trees for the case example. According to its definition, a critical failure in a unit is characterized by the simultaneous occurrence of an internal fault event on the unit, followed by its main protection failure, and any backup protection failure of any adjacent unit. This logic can be translated on a typical failure tree for each unit, shown on Figure 7.

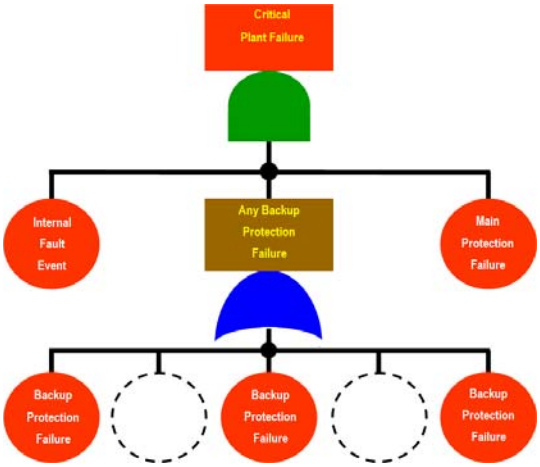

Figure 7 – Critical Failure Tree

Note that this tree will have as many leaves as there are backup protection on adjacent units or near stations, depending on the system topology and adjustment of protection systems. The setting of each relay system and its trip path determine which protective apparatus acts as backup protection for each other unit. As a rule, if possible, each protection set should act as backup for its adjacent units, subject

to coordinating criteria and technology. This is a complex question that must be elicited by the engineering department entitled of protection setting, or by consulting the operating studies of each company, as it depends on the type of protection used. Figure 8 shows, by a dependency graph, which unit acts as backup protection to each other, on the Recife II Substation. In this picture, an arrow connecting two units (shown as circles) represents a unidirectional backup protection of the originating unit over the pointed unit. Single lines connecting two units represent a bi-directional backup protection, that is, each unit acts as a backup protection and is protected by the other.

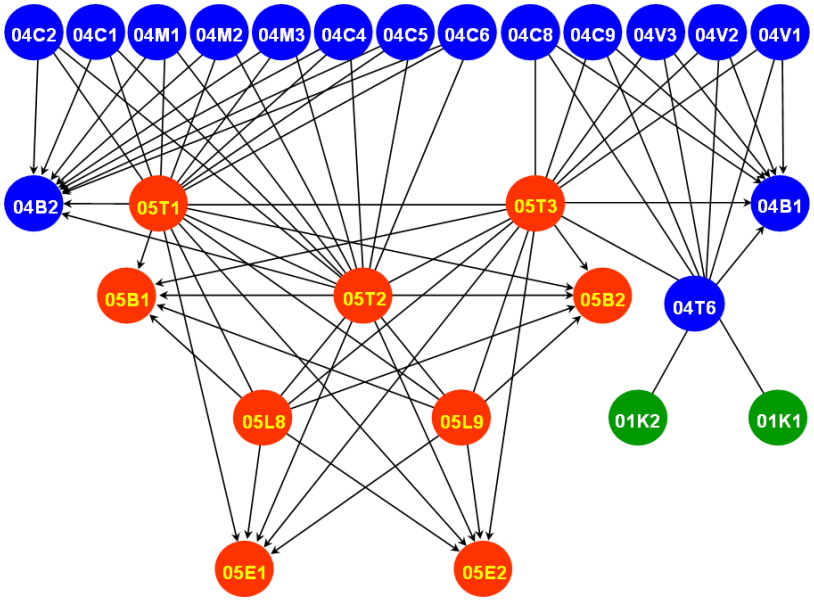

Figure 8 – Recife II Backup Protection

This influence graph must be merged to the logic of Figure 7 to specialize the critical failure tree of each unit, down to the failure of each primary protection system. The expanded failure tree for a catastrophic plant failure, including these sub trees is shown on Figure 9.

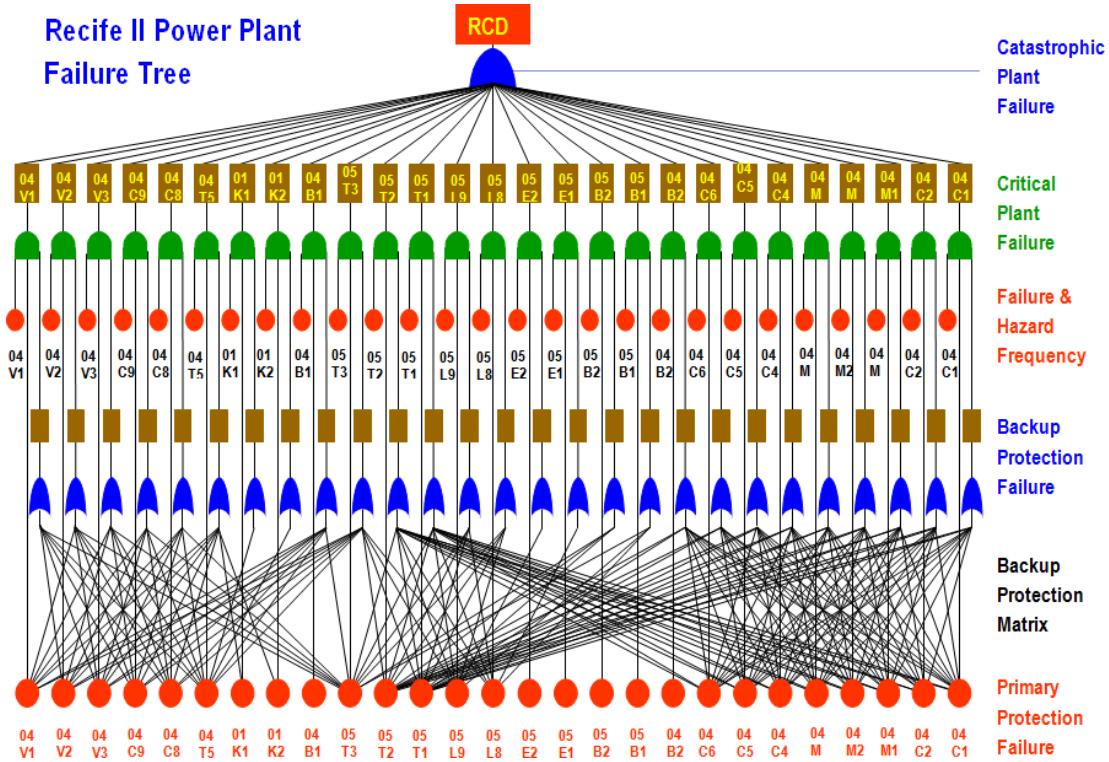

Figure 9 – Recife II Power Plant Failure Tree

Note the denser part in this picture introduced by the encoding of the logic of backup protection and how it affects the complexity of the resulting tree. Further details could be added, such as expanding the primary events, represented as small circles on this picture. These events represent the primary faults on the unit, or secondary faults on protection and auxiliary equipment. The expansion of primary events representing unit faults would imply on the detailed modelling of each unit, according to its constituent parts and specific failure modes. The resulting tree would increase in dimension and complexity. Also, the expansion of primary events associated to protection faults could be made by modelling each relay, instrument transformer and circuit breaker as a tree relating the failure modes of their constituent parts. Further increase in tree complexity and dimension would result from the inclusion of common mode of faults. A practical decision must be taken as the limit of modelling of the failure tree. Besides complexity, this paper proposes to limit the dimension of the tree according to available statistics of past failures, allowing the mathematical evaluation of the tree. That is, the tree should be expanded until all primary events are covered by available statistical data, such as failure rates and reliability. This approach is in accordance with the objective of risk assessment, where the focus is on major accidents, and not on small faults. In the example plant, this is equivalent to consider as primary events only the failure of each unit, as well as each protection system of the plant, as their failure rates can be deducted from maintenance records.

8. Plant Model

A mathematical plant model must be defined to elicit all statistic data needed for risk assessment. This model will be derived from the fault tree just developed. Total risk incurred for an entire plant can be assessed from the top event probability. From the structure of Figure 9 the catastrophic event is formed by the union of all critical events, so that its function structure can be expressed by:

$$R = \bigcup_{i \in S} R_i \quad ,$$

and its probability by:

$$R = 1 - \prod_{i \in S} (1 - R_i) \quad ,$$

where R is the top event probability, R_i is the probability of occurrence of critical event i, and S is the set of all units in a plant. According to picture 7, a critical event happens when there is an equipment fault E_i, with the simultaneous failure of its primary protection P_i and all backup protection, or in structure logic function:

$$R_i = E_i \cap P_i \cap \bigcup_{j \in B_i} P_j \quad ,$$

where B_i is the set of backup protection for unit i. In probabilistic terms, this can be expressed as

$$R_i = E_i P_i \left[1 - \prod_{i \in B_i} (1 - P_j) \right] ,$$

where E_i is the probability of a fault in unit i, and P_i and P_j are the probability of failures on its primary and backup protections, respectively. From this, the function of structure for the top event reduces to:

$$R = \bigcup_{i \in S} \left[E_i \cap P_i \cap \left(\bigcup_{j \in B_i} P_j \right) \right] ,$$

and the probability of catastrophic events by:

$$R = 1 - \prod_{i \in S} \left\{ 1 - E_i P_i \left[1 - \prod_{j \in B_i} (1 - P_i) \right] \right\}.$$

Now, let F be the mean frequency (rate) of occurrence of catastrophic events in the plant, given by:

$$F = \frac{dP}{dt} = \sum_{i \in S} \left(\frac{\partial P}{\partial E_i} \frac{dE_i}{dt} + \frac{\partial P}{\partial P_i} \frac{dP_i}{dt} \right),$$

where the total derivatives are rates of changes of the associated binary variables from the normal to faulty state (0 to 1), and partial derivatives are probabilities of the top event being dependent on the state of each primary event. Total risk can be evaluated by this rate or by pondering each parcel of this expression by its associated consequence:

$$R = C \frac{dP}{dt} = \sum_{i \in S} \left(C_{Ei} \frac{\partial P}{\partial E_i} \frac{dE_i}{dt} + C_{Pi} \frac{\partial P}{\partial P_i} \frac{dP_i}{dt} \right),$$

where C = mean cost or consequence of a catastrophe on the plant, C_{Ei} = cost of a unit i fault without protection, and C_{Pi} = cost of a protection fault on unit i. Now, the cost of a transition in a protection status can be discarded as negligible, when compared to the cost of a failure in the protected unit. So, total risk can be evaluated by:

$$R = \sum_{i \in S} \left(C_{E_i} \frac{\partial P}{\partial E_i} \frac{dE_i}{dt} \right),$$

In this expression, C_{Ei} and DE_i/dt are primary data for each unit, given, for example, by the capital cost and failure rate F_i for each protected equipment:

$$F_i = \frac{dE_i}{dt}.$$

The partial derivatives are probability expressions readily derived as

$$\frac{\partial P}{\partial E_i} = P_i \left[1 - \prod_{j \in B_i} (1 - P_i) \right].$$

Note that this expression measures the probability of unit i operating without primary and backup protection. Each P_i is also a primary data necessary for each protection system on the plant. The final expression for the catastrophic risk is then:

$$R = \sum_{i \in S} \left\{ C_{E_i} P_i \left[1 - \prod_{j \in B_i} (1 - P_i) \right] F_i \right\}.$$

To evaluate this expression, the analyst must have figures for the cost and failure rates of all high voltage units, and probabilities of each protection failure.

9. Case Study

Table I shows the figures derived from CHESF historical data, to be applied to Recife II substation.

Table I – Failure Frequencies and e Probability of Protection Failure

Equipment	Failure Frequency (1/h)	Probability of Protection Failure
Synchronous Condenser	4,9044e-4	0,459771
Line	1,0825e-3	0,046851

Bus Bar	4,4915e-5	0,324961
Transformer	1,4977e-4	0,153101
Reactor	1,8701e-5	0,660874

The following graph shows the result of applying the above expression for Recife II substation.

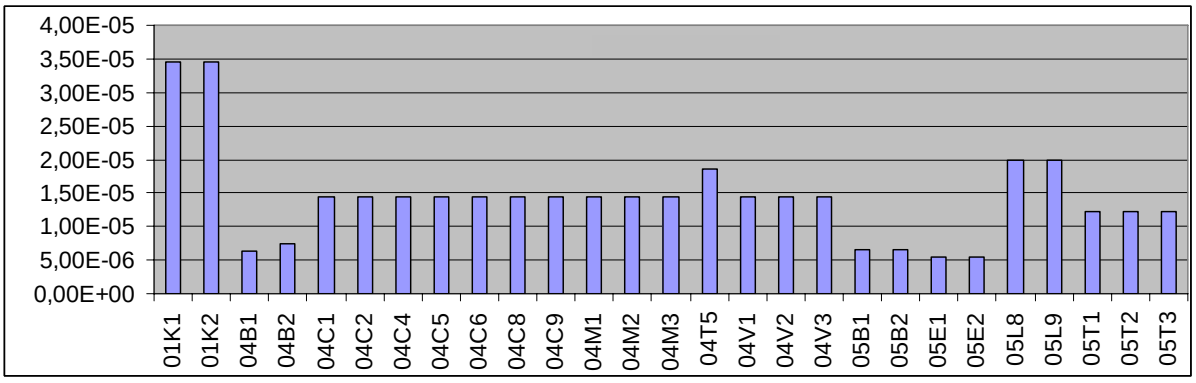

Figure 10 – Hour Distribution of Catastrophic Risk at SE Recife II Substation

Note, in this Picture, the high relative risk of synchronous condensers 01K1 and 01K2 and low risk of bus bars and reactors. These agree with the history of loss of similar equipment at other CHESF stations. The identification of major risk areas on the plant can be determined by defining an index of relative risk contributed by each unit, through its failure rate, to the catastrophic risk:

$$RE_i = \frac{F_i}{R}\frac{\partial R}{\partial F_i}\frac{C_i P_i\left[1-\prod_{j\in B_i}(1-P_j)\right]F_i}{\sum_{k\in S}\left\{C_k P_k\left[1-\prod_{j\in B_i}(1-P_j)\right]F_k\right\}}.$$

The following graph shows the result of applying the above expression for Recife II substation.

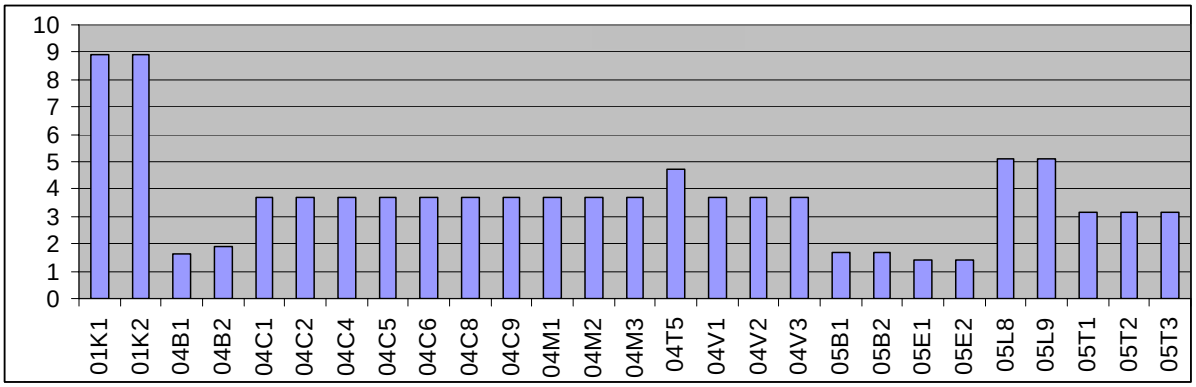

Figure 11 – Percent Distribution of Catastrophic Risk at SE Recife II Substation

This graph confirms again that the synchronous condensers are the most risky areas of the station. A similar index can be defined to measure the relative contribution of the protection reliability of each item on the plant catastrophic risk:

$$RP_i = \frac{P_i}{R}\frac{\partial R}{\partial P_i}\frac{C_i P_i\left[1-\prod_{j\in B_i}(1-P_j)\right]F_i + P_i\sum_{j\in B_j}C_j P_j F_j}{\sum_{k\in S}\left\{C_k P_k\left[1-\prod_{j\in B_i}(1-P_j)\right]F_k\right\}}.$$

The following graph shows the result of applying the above expression for Recife II substation

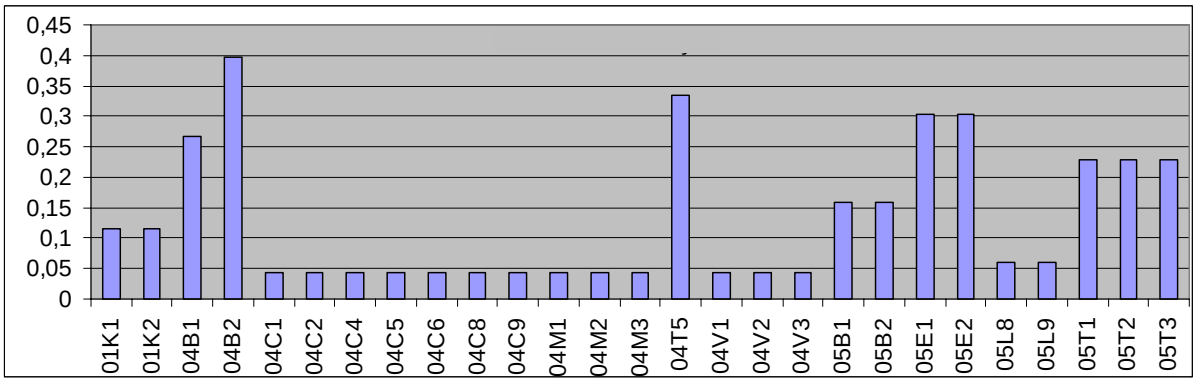

Figure 12 – Relative Risk Distribution of Protection at Recife II substation

It is seen that bus 04B2 and transformer 04T5 are the equipments more sensitive to catastrophic risk due to protection failure. High speed differential protections are suggested to these buses, to reduce the catastrophic risk of the substation.

10.Applications

Risk assessment of electric power plants may be of interest to many professionals: (1) technical personnel involved on planning, maintenance and operations of power systems; (2) utilities and insurance managers and technicians interested on economic and business consequences of major accidents in the electric industry; and (3) environmental, financing and regulatory agencies and personnel seeking legal and/or social safety assurance for large enterprises. Beside its intrinsic value as a decision tool, risk analysis has a definite didactic effect as it forces the analyst to make explicit the behaviour of the process, and its dangers. By presenting a real case, it is hoped that this approach will contribute to spread the benefits of probabilistic risk assessment to the electric industry.

BIBLIOGRAPHY

[1] Siqueira, I. P., “Optimum Reliability-Centered Maintenance Task Frequencies for Power System Equipments”, 8th PMAPS, IEEE, 2004.
[2] Siqueira, I. P., “Measuring the Impact of an RCM Program on Power System Performance”, IEEE PES General Meeting, IEEE, 2005.
[3] Billinton, R., Allan, R. N., “Reliability Evaluation of Engineering Systems”, Pitman, 1983
[4] Endrenyi, J., “Reliability Modeling in Electric Power Systems”, John Wiley & Sons, 1978.
[5] Sullivan, R. L., “Power System Planning”, McGraw-Hill, 1977.
[6] Sage, A. P., “Methodology for Large-Scale Systems”, McGraw-Hill, 1977.
[7] Li, W., “Risk Assessment of Power Systems – Models, Methods, and Applications”, Wiley, 2005
[8] Siqueira, I.P., “Manutenção Centrada na Confiabilidade – Manual de Implementação”, ISBN 85-7303-566-8, Editora QualityMark, Rio de Janeiro, Brazil, 2005.
[9] Henley, E. J., “Designing for Reliability and Safety Control”, Prentice Hall, Inc., New Jersey, 1985.
[10] NUREG-0492, Fault Tree Handbook, Systems and Reliability Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.
[11] Raafat, H., Risk Assessment Methodologies, University of Portsmouth, ISBN 1 069959434.