SecurMining 2.0: A Data Mining Software Package for Security Analysis In the Portuguese Transmition System

C. I. Faustino Agreira and C. M. Machado Ferreira
Instituto Politécnico de Coimbra
Instituto Superior de Engenharia
Coimbra, Portugal
crisf@ieee.org

R. Pestana
REN - Rede Eléctrica Nacional, S.A.
rui.pestana@ren.pt
Instituto Superior de Engenharia
Lisboa, Portugal
rpestana@deea.isel.ipl.pt

F. P. Maciel Barbosa
Inesc Tec and Faculdade de Engenharia, Universidade do Porto
Porto, Portugal
fmb@fe.up.pt

Abstract—**The software package SecurMining2.0 was developed to study and analyse the security of the Portuguese Transmition System, but can be used to study the security of any other transmission system. The computer program runs in WindowsTM environment and uses three different units. The pre-processing unit that defines the load diagram contains complete information concerning the topology of the Portuguese Transmission System and the characteristics of the generators, transformers, lines, loads and interconnections with Spain. The processing unit has three different modules to solve the security analysis problem. The first module generates a data base with all the information required for the power flow and for the security analysis studies. This data is obtained using the PSS/E 30.0 software from Siemens Power Transmission Distribution, Inc., and Python [1-2]. The second module produces the list of the contingencies, using an AC power flow, calculates the severity indices and makes a initial interface with the software Rose [3]. Finally, the third module uses a new methodology for filtering and ranking the contingencies using the Rough Set Theory and makes an interface with the software package ROSE [3]. The post-processing unit is a powerful tool that displays and analyses the security results. Finally, some conclusions that provide a valuable contribution to the understanding of the Portuguese Transmition Systems security analysis are pointed out.**

Keywordst: Contingencies analysis, Portuguese Transmition systems, Rougt set theory; security analysis.

I. INTRODUCTION

On-line security analysis is one of the most important EMS functions, since it entails the evaluation of a power systems ability to withstand dangerous contingencies and to survive to a normal or acceptable operating point [4]. The purpose of the electrical power system is to supply the consumers with continuity and quality as economically as possible [5]. To accomplish these objectives the system must to keep the profile of the tension in the consumers and to have adequate levels of reliability [6]. For an electric power system the security analysis is of a very important task either when during the planning or during the operation of the system. Taking in account the complexity of this problem, some efforts have been made to find efficient methods to manage the system. The complexity of these studies results from the fact that the majority of the operators ignore part of the available information in the Electrical Systems [6]. Operators of the systems are confronted daily with unpredictable events in their power systems, 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. Incidents are unpredictable disturbances and recent experiences prove that severe contingencies happen.

The importance of an uninterrupted electric power supply makes the study of power system security operation very important. A set of security analysis functions is usually developed to help the operator monitor to control the security of the power system. Security studies for the Portuguese Transmission System are very important since the security system is height recognized by the Portuguese authorities.

This paper focuses on the analysis of the Portuguese Transmition Systems using data that is produced through operating point simulation, for contingency studies. The Rough Set Theory was used to validate a new set of severity index (new attributes), to point out the "nature" of given contingencies.

In this paper it is described the developed software package and some security studies with the Portuguese Transmition System are presented. These computer programs run in Windows^{TM} environment and use three different units (blocks). The pre-processing unit defines the load diagram, contains complete information concerning the topology of the Portuguese Transmission System and the characteristics of the generators, transformers, lines, loads and interconnections with Spain. The processing unit has three different modules to solve the security analysis problem. The first one generates a data base with all the information required for the power flow and for the security analysis studies. The second one produces the list of the contingencies, using an AC power flow, calculates the severity indices and makes an initial interface with the software Rose [3]. Finally, the third module uses a new methodology to filter and rank the contingencies were the Rough Set Theory is applied and makes the interface with the software package ROSE [3] too. The post-processing unit is a powerful tool that displays and analyses the security results. This unit has one module that transforms the large amount of results produced by the processing unit in a friendly engineering solution.

II. THE SOFTWARE PACKAGE SECURMINING 2.0

The SecurMining2.0 software package was developed for the Portuguese Transmition System and the main purpose of this package is to provide an easy security analysis tool that allows modeling any power system component with the desired complexity. The computer programs were developed in Delphi language and run on a personal computer. A friendly on-line help is always available. In this section the pre-processing, the processing and the post-processing units are described. Fig. 1 shows the overall structure of the software package SecurMining2.0 [1].

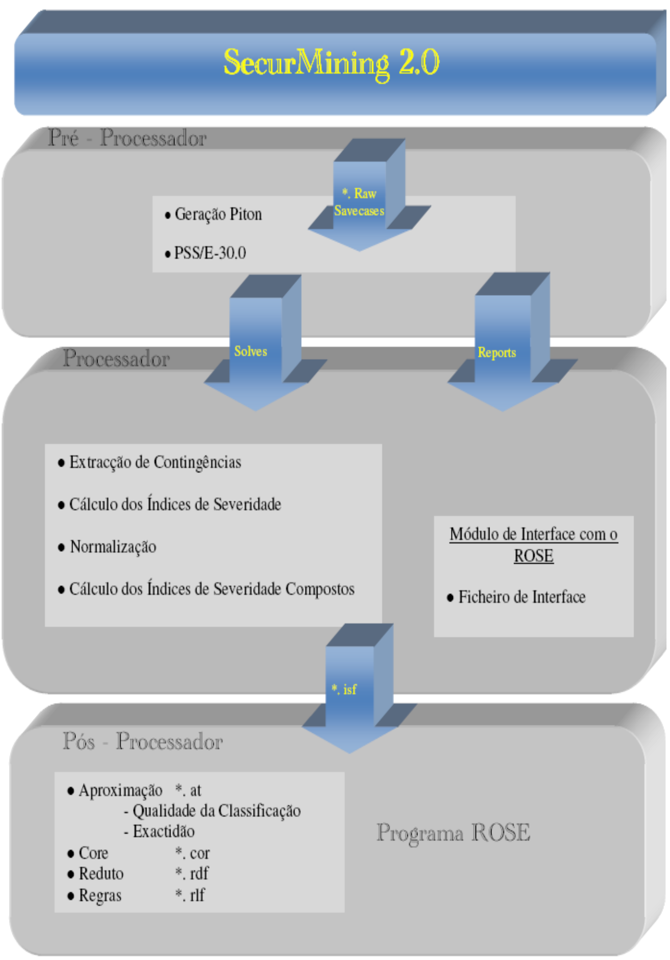


Figure 1. The structure of the software package SecurMining2.0.

This software package includes various sequential modules and the interface with the software Rose [7].

Fig. 2 shows the work space of the SecurMining 2.0.

Figure 2. SecurMining2.0.

A. *The pre-processing unit*

The pre-processing unit has one module. In order to obtain the steady state initial conditions and to solve the security analysis problem it requires input data for the following mathematical models: network models, device static models and load models. This data is obtained using the PSS/E 30.2. This software from Siemens Power Transmission Distribution, Inc is used by the Portuguese Transmition Company, REN.

A small program to check the files input of the savecases was developed. This program builds multiple language scripts in Python, used in PSS/E, in order to automate the analysis of the power flows. In this way each day of the year is analyzed at once, automatically and sequentially, from each of the scripts created. The number of tests decreased from 17 520 cases to 365, corresponding to one day every year. The output results of each analysis of the PSS/E_30.0 are stored into several files, which correspond to 48 “Solves”, each file containing a list of contingencies for the day in question. These files are used for further analysis by the processor. The directory that has the power flow is called “Solve”. The Reports directory is obtained with PSS/E_30.0 and is where the outputs files of each 365 testes are stored. The power flow allows to know the state of the system and is obtained using the Newton-Raphson model [8].

B. *The processing unit*

The processing unit has four different modules to study the security analysis problem. The first one generates a data base with all the information required for the power flow to the security analysis studies and produces the first initial list of the contingencies, with an AC power flow and a contingency analysis (n-1). The second module calculates the severity indices, with different methods and the third module normalize the severity indices [1], [4], [9-10], [12-13]. The fourth module calculates the composed indices and uses a new methodology for filtering and ranking the contingencies in the Portuguese Transmission system using the severity indices. Finally, the fifth module makes an interface with the software package ROSE [3].

The database obtained by PSS/E_30.0 intends to be manipulated by various processing units and is composed of several modules. Fig. 3 shows the interface created by the program with all existing elements in the pre-processor and pos-processor.

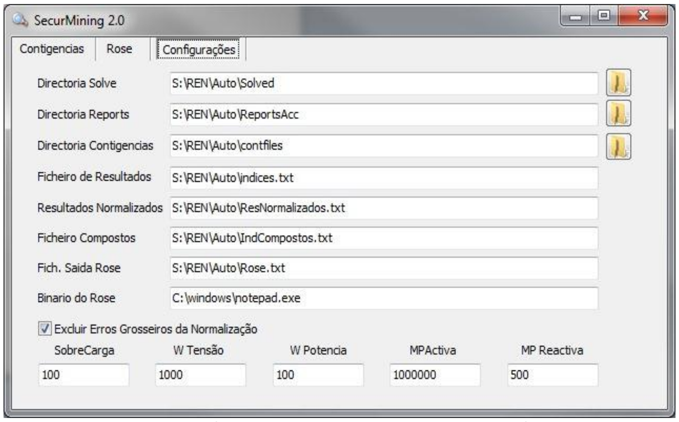


Figure 3. Software package SecurMining2.0 configuration.

Fig. 4 shows the user interface. The program allows to check for inconsistencies, analyses the entire database and verify if all files are correct and if they do not have same incomplete database files. To generate the individual files for each contingency it is necessary to exclude the inconsistencies. The program permits to know how many contingencies in the files are examined. It also excludes gross errors in the reading and calculations that could vitiate the standardization and subsequent analysis of results. The calculation time that the package programs developed for each operation (see Fig.4) is approximately 60/80 ms for Savecase.

Figure 4. Contingencies evaluation whith the software package SecurMining2.0.

The processor unit of the software package SecurMining2.0 is a powerful tool that allows to visualize and analysevisualizing and analysing the results obtained. This unit allows to the user a quick review of a large amount of information, transforming it in an engineering solution. This analyse can be presented in a graph or analytically way and is performed for large databases.

The data analysed by the user is:

-overloads in the transmition lines in %

-the number of overloads and the number of voltage violation;

-the maximum and minimum level of the voltage;

-the severity indices related to the power η_P;

-the severity indices related to the voltage η_V;

-the severity indices related to the overloads SI_{OL};

-the severity indices related to the real edge of the active power $Pmar\ SI$;

-the severity indices related to real edge of the reactive power $Q\max\ SI$;

-the overall severity indices SI;

C. *The interface with ROSE*

This module creates a file that interfaces with the software ROSE [3]. Transforms all the information in the initial database and extracts the Savecases for the year 2008 at different levels of severity. The codes used to calculate each of the attributes (Rough Set Theory) considered, were evaluated in two distinct ways. The attributes related to indices of severity, were calculated using a normal distribution. The remaining attributes were considered as described in REN Procedures Manual and consulting the Systems Operators of the Portuguese Transmition System [REN08].

The attribute codes can be changed by replacing the default values calculated by the program, entering manually other values. Using the configured values, the program creates a table in the form of *. *isf* file with all information of the network, prepared to be processed in the package of computer programs ROSE [3].

Fig. 5 shows the interface created with Rose. This interface applies the Rough Set Theory approach to the Portuguese Transmition System security studies.

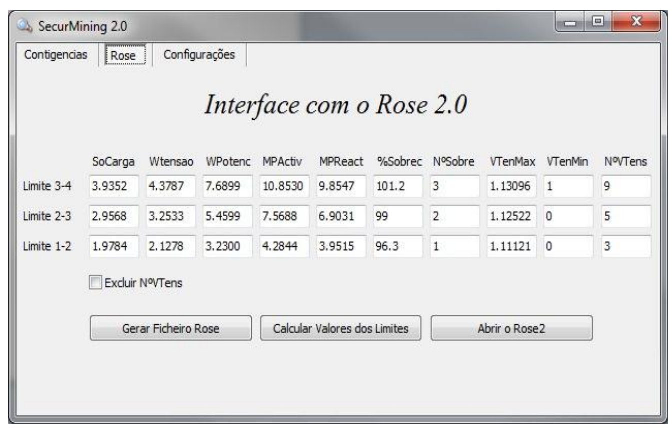


Figure 5. Interface with Software ROSE.

D. *The post-processing unit*

Through the software ROSE the results are obtained using the Rough Set Theory that permits to view the multiple files, with the final results of processing, such as Core, Reduct, Approaches, Classifications and Rules [7]. These rules will allow a clear and succinct analysis of the final results of security of power systems, in this case the Portuguese

Transmition Systems. The post-processing unit is a powerful tool that allows to display and analyse the security analysis results produced by the processing unit. The module of the post - processing unit are designed to take advantages of the advanced user interface features of the Windows^{TM} environment. This unit enhances the user ability to analyse a large amount of output data and to produce visually appealing graphic representations of the results obtained with the modules. Summary and detailed reports are also available to present the solutions produced with the processing unit modules. The post processing, shows the results of the software package ROSE [1-2].

III. APLICATION EXAMPLE

This study was realized in the Portuguese Transmission System (Fig.6). The network model has 513 busbars, 636 transmission lines, 197 generators and 684 transformers. A first order contingency study was carried out for all the transmission lines. Were simulated 17 520 savecases, what it is equivalent to obtain savecases every 30 minutes throughout twelve months in the year of 2008, supplied by the Portuguese Transmission System.

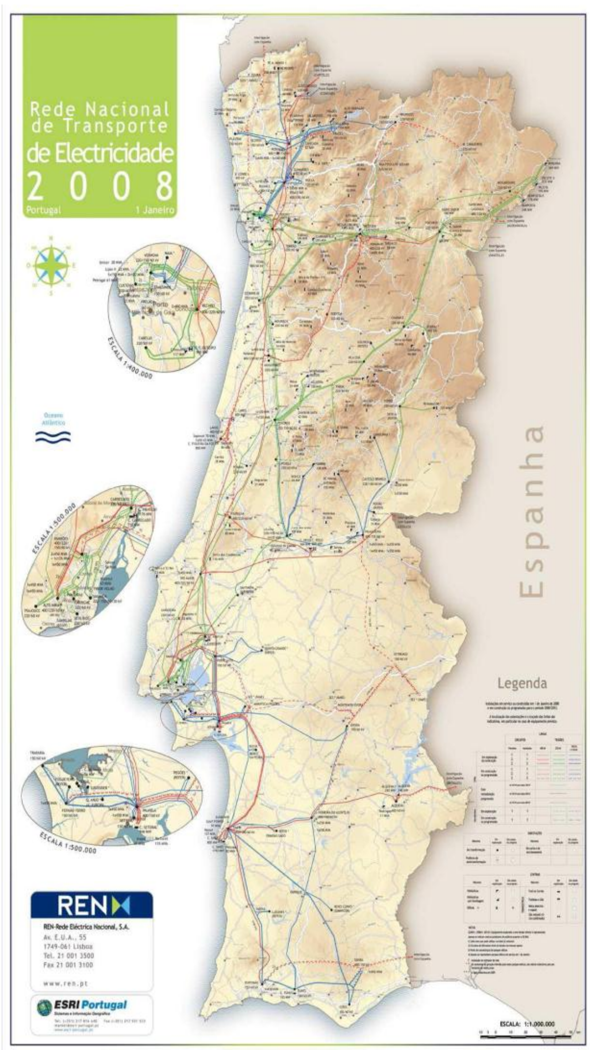


Figure 6. Portuguese Transmition System [14]

IV. RESULTS

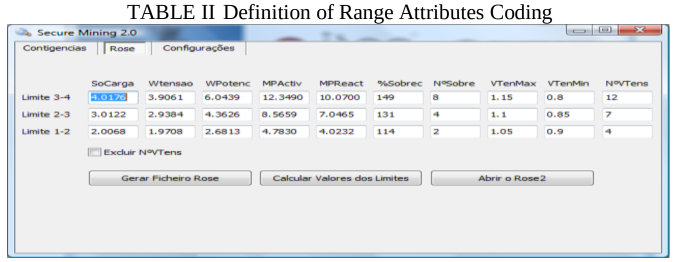
The results were obtained with the package software *SecurMining2.0*.This software package is an interface with the PSS/E – 30.2 Siemens used by Portuguese Transmition System [1-2]. Of 17 520 Savecases only those that presented a power flow in the transmition line above 90% and violation of the voltage had been considered. In order to carry through the study and analysis of security of the Portuguese Transmission System using the Rough Set theory, it was necessary to know the state pre-contingency of the system. It was required to precede a study of the multiple power flows using the computational package PSS/E 30.2. Through these power flows the first list of contingencies was obtained and used to simulate the algorithm developed for ranking and assessment of the contingencies severity. A first order contingency study was carried out and it was obtained a list of 6777 contingencies that allows the construction a contingency control database [1]. Due to large number of results produced, only some of the most significant are shown in this paper.

The specified attributes used are as follows:

A_1 – overloads in the transmission lines;
A_2 – number of overload transmission lines;
A_3 – severity indices related to the power;
A_4 - severity indices related to the voltage;
A_5 – power severity indices related to the voltage magnitude
A_6 - power severity indices related to the voltage phase
A_7 – severity indices related to the overloads
A_8 - severity indices related to the real power margin
A_9 – Severity indices related to the reactive power margin
Dec. – Security

The decision attributes (Dec.) is divided in four states, Normal, Alert, Emergency I and Emergency II. Table I presents a set of information related to a contingency control database for the year f 2008. Table II shows the chosen range for the coded qualitative attributes. The condition attributes are coded into four qualitative terms: Low, Medium, High and Full. Due to large amount of information, only the final rules are presented. A powerful interface between the SecurMining2.0 software package and the ROSE computer program was used.

TABLE II Definition of Range Attributes Coding



Secure Mining 2.0

Contigencias | Rose | Configurações

	SoCarga	Wtensao	WPotenc	MPActiv	MPReact	%Sobrec	NºSobre	VTenMax	VTenMin	NºVTens
Limite 3-4	4.0176	3.9061	6.0439	12.3490	10.0700	149	8	1.15	0.8	12
Limite 2-3	3.0122	2.9384	4.3626	8.5659	7.0465	131	4	1.1	0.85	7
Limite 1-2	2.0068	1.9708	2.6813	4.7830	4.0232	114	2	1.05	0.9	4

Excluir NºVTens

Gerar Ficheiro Rose | Calcular Valores dos Limites | Abrir o Rose2

TABLE I Attributes Represented by the Set

Cont. Nº	Atributes									
	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	Dec.
1	1	1	1	1	1	1	1	2	1	N
2	1	1	1	1	1	1	1	2	1	N
3	1	1	1	1	1	1	1	3	1	N
4	1	1	1	1	1	1	1	3	1	N
5	1	1	1	1	1	1	1	3	1	N
6	1	1	1	1	1	1	1	3	1	N
7	1	1	1	1	1	1	1	3	1	N
8	1	1	1	1	1	1	1	2	1	N
9	1	1	1	1	1	1	1	2	1	N
10	1	1	1	1	1	1	1	3	1	N
11	1	1	1	1	1	1	1	3	1	N
12	1	1	1	1	1	1	1	3	1	N
13	1	1	1	1	1	1	1	3	1	N
14	1	1	1	1	1	1	1	3	1	N
---	---	---	---	---	---	---	---	---	---	---
---	---	---	---	---	---	---	---	---	---	---
---	---	---	---	---	---	---	---	---	---	---
6766	1	1	1	1	1	1	1	2	1	N
6767	1	1	1	1	1	1	1	2	1	N
6768	1	1	1	1	1	1	1	2	1	N
6769	1	1	1	1	1	1	1	2	1	N
6770	1	1	1	1	1	1	1	2	1	N
6771	1	1	1	1	1	1	1	2	1	N
6772	1	1	1	1	1	1	1	2	1	N
6773	1	1	1	1	1	1	1	2	1	N
6774	1	1	1	1	1	1	1	3	1	N
6775	1	1	1	1	1	1	1	2	1	N
6776	1	1	1	1	1	1	1	2	1	N
6777	1	1	1	1	1	1	1	2	1	N

Table III shows the approximation of the objects in the Decision levels.

TABLE III Approximation of the Objects

Decision Level	Nº of objects	Approximation Upper	Approximation Lower	Approx. of classification Precision
Normal	6547	6537	6656	0.9821
Alerta	118	14	133	0.1053
Emergência I	84	79	176	0.4489
Emergência II	28	28	28	1.0000

Using this computer software packages was verified that the attributes A_1, A_3, A_4, A_6, A_7 and A_9 are the Core and the Reduct of the set of contingencies. The quality of classification for all conditions and the attributes in the core was 0.9824. The precision of the approximation of the classification for de contingencies in Emergency II was 1.000, which means 100% of certainty.

According to the algorithm described, it was possible to compose the above set of rules that incorporate the range values in the final set of rules and approximate rules that contains the knowledge of a initial database range values obtained with the SecurMining2.0 software package.The Rules are divided in four sets. The first set contains the rules for Normal State; this set is composed with 2 (two) exact rules too. The second set contains the rules for Alert State, and contains 7 (seven) exact rules. The thirty set is composed of 2 (two) exact rules and characterizes the Emergency I State. Finally, the last set of rules characterizes the Emergency State II and is composed of 4 (four) exact rules. In this study five approximate rules were considered (L is a Low value, M is Medium value, H is a high value and F is a Full value). Due to large amount of information only some final rules are presented.

Exact Rules for Normal State:

1 – If (A6 is 1) then S = N
2 – If (A4 is 1 and A6 is 2 and A7 is 2 and A8 is 2) then S = N

Exact Rules for Alert State:

1 – If (A3 is 4 and A6 is 2) then S = A
2 – If (A3 is 3 and A6 is 2) then S = A
3 – If (A4 is 2 and A6 is 2) then S = A
4 – If (A6 is 2 and A7 is 3) then S = A
5 – If (A3 is 2 and A6 is 2 and A8 is 1) then S = A
6 – If (A5 is 4 and A6 is 2) then S = A
7 – If (A3 is 3 and A7 is 2) then S = A

Exact Rules for Emergency I State:

1 – If (A6 is 3) then S = E1.
2 – If (A6 is 4 and A7 is 1 and A8 is 2) then S = E1.

Exact Rules for Emergency II State:

1 – If (A6 is 4 e A8 is 1) then S = E2.
2 – If (A6 is 4 e A8 is 3) then S = E2.
3 – If (A6 is 4 e A7 is 2) then S = E2.
4 – If (A6 is 4 e A7 is 3) then S = E2.

Approximate Rules:

1 – If (A3 is 1 and A4 is 1 and A6 is 2 and A7 is 2 and A8 is 1) then S = N or S = A.
2 – If (A4 is 1 and A6 is 2 and A7 is 2 and A8 is 3) then S = N or S = A.
3 – If (A3 is 2 and A8 is 3) then S = N or S = A.
4 – If (A5 is 2 and A6 is 2) then S = N or S = A.
5 – If (A3 is 1 and A5 is 1 and A6 is 2 and A7 is 1) then S = N or S = A or S = E1

V. Conclusions

This paper presents a security analysis simulation software package to study the security analysis of a power system and a study with the Portuguese Transmission System is presented and analysed. The knowledge acquisition process is a complex task, since the experts have difficulty to explain how to solve a specified problem. In this paper, a new learning approach to derive rules from incomplete data sets based on the Rough Set Theory is proposed.

The study presents a systematic approach to transform examples in a reduced set of rules. A new learning approach to derive rules from incomplete data sets based on the Rough Set Theory is proposed and was applied to the Portuguese Transmition System security studies. This theory was used to study and analyse the steady–state contingency analysis and classification of the Portuguese Transmition System. The results that were produced using this theory and a set of rules for the four scenarios is proposed: Normal, Alert, Emergency I and Emergency II. The importance of the chosen range for the coded qualitative attributes is shown.

The pre-processing, the processing and post-processing units were described. An application example of the developed computer programs was presented. The Portuguese Transmission System can use successfully this security analysis tool in project assignments of power system analysis. Researchers can use this package for security analysis and introduce new improvements easily, particularly in the modeling of the electric power system devices and security indices

Acknowledgment

“The firth author would like to thanks *“Fundação para Ciência e Tecnologia, FCT”*, that partially funded this research work through the PhD grant nº: SFRH/BD/38152/2007.

References

[1] C. I. Faustino Agreira, *"Técnicas de Data Mining para estudo e análise da segurança dos Sistemas Eléctricos de Energia"*, Ph.D. Thesis, FEUP,2010 (in portuguese).

[2] C. F. Faustino Agreira, R. Pestana, C. M. Machado Ferreira and F. Maciel. Barbosa, "Portuguese Transmission System contingencies analysis using the rough set theory" in. 2010 Cigré – Assessing and Improving Power System Security, Reliability and Performance in Light of Charging Energy Sources Symposium., Recife, Pernambuco, Brazil, 3-6 April 2011

[3] ROSE2 – Rough sets data explorer. Laboratory of Intelligent Decision Support Systems of the Institute of Computing Science, Poznan,[Online]. Available:.http://www.idss.cs.put.poznan.pl/soft ware/rose

[4] J. Wood, B. F. Wollenberg, Power Generation Operation and Control, 2nd Ed., New York: John Wiley & Sons, 1996.

[5] Susana Almeida, Rui Pestana and F. Maciel. Barbosa, "Severe contingencies Analysis in Portuguese Transmission System," in Proc. 41th Universities Power Engineering Conference Conf., 2006. Newcastle, UK.

[6] C. I. Faustino Agreira, R. Pestana, C. M. Machado Ferreira, F. P. Maciel Barbosa, “The Severity Indices applied to the Portuguese Transmission System”, in XIICLEEE 12Th Conferência Luso-Espanhola de Engenharia Electrotécnica, Azores, Portugal, 2011.

[7] Z. Pawlak, Rough Sets–Teorical Aspects of Reasoning about Data, Kluwer, 1991

[8] Stevenson, W. D. and Grainger, J.J. “Power System Analysis”, Singapore, McGraw-Hill, 1994.

[9] Agreira Faustino I. C., Ferreira Machado C. M., Pinto Dias J. A. and Barbosa Maciel F. P., “Contingency Screening and Ranking Assessment of an Electric Power System using Different Security Performance Indices” in Proc. of the 8º Congresso Luso-Espanhol de Engenharia Electrotécnica, CLEEE, Vilamoura, July, 2003

[10] Agreira Faustino I. C., Ferreira Machado C. M., Pinto Dias J. A. and Barbosa Maciel F. P., “Contingency Screening and Ranking Algorithm using Two Different Sets of Security Performance Indices” in Proc. 2003 IEEE International Conference on Electric Power Engineering, Power Tech’03, CD-ROM, Bologna, Italy, June, 2003

[11] Çaglar R., Özdemir A., Mekiç F., “Contingency Selection Based on Real Power Transmission Losses”, IEEE International Conference on Electric Power Engineering, PowerTech’99, CD-ROM, Budapest, Hungary, 29 August – 2 September 1999.

[12] Çaglar R., Ozdemir A., “Composite Electric Power System Adequacy Evaluation Via Transmission Losses Based Contingency selection Algorithm”, in Proc. 1999 IEEE International Conference on Electric Power Engineering, Power Tech’99, CD – ROM, 29 August - 2 September, Budapest, Hungary.

[13] Jagabondhu Hazra, and Avinash K. Sinha, “Identification of Catastrophic Failures in Power System Using Pattern Recognition and Fuzzy Estimation” IEEE Transactions on Power Systems, Vol. 24, No. 1, pages 378-387 February 2009.

[14] Portuguese Transmission System. Available: www.ren.pt.