DYNAMIC SECURITY EVALUATION FUNCTIONS IN THE MORECARE PROJECT

J. A. Peças Lopes (1), N. Hatziargyriou (2), H. Vasconcelos (1), J. N. Fidalgo (1), G. Damianos (2), E. Karapidakis (2)

(1) - INESC Porto - Instituto de Engenharia de Sistemas e Computadores do Porto
and DEEC/FEUP - Fac. de Engenharia da Universidade do Porto
Rua Roberto Frias 378, 4200 465 Porto, Portugal; email: jpl@fe.up.pt

(2) – Power Systems Division, National Technical University of Athens

ABSTRACT**:**
This paper describes the security assessment functions of an advanced control system for secure operation of isolated networks with increased renewable penetration, developed within the MORECARE project. One of the key features of this project is related with the capability of assessing on-line dynamic security and providing preventive control measures that can assure a robust operation for the system regarding some disturbances.
The paper describes with some detail the general approach followed to derive these evaluation functions, which are based in functional knowledge generated off-line through computational simulation. Techniques like Decision Trees, Artificial Neural Networks and Hybrid Regression Trees were successfully exploited and integrated with other mathematical technical do deal with the problem.

Keywords: Dynamic Security Assessment, Isolated Power Systems, Preventive Control, Decision Trees, Artificial Neural Networks, Hybrid Regression Trees, Wind Power.

I. INTRODUCTION

In autonomous power systems, dynamic security assessment is a key issue in the operation and management of the networks. In fact, sudden changes of system operating conditions must be quickly and efficiently compensated by generators to avoid frequency excursions or high df/dt variations, which may trigger the operation of system frequency relays, like under frequency protection relays of generators, provoking system collapse. This means that expected system frequency excursions and df/dt values, for the most important disturbances, must be assessed in a fast way to help in defining the more robust operating strategies. In addition, under- or over-voltages might disconnect generation and the system should be able to face also these disturbances.

Dynamic security assessment is therefore one of the main concerns in the MORECARE project, where a prototype of an advanced control system for operators advice was developed.

On-line dynamic analysis of system behavior for a number of pre-specified disturbances is practically impossible using conventional tools. Therefore "Learning from examples" techniques, e.g. Decision Trees (DT), Hybrid Regression Trees (HRT) or Artificial Neural Networks (ANN), are then used to provide accurate and fast evaluation of system dynamic security by defining security rules and security functions. These structures need to be extracted from a "Data Set" and are used for evaluating the dynamic security of the system and for providing security restrictions in the Unit Commitment (UC) and Economic Dispatch (ED) modules, in order to arrive at the most economic and secure operating strategies.

The main stages followed for the development of these functions within this project were:

a) Identification and analysis of the critical operating conditions and disturbances for each system;
b) Generation of functional knowledge ("*Data Set*: *Learning Set and Test Set*") about the behavior of the systems, under the selected disturbances;
c) Derivation of security structures and security rules;
d) Evaluation of the quality of the security assessment (SA) functions;
e) Development of preventive control approaches.

This paper describes the approach followed in the development of these functions, including some specific results obtained for the systems of Crete and Madeira.

II. GENERAL ARQUITECTURE OF THE SA FUNCTIONS IN MORECARE

As explained in [1], in order to present to the system operator the operation strategy suggestions for a given time horizon, the MORECARE system must perform two main execution cycles. This procedure is summarized in the flow-char of Figure 1. This task scheduling is appropriate for relatively larger systems comprising steam and diesel or gas units. The operation suggestions that are presented to the operator should lead to the most economic strategy, assuring at the same time system security relatively to a given set of critical disturbances. This requires therefore security evaluations when solving the UC problem and a security complementary checking after the determination of the ED solution, due to possible changes in the system operating conditions.

In the MORECARE project, security assessment functions can be used for two main purposes: security evaluation and

preventive control for a given operating point and having in mind the disturbance under consideration.
As frequency behavior is here the matter of concern, when the security degree is not enough, a preventive control strategy can be determined exploiting two main avenues:

- Rescheduling units;
- Re-dispatching active powers among generators.

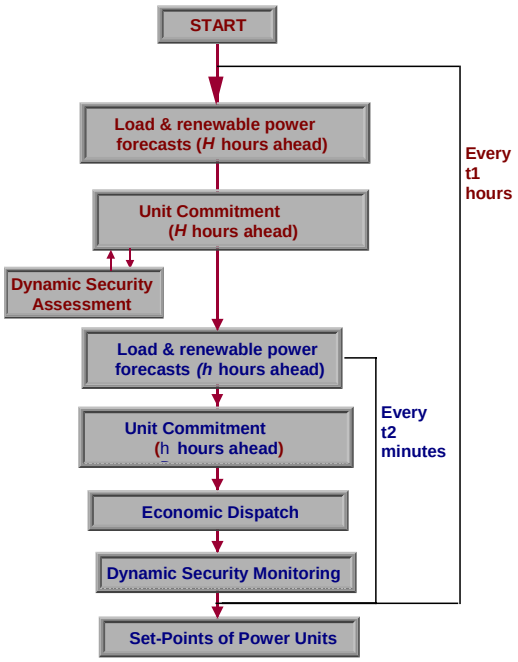

Figure 1 - Main execution cycles of the MORE CARE system

The determination of the appropriate active power re-dispatch may be performed exploiting rules derived from the DTs or through sensitivities of neural networks. However, this re-dispatch can, in some cases, be an insufficient preventive control measure because no solution is available. Therefore, the hypothesis of rescheduling generating units should also be considered.

The MORECARE security functions were then implemented at two different levels:

- Dynamic security assessment (DSA), by performing rescheduling of the unit-commitment proposed solutions;
- Dynamic security monitoring (DSM), by evaluation the dynamic security of the power system for the economic dispatch proposed solution or for the online situation; and by suggesting re-dispatching of these solutions in order to achieve security.

A. Dynamic Security Assessment

Under operator's request, the dynamic security assessment (DSA) module evaluates the dynamic security of the Unit Commitment (UC) solution proposed for the highest planning horizon.

The implementation of this approach was performed by embedding the fast security assessment evaluation in the Long Term Unit Commitment (UC) module, as an additional restriction. This was modeled trough a Genetic Algorithm approach with insecurity margins to penalize insecure solutions. Since the security evaluation is provided by Artificial Neural Network (ANN) or Decision Trees (DT), each security evaluation is extremely fast.

Including security restrictions in the UC module increased the execution time of the module, however without compromising the proper operation of the MORECARE system.

B. Dynamic Security Monitoring

Under operator's request, the dynamic security monitoring (DSM) module has the task to evaluate the dynamic security of the power system, for the solution outputted by the economic dispatch (ED) module or for the current system operating stage. When insecurity is detected, this module may suggest an alternative secure dispatch solution. These measures directly act on the solution to be presented to the operator, which are provided in the form of new produced generators set points, based on a sensitivity analysis of the ANN outputs with respect to the inputs.

III. GENERATION OF FUNCTIONAL KNOWLEDGE

The generation of a representative knowledge *Data Set* of frequency dynamic behavior is a key stage for the success of this approach. An innovative data set generation procedure was adopted aiming at building an adequate knowledge base, able to describe implicitly the system dynamic security behavior of power systems with large wind power production.

This phase was based on the Structured Monte Carlo Sampling, considering system oddities and producing different settings for: system load level, non-dispatchable synchronous generation, asynchronous generation including wind power production, unit commitment and dispatch solution for the dispatchable synchronous generators. At the same time, other simplification techniques were used, like grouping similar generation units at the same power plant, in order to decrease the number of necessary patterns to be considered. This approach was able to embrace all the system operating conditions and generate feasible operating scenarios, with a viable number of samples, decreasing computational time without compromising the data set quality.

The automatic procedure developed to generate the DS is presented in Figure 2 and consists of the following main steps:

1. Construction of Hypercells

The DS operating range is previously defined and divided into *hypercells*. This procedure is performed according to the range and resolution assigned for the independent operating conditions to change, namely the total system load (*Pload)* and the non-dispatchable production (*Pnd)*.

2. Structured Monte Carlo Sampling
For each *hypercell*, the *Pload* and all *Pnd* variables are randomly sampled. In this procedure, besides the active generation sampling, the on/off status of the machines may also be sampled with a pre-defined probability.

3. Units Scheduling
For each *Pload/Pnd* scenario, a scheduling module considers all feasible scheduling combination of the dispatchable units, taking into account: maximum and minimum acceptable production limits of each unit and a spinning reserve criterion.

4. Dispatch
For each *feasible units scheduling scheme*, a dispatch module randomly distributes the insufficiency of power production by the units that were defined to be in operation by the scheduling module, considering again their production limits.

5. Power Flow
For each *selected dispatch solution*, the steady-state operating conditions are obtained through a power flow calculation. Before power flow solution, the total active load is splited by system loads and there is a previous definition on power factor for PQ synchronous generators, voltage values for PV synchronous generators and Mvar value for the local capacitor bank (including asynchronous generators).

6. Feasible Steady-State Solution
Before starting the dynamic simulation, the feasibility of the power flow solution is checked regarding system operating restrictions.

7. Dynamic Simulation
For each accepted steady-state solution and considered disturbance, a dynamic simulation analysis is performed in order to get the dynamic security indices. Namely, regarding the security problem under analysis for the study system, the considered security index was the maximum value reached by negative frequency deviations Δf (due to the importance of the relay settings of the load shedding frequency protection devices) and the maximum frequency rate of change (df/dt).
After each dynamic simulation analysis, a pattern is added to the DS, being characterized by the set of candidate attributes and the security indices Δf and (df/dt).

Some other requirements can be included in the DS generation procedure in order to increase the number of operating points near the security border, as described in [2].

IV. DESIGN OF SA STRUCTURES

The design of the security assessment structures involved two main interactive stages: attributes selection and derivation of security structures.

In order to perform accurately security assessment and preventive control, the set of attributes chosen to represent system state should have the following main characteristics:

- To be related with the dynamic phenomena under study;
- The number of attributes should be as low as possible without losing relevant information. (the concept of "equivalent machine" was used to group similar generators operating in parallel in the same plant);
- To use independent (or easy related) and dispatchable variables for further control use.

For instance generated powers and spinning reserves were found to be very interesting variables due to their relation regarding the phenomena under analysis and being also workable for the preventive control algorithms, as described in [2]. Although during an initial stage of this research, a feature selection mathematical approach (based on an F measure of separability) was used [5], the selection of relevant variables that feed the SA structures was only based in engineering judgment, according to the variable's properties described above.

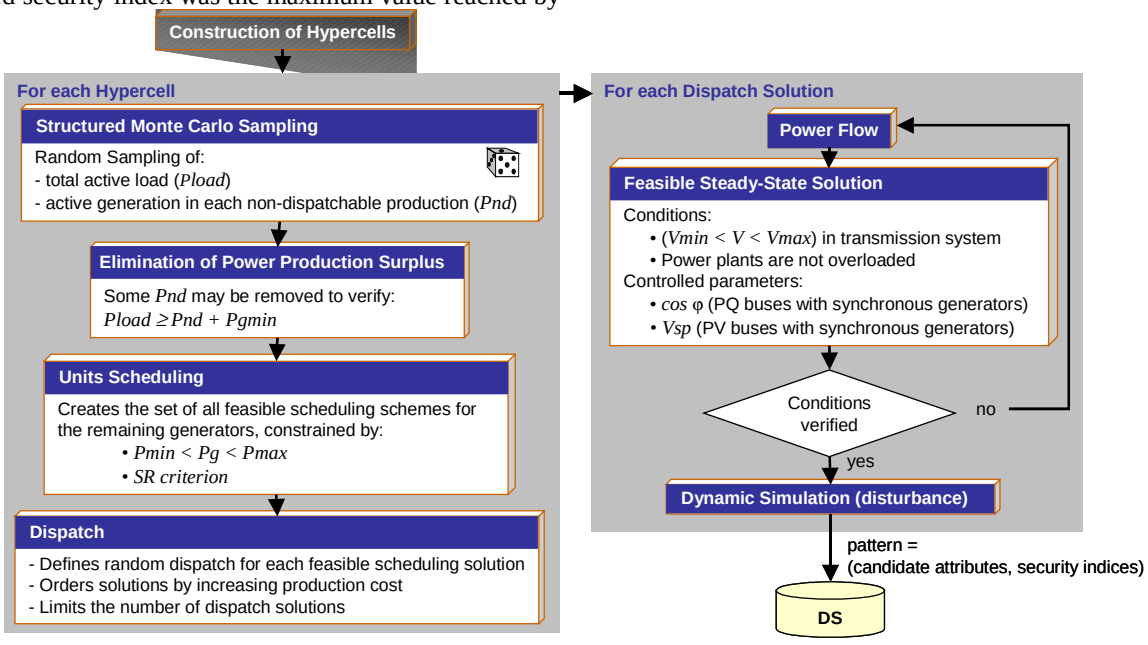

Figure 2 – Data Set generating flowchart

Three approaches have been used in this research to derive different alternative types of SA structures. Decision Trees are able to provide a classification in secure/insecure and ANN and Hybrid Regression Trees do provide an evaluation of the degree of robustness of the system through the emulation of the security indices.

A. Decision Trees

Decision trees are classification structures able to provide a classification in stable / unstable for each operating point under analysis. The construction of a DT starts at the root node with the whole learning set of pre-classified Operating Points (*secure / insecure*). The initial classification in *secure / insecure* is performed by observing the security indices values, calculated in the DS generation stage, and checking this value relatively to a security threshold that is naturally system dependent and that is related with frequency relay settings installed in the power system.

The construction of the DT is made through successive dichotomic tests that split the remaining data into a number of most "purified" mutually exclusive sub-tests, where the *a priori* classification is to be reproduced. A detailed description of this method is given in [3]. The DT is made of internal nodes and terminal nodes that can be leafs (where a *sufficiently* pure amount of data exists) or dead-ends. Each of the terminal nodes receives a classification according to the majority of the LS operating points classification that belong to that node.

B. Neural Networks

In this work we have used feedforward ANN, which were trained with the Adaptive Backpropagation (ABP) algorithm [4]. The stop training criterion was based in the well known cross validation principle, which fights against overfitting.

The ANN are trained for an architecture where the inputs are the relevant attributes that describe each operating point in the DS and the outputs are the one or two security indices, mentioned before.

ANN was chosen to perform SA functions, not only because they perform consistently better than traditional statistical methods in the dynamic security classification of power systems [5], but also because they provide evaluation of the system security degree, through the emulation of the security indices values.

C. Hybrid Regression Trees

The Hybrid Regression Tree (HRT) applied technique, is an automatic learning technique approach based on a Kernel Regression Tree (KRT) method, which integrates the classical Regression Trees (RT) with kernel regression [6]. This applied HRT approach, may provide 2 types of tree structures:

- a RT security structure, by considering the mean value as the predicting model to use at the tree terminal nodes (i.e. at the leafs);
- a KRT security structure, by considering a kernel regression as the predicting model to use at the tree terminal nodes. In all the current work, a K=3 was applied for the K-Nearest Neighbor rule, used to set the bandwidth of the regression model.

When applied to perform SA of power systems, the HRT approach may be used mainly to perform two types of functions:

- fast on-line security evaluation;
- extraction of interpretable security rules.

In fact the HRT can approximately reproduce the security indices values and provide in this way an evaluation of the robustness degree of the system. At the same time, since it contains a structure of **if then else** rules, it is possible to extract interpretable security rules, that can be used for preventive control purposes.

V. EVALUATION OF SA STRUCTURES QUALITY

The numerical indices used to evaluate the quality of the SA structures were, for ANN and HRT, the following:

Mean Absolute Error given by

$$MAE = \frac{1}{N(TS)} \sum_{OP_i \in TS} \left| y_i - \hat{y}_i(OP_i) \right|$$

Root Mean Squared Error given by

$$RMSE = \sqrt{\frac{1}{N(TS)} \sum_{OP_i \in TS} \left(y_i - \hat{y}_i(OP_i) \right)^2}$$

where:

$N(TS)$: Number of operating points (OP) in the testing set;

y_i: Real value of the security index, for OP_i;

$\hat{y}_i$: Value estimated by the structure, for the security index of OP_i.

The classification accuracy of each obtained structure was estimated by the following misclassifications rates:

$$\text{Global Class. Error} = \frac{\text{Nº}\{\text{OP of the TS incorrectly class.}\}}{\text{Nº}\{\text{OP of the TS}\}} \times 100\%$$

$$\text{False Alarm Error} = \frac{\text{Nº}\{\text{"secure" OP of TS class. as "insecure"}\}}{\text{Nº}\{\text{"secure" OP of the TS}\}} \times 100\%$$

$$\text{Missed Alarm Error} = \frac{\text{Nº}\{\text{"insecure" OP of TS class. as "secure"}\}}{\text{Nº}\{\text{"insecure" OP of the TS}\}} \times 100\%$$

These evaluation tests were performed for each relevant disturbance in each system (Crete and Madeira). From this analysis it was possible to identify that the most performing

SA structures, regarding accuracy in predicting or evaluating security and computational time, were DT and ANN. In fact HRT, although showing a comparable accuracy relatively to DT and ANN, were demanding larger computational requests namely in terms of memory (since the LS needs to be stored together with the security rules) and larger computational times, because when used for security prediction purposes a regression procedure needs to be used which may become more burden.

Therefore only DT and ANN were installed in the MORECARE prototype systems running in Madeira and Crete. The exploitation of these structures can then be activated by the operator, for each of the considered relevant disturbances.

VI. DYNAMIC SECURITY MONITORING

In the advanced control system, a security monitoring for the selected disturbances is performed continuously, which means that each trained ANN or DT (one for each considered disturbance) will be continuously fed with system attributes and will output the expected negative frequency deviation Δf (if an ANN is used) or will provide a secure / insecure classification if a DT is adopted. The attributes that feed the SA structure can be the output of the proposed dispatch solution or the same variables related with the present system operating conditions.

Two approaches have been developed to deal with the need to identify preventive control measures when insecurity is detected:

a) Heuristic approach based on the combined use of DT and economic dispatch;
b) Systematic approach based on a gradient iterative procedure that exploits the sensitivities of the ANN inputs relatively its output (the security index) to move the system towards a security region.

A. Heuristic Preventive Control Approach

Crossing the DT requires a simple checking of few rules and leads to a leaf of secure or insecure OPs. If the leaf is secure, the units' set points are displayed to the operator. In case of an insecure leaf or a deadend with a low security index, an alternative dispatch solution in the neighborhood of the previous solution is sought for, as follows: The test of the last splitting node of the DT is recorded and its threshold value P_u is used as equality constraint fixing the power produced by the respective generating unit. This restriction is then added to the Economic Dispatch problem that is then solved again for a total load that is now reduced in the amount of the power that is assigned to the generating that imposed the restriction. This procedure is applied iteratively until crossing the DT leads to a terminal node with a secure index. A complete description of this approach can be found in [7].

B. Exploiting ANN Sensitivities

This approach aims also in presenting to the system operator an alternative secure dispatch solution after an insecure state is detected. An exchange of power among generators is performed in order to move system towards security. For that purpose, a gradient based iterative procedure was implemented, where each step is given towards the security domain. Gradient directions are based on ANN sensitivity coefficients considering, at the same time, dependencies among ANN inputs. In this approach the solution may include redispatch of conventional units, but also connection / disconnection of wind generators.

Having in mind that the power system may have several independent producers, the search is constrained, in a first approach, to the utility generators. Although there are some agreements between utility and independent producers in what respect system control in case of insecurity, in this study the generators belonging to independent producers were considered as "non-controllable" – the most restrictive situation. A detailed description of the application of this method to the case of Madeira power system can be obtained in [2].

Both approaches will not necessarily lead to optimal solutions from the economic point of view. However they are able to provide an answer for those situations where is insecurity is detected and an alternative solution needs to be identified to increase operators confidence regarding the system dynamic behavior. The implementation of these preventive control measures will always be done on operators decision, namely for instance when due to abnormal atmospheric conditions the operator decides to increase robustness of operation.

VII. SOME RESULTS

The SA structures have been integrated in the MORECARE software and are presently being exploited in the prototypes running in Madeira and Crete. In Figure 3 (system installed in Crete), the Security Assessment screen displayed on call, is presented. On top of the screen, the load at critical buses, the current production of the wind parks and the production of the various thermal units in the two thermal stations are displayed in the form of bar charts.

The Dynamic Security Assessment results for 48 hours ahead, are displayed in the main screen under the forecasted load curve in the form of lines representing the expected frequency in case of the considered disturbances. The expected frequency is provided by the ANN structures. In this example it is shown that the expected frequency deviation in case of a short-circuit event is near the security threshold for most of the time. This contingency has a low probability of occurrence, unless the weather conditions are bad, and the operator might select to ignore it. Namely, between 1 and 8 o'clock however, the expected frequency deviation is shown to be very near the 49 Hz. It is characteristic that this period corresponds to the low load period, when a significant wind power penetration can lead to poor dynamic security. In this

case, the operator can seek alternative dispatch using the mentioned approaches.

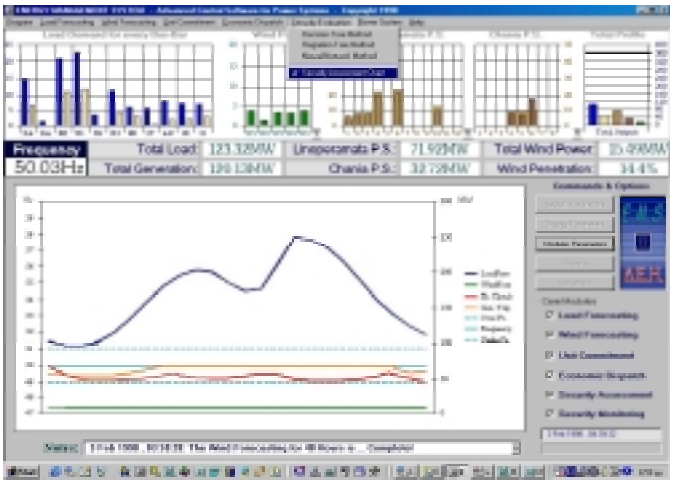

Figure 3 – Man-Machine Interface of on-line DSA.

An example of a DT used for the Cretan power system and for a machine outage is presented next in figure 4.

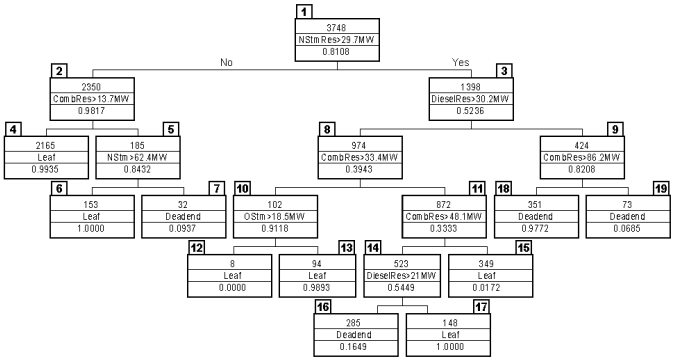

Figure 4 – Decision Tree for a Machine Outage disturbance

The quality of the SA structures used can be observed through the performance results obtained for two disturbances, one in the Cretan system (machine outage) and the other in the Madeira system (short circuit in a selected bus at the western side of the island, causing the disconnection of several wind parks and hydro plants). Table 1 describes these results.

The classification errors were obtained in a test set that contains around 30% of the total DS operating points. By analyzing these results (which give a good image of the typical performance behavior), we may conclude that, in general, ANN provide better classification performance results and are able to predict the system frequency deviation or df/dt for a specified disturbance. However DT rules can be easily understood and exploited for preventive control as mentioned.

More information on the quality of the preventive control procedures mentioned in this paper can be obtained in [2,7].

Table 1 – Evaluation of quality of SA structures

	Disturbance in Cretan power system	Disturbance in Madeira power system
Nº of Sec OP	1136	6616
Nº of Insec OP	4599	1412
MAE	------	0.023
RMSE	------	0.037
Total Error (%)	3,473	0,33
False Alarm Error (%)	4,684	0,30
Missed Alarm Error (%)	3,141	0,48

VIII. CONCLUSIONS

The development and use of SA applications is of crucial importance in helping defining the operation policies of isolated power systems where non-controllable power sources (like wind power) have important share of the production. In this project the application of tools that exploit functional knowledge of the system (gathered off-line) was the key for the success of the dynamic security assessment and monitoring. Further research is needed to address issues related with automatic adaptation of the SA structures to system expansion.

REFERENCES

[1] N. Hatziargyriou, etal., "The MoreCare System Overview", to be presented at the MedPower 2002 Conference, Athens, November 2002.

[2] H. Vasconcelos, J. Fidalgo, J. Peças Lopes, "A General Approach for Security Monitoring and Preventive Control of Networks with Large Wind Power Production", Proc. 14th PSCC, Sevilla, June 2002.

[3] Louis A. Wehenkel, "Automatic Learning Techniques in Power Systems", Kluwer Academic Publishers, ISBN 0-7923-8068-1, 1998.

[4] F. M. Silva, L. B. Almeida, "Acceleration Techniques For The Backpropagation Algorithm", In Neural Networks, L. B. Almeida and C. J. Wellekens (Eds.), Springer-Verlag, 1990.

[5] J. N. Fidalgo, J. A. Peças Lopes, V. Miranda, "Neural Networks Applied To Preventive Control Measures For The Dynamic Security Of Isolated Power Systems With Renewables", IEEE Transactions on Power Systems, Vol. 11, November 1996.

[6] Torgo, L., *"Kernel Regression Trees"*, poster paper of the European Conference, on Machine Learning (ECML-97), Internal Report of the Faculty of Informatics and Statistics, University of Economics, Prague, 1997.

[7] E. Karapidakis, N. Hatziargyriou, "On-line Preventive Dynamic Security of Isolated Power Systems Using Decision Trees", IEEE Trans. on PWRS, June 2002.

Acknowledgments

The authors express their gratitude to the EU-DGXII for funding the project N°:NNE5-1999-00726 "MORE CARE".