On-line Dynamic Security Assessment based on Kernel Regression Trees

J. A. Peças Lopes (1,2)
jpl@duque.inescn.pt
(1) FEUP – Faculdade de Engenharia da Universidade do Porto, Porto – Portugal

M. H. Vasconcelos (2)
hvasconcelos@inescn.pt
(2) INESC - Instituto de Engenharia de Sistemas e Computadores, Porto – Portugal

Abstract: This paper presents a new approach to perform on-line dynamic security assessment and monitoring of electric power systems exploiting a statistical hybrid learning technique – the Kernel Regression Trees. This technique, besides producing fast security classification, can still quantify, in real-time, the security degree of the system, by emulating continuos security indices that translate the power system dynamic behavior. Moreover it can provide interpretable security structures. The feasibility of this approach was demonstrated in the dynamic security assessment of isolated systems with large amounts of wind power production, like in the Crete island electric network (Greece). Comparative results regarding performances of Decision Trees and Neural Networks are also presented and discussed. From the obtained results, the proposed approach showed to provide good predicting structures whose performance stands up to the performance of the two other existent methods.

Keywords: Power system security, Dynamic security assessment, Automatic learning, Regression trees, Kernel regression models, Wind power generation.

I. INTRODUCTION

Fast dynamic security assessment is becoming one of the key issues in the operation of networks, namely when managed within a competitive and deregulated electricity market environment. The increased penetration in the system of independent power producers and specially wind power is also contributing to decrease system robustness. In isolated power systems, like the ones operating in large islands, this problem is quite critical and deserves a special care.

In the last decade a big research effort has been developed in the field of the application of automatic learning techniques to deal with this problem. Pattern Recognition, Decision Trees, Neural Networks and Regression Trees have been used to provide fast security assessment in several domains. Some examples can be found in [1] and [2].

The application of these techniques in the dynamic security assessment of isolated systems has been particularly well succeeded, as demonstrated by the Lemnos project [3]. The main problems faced by isolated electrical power systems are related to system security, control of frequency and management of system generation reserve.

A common aspect to all these problems is the requirement to ensure that sufficient reserve capacity exists within the system to compensate for sudden loss of generation. Thus, mismatches in generation and load and/or unstable system frequency control might lead to system failures. This type of instability is termed frequency instability and depends on the ability of the system to restore balance between generation and load following a severe system disturbance with minimum loss of load [4]. Generally, frequency instability problems are associated with inadequacies in equipment responses, poor coordination of control and protection equipment or insufficient generation reserve.

In medium-sized or large isolated power systems with high penetration of wind power sources, wind power production has a strong influence in the dynamic security and economy of dispatch and generation schedule. Thus, besides load forecast, the suggested units scheduling and generation dispatch must consider wind power forecast and, contrary to interconnected systems, can no longer be performed off-line. Economic operation must be divided into a unit commitment module and a dispatch module that are performed in sequence, with an optional intermediate decision step that allows the operator to take into account information automatically produced by a module of fast dynamic security assessment. In this way, the wind power penetration can be increased without jeopardizing the system security. Such functions have been developed and are integrated within an advanced control system tailored to the needs of small isolated power systems with increased wind power penetration.

Such a work was developed within the framework of an European R&D project of the JOULE/THERMIE program - the CARE project. The CARE system is an advanced control system that aims to achieve optimal utilization of renewable energy sources, in a wide variety of medium and large size isolated systems with diverse structures and operating conditions [5]. During 1999, a pilot installation of this system was installed on the energy management center of Crete island.

The objective of this paper is to present a methodology that applies Kernel Regression Trees (KRT) – a new procedure of automatic learning presented by Torgo in 1997 [6] – to perform fast dynamic security assessment and security monitoring. The application domain is related with the operation of isolated systems with high penetration from wind power production. The security evaluation structures provided by this approach were integrated into the previously mentioned CARE system.

The KRT security evaluation structures that can be obtained provide a classification on dynamic security. Moreover, they also produce the degree of security, which is evaluated by

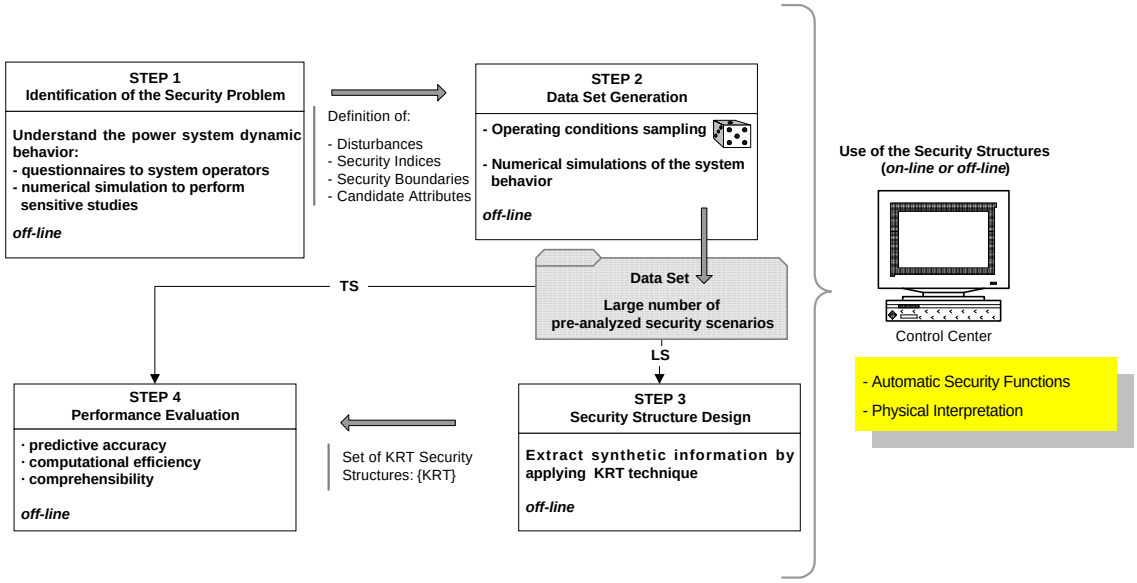

Fig. 1 – Main steps to apply Kernel Regression Trees to perform dynamic security assessment

emulating the expected value of a security indices that translate the power system dynamic behavior. Comparative results regarding performances of two other automatic learning techniques, namely Decision Trees (DT) and Artificial Neural Networks (ANN), are presented and discussed.

II. MAIN STEPS TO APPLY KRT

Four main steps must be considered in order to apply Kernel Regression Trees to perform dynamic security assessment (see Fig. 1). All these steps are performed off-line. The final product of the procedure – the security structures – is to be used in an on-line environment in the power system control center, or to obtain physical interpretation of the system behavior. These steps are synthetically described below.

A. *Step 1: Identification of the Security Problem*

The first thing to do is to identify the dynamic security problem to evaluate. This analysis involves a procedure of understanding the power system dynamic behavior, namely to identify the potential situations for which the system may lose security. This typically requires making questionnaires to the system operators, and also performing sensitivity studies by running analytical tools of dynamic simulation. This first step defines the structure of the data set to generate, namely:

- the disturbances for which is important to known the expected behavior of the system;
- the security indices to predict, y, and corresponding security boundaries;
- the measurement vector of candidate attribute, $OP = [a_1,a_2,...,a_{Na}]$, to use in order to characterize the system operating points.

A complete security assessment should include all the disturbances that are eminent to occur and might endanger the power system security. The selection of the security indices, must be made having in mind that what is important to predict is the "distance" to the security boundary if a pre-defined disturbance occurs. Some typical security indices used for frequency stability problems are:

a) Maximum and minimum values reached by transient frequency deviation (f_{max} and f_{min});

b) Maximum value reached by the rate of frequency changes (df/dt_{max}).

The selection of the candidate attributes is a very important issue in the procedure because, in order to achieved good results, it is required to use as candidate attributes the power system operating parameters that have influence on the type of dynamic behavior to predict. Candidate attributes are operating parameters that can be directly or indirectly measured from the power system and which can be of the following two main categories: a) Pre-disturbance steady state variables; b) Post-disturbance transient state variables.

B. *Step 2: Data Set Generation*

This step concerns with the generation of a large data set (DS) of pre-analyzed security scenarios of the system behavior, consisting of samples with the form (OP,y). These samples will be the input data to the design and performance evaluation of the security structures. In fact, to design a security structure a learning set (LS) is required, whereas to evaluate its performance characteristics an independent testing set (TS) is also required. The LS and TS, although independent, must result from the same distribution. Therefore, they must be obtained by randomly dividing the DS, resulting in the following sets:

$$LS = \{(OP,y)_1,...,(OP,y)_{N(LS)}\}; TS = \{(OP,y)'_1,...,(OP,y)'_{N(TS)}\} \quad (1)$$

Luis Torgo in [7] claims that to have a sufficient amount of samples in the LS and TS to ensure quality of the KRT security structure and reliable error estimates, the following method must be used to decide the size of the TS:

$$\#\{TS\} = min(0.3\times\#\{DS\},1000) \quad (2)$$

The data set generation procedure can be summarized as follows:

Given an operating range and resolution, a data set of samples is created that reflects the dependency of the system behavior (i.e., the security index y) with the variation in its operating conditions (i.e., the measurement vector OP).

For the particular problem under analysis, the operating conditions that are usually considered to change between samples are the following: a) system load level; b) penetration of renewable power sources; c) network configuration; d) unit commitment and generation dispatching schemes. These operating conditions must have high influence on the dynamic behavior *y* to predict. Otherwise, they will unnecessarily increase the number of samples to generate, without improving the information contained in the DS.

In the generation procedure, among the operating conditions to change, the ones that are independent parameters (i.e., their values do not depend on other operating conditions) are randomly sampled by a systematic method, according to a pre-defined operating range and resolution. Then, for each sample, a unit commitment and economic dispatch module prepare the generation scenarios. Finally, both measurement vector *OP* and dynamic behavior *y* of each sampled operating scenario are provided by running a proper analytical tool that simulates the system behavior.

When defining the operating scenarios to create the samples, the actual operating practices that are performed in the power system must be considered. This is a very important issue because if the information contained in the data set does not reflect the mechanism of the system behavior in a proper way, then, in spite of having a good testing accuracy, there is no assurance that the extracted structures will be accurate enough when making prediction to real life operating scenarios. For the same reason, the data set should consist on an enough number of samples to cover all possible states of the power system under study. Therefore, the generated OPs must cover the breadth of the system operating range and with the best possible resolution. Specially, in order to obtain good accuracy when predicting security classification, the data set must have good resolution in the neighborhood of the security boundary. This can be improved by generating more samples. However, the computational time for the generation and predicting procedure will always introduce some limitation to this number.

C. *Step 3: Security Structure Design*

After the LS and TS being generated, it is then possible to apply the Kernel Regression Trees technique to extract security structures from the LS, which are designed in order to be the best approximation to the unknown function $y = f(OP)$.

D. *Step 4: Performance Evaluation*

To select the best security structure within the set of the extracted ones, the designed structures are applied to the TS to evaluate their performances. According to the control center requirements, the security structures can be evaluated by looking into account three main issues: a) predictive accuracy; b) computational efficiency; c) comprehensibility of the security structures. This evaluation is mandatory to be performed since it is the only way that allows comparing predicting performance between different automatic learning methods, and between security structures extracted by a same automatic learning method. The comprehensibility of the designed structures is a quite interesting feature as preventive control procedures can be extracted from the security structures if their complexity is not very large.

III. APPLICATION OF KERNEL REGRESSION TREES

As the Kernel Regression Tree approach is being applied for the first time in the dynamic security assessment field, a short description of the main stages of the method are included in the next paragraphs. The Kernel Regression Tree is an hybrid algorithm that integrates Regression Trees (RT) with Kernel Regression (KR), dealing with continuous goal variables (i.e. regression problems). The model used in this research to obtain the KR is the one described by L. Torgo in [6]. The design of a RT consists in the extraction of interpretable security rules. The existing RT approaches differ in the predicting function used in the leafs. For instance, in CART [8] a mean value of *y* is used, whereas Karalic [9] and Quinlan [10] use a linear regression function. Kernel Regression models ([11] - Watson; [12] - Nadaraya), which is a non-parametric statistical methodology, provide quite opaque models of the data, but, on the other hand, are able to approximate highly non-linear functions. By integrating this regression procedure in the tree leafs, we can obtain a model with a better accuracy, by increasing the non-linearity of the functions used at the leafs. Furthermore, in highly non-linear problems, by integrating kernel regression models in the tree leafs, it is possible to overcome the limitations of the individual kernel regression model, both in terms of accuracy and computational efficiency [13].

The design of a KRT involves two interrelated stages:

- Design of a binary tree structure by considering the mean value as the model to use at the tree leafs, which consists in designing a regression tree (RT);
- Obtain the KRT structure by assigning a kernel regression model to make prediction in the tree leafs.

The technique applied to avoid overfitting problems was a pruning algorithm based in the one presented in CART [8]. To perform this algorithm, first a very large RT, which is supposed to overfit the LS, must be designed by applying stop-splitting rules.

A. *Design of a Regression Tree Using Stop-Splitting Rules*

The design of a RT is determined by the following two issues: a) the optimal splitting test; b) the stop-splitting rules. Starting with the root node, which corresponds to the LS, the growing of the RT is made by successively splitting their nodes. This splitting is performed by a test defined as:

$$\{a_k(sample) > u_k\}? \quad (3)$$

where u_k is the optimal threshold value of the chosen candidate attribute a_k. By applying this test to all the samples in the node, two successor nodes are created, which correspond to the two possible instances of the test $\{a_k(sample) > u_k\}$ and $\{a_k(sample) \le u_k\}$. The design of the RT consists in explaining as much as possible the variance of the security index *y* observed in the LS. According to this goal, the split of each node must be performed according to an *optimal splitting criterion*, which corresponds to the split *"s"* that maximizes:

$$\Delta s^2(s,t) = s^2(t) - P_L \times s^2(t_L) - P_R \times s^2(t_R) \quad (4)$$

where: $s^2(t)$ - variance of *y* at the learning samples stored in node *t*; P_L and P_R - proportion of the number of learning samples at the left and right successor nodes; $s^2(t_L)$ and $s^2(t_R)$ - variance of *y* at the left and right successor nodes.

The procedure continues splitting the created successor nodes, until a stop-splitting criterion is met for all the non-split nodes. The criterion used is defined by the two stop-splitting rules:

– Rule 1: It is not possible to further reduce variance of *y* in a statistically significant way. This corresponds to verify if a minimum number of learning samples, N_{min}, has been reached in the node.

– Rule 2: The variance of *y* has been sufficiently reduced. This corresponds to verify if a minimum value $s^2(y)_{min}$ as been reached in the node.

B. *Predicting with Kernel Regression Models in the Tree Leafs*

Once the design of the RT, to obtain a KRT structure, a kernel regression model is assigned to make prediction at the tree leafs. Given a new unseen operating point *Q*, a prediction for its security index, *y(Q)*, is obtained by applying a regression model to the learning samples stored in the RT leaf that verifies the *Q* operating conditions. Kernel Regression models make prediction by a weighted average of the response *y* of the form:

$$y'(Q) = \frac{\sum_{i=1}^{samples} K_h[D(Q,OP_i)] \times y_i}{\sum_{i=1}^{samples} K_h[D(Q,OP_i)]} \quad (5)$$

where $D(Q,OP_i)$ - normalized distance function measured in the attributes hyperspace; *h* - bandwidth value; $K_h[x] = K[x/h]$, being $K(.)$ the Kernel function. The prediction is obtained using the samples (also denominated by *neighbors*) that are "most similar" to *Q*, being this similarity measured by the distance function. The Kernel function estimates the weight of each neighbor, giving more weight to neighbors that are nearest to *Q*. The design of the kernel regression model includes the choice of the distance function, the bandwidth value, and the kernel function. In the implemented model it was used an Euclidean distance, a k-nearest neighbor (KNN) rule to define the bandwidth, and a Gaussian $K(d) = e^{-d^2}$ to define the kernel function. KNN method sets the bandwidth value *h* as the distance *D* to the k-nearest neighbor of *Q*. It also sets that only the k-nearest neighbors will be used to make prediction.

C. *Design of Kernel Regression Trees by Applying a Pruning Algorithm*

The implemented pruning algorithm, applied to design a KRT structure, comprises the following stages:

1) Design a very large regression tree, RT_{max}, which is supposed to overfit the LS, by applying the previously described design procedure that exploits only the stop-splitting rules.
2) Generation of a sequence of pruned trees with decreasing complexity, $RT_1 \succ RT_2 \succ \ldots \succ root$ where $RT_1 \prec = RT_{max}$, by progressively pruning RT_{max} upward in the "right way" until being reached the root. Note that a subtree RT_i of *RT* is referred as a pruned tree of *RT* if $root(RT_i) = root(RT)$, which can be denoted by $RT \succ RT_i$. To generate the sequence of pruned trees, a selective pruning process is applied, that generates a reasonable number of pruned trees of RT_{max}, with decreasing size, such that each subtree is the "best" pruned tree in its size range. To make this selection, a *minimum error-complexity criterion* is applied as described in [8].
3) By considering the kernel regression model previously described to make prediction at the tree leafs of the generated set of regression trees, $\{RT\}=\{RT_1,RT_2,\ldots,root\}$, results a set of kernel regression trees, $\{KRT\}=\{KRT_1, KRT_2,\ldots,root\}$.
4) To select, among the available set $\{KRT\}$, the more suitable security structure to make on-line dynamic security assessment, the designed structures are applied to the TS to obtain an accurate estimation of their performances, namely predictive accuracy and computational efficiency.

IV. CASE STUDY AND RESULTS

This section presents the results obtained with the proposed Kernel Regression Tree approach, to perform fast dynamic security assessment of the Crete power system. The study case system is a realistic model of the power system of the Crete island, projected for the year 2000. It comprises several types of oil-fired units and a meshed 150 kV transmission network, where a peak load of approximately 360 MW and an installed wind power of 81 MW was considered. The generation of the Crete data set was developed by National Technical University of Athens (NTUA), within the framework of the CARE project. The data set comprises 2765 samples, which 1844 belong to the LS and 921 to the TS. Each sampled scenario was pre-analyzed using an analytical tool of dynamic simulation – EUROSTAG software – to extract, among others, the following security indices: $y_1 = f_{min}$ *due to machine loss*; $y_2 = f_{min}$ *due to short circuit*. To verify system security regarding f_{min} security index, the following security boundary was considered:

If $f_{min} \leq 49$ *Hz* ***then*** *sample is "insecure";*
else *sample is "secure".*

For the vector of candidate attributes that characterizes each OP, 22 pre-disturbance steady-state operating parameters were selected. A more detailed description of the power system and applied data set generation procedure can be found in [14]. Because of lack of space, only some comparative results regarding performances of Decision Trees (DT) and Neural Networks (ANN) are presented in this paper. The DT and ANN used approaches are the ones described in [3]. The ANN approach was applied to obtain a security structure for the y_1 and y_2 security indices, whereas a DT structure was obtained only for the y_2 security index.

The testing set (TS) predictive accuracy results, obtained for the designed security structures, are presented in Fig. 1 and Fig. 2. The classification errors used were the *global*, *false alarm* and *missed alarm errors*. In order to quantify regression errors, the indicators used were the *mean absolute error* and the *root mean square error* (*MAE* and *RMSE*). In each figure, the number of secure and insecure samples in the TS is also presented.

From the obtained regression errors, one can observe that, regarding the evaluation of the system security degree, among the ANN and KRT approaches the latest one showed to be more accurate for the y_1 security index, whereas for the emulation of y_2, it is not possible to state clearly that one approach is more accurate than the other.

Regarding security classification, among the ANN and KRT approaches, the previous one showed to achieve smaller errors for the y_1 security index and higher ones for the y_2 security index. Regarding the DT performance for the y_2 security index (machine loss), the KRT showed to provide smaller *global* and *false alarm* errors and a lightly higher *missed alarm*.

For the obtained KRT structures, the estimated values of their response time to predict a security index for one operating point is quite small (in the order of milliseconds in a Pentium II machine), being therefore suitable for on-line implementation.

Making a general analysis, we can say that all the three approaches were able to provide efficient security structures, and with comparable predicting error performances. Based on the KRT proposed technique, simple, interpretable and reliable security structures can be provided. The KRT and ANN methods have the advantage of producing simultaneously a classification structure and giving the degree of robustness of the system, whereas the DT method can only perform security classification. On the other hand, the KRT and DT methods can provide interpretable rules of the system security class (i.e., classification rules), whereas ANN always provide quite opaque models of the data. Besides classification rules, the KRT method can still provide interpretable rules of the system security degree (i.e., regression rules).

To illustrate a KRT structure, Fig. 3 presents the tree structure with equivalent regression and classification rules, of a KRT (with 9 nodes) obtained for the y_2 security index. This tree contains nodes of two types: non-terminal and terminal nodes (leafs). The root node (node number 1) includes information related with the total number of stored learning samples (1844 - total LS), the *variance* (s^2) of the security index in the LS and the splitting test. Non-terminal nodes present the node number, containing also information related to the splitting test. The leaf nodes present information related with the node number, the number of learning samples stored there (*N*), and the *Mean* and variance of the security index in those samples. In this classification structure one can assign a given degree of security to each leaf accordingly to its *Mean* value. Namely, for this example, the security structure can be translated into the interpretable regression and classification rules that are also presented in Fig. 3.

An important feature of this approach is that a given KRT structure, although being selected among the {*KRT*} set with a specific objective (classification, emulation or interpretation),

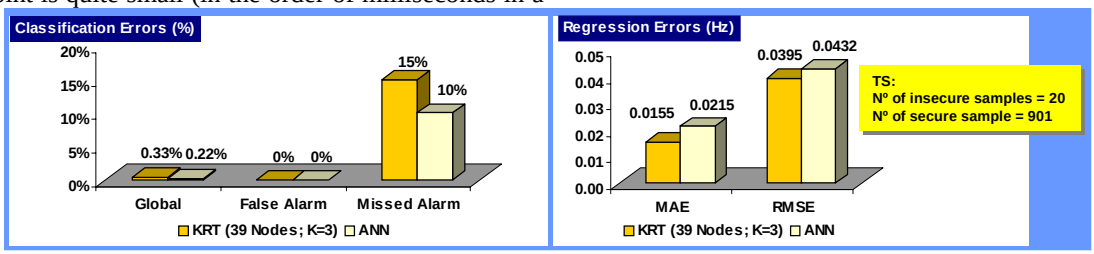

Fig. 1 – TS performance evaluation results for the KRT and ANN approaches (y_1 *security index*)

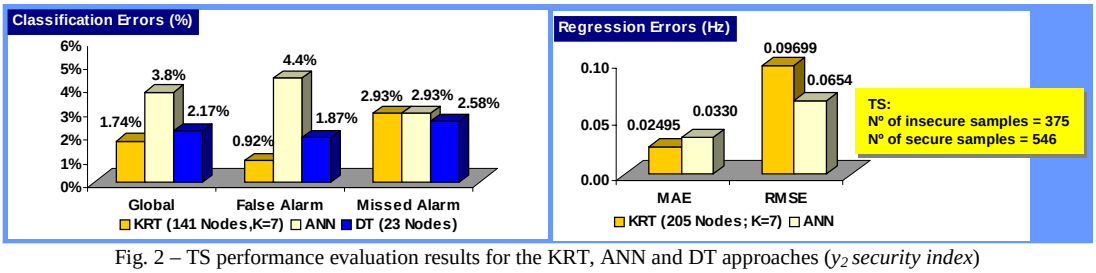

Fig. 2 – TS performance evaluation results for the KRT, ANN and DT approaches (y_2 *security index*)

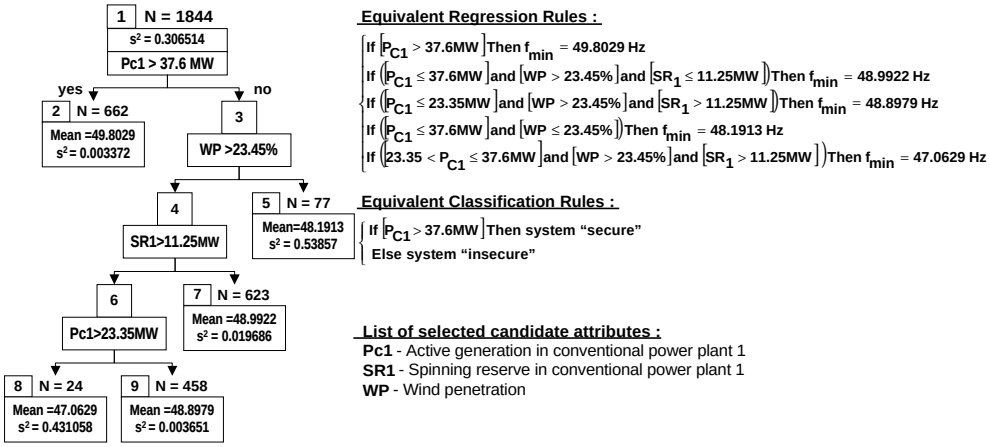

Fig. 3 – KRT security structure with 9 nodes and extracted regression and classification rules (y_2 *security index*)

can always be used simultaneously, in a consistent way, to perform the three previous functions. This provides a framework, such that a KRT used for on-line security evaluation, can be exploited afterwards for preventive control purposes, namely by the extracted security rules.

V. CONCLUSIONS

This paper described a new hybrid automatic learning technique, named as Kernel Regression Tree, to make, for the first time, dynamic security assessment of power system in the field of frequency stability problems. Within the framework of the European R&D project JOULE/THERMIE, the implemented KRT approach was integrated within the advanced control system that is being installed, during the present year, on the energy management center of Crete island, to perform dynamic security assessment functions. From a performance evaluation of the obtained results and a comparative assessment with Decision Tree and Artificial Neural Network, the KRT showed to provide good predicting structure whose performance stands up to the performance of the two other existent methods.

VI. ACKNOWLEDGMENTS

The authors would like to thank the financial support of PRAXIS XXI within the "Subprograma Ciência e Tecnologia do 2º Quadro Comunitário the Apoio" and to EU project JOR3-CT96-0119. They are also grateful to all the other members of the project JOR3-CT96-0119 for their contributions.

VII. REFERENCES

[1] L. Wehenkel, "Contingency severity assessment for voltage security using non-parametric regression techniques", IEEE PES 1995 Winter Meeting.

[2] J.A. Peças Lopes and F. Fernandes, "Fast Evaluation of Voltage Collapse Risk Using Machine Learning Techniques", Proceedings of VI SEPOPE, S. Salvador ad Baia, Brazil, May 1998.

[3] ARMINES, NTUA, INESC, RAL, PPC, "Development and implementation of an advanced control system for the optimal operation and management of medium-sized power systems with a large penetration from renewable power sources", Final report of EU-DG XII JOULE II project JOU2-CT92-0053. Edited by the Office for Official Publications of the European Communities, Luxembourg 1996.

[4] P. Kundur, Power Systems Stability and Control, McGraw – Hill, 1993 ISBN 0-07-035958-x.

[5] N. Hatziargyriou et al., "Control of isolated power systems with increased wind power integration", Proceedings of IEE med. Power Conference, Lefkosia, Cyprus, November 1998.

[6] L. Torgo, "Kernel Regression Trees", poster papers of the European Conference, on Machine Learning (ECML-97), Internal Report of the Faculty of Informatics and Statistics, University of Economics, Prague. ISBN:80-7079-368-6, 1997.

[7] L. Torgo, "Error Estimates for Pruning Regression Trees", Proceedings of the 10th European Conference on Machine Learning (ECML-98), Nedellec,C. and Rouveirol,C. (eds.). Lecture Notes in Artificial Intelligence 1398, Springer Verlag, 1998.

[8] L. Breiman, H. F. Friedman, R. A. Olshen, C. J. Stone, "Classification and Regression Trees", Wadsworth International, 1984.

[9] A. Karalic, "Employing Linear Regression in Regression Tree Leaves", Proceedings of ECAI-92, Wiley & Sons, 1992.

[10] J. R. Quinlan, "Learning with Continuos Classes", Proceedings of the 5th Australian Joint Conference on Artificial Intelligence,. World Scientific, 1992.

[11] G. S. Watson, "Smooth Regression Analysis", Sankhya: The Indian Journal of Statistics, Series A, 26: 359-372, 1964.

[12] E. Nadaraya, "On estimating regression", Theory of Probability and its Applications, 9:141-142, 1964.

[13] L. Torgo, "Functional Models for Regression Tree Leaves", Proceedings of the International Conference on Machine Learning (ICML-97), Fisher,D.(ed.), Morgan Kaufmann Publishers, 1997.

[14] N. Hatziargyriou, J. A. Peças Lopes, E. Karapidakis, M. H. Vasconcelos, "On-Line Dynamic Security Assessment of Power Systems in Large Islands with High Wind Power Penetration", Proceedings of PSCC´99 - 13th Power Systems Computation Conference, vol. 1, Trondheim - Norway, June 1999, pp. 331-337.

VIII. BIOGRAPHIES

João A. Peças Lopes was born in Portugal in May 1958. He graduated in Electrical Engineer from the Engineering Faculty of Porto University (FEUP) in July 1981, and obtained the Ph.D: and Aggregation degrees also from FEUP in October 1988 and November 1996 respectively. Dr. Peças Lopes is presently Assistant Professor with Aggregation at FEUP and Assistant Coordinator of the Power Systems unit at INESC Porto.

Maria Helena Vasconcelos was born in Porto, Portugal, on March 19, 1973. She graduated in Electrical Engineer from the Engineering Faculty of Porto University (FEUP) concluded in July 1996, and obtained the MSc. from FEUP in October 1999. Since September 1996 she works as a researcher in the Power System Unit of INESC Porto, having performed research work in automatic learning techniques and consultancy studies in the field of frequency stability, small-signal stability and security exploration of power system.