ON-LINE DYNAMIC SECURITY ASSESSMENT OF ISOLATED NETWORKS INTEGRATING LARGE WIND POWER PRODUCTION

J. A. Peças Lopes[1] **N. Hatziargyriou**[2] **M. Vasconcelos**[1] **E.Karapidakis** [2] **J. Fidalgo** [1]

1 Faculdade de Engenharia da Universidade do Porto (FEUP) and INESC-Porto, Largo de Mompilher, 22, 4007 Porto Codex, Portugal, e-mail: jpl@riff.fe.up.pt
2 Department of Electrical and Computer Engineering, National Technical University of Athens, (NTUA) 9, Heroon Polytechniou,, 157 73 Zografou, Athens, Greece, e-mail: nh@power.ece.ntua.gr

ABSTRACT

The paper describes the on-line dynamic security assessment functions developed within CARE. These functions are based exclusively on the application of machine learning techniques. A description of the problem and the data set generation procedure for the Crete island power system are included. Comparative results regarding performances of Decision Trees, Kernel Regression Trees and Neural Networks are presented and discussed.

1. INTRODUCTION

In isolated networks where there is a large penetration of wind power production, system security and control of frequency are major problems in the operation of the system. A common aspect to these problems is the requirement to ensure that sufficient reserve capacity exists within the system to compensate for sudden loss of generation (Kundur and Morison, 1997).

Fast wind power changes and very high wind speeds resulting in sudden loss of wind generator production can cause frequency excursions and dynamically unstable situations (Hatziargyriou, Karapidakis and Hatzifotis, 1998). Moreover, frequency oscillations might easily trigger the under-frequency protection relays of the wind parks, thus causing further imbalance in the system generation/load. The dynamic behaviour performance of these systems depends not only on the total load and the size of the conventional units in operation, but also on their location and the response of the available spinning reserve (Hatziargyriou et al, 2000).

In order to guard isolated power systems against the consequences of these disturbances it is necessary to keep acceptable security levels in the network. On-line dynamic security assessment and monitoring are very important functions to assure these requirements. Such security functions have been developed and integrated within the CARE control system.

Conventional dynamic security evaluation is, however, a large time consuming task and therefore unsuitable for on-line purposes. Application of machine learning techniques is the approach that enables to cope with the time computational reduction needs.

This paper describes the application of machine learning techniques to the on-line dynamic security assessment of the Crete island power system, considering the large degree of wind power production levels foreseen for a near future. Advanced inductive inference and statistical methods as well as artificial neural networks were used to provide on-line dynamic security assessment and security monitoring of these systems.

The security evaluation structures that were obtained provide a classification on dynamic security when Decision Trees and Regression Trees are used while an emulation of the security index is provided when Kernel Regression Trees and Neural Networks are used. The availability of the degree of security, (which in this case is evaluated by predicting the expected minimum value of system frequency and the maximum rate of frequency change for a selected disturbance) is also most important as it helps evaluating the robustness of the system.

In the CARE software, security evaluation functions can be activated “on call” by the operator, namely security monitoring. These functions provide the security robustness information needed by the CARE operation algorithm, as described by Hatziargyriou et al, 2000.

2. THE STUDY CASE SYSTEM

The development of these procedures was performed over a realistic model of the power system of Crete, projected for the year 2000. As mentioned by Hatziargyriou et al., 2000, all WPs, with only a few exceptions, will be installed at the eastern part of the island of Crete, that presents the most favorable wind conditions. As a result, in case of faults on some particular lines the majority of the wind parks will be disconnected. Furthermore, the protections of the WTs might be activated in case

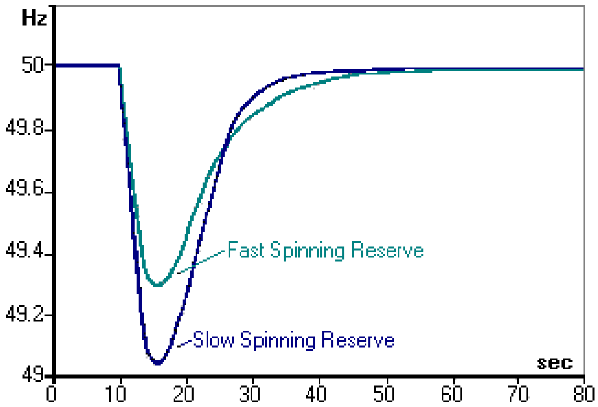

Figure 1. Frequency change.

of frequency variations, decreasing additionally the dynamic stability of the system. This might happen in case of frequency variations caused by wind fluctuations, conventional unit outages, faults or other disturbing conditions.

Extensive simulations on the power system model have been performed using EUROSTAG software in order to identify and understand the problems from a physical point a view. From these studies it was possible to conclude that for the most common wind power variations, the system remains satisfactorily stable, if sufficient spinning reserve is provided. On the other hand for various short-circuits and conventional unit outages, the system frequency undergoes fast changes and might reach very low values. In any case, the dynamic security of the system depends critically on the amount of spinning reserve provided by the conventional machines and the response of their speed governors.

As an example, Figure 1 shows the change of the system frequency in two different operating conditions, following the disconnection of three wind parks producing approximately 30 MW. First, the system is considered to operate with 28% of wind power, equal to 46 MW and with the fast thermal units, such as the Diesel machines and gas turbines to provide the spinning reserve (fast spinning reserve). The lower value of the frequency is 49.31Hz. Secondly, the system is again considered to operate with the same high penetration of wind power but with the slower machines, such as the steam turbines to cover mainly the spinning reserve plus some Diesel machines (slow spinning reserve). In this case, the lower frequency value, which is equal to 49.04Hz, will cause the operation of the protection devices of the rest of the wind parks. The total wind power disconnection may lead the system to collapse.

3. APPLICATION OF MACHINE LEARNING TECHNIQUES

The application of machine learning techniques in the field of dynamic security assessment requires a four step approach,

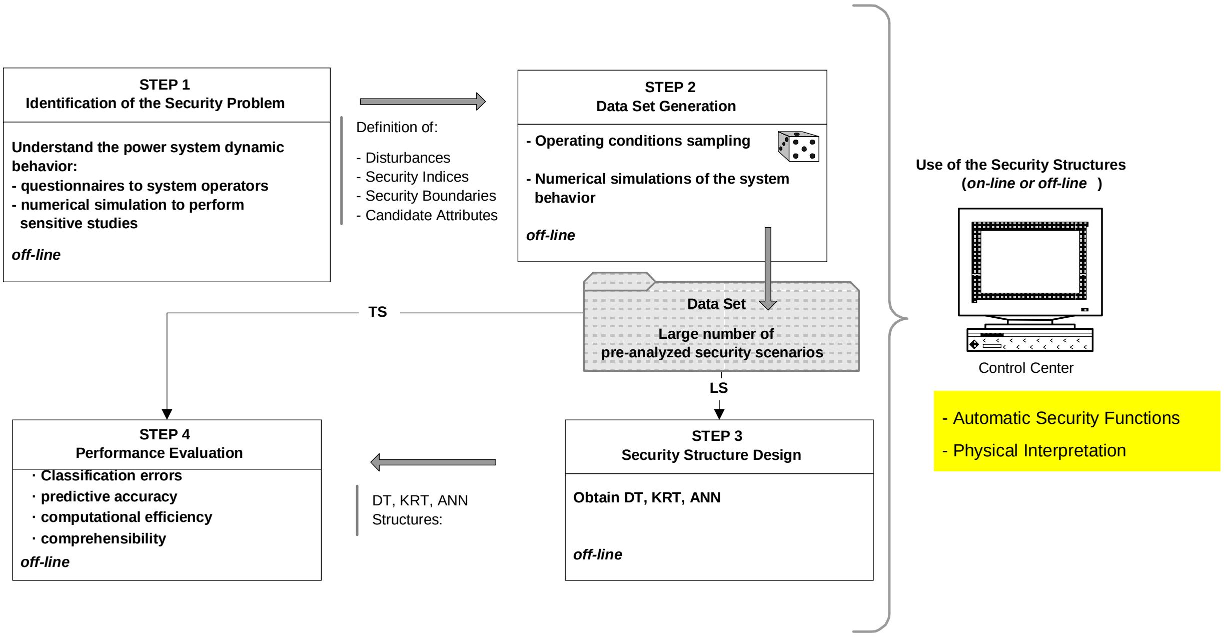
STEP 1
Identification of the Security Problem
Understand the power system dynamic behavior:
- questionnaires to system operators
- numerical simulation to perform sensitive studies
off-line
Definition of:
- Disturbances
- Security Indices
- Security Boundaries
- Candidate Attributes
STEP 2
Data Set Generation
- Operating conditions sampling
- Numerical simulations of the system behavior
off-line
Data Set
Large number of pre-analyzed security scenarios
TS
LS
STEP 3
Security Structure Design
Obtain DT, KRT, ANN
off-line
DT, KRT, ANN Structures:
STEP 4
Performance Evaluation
· Classification errors
· predictive accuracy
· computational efficiency
· comprehensibility
off-line
Use of the Security Structures
(on-line or off-line)
Control Center
- Automatic Security Functions
- Physical Interpretation

Figure 2 – Main steps to apply Machine Learning to perform dynamic security assessment

that includes:

1- the identification of the security problem, where a physical understanding of the phenomena is performed in order to help selecting attributes that characterize the operating conditions relatively to the security problem;
2- Generation of a data set with information regarding the behavior of the system in several operating conditions;
3- Design of security evaluation structures that afterwards will be used on-line providing to the operators information on the system robustness for the disturbances under consideration; Decision Trees (DTs), Regression Trees (RT), Kernel Regression Trees (KRTs) and Artificial Neural Networks (ANN) were used in a competitive way in this work;
4- Performance evaluation, necessary to assess the quality of the security evaluation structures obtained in step 4.

Figure 2 describes schematically the procedure to be followed when dealing with these techniques.

4. CREATION OF THE LEARNING & TEST SETS

The application of machine learning techniques are based on previous knowledge about the behaviour of the system, obtained from a large number of off-line dynamic simulations that define a data set. This data set is afterwards split in two sub-sets: a learning set (LS) and a testing set (TS). The learning set is required to extract the knowledge needed to derive automatic security evaluation structures. It consists of a large number of operating points (Ops) covering all possible states of the power system under study in order to ensure its representativity. Each OP is characterised by a vector of pre-disturbance steady-state variables, called attributes, that can be either directly measured (powers, voltages etc.) or indirectly calculated quantities (wind penetration, spinning reserve etc.). The quality of the selected attributes and the representativity of the LS are very important for the successful implementation of the automatic structures.

For the creation of the global data set, a large number of initial operating points (Ops) are obtained by varying randomly the load for each load busbar, the wind power for each wind park and the wind margin. These variables are assumed to follow normal distributions around three operating profiles:

1. Low-load operating condition with a total load P_L =100MW.
2. Medium-load operating condition with P_L =180MW.
3. High-load operating condition with P_L =280MW.

For each one of the 11 load busbars and each one of the 4 aggregate wind parks in operation, a perturbation of approximately ±10% is applied around each one of the above operating profiles. A dispatch algorithm approximating actual operating practices followed in the control system of Crete is applied next in order to complete the pre-disturbance OPs. For a given load demand P_L and wind power P_W, the total conventional generation P_C is given by

$$P_C = P_L – P_W \qquad (1)$$

and is after dispatched to the units in operation, depending on their type and their nominal power.

For each one of the produced OPs a number of possible disturbances has been simulated, where EUROSTAG was used to obtain the system dynamic behaviour. Two major disturbances have been finally selected after studying extensively the behavior of the network for several disturbances. These are:

a) outage of a major gas turbine

b) three phase short-circuit at a critical bus near the Wind Parks.

In fact, a unit disconnection is a frequent event and a tree-phase fault, although rare, is a severe event that can occur during stormy conditions.

For each OP the minimum value of system frequency and the maximal rate of frequency change are recorded. Both of these parameters are checked against the values that activate the under-frequency relays that protect the WPs, and the OPs are then labelled as secure/insecure.

The list of activated attributes, that characterise each OP, includes namely:

- Active and reactive power of all power sources.
- Spinning reserve of the conventional units.
- Wind power penetration, expressed as the ration of the total wind power to the load of the system.
- Wind margin, expressed as the ratio of the conventional units spinning reserve to the total wind power.
- Active and reactive loads.

The variable used to verify security is the minimum frequency the system experiments after the disturbance.

The security criteria used was

If *fmin* <= 49 Hz **then** the system is insecure

else is secure

Table 1 - List of selected Attributes

AT ID	Description	units	symbol
AT23	Wind Park 1	MW	-
AT24	Wind Park 2	MW	-
AT25	Wind Park 3	MW	-
AT26	Wind Park 4	MW	-
AT27	Wind Power$_{TOTAL}$	MW	ΣP_W
AT28	Wind Q.$_{TOTAL}$	MVAr	-
AT37	Power Gen.1	MW	Pg1
AT38	Spinning Res.1	MW	SR1
AT39	Power Gen.2	MW	-
AT40	Spinning Res.2	MW	-
AT41	Power Gen.3	MW	Pg3
AT42	Spinning Res.3	MW	-
AT43	Power Gen.4	MW	-
AT44	Spinning Res.4	MW	-
AT45	Wind Penetration	%	WP
AT46	Wind Margin	-	-
AT47	Active Power	MW	-
AT49	Reactive Power	MVAr	-
AT51	Conv. Gen. $_{TOTAL}$	MW	ΣP_C
AT52	Total Active Load	MW	ΣP_L
AT55	Total React. Load	MVAr	-
AT57	Capacitors	MVAr	-

Using the approach described in this section, 2765 acceptable operating points have been obtained, which are divided in the two sets mentioned before, (by sending 2 OPs to the LS and 1 OP to the TS). The LS comprises 1844 OPs and the TS used for testing the developed classifiers comprises 921 OPs. In this way, the capability of the security evaluation structures to evaluate correctly the security of unforeseen states can be estimated on a more objective basis.

5. DESIGN OF SECURITY EVALUATION STRUCTURES

5.1 Decision Trees

The decision tree methodology is a non-parametric learning technique able to produce classifiers about a given problem in order to deduce information for new unobserved cases. The construction of a DT starts at the root node with the whole LS of pre-classified OPs. These OPs are analysed in order to select the test T that splits them “optimally” into a number of most “purified” subsets. For the sake of simplicity, a two-class partition is considered. The test T is defined as:

$$T: A_i \leq t \qquad (2)$$

where t is the optimal threshold value of the chosen attribute A_i.

The selection of the optimal test is based on maximizing the additional information gained through the test. The selected test is applied to the LS of the node splitting it into two subsets, corresponding to the two successor nodes. The optimal splitting rule is applied recursively to build the corresponding subtrees. In order to detect if one node is terminal, i.e. “sufficiently” class pure, the stop splitting rule is used, which checks whether the entropy of the node is lower than a present minimum value. If it is, the node is declared a leaf, otherwise a test T is sought to further split the node. If the node cannot be further split in statistically significant way, it is termed a deadend, carrying the two class probabilities estimated on the basis of the corresponding OPs subset. A more detailed technical description of the approach followed is described by Hatziargyriou, Papathanassiou and Papadopoulos, 1995.

5.2 Kernel Regression Trees

The Kernel Regression Tree (KRT) is an hybrid algorithm that integrates recursive partitioning (regression trees – RT) with kernel regression (KR), dealing with continuous goal variables (i.e. regression problems).

Like in decision trees, the design of a RT consists in the extraction of interpretable security rules. Kernel regression models 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 that keeps the efficiency and interpretability of a RT, but with a better accuracy, by increasing the non-linearity of the functions used at the leaf nodes.

The regression problem consists in obtaining a functional model that relates the *output y* with the *inputs* $a_1, a_2, ..., a_n$ (OP attributes), where the output *y* (denominate as goal variable) is, in this case, a numerical value of any electrical security index of the power system. For the problem under analysis the security index adopted is the minimum frequency - fmin (Hz). The design of a KRT involves two stages:

- Determination of the regression tree;

- Definition of the regression models in the leafs.

Building the RT

The learning of a RT consists in the decomposition of the attribute hyperspace into a hierarchy of regions. In our application, it consists in the decomposition of the LS into regions where the severity/security of a disturbance (*y* value) is as constant as possible. The main practical difference between decision and regression trees, is that the latter determines automatically the appropriate numerical value of the severity into subintervals, whereas the former merely reproduce a predefined classification.

Starting with the root node (and exploiting the learning set data), the growing of the RT is made by successive splitting their nodes. The splitting rule of a node is defined by a dichotomic test as described in (2).

The split of each node, i.e. the optimal splitting test, is determined so as to reduce as much as possible the MSE (Mean Square Error) of y. In other words, the best split is the one that provides a maximum amount of information on the security index (*y*). Thus, the optimal split *s* at each node *n* is the one that maximizes:

$\Delta \mathrm{MSE(y)_{sn}} = \mathrm{MSE(y)_n} - \mathrm{P_L MSE(y)_{nL}} - \mathrm{P_R MSE(y)_{nR}}$ (3) where:

– $\mathrm{P_L}$ and $\mathrm{P_R}$ is the proportional number of OPs at the left and right subsets resulting from the split;

– MSE(y)$_\mathrm{n}$ is the mean square error at node n;

– MSE(y)$_\mathrm{nL}$ and MSE(y)$_\mathrm{nR}$ are the mean square error at the left and right subsets.

This splitting rule is the one described by Breiman et al. (1984) and employed in CART. Once the optimal test is found, the next step consists in creating two successor nodes, corresponding to the two possible instances of the test

$$\{a_k() > u_k\} \text{ and } \{a_k() \leq u_k\}.$$

The procedure continues splitting the created successor nodes, until a stop splitting criterion is met. This decides whether a node should indeed be further developed or not. There are the two possible stop splitting rules:

- Rule 1: It is not possible to reduce the MSE further in a statistically significant way;
- Rule 2: The variance has been sufficiently reduced;

When, in a node, one of these rules is verified it becomes a terminal node, i.e. a leaf node. Stop splitting at leaf nodes prevents the tree from overfitting the learning set, and hence allows the method to reach a better compromise between accuracy and simplicity.

Deriving Kernel regressors

To obtain a KRT structure, a kernel regression model is developed 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* (fmin in our case)of the form:

$$y'(Q) = \frac{\sum_{i=1}^{samples} K_h[D(Q,OP_i)] \times y_i}{\sum_{i=1}^{samples} K_h[D(Q,OP_i)]} \qquad (4)$$

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.

Kernel Regression Trees are usually characterized by a large complexity which may decrease its explanation capabilities, namely when used for understanding the reasons of some phenomena. For that purpose pruning techniques have been used, as described by Peças Lopes and Vasconcelos, 2000, to derive simpler structures that do not compromise, however, the accuracy of the security evaluation structures.

It is important to mention that according to the final purpose for which the KRT is aiming (security classification, index prediction or phenomena interpretation) different KRT can be obtained.

5.3 Artificial Neural Networks

For the application of ANN techniques, two multi-layer ANNs were trained (one for each disturbance) using an adaptive back propagation algorithm (a description of the applied algorithm is provided by Miranda et al., 1995). For the two ANNs the following structure was selected (see Figure 3): one input layer with 22 attributes as inputs, one hidden layer with 8 neurons and one output layer with the two security indices as outputs. The 22 inputs are the attributes presented in table 1.

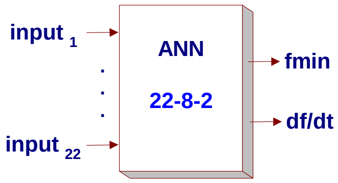

Figure 3 – Structure selected for training the ANNs

6. NUMERICAL RESULTS

In any machine learning approach the quality of the results needs to be evaluated through classification errors, (global classification error, false alarm and missed alarm errors) relatively to *a priori* classes or by quantifying mismatches relatively to the target output values *y*, in this case the minimum frequency - *fmin*. These indicators are namely the mean relative error, the mean absolute error and the mean square error. The performance evaluation, in terms of classification, for both disturbances are shown in the next tables for the DT and RT approaches.

Table 2 - Performance evaluation with DT and RT

Disturbance (Machine-Loss)		
	DT	KRT
Global Error	1.84%	0,33%
False Alarm	1,31%	0,00%
Missed Alarm	4,4%	15,0%

Table 3 - Performance evaluation with DT and RT

Disturbance (Short-Circuit)		
	DT	KRT
Global Error	2.17%	2,39%
False Alarm	1,87%	1,83%
Missed Alarm	2,58%	3,22%

Figures 4 and 5 describe the DT and RT designed for the Short-circuit disturbance. In these figures, the total number of operating points in the learning set belonging to this node are presented aside the node number. The contents of the box representing each node are respectively:

- For DT - the ratio of the secure operating points over the total number of LS OPs belonging to the node and the splitting test for non terminal nodes; Leaf nodes with a safety ratio larger than 0,5 correspond to secure nodes;
- For RT – the mean value of the security index (Hz) and the variance of the index regarding the OPs belonging to that node (for terminal nodes); For non-terminal nodes the splitting test is included only.

In Regression Trees one can assigned a given degree of security to each leaf accordingly to the mean value of the OPs that belong to the node.

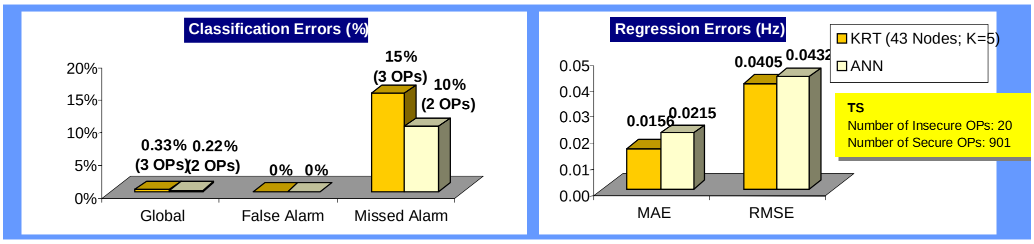

Figure 6 – TS performance evaluation results for Crete ($y_{,Crete}$: f_{min} *due to machine loss*)

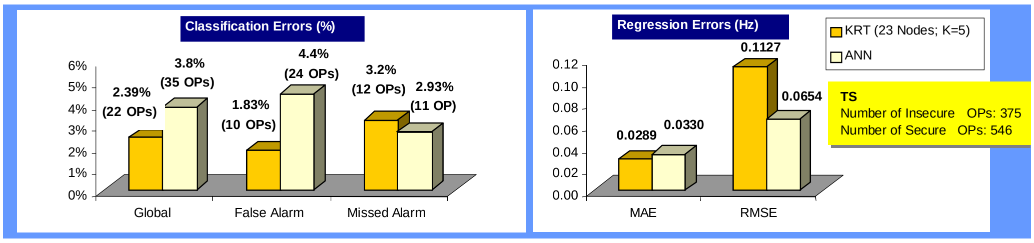

Figure 7 – TS performance evaluation results for Crete ($y_{,Crete}$: f_{min} *due to short circuit*)

For the prediction of the minimum frequency value associated to each OP, kernel regressors, that employ expression (4), were used exploiting the data available at each terminal node of the RT, as well as ANNs with the architecture of figure 3.

KRTs demonstrated to be able to predict the security index with good accuracy. Figures 6 and 7 enable to compare the performance of ANNs and KRT in classification and prediction of security for the 2 disturbances considered.

Extensive results from the application of these procedures in the Crete network and in the Terceira island system can be found in the final CARE report, 1999.

From the results obtained with the three approaches one can derive the following main conclusions:

- Both DTs and KRTs were capable of selecting the same attributes as the most important ones (although sometimes in a different order);
- When used for security classification all the 3 approaches lead to small classification errors, although in the cases where not enough information is available, ANN and KRT show to performe worse.
- KRTs have the advantage of producing simultaneously a classification structure, capable of being interpreted as described in rules of figure 5, and giving the degree of robustness of the system through the predicted value of *fmin*;
- All the security evaluation structures are able to provide information on the system security in a very fast way; However, if KRTs (namely the ones obtained after pruning) are used for prediction purposes they demand more time in the prediction task than ANNs or DTs.
- The DTs present, in general, simpler classification structures, which makes easier any interpretation of the phenomena and the identification of the influence of the relevant parameters.

The security evaluation structures were integrated in the CARE software as modules, activated “on call” by the operators. Each module has its specificity, in terms of computational needs, and specially KRT demand that the learning set operating points should be kept in the system data base, to be exploited during the operation stages.

7. CONCLUSIONS

This paper described the approach developed to deal with the problem of evaluating, in a fast way, dynamic security of isolated systems with large shares of with power integration. Evaluation structures based on the application of machine learning techniques were successfully used for that purpose.

These structures were integrated in the dynamic security assessment module of the advanced control system of the island of Crete, helping to identify the operating conditions and parameters, namely wind power penetration, that lead to a less robust operation of the system.

REFERENCES

P. Kundur, G.K. Morison, “A Review of Definitions and Classification of Stability Problems in Today’s Power Systems”, Panel Session on Stability Terms and Definitions, IEEE PES Meeting, Feb. 2-6, 1997, New York.

N. Hatziargyriou, E. Karapidakis, D. Hatzifotis, “Frequency Stability of Power Systems in large Islands with high Wind Power Penetration”, Bulk Power Systems Dynamics and Control Symposium – IV Restructuring, Santorini, August 24-28, 1998.

N. Hatziargyriou, G. Contaxis, M. Papadopoulos, B. Papadias, J.A. Peças Lopes, M. Matos, G. Kariniotakis, E. Nogaret, J. Halliday, G. Dutton, P. Dokopoulos, A. Bakirtzis, A. Androutsos, J. Stefanakis, A. Gigantidou, “Advanced Control Advice for Power Systems with Large-Scale Integration of Renewable Energy Sources – The CARE System”, Companion paper in this issue of Wind Engineering, 2000.

N. Hatziargyriou, S. Papathanassiou, M. Papadopoulos, “Decision Trees for Fast Security Assessment of Autonomous Power Systems with large Penetration from Renewables”, IEEE Transactions on Energy Conversion, Vol. 10, Nr. 2, June 1995.

L. Breiman, et.al, “Classification and Regression Trees”, Wadsworth International, 1984.

J. Peças Lopes, M. H. Vasconcelos, “On-Line Dynamic Security Assessment Based on Kernel Regression Trees”, Paper to be presented to the IEEE Winter Meeting 2000, Singapore, January 2000.

V. Miranda, J. Fidalgo, J. Peças Lopes and L. Almeida, "Real Time Preventive Actions for Transient Stability Enhancement with a Hybrid Neural Network - Optimization Approach", Trans. on IEEE, PWRS, Vol. 10, May 1995.

“CARE: Advanced Control Advice for power systems with large scale integration of Renewable Energy sources”, contract JOR3-CT96-0119, Final Report, August 1999.

Acknowledgment:

The authors would like to thank the EU for funding project JOR3-CT96-0119. They are also grateful to all the other members of the project for their contributions.