MicroGrids Dynamic Security Assessment

C. L. Moreira*, and J. A. Peças Lopes* **
* INESC Porto – Instituto de Engenharia de Sistemas e Computadores do Porto
** FEUP – Faculdade de Engenharia da Universidade do Porto
Campus da FEUP, Rua Dr. Roberto Frias 378, 4200-465 Porto, (*Portugal*)

***Abstract*--MicroGrids comprise low voltage distribution systems with distributed energy sources, storage devices and controllable loads, operated interconnected with the main power grid or autonomously, in a controlled coordinated way. Storage devices are absolutely essential for MicroGrid autonomous operation. However, depending on the operating conditions, their limited storage capacity is a major drawback and might compromise successful MicroGrid islanded operation. In this paper is proposed an index to evaluate MicroGrids security regarding an unplanned transition to islanded operation due to disturbances in the upstream Medium Voltage network. An Artificial Neural Network tool is proposed to forecast the security index for a credible range of operating scenarios. The usage of Artificial Neural Networks is emphasized due to its computational speed for on-line performance and its flexibility for providing corrective actions for insecure operating conditions in order to achieve a seamless transition from interconnected to islanded operation.**

***Index Terms*--Artificial neural network, dynamic security, frequency control, microgrid**

I. NOMENCLATURE

ANN	Artificial Neural Network
DG	Distributed Generation
DSA	Dynamic Security Assessment
FESS	Flywheel Energy Storage System
LC	Load Controller
LV	Low Voltage
MC	Microsource Controller
MG	MicroGrid
MGCC	MicroGrid Central Controller
MS	Microsource
MV	Medium Voltage
PV	Photovoltaic
SOFC	Solid Oxide Fuel Cell
SSMT	Single-Shaft Microturbine
VSI	Voltage Source Inverter

II. INTRODUCTION

The interconnection of small modular generation system (PV, fuel cells, microturbines, small wind generators) and storage devices to LV distribution system, as in Fig. 1, will lead to a new energy system paradigm, usually referred as the MicroGrid [1]-[5]. These MS are small units of less than 100 kWe, most of them with power electronic interfaces, using either renewable energy sources or fossil fuel in high efficiency local co-generation mode. Depending on the primary energy source used, the MS dimension and the type of power interface, they can be considered as non-controllable, partially controllable (e.g. renewable sources that can reduce the power output only) and controllable (e.g. small co-generation units and storage units). A MG can be an extremely flexible cell of the electrical power system if properly controlled through management and control systems. Two different modes of operation can be envisaged [4]:

- Normal Interconnected Mode – the MG is connected to the MV grid, being either partially supplied from it or injecting some amount of power into it;
- Emergency Mode – the MG operates autonomously when the disconnection from the upstream MV network occurs due to planned or unplanned events (e.g. maintenance actions or faults in the MV network, respectively).

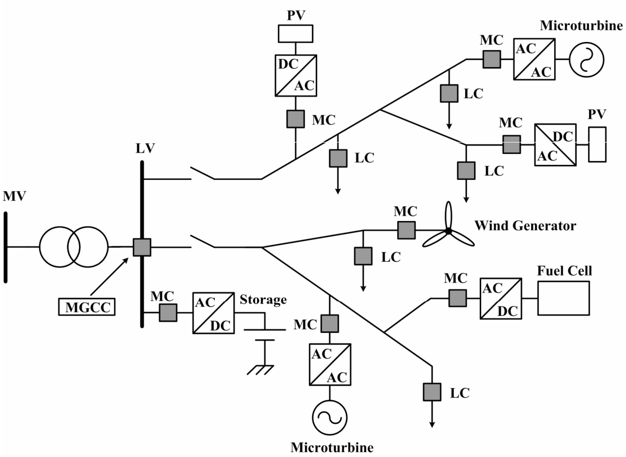


Fig. 1. MG architecture, comprising MS, loads and control devices

A typical MG architecture is presented in Fig. 1. The MG operation philosophy developed by the authors is based on an hierarchical type control approach headed by the MGCC [3]-[4]. A network of controllers with local intelligence (LC and MC) has to be installed, defining a secondary layer in the hierarchical control structure. In this control structure the information to be exchanged should be limited to the minimum information necessary to achieve a large effectiveness and autonomy, namely during emergency operation. The results presented in [4] highlight that under abnormal operating conditions only a network of local controllers can deal effectively with the resulting transient phenomena. However, frequency control problems arise during islanded operation due to

This work was supported by the European Commission within the framework of the MORE MICROGRIDS project, Contract No. 019864 – (SES6) and by FCT – Fundação para a Ciência e a Tecnologia (Portugal) under the grant SFRH/BD/16473/2004.

the slow response of MS to control signals and due the inexistence of rotating masses directly connected to the grid (inertialess system). Sudden islanding of the MG due to faults occurring in the MV network may cause high unbalances between local load and generation which must be compensated by local MS and through a very efficient use of storage devices and load shedding mechanisms [4].

A system with clusters of MS designed to operate in an island mode requires some form of storage to ensure initial energy balance during transients [1-5]. The necessary storage can come in several forms: batteries or supercapacitors on the DC bus for each MS or by a direct connection of storage devices to the AC system (e.g. flywheels). FESS applications in MG are very promising since flywheel offer the advantage of a longer lifetime, high efficiency and grater depth of discharge than batteries [9]-[11]. Furthermore, and in contrast to what happens in chemical batteries, state of charge determination in FESS is very easy, since it depends only on its speed of rotation.

A critical security trait for MG operation is to ensure they can run into islanded operation following an unexpected event without collapse due to insufficient energy storage. Depending on the MG operating conditions, such as local load, local generation profile and MS availability for active power/frequency regulation, high amounts of energy may be required to be injected in the MG in the first moments subsequent to islanding. Due to the slow response of controllable MS to control signals, the most significant part of this energy must be provided by FESS, which has a finite storage capacity. This problem is related to frequency stability, since it depends on the MG ability to restore balance between load and generation during islanded conditions and with the minimum loss of load. Therefore, MG islanding requires an efficient load shedding strategy in order to handle the problems resulting from limited storage capacity and from a generation deficient island.

The on-line management of load shedding mechanisms requires detailed knowledge about the MG dynamic behavior for each specific scenario. Furthermore, the definition an index able to quickly characterize MG security is required. The selection of the security index 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. For each disturbance to be considered the traditional and most accurate analysis involves the numerical solution of a system of non-linear equations, which is a very demanding and time consuming computational task and it is not suitable for on-line purposes. Therefore, artificial intelligence based tools, such as ANN, are alternative approaches since they provide effective means of extracting high level knowledge from large data sets in order to help on-line system management regarding these dynamic issues. The referred data sets should contain detailed information about MG dynamic behavior. This information should be generated off-line by making use of appropriated simulation platforms, as the one presented in [4]. Moreover, ANN have fast time responses which are adequate for real time response and provide an analytical tool to compute derivatives of a security parameter relatively to the control variables in order to compute the preventive control actions [6]-[8].

This paper describes an approach to assist the MGCC on the fast and reliable identification of MG insecure operating conditions and on the definition of the load shedding strategy in order to guarantee system survival following islanding. MG communication infrastructure and the hierarchical control system shown in Fig. 1 [4] are of paramount importance for the effective application of such a procedure. The MG management and control system will be responsible for taking system measurements to perform security analysis and communicate the remedial measures to MG local controllers. By performing DSA in a MG, it is possible to increase costumer benefits arising from such an ambitious exploitation of DG integration in LV distribution networks.

III. ANN FOR MICROGRIDS DYNAMIC SECURITY ASSESSMENT

The application of ANN to perform DSA involves four major steps:

- Identification of the security problem
- Data set generation
- Security structure design
- Definition of preventive control actions

All these steps are to be performed off-line. The final product of the procedure – the security structures – are to be used in an on-line environment as a software module of the MGCC or to obtain physical interpretation of the system behaviour.

The identification of the MG dynamic security problem involves a procedure of understanding its dynamic behaviour, namely the identification of potential situations for which the system may lose stability. This step relies on time domain dynamic simulation of fully defined system models. Thus the simulation platform and the control strategies presented in [4] were used to generate the required data set. The simulation platform includes dynamic models for several types of MS (SOFC, SSMT, small wind generators and PV) and the correspondent power electronic interfaces, as well as the network control functions. The general MG control strategy assumed in this paper is based on the Single Master Operation principle described in [4]. Thus, the MG includes a storage device, which is responsible for balancing load and generation during MG islanded operation. The other controllable MS such as fuel cells and microturbines respond to the load-frequency control system according to the strategy presented in [4].

The data set generation procedure consists of a data set of samples that reflects the dependency of the system behaviour (i.e., the security index) with variations in its operating conditions. Each data set operation point can be characterized by a large number of system variables. However, ANN inputs should be selected taking into account that they are able to conveniently characterize system behaviour and are small enough to avoid a large number of ANN parameters. The ANN inputs should also contain a set of monitorable and controllable variables in order to exercise preventive control actions upon the system if insecure operation conditions are detected [6]. Additionally, these variables should be directly obtained from the MGCC data base, which periodically receives information about MG operating conditions. Most of these variables are related to MS power production levels and to MG load.

IV. Identification of the MicroGrid Security Problem

In conventional power systems, particularly in the isolated ones, the critical issue for assessing dynamic system security is the frequency deviation or the rate of change of the frequency following some pre-identified disturbances, which may lead to load curtailment or to generation tripping due to the activation of frequency relays [6]-[7]. Therefore, the maximum under-frequency deviation, sometimes combined with the rate of change of the system frequency, is chosen as an index for characterising conventional power system security.

In a MG operating under islanded conditions, frequency stability problems are related to imbalances between local load and generation. The MG primary frequency regulation method is based on a droop control strategy implemented in VSI coupled to storage devices. The droop characteristics can be written as follows [4]:

$$\begin{aligned} w &= w_0 - k_P \times P \\ V &= V_0 - k_Q \times Q, \end{aligned} \qquad (1)$$

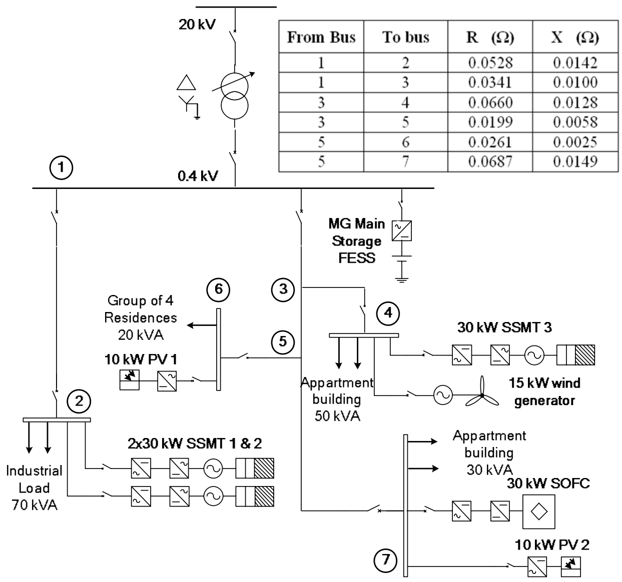
where P and Q are the VSI active and reactive power outputs, k_P and k_Q are the droop slopes (positive quantities) and ω_0 and V_0 are the idle values of the angular frequency and voltage (values of the inverter angular frequency and terminal voltage at no load conditions). The MG operating philosophy presented in [4] considers a storage device coupled to a VSI and a set of controllable MS responding to a secondary load-frequency control strategy to restore frequency to the nominal value during MG islanded operation. The VSI is responsible for balancing load and generation in the islanded MG following any disturbance. In case of a power variation ΔP in the islanded MG, Eq.1 can be used to compute MG frequency in the moments subsequent to islanding:

$$w' = w_0 - k_P \times \Delta P \qquad (2)$$

Eq. 2 shows also that frequency variation in the islanded MG is perfectly controlled by the droop settings. Hence, in contrast to what happens in conventional power systems, frequency deviation is not an important issue to characterize MG security. A critical issue to ensure the MG do not collapse do to insufficient energy storage to balance load and generation during islanded conditions is to guarantee FESS do not run out of energy. For this reason, a suitable index to evaluate MG security following each pre-defined disturbance is the energy required to be injected in the islanded MG in order to balance local load and generation. The MG is considered insecure if the energy required to be injected in the system following a certain disturbance is grater than the storage device capacity.

V. The MicroGrid Test System

The single line diagram of the LV test system used in this research is shown in Fig. 2. This LV test system comprises an industrial load, a LV distribution feeder serving a residential area, several MS connected to the grid and a FESS to allow MG running into islanding operation. The values of the loads shown in Fig. 2 corresponded to simultaneous load values for this LV grid.



From Bus	To bus	R (Ω)	X (Ω)
1	2	0.0528	0.0142
1	3	0.0341	0.0100
3	4	0.0660	0.0128
3	5	0.0199	0.0058
5	6	0.0261	0.0025
5	7	0.0687	0.0149

Fig. 2. MG test system

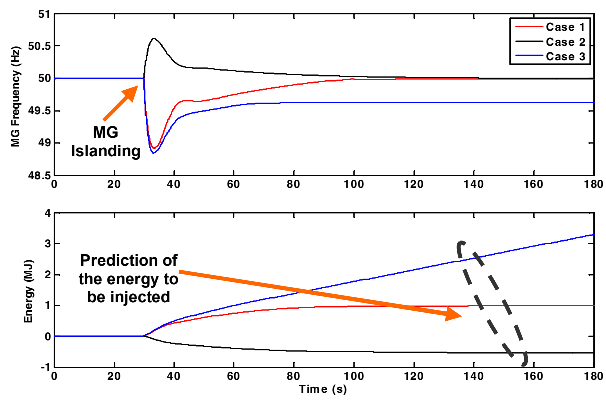


Fig. 3. Frequency and energy injected by FESS for several operating conditions during and subsequent to MG islanding

Fig. 3 illustrates typical MG dynamic behaviour and the energy required to be injected by the FESS during and subsequent to system islanding in several operating conditions, which are characterized in Table I. In cases 1 and 3, the MG is importing power from the MV network and the FESS must inject energy after MG islanding; in case 2, the MG is injecting power into the MV network and therefore the FESS must absorb the energy surplus after MG islanding. In case 3 it is also possible to observe that the MG does not have enough generation capabilities for load/frequency regulation. In this case, MG frequency is not restored to the nominal value and the FESS will kept injecting energy, which is not an admissible situation due to its limited storage capacity.

TABLE I
SCENARIOS CHARACTERIZATION

	Case		
	1	2	3
SSMT 1 + SSMT 2 Active Power (kW)	6,5	41,1	24,4
SSMT 3 Active Power (kW)	4,7	13,4	24,3
SOFC Active Power (kW)	14,9	29,9	29,5
PV1 + PV2 Active Pover (kW)	4,8	16,2	2,5
Wind Generator Active Power (kW)	6,31	13,9	3,7
Power Imported from the MV Network (kW)	55,7	-28,1	65,5

VI. SECURITY ASSESSMENT TOOL DESIGN

The results presented in Fig. 3 do not take into account the limited storage capacity of the FESS. Nevertheless, these results illustrate the need of a fast and efficient toll for an on-line prediction of the energy required to be injected into the MG following system islanding and for determining remedial actions if an insecure state is detected. The main goal is to obtain a relationship between pre-contingency MG operating parameters able to predict the energy required to be injected by the FESS, and to determine remedial actions for insecure operating scenarios.

A. Data Set Generation

A structured Monte Carlo sampling method [12] was used in order to generate knowledge about MG dynamic behaviour, since it demonstrates to provide a well distributed and highly representative data set throughout the defined operating range. The MG operating conditions that influence its behaviour regarding the proposed security index are identified in Table II. The credible range and the resolution used for each one of the selected variables are also specified in Table II. Very simple restrictions were considered in the data set generation procedure, and therefore an almost uniform covering of all the possible MG operating scenarios was achieved. One of the restrictions is related to power production in valley hours and peak load hours. If the MG load is bellow 30%, it was considered that the power production in SOFC and SSMT must be lower than 60% of their nominal capacity. Conversely, if the MG load is higher than 60%, SOFC and SSMT production should be higher than 20%. Sampling on the PV production for night hours operation is not performed, since its production is zero.

The Monte Carlo parameters of Table II correspond to the MG operating conditions in which the sampling method is applied. The definition of the data set resolution was performed by defining the number of intervals considered for the operating range of each parameter. By defining the resolution of each parameter, the data set operating range (a 6-dimension hyperspace) is divided into hypercells. The data set generation procedure consists on the random sample over the Monte Carlo Parameters of Table II, according to the pre-defined operating range and resolution. It is a set by step procedure in which a pre-defined number of values of the 6-dimension hyperspace are sampled in each hypercell using an uniform distribution for each variable [12].

TABLE II
MONTE CARLO VARIABLES

Monte Carlo Parameter	Range (p.u.)	Resolution
SSMT 1 + SSMT 2 Active Power	[0.1; 1]	5
SSMT 3 Active Power	[0.1; 1]	5
SOFC Active Power	[0.3; 1]	5
PV1 + PV2 Active Pover	[0; 1]	3
Wind Generator Active Power	[0; 1]	3
MicroGrid Agregated (Total) Load	[0.2 1]	5

B. Artificial Neural Network Design

The use of ANN is intended for an on-line and accurate evaluation of system security relatively to the pre-defined disturbance and indented for extracting high level knowledge from the generated data set.

Each point of the generated data set is characterized by a set of system measurements (physical MG parameters), that are to be exploited in order to identify those who have enough discriminating abilities to be used as the inputs of the ANN. In this paper, the following set of system parameters is used:

- Active power generated by each MS (P_i)
- MG total active power (L)
- Reserve margin in controllable MS such as SSMT and SOFC ($R_i = P_i^{nom} - P_i$, where P_i^{nom} is the nominal power of each controllable MS).

The variables selected as inputs for the ANN are easily obtained from the MGCC data base, which is periodically updated with data provided by MG local controllers (LC and MC) by using the communication infrastructure. These sets of variables implicitly contain the information required to derive the MG dynamic behaviour characterized by the proposed security index. Thus, the output of the ANN will be the energy E injected by the FESS during a time interval of two minutes subsequent to MG islanding. This time interval was chosen taking into account the large number of dynamic simulations performed in order to build the data set and because such time is the one required to obtain a stabilized response of the controllable MS, as it can be observed in Fig. 3.

C. Preventive Control Strategy

If an unstable MG operating condition is detected, remedial actions must be derived in order to ensure that the MG securely moves to islanding operation in the event of a disturbance in the MV network. As the ANN emulates the behaviour of the energy injected by the FESS, the remedial actions can be determined by finding the values of the control variables that satisfy the following constraint for each insecure scenario:

$$E < E_{\max} \quad (4)$$

where $E_{\max}$ is the maximum amount of energy that can be injected by the FESS.

It will be frequent that MG will not have enough generation capabilities in order to supply the entire load during islanding operation, leading to the adoption of load shedding strategies. Furthermore, adding a security constraint to an economic dispatch problem for the MG will increase the electricity price, and it will not be a very likely situation due to the existence of thermal and electric loads, which should be met during the interconnected operation mode. In case of system islanding, this restriction must be relived in order to achieve load-frequency control capabilities. Therefore, it is suggested that the preventive control strategy will be based on load shedding mechanisms. Determining the minimum amount of load to be shed L_{shed} in order to satisfy Eq. 4 can be easily performed through a gradient technique and by computing the derivative $\partial E/\partial L$, as described in [6], in order to solve the equation $E - E_{\max} = 0$.

By exploiting the control capabilities offered by the MG local controllers, it will be possible to derive a strategy based on changes in the active power production in MS and in load curtailment that ensures MG will securely move to islanding operation. The derived security structure will run periodically under the MGCC as a software module. If an insecure scenario is detected, the preventive control strategy is applied in order to determine the corrective actions to be performed in case MG islanding occurs. In conventional power systems, the usual practice is to derive corrective actions to be suggested to system operators or to be included as security constraints in the unit commitment and in the economic dispatch modules [6]-[8]. In the case of a MG, the corrective actions are to be sent as set points to MG local controllers and are activated only if MG islanding effectively occurs. Detection of MG islanding by local controllers will be performed by measuring system frequency. System frequency is also a parameter that will be estimated by another ANN obtained in a similar way to what is done for dynamic security assessment in conventional power systems. This ANN can be used for a precise tuning of local controllers, namely by defining the frequency at which the local control measures will take place.

VII. Results and Discussion

The numerical results obtained for the test system presented in Fig. 2 are described and discussed next. In order to generate the corresponding data set, the procedure described in section VI was used. The generated data set contains 6400 operating points, which were split in a training set and a test set containing respectively 2/3 and 1/3 of the total operating points. The training set is used for training the ANN and the test set for performance evaluation purposes. For the ANN design procedure, the MATLAB Neural Network Toolbox was used. ANN parameters were found through the Levenberg-Marquart back propagation algorithm. In order to obtain the best ANN performance, different ANN topologies (number of layers and number of neurons in each hidden layer) were tested. The inputs for the ANN were described in section VI. Regarding the single line diagram shown in Fig. 2, SSMT 1 and 2 are operated continuously in parallel; therefore, its output power is combined in a single variable corresponding to the total power injected in the bus number 2. Due to the small geographical span of the MG, it was also assumed that the radiance can be assumed to be equal for both PV 1 and PV 2 and therefore total PV production is combined in a single variable by adding the power production each PV generator.

The results presented next refer to the ANN with the best performance. The ANN has 9 inputs, two hidden layers with 18 and 9 neurons respectively and a single output, which is the proposed MG security index. Fig. 4 depicts the linear regression between the predicted and observed values of the energy injected by the FESS for the MG two minutes after islanding. The obtained performance in terms of the Mean Absolute Error (MAE) and Root Mean Square Error (RMSE) are also presented in Fig. 4. Despite the simple structure adopted for the ANN to represent MG dynamic behaviour, the performance parameters demonstrate the quality of such a tool for evaluating the dynamic security of a MG.

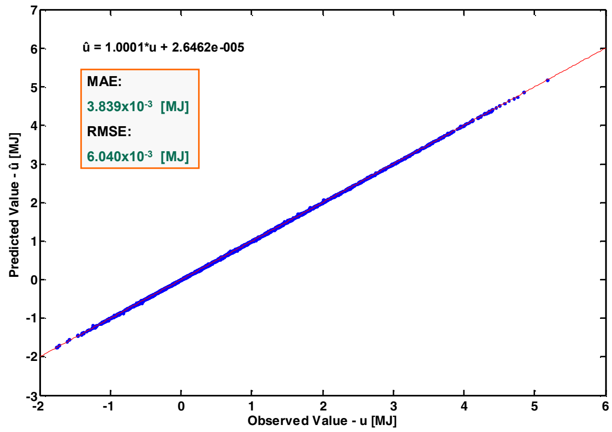


Fig. 4. Observed and predicted values and the linear regression model results

In order to decide if the MG is operating in a secure or insecure scenario, it is necessary to define the value of the energy that is available to be injected into the islanded system by the FESS. By defining the security condition as $E < 0.8\ MJ$, one can use the ANN-based tool in order to calculate the amount of load to be shed for an operating scenario identified as an insecure one by applying the proposed preventive control strategy. For illustration purposes, the procedure is described graphically next. The curves shown in Fig. 5 correspond to two different operating conditions, which are characterized in Table III. For these scenarios, all the operating conditions are maintained constant and the MG load is varied in order to plot the graphs. The interception of the horizontal line (corresponding to the energy level of *0.8 MJ*) with the energy function of each scenario defines the maximum value the MG load should be in order to not exceed the pre-defined amount of energy that can be injected into the MG during two minutes after islanding. The difference between the actual MG load and the load calculated as stated before corresponds to the amount of load to be disconnected in the moments subsequent to MG islanding (Table III).

TABLE III
SOME INSECURE SCENARIOS – LOAD SHEDDING

	Case 1	Case 2
SSMT 1 + SSMT 2 Active Power (kW)	25.49	12.27
SSMT 3 Active Power (kW)	9.99	7.54
SOFC Active Power (kW)	10.96	13.79
PV1 + PV2 Active Power (kW)	1.50	6.96
Wind Generator Active Power (kW)	15.02	-------
MicroGrid Total Load (kW)	138.81	107.58
Energy Injected by the FESS (MJ)	1.62	1.27
Load Curtailment (kW)	28.21	21.14

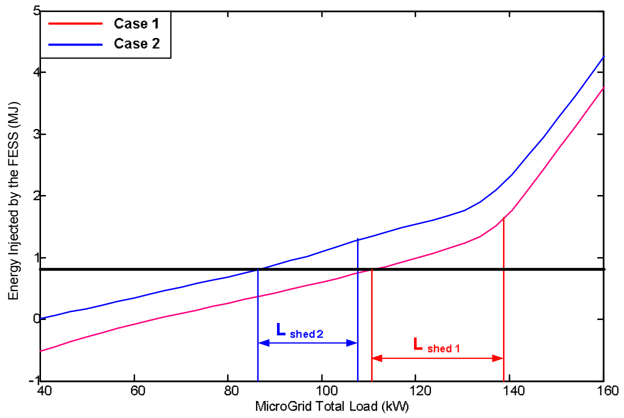


Fig. 5. Determination of the amount of load to be shed

If an insecure state is detected, the preventive control strategy determines the amount of load to be disconnected and defines the suitable load shedding set points for each LC. Each LC will be sensitive to the frequency deviation in order to detect MG islanding and to disconnect the pre-defined amount of load. Therefore, the definition of the frequency level at with the corrective action should take place must also be communicated to MG load controllers. An ANN can also be used to forecast the MG frequency deviation as a function of the operating conditions, similarly to the process used to predict the security index. An ANN using the same inputs used for the prediction of the security index and containing two hidden layers with 12 and 6 hidden neurons is able to emulate MG frequency deviation. It presents the following performance indexes:

$$MAE : 0.0031\ Hz$$
$$RMSE : 0.0039\ Hz$$

The use of the droops to estimate the frequency deviation as presented in section III introduces some errors due to the initial response of controllable MS and to the time constant associated to the VSI. Predicting MG frequency deviation using an ANN tool has a better performance. Combining the information provided by the ANN used to predict the MG security index with the ANN used for the prediction of MG frequency deviation, it is then possible to tune accurately MG local controllers.

VIII. CONCLUSION

This work describes the application to MicroGrids of the Dynamic Security Assessment concept and the derivation of preventive control measures to allow successful grid islanding. The use of such tools is of paramount importance for the on-line MG operation and management, aiming its survival after the occurrence of contingencies in the main power system. From results obtained in a LV test MicroGrid it is possible to conclude that the derived approach provided encouraging results. In fact, reduced test errors demonstrate the quality and the feasibility of the proposed security assessment tool when dealing with this problem. This approach allows coping with a wide range of operating scenarios.

The tool used to predict the energy injected by the FESS following MG islanding can be further exploited in an optimization process in order to define the sizing of MG storage devices, by taking into account the cost of unsupplied loads and credible generation and consumption profiles.

ACKNOWLEDGMENT

The authors thank to the research team of the MORE MICROGRIDS project for the valuable discussions.

C. L. Moreira wants to express his deep gratitude to Fundação para a Ciência e a Tecnologia (Portugal) for the support during the development of this work.

REFERENCES

[1] Lasseter, R.; Piagi, P.: *Providing premium power through distributed resources*. Proc. 33rd Hawaii International Conference on System Science, January 2000.

[2] Lasseter, R.: *Microgrids*. IEEE PES Winter Meeting, 27-31 January 2002, vol. 1, pp. 305-308.

[3] A. Peças Lopes, J.; Tomé Saraiva, J.; Hatziargyriou, N.; Jenkins, N.: *Management of MicroGrids*. [Online] Available: http://microgrids.power.ece.ntua.gr/documents/Microgrids_management_jieec2003.pdf.

[4] A. Peças Lopes, J.; L. Moreira, C.; G. Madureira, A.: *Defining control strategies for MicroGrids islanded operation*. IEEE Transactions on Power Systems, May 2006, vol. 21, no. 2, pp. 916-924.

[5] Piagi, P.; Lasseter, R.: *Autonomous control of Microgrids*. IEEE PES General Meeting, 18-22 June 2006.

[6] N. Fidalgo, J.; A. Peças Lopes, J.; Miranda, V.: *Neural networks applied to preventive control measures for the dynamic security of isolated power systems with renewables*. IEEE Transactions on Power Systems, November 1996, vol. 11, no. 4, pp. 1811-1816.

[7] S. Karapidakis, E.; Hatziargyriou, N.: *Online preventive dynamic security of isolated power systems using decision*

trees. IEEE Transactions on Power Systems, May 2002, vol. 17, no. 2, pp. 297-304.

[8] Vasconcelos, H.; A. Peças Lopes, J.: *ANN design for fast security evaluation of interconnected systems with large wind power production.* Proc. PMAPS 2006 – The 9th International Conference on Probabilistic Methods Applied to Power Systems, 11-15 June 2006, Stockholm, Sweden.

[9] Hebner, R.; Beno, J.; Walls, A.; *Flywheel batteries come around again.* IEEE Spectrum, April 2002, vol. 39, issue 34, pp. 46-51.

[10] O. Cimuca, Gabriel; Saudemont, Christophe; Benoît, Robyns; M. Radulescu, Mircea: *Control and performance evaluation of a flywheel energy-storage system associated to a variable-speed wind generator.* IEEE Transactions on Industrial Electronics, August 2006, vol. 53, no. 4, pp. 1074-1085.

[11] H. Kenny, Barbara; E. Kascak, Peter; Jansen, Ralph; Dever, Timothy; Santiago, Walter: *Control of a high-speed flywheel system for energy storage in space applications.* IEEE Transactions on Industrial Applications, July/August 2005, vol. 41, no. 4, pp. 1029-1038.

[12] Vasconcelos, H.; N. Fidalgo, J.; A. Peças Lopes, J.: *A general approach for security monitoring and preventive control of networks with large wind power production.* Proc. PSCC 2002 – the 14th Power Systems Computation Conference, June 2002, Seville, Spain.