A collaborative framework for multi-area dynamic security assessment of large scale systems

Louis Wehenkel*, Mevludin Glavic* and Damien Ernst†
*Department of Electrical Engineering and Computer Science, University of Liège, Belgium.
†Supelec, Rennes, FRANCE.

***Abstract*— In this paper we propose a collaborative framework to carry out multi-area dynamic security assessment over an interconnection operated by a team of TSOs responsible of different areas. In this framework each TSO does his part of the work and, thanks to information exchange and coordination rules, potential security problems can be detected by all the involved TSOs. We find that distributed multi-area security assessment is achievable and useful if, on the one hand, each TSO can provide an appropriate dynamic equivalent model of his area and if, on the other hand, he is able to publish stability bounds on his inflows under which the dynamic performance of his system would remain acceptable. We then discuss the notions of dynamic equivalent model and external stability domain characterization of an area and identify techniques for deriving such equivalents and stability bounds within the proposed framework.**

I. Introduction

Due to economic, environmental, and regulatory pressures electric power systems tend to interconnect more strongly, grow in size, and operate closer to their stability limits. Consequently, the proper management of these systems becomes more an more complex from all perspectives (planning, operation, control, etc.). In spite of the fact that our knowledge of power system dynamics and the quality of available dynamic security analysis software have significantly progressed during the last few decades, the frequency of blackouts or quasi-blackouts in the recent years has been significantly higher than during the seventies, eighties and early nineties. Thus, the perception of the stakeholders of this field is that significant efforts have to be made urgently in order to be able to reestablish the security of electricity supply at the expected level, or at least to prevent its further degradation during the coming years.

Among the topics that are being debated by the experts, one that has received quite a lot of attention concerns the question of whether it is more appropriate to restructure the planning, operation and control of interconnected electric power systems in a top-down or bottom-up approach. In this context, a top-down approach would imply to create one or several higher level organizations (so-called MEGA-TSOs), and to transfer some of the responsibilities of TSOs at this level. A bottom-up approach, on the other hand, would imply to strengthen the exchange of information among TSOs and improve the mutual coordination of their activities. Currently, top-down approaches are being implemented in North-America and Russia, while the bottom-up one prevails in the European interconnection. One is forced to admit that none of these experiences is totally convincing, since both of them have not been able to prevent the occurrence of some major blackouts or quasi-blackouts in the recent years [1]–[3].

In this paper, we consider the bottom-up approach. Within this context, some work has already been done in the recent years to address the problems of state-estimation and static-security assessment (load-flow computations) [4]–[10]. But there remain several open questions which have been insufficiently well treated, such as the case of multi-area dynamic security assessment, security control and optimization, but which need also to be addressed if one wants to implement a bottom-up approach to large electric power systems planning, operation and control.

We focus on the specific question of whether and under which technical conditions it would be feasible, useful, or desirable to carry out real-time dynamic security assessment in a distributed way in a large multi-area interconnection. To this end, we propose to use the generic collaborative framework described in [9] (and further studied in the context of static security assessment in [10]) and analyse its features. More precisely, we consider how to carry out dynamic security assessment over an interconnection, in a framework where each TSO does part of the work and, thanks to minimal but sufficient information exchange and adequate coordination rules, all potential instabilities could be detected by all the involved TSOs.

Our analysis shows that distributed multi-area dynamic security assessment would be achievable and useful if, on the one hand, each TSO could provide an appropriate equivalent dynamic model of his area to all other TSOs and if, on the other hand, he would agree to publish bounds on his inflows under which he can ensure that the dynamic performance of his system will remain acceptable. We also discuss some techniques for computing such equivalents and bounds and examine the conditions under which one could expect that all TSOs will be willing to exchange the required information.

The paper is organized as follows. Section II describes the principles of the proposed collaborative multi-area dynamic security assessment framework. Section III considers the implementation in this scheme of the construction, exchange and use of dynamic equivalents and stability domains computed by each TSO for his subsystem. Section IV discusses the overall approach in terms of feasibility and desirability, concludes and gives suggestions for future research directions.

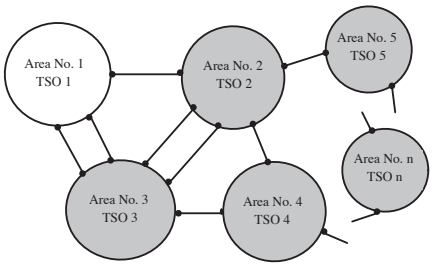

Fig. 1. A multi-area interconnected power system

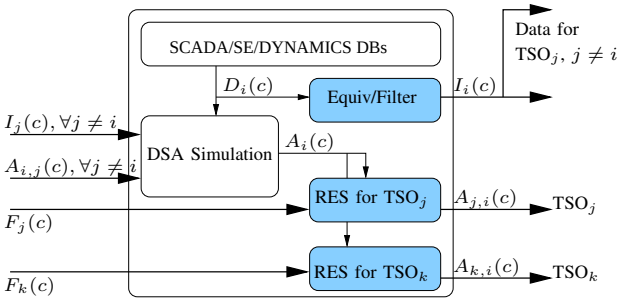

Fig. 2. Computations and data flows for TSO$_i$ (novel functions in blue)

II. A COLLABORATIVE FRAMEWORK FOR DYNAMIC SECURITY ASSESSMENT OF MULTI-AREA SYSTEMS

In this section we look at real-time multi-area security assessment in a rather abstract way and without making any distinction between static and dynamic aspects.

A. Single TSO viewpoint on security assessment

Let us consider a large scale (synchronously or asynchronously) interconnected electric power system as depicted in Figure 1. We adopt the viewpoint of one of the TSOs (for example, TSO$_1$ highlighted in Figure 1) in order to formulate the objectives of security assessment. We focus on the real-time context i.e. the objectives that TSO$_1$ follows when he carries out security assessment in real-time. Notice that we consider below that a tie-line interconnecting the system of TSO$_i$ with that of TSO$_j$ belongs to both areas i and j.

The primary goal of TSO$_1$ is to detect among all plausible contingencies that could happen in his area those that would lead to undesired system performance in his area. He will also be interested in identifying events originating in other subsystems that would affect the integrity of his own area, and may wish to detect contingencies or maneuvers originating in his area that would lead to problems outside his area.

If TSO$_1$ were alone to make this assessment, he would thus have to carry out the following procedure: (i) run state-estimation from a real-time snapshot of the whole interconnection; (ii) set up static and dynamic models and a contingency list for the whole interconnection; (iii) evaluate the consequences inside his area of all contingencies, and the consequences outside his area of all contingencies originating in his area. Obviously, if all TSOs would consider themselves as alone, each one of them would have to do this work on his side from his own viewpoint of what is inside and outside.

B. Assumptions for collaboration

Let us state some assumptions which will make it possible to share security assessment among the TSOs in a fair way, while reaching the same quality of analysis, i.e. the detection among all plausible contingencies over the whole interconnected system of those that might lead to undesirable consequences somewhere in the system and the notification in real-time of potential threats to the concerned[1] TSOs.

[1]A TSO is *concerned* by a dangerous contingency if it leads to undesirable consequences in his own system or if it originates inside his system.

Our first assumption is that each TSO$_i$ wants to identify the dangerous contingencies among those that would originate in his system (including his tie-lines) irrespectively of whether the undesirable consequences of these contingencies are localized in his own area or an other area.

Our second assumption is that each TSO$_i$ can provide enough information to any TSO$_j$ ($\forall j \neq i$) so that TSO$_j$ can detect among the contingencies that he will analyze those that have undesirable consequences in the area of TSO$_i$.

Our last assumption is that if TSO$_i$ has identified some contingency in his subsystem which has potentially undesirable consequences in the system of TSO$_j$, he is willing to inform TSO$_j$ and provide him with the information needed to evaluate these consequences.

We believe that these assumptions are quite reasonable. Below we will analyze regulatory and technical concerns that have to be solved to ensure also their feasibility. If all these conditions were satisfied, then one can distribute the work among TSOs in the following way.

C. Distribution of information and computations

The framework that we propose is a symmetric scheme where all TSOs carry out their work in parallel and in the same way, thrust each other, are fair, and do their best to identify potential security threats. Let us denote by $D_i(c)$ the real-time data about the system of TSO$_i$ (SCADA, state-estimator output, contingency lists etc.) that he obtains from his own EMS system at some security assessment cycle c. We propose that TSO$_i$ does the following at each cycle (see Figure 2):

- TSO$_i$ computes from $D_i(c)$ the information $I_i(c)$ that he will provide to all other TSOs about his system.
- TSO$_i$ broadcasts $I_i(c)$ to all other TSOs. At the same time, he collects $\{I_j(c), \forall j \neq i\}$ broadcasted by them.
- TSO$_i$ computes the consequences of all the plausible contingencies originating in his area. He uses in this process $D_i(c)$ and $\{I_j(c), \forall j \neq i\}$. Let us call the results of this assessment $A_i(c)$.
- For each $j \neq i$, TSO$_i$ computes from $A_i(c)$ and $I_j(c)$ the contingencies that are possibly dangerous for TSO$_j$ and the information required by TSO$_j$ to evaluate the consequences in his system of these latter. We call this information $A_{j,i}(c)$.
- For each $j \neq i$, TSO$_i$ sends $A_{j,i}(c)$ to TSO$_j$. At the same time, he collects $A_{i,j}(c)$ sent by TSO$_j$ to him.

- TSO$_i$ uses $\{A_{i,j}(c), \forall j \neq i\}$ and $D_i(c)$ to evaluate the exact consequences in his area of the contingencies originating in other areas that were signalled as potentially dangerous for his area by the other TSOs.

In Figure 2 the boxes in blue correspond to the novel functions that are specific to our collaborative multi-area scheme, and the function which sends analysis results (RES) to other TSOs is replicated as many times as there are other TSOs.

D. Detailed vs reduced exchange of information

1) Detailed information exchange: A (rather) trivial way to implement the above scheme is to exchange at any time all the available information. With our notations, this would consist in setting $I_i(c) = D_i(c)$ and setting $A_{j,i}(c) = A_i(c)$. In other words the TSOs would exchange all their data at each cycle and all the results of their security assessment computations. We call this the distributed computation scheme with *detailed* information exchange.

2) Reduced information exchange: The detailed scheme can be modified into a scheme of mere *reduced* information exchange in the following way.

First we assume that each TSO$_i$ reduces the information $I_i(c)$ sent to the others to the following three items:

- an equivalent model of the system of TSO$_i$ which allows to compute voltages at the boundary buses from currents. We will denote by $E_i(c)$ such an equivalent;
- detailed real-time data about tie-lines originating in the area of TSO$_i$. We will call this data by $T_i(c)$;
- a filtering procedure which allows to decide whether some current injections into the system of TSO$_i$ are able to yield constraint violations or instabilities in his system. We will denote this filtering procedure by $F_i(c)$.

Second we assume that TSO$_i$ computes $A_{j,i}(c)$ according to the following steps:

- he uses the equivalent models $\{E_j(c), \forall j \neq i\}$ together with his own data $D_i(c)$ to simulate effects $A_i(c)$ of the contingencies originating in his system;
- he applies the filter $F_j(c)$ to $A_i(c)$ to identify the contingencies that could endanger the system of TSO$_j$;
- he computes $A_{j,i}(c)$ by extracting from $A_i(c)$ the post-contingency tie-line currents into the system of TSO$_j$, for each one of the identified contingencies;
- he uses the post-contingency currents $A_{i,j}(c)$ computed and sent to him by the other TSOs and his own system data $D_i(c)$ to compute the internal state of his system for each potentially dangerous external contingency.

In this scheme, the data exchange may be significantly reduced at the expense of additional computations. Indeed, each TSO now has to compute at each cycle an equivalent model and a contingency filtering procedure that he will send to others instead of his detailed data. In addition, for each external contingency detected as potentially dangerous for his system by another TSO, he will have to compute the internal effects in his system from the post-contingency currents provided by this other TSO. On the other hand, the complexity of the security assessment studies carried out by each TSO will normally be reduced significantly in this scheme. Indeed, for the simulation of his internal contingencies a TSO will use a detailed model only of his area together with the equivalent models of the other ones; for the evaluation of internal effects of external contingencies he will use his detailed model of his own system together with the post-contingency currents of his tie-lines computed by the other TSOs.

Thus, if the equivalent models $\{E_i(c), \forall j \neq i\}$ are compact and if the filtering procedures are selective enough, the security assessment computations and the communication requirements of each TSO$_i$ could indeed be significantly reduced in the reduced information scheme.

3) Comparison with a centralized computation scheme: Let us first notice that with respect to a central computation scheme where a single node carries out all the computations, the distributed computation schemes have a redundancy in computations: indeed the contingencies consisting of events on the tie-lines are computed twice.

Moreover, in terms of communications, the requirements are different: in the distributed scheme with detailed information the data $D_i(c)$ have to be broadcasted to all other TSOs, while in a centralized scheme it would just be sent to the central computing node; on the other hand, with the centralized approach the results of computations for each contingency leading to threats in some area would have to be sent back to the TSO of this area.

With respect to these two schemes the main weakness of the distributed scheme with reduced information is that its quality relies on the quality of the equivalent models and filtering procedures that are provided by each TSO.

E. Verification of information quality and incentives

The redundant computations of the distributed scheme can be exploited to verify the quality of the information exchanged among TSOs. Indeed, when assessing the consequences of a tie-line contingency between TSO$_i$ and TSO$_j$, TSO$_i$ uses a detailed model of his area and the equivalent model provided by TSO$_j$ (and of the other areas), while the situation is reversed for TSO$_j$. If the equivalent models are of good quality, these computations should lead to the same results in terms of post-contingency tie-line flows of all interconnections. In principle all TSOs can verify this consistency, provided that it is agreed that post-contingency currents subsequent to the tripping of (or a fault on) a tie-line are systematically broadcasted. Notice also that with the information made available by the framework, each TSO can actually verify the consequences on his system of all possible events in all possible tie-lines in the system, if he wishes to do so.

In addition to the possibility of verification, another essential feature of the scheme is to create incentives for each TSO to provide high-quality equivalents and filters to the others. Indeed, the information $A_{i,j}(c)$ that TSO$_i$ will receive in return from the other TSOs depends critically on the quality of the information $I_i(c)$ that he provides to them.

Taken together, these two features of the framework are probably sufficient to make sure that the TSOs will do their best to provide high quality information to the others.

While the quality of the contingency filters F_i provided by the TSOs is less critical, there is also some natural incentive for this. Indeed, a too optimistic filter (leading to many non-detections) creates the risk for TSO_i that some dangerous external contingency will not be detected. On the other hand, a too pessimistic filter (leading to many false alarms) will lead to higher data traffic and give the impression to the other TSOs that the system of TSO_i is less secure than it actually is.

F. Regulatory and technical feasibility

The kind of information that a TSO will be able to exchange with other TSOs depends on regulatory aspects (confidentiality obligations, or on the contrary obligation of transparency) and on technical feasibility. From the technical point of view the trade-off between detailed information and black-box equivalents is as follows: detailed data is theoretically easy to provide but practically difficult to exchange and exploit; good and compact equivalent models are theoretically difficult to provide but practically easy to exchange and exploit. Therefore, the possibility to implement the framework will depend on progress both in regulatory frameworks and in technical state-of-the-art.

III. Practical considerations

To decompose the dynamic modelling and stability assessment of a multi-area power system into sub-problems related to each area, we clarify in this section what we mean by dynamic model of an area and what we mean by a description of its stability domain. On the road, we also discuss methods to build models of reduced order and approximate stability domain descriptions of a area from the information available to a TSO responsible for this area.

A. Construction and use of dynamic equivalents

For the sake of the explanation, let us consider a power system composed of two areas only and neglect some details pertaining to some specific kinds of models such as discontinuities, delays etc.

1) On the notion of dynamic model of a subsystem: In a totally general and very abstract way (see e.g. [11]), one can view a dynamic model of a system as a set of constraints over the behaviours of all the variables of interest to describe this system. Often, these behaviour constraints are expressed in terms of mathematical equations. For example, in the case of electric power systems dynamic security assessment, a dynamic model is classically written as

$$\dot{x} = f(x, y, u) \quad (1)$$
$$0 = g(x, y, u), \quad (2)$$

where the variables of interest are voltages and currents (y), those related to generator dynamics (denoted by x), and the inputs u which can be used to take into the account the effect of contingencies.

In a system with two areas, these eqautions become

$$\dot{x}_1 = f_1(x_1, y_1, y_{1,2}, u_1) \quad (3)$$
$$0 = g_1(x_1, y_1, y_{1,2}, u_1), \quad (4)$$
$$\dot{x}_2 = f_2(x_2, y_2, y_{2,1}, u_2) \quad (5)$$
$$0 = g_2(x_2, y_2, y_{2,1}, u_2), \quad (6)$$
$$0 = c_{1,2}(y_{1,2}, y_{2,1}), \quad (7)$$

where the subscript i denotes the internal variables participating in the dynamic model of system i, and those with subscript i, j those of system i which can also be seen from j. The first two equations describe the dynamic model of system 1, the second two that of system 2 and the last equation states the coupling constraints imposed by their interconnection written from the viewpoint of TSO_1. In power systems, the variables i, j are the currents in interconnections and voltages at interconnecting nodes and the status of inputs acting on the interconnections. At steady state, $u = 0$, and $f(x, y, 0) = g(x, y, 0) = 0$.

2) Equivalent models for DSA: Let us consider the viewpoint of TSO_1 when he analyzes contingencies occurring inside his system. TSO_1 can use the above dynamic model to carry out simulations and determine the behaviour of the variables that are of interest to him. When he looks at consequences inside his system, he is not interested by the variables x_2, y_2 which pertain to the internal behaviour of area 2. Thus these variables become *latent* variables for TSO_1, according to the terminology of [11],

Thus, for the sake of this analysis, the detailed equations of area 2 could be replaced by any other dynamic model, provided that it imposes the same constraints on the behaviour of the interface variables $y_{2,1}$. Thus in a totally general and very abstract view, a dynamic *equivalent* model of system 2 seen from system 1 is merely a set of constraints on the possible trajectories of the interface variables $y_{1,2}$ which can be imposed together with the model of system 1 and the coupling constraints (7) to model the dynamic behavior of system 1.

In power systems dynamic security assessment it is convenient to formulate the equivalent model by a set of equations with similar structure to the regular power system dynamic models, namely

$$\dot{\hat{x}}_2 = \hat{f}_2(\hat{x}_2, \hat{y}_2, y_{2,1}) \quad (8)$$
$$0 = \hat{g}_2(\hat{x}_2, \hat{y}_2, y_{2,1}), \quad (9)$$

where $\hat{y}_2$ and $\hat{x}_2$ replace the detailed variables y_2 and x_2 and $\hat{f}$ and $\hat{g}$ are defined under the assumption that $u_2 = 0$ (no internal disturbances in area 2). Ideally, this equivalent model is such that the dimension of $\hat{x}_2$ and $\hat{y}_2$ are as small as possible while imposing the same constraints on the behaviour of $y_{2,1}$ as the original model.

Obviously, this scheme is straightforward to generalize to the case of more than two areas. In general, when TSO_i carries out dynamic simulations, he will use in place of detailed models of the other areas the equivalent ones together with all the coupling constraints among all areas.

3) Exploitation of the dynamic equivalents: In our framework, it is the responsibility of TSO_i to provide the equivalent model of his area to other TSOs. Then, any TSO can simulate the behaviour of his area and of the interface variables (voltages and currents) coupling all areas, for any contingency originating in his area.

Let us denote by $y_i^k(0:T) = \{y_{i,j}^k(t), \forall j \neq i, \forall t \in [0;T]\}$ the trajectories of the interface variables of area i computed by some other TSO_k upon the simulation of one of his internal contingencies. If TSO_k sends the information $y_i^k(0:T)$ to TSO_i the latter can use this information as a model of the remaining systems of the interconnection and couple it with its own internal model to compute the detailed behaviour of his area for the simulated contingency.

4) Construction of dynamic equivalent models: Since the early days of power systems, a lot of work has been done in order to build dynamic equivalents [12]–[17]. The approaches include: coherency-based methods, modal-based methods, and combinations of the two. Also ad hoc methods have been in use, where the dynamic equivalent uses part of the detailed structure of the equivalenced area together with nonlinear models of some of its generator and load dynamics and a linearized representation of the rest of the system.

Whatever the precise method and type of dynamic equivalent, all of them fit in the framework described above. However, in order to ensure that the dynamic equivalents are accurate enough, they need to be properly maintained in real-time. Indeed, compact dynamic equivalent models have typically a limited range of validity and when the topology, generation dispatch, or load change significantly they need to be refreshed. We believe that in a context where each TSO carries out a lot of detailed dynamic security assessment studies in real-time, it should be possible to exploit and complement these analyses with a new satellite function which task would be to maintain the equivalent model of the area under the responsibility of each TSO.

Within this respect we would like to pinpoint some recent research carried out in constructing the dynamic equivalents through artificial neural networks reported in [18], [19] and [20]. The developed methodologies provide a voltage-current dynamic equivalent of an external system with unknown structure. In [18] and [19] two neural networks are used, one to extract states of the reduced order equivalent and one to predict the new states values of the external system. In [20] the external system is represented in an input-output formulation and only one neural network is used to predict system dynamic behavior. The neural networks could be trained in real-time by exploiting the results of the time-domain simulations that each TSO runs with his detailed model for all his contingencies.

B. Construction and use of stability domain descriptions

In order to reduce the burden of computation in dynamic security assessment it is useful to complete the tool for time-domain simulation with some filtering techniques, which allow to assess at low computational cost whether a certain contingency is likely to be dangerous. In our framework, we propose that TSO_i provides to the other TSOs a filtering procedure which would allow them to detect whether one of the contingencies they have analyzed is potentially dangerous for area i. We propose to construct such a filter by automatic learning of an external stability domain description.

1) On the notion of external stability domain: Let us consider again the subsystem 2 of the preceding section. Contingencies in area 1 act on subsystem 2 via the coupling constraints on the interface variables $y_{2,1}$. When a contingency is simulated by TSO_1 he computes the trajectory of $y_{2,1}(0:T)$. The question he wants to answer is whether the resulting behaviour of system 2 will be stable or not. If he can determine with sufficient certainty that it will be stable, he doesn't have to send the corresponding data to TSO_2 and the latter doesn't have to carry out the computation of the internal behaviour of his system.

Denoting by $y_{2,1}^{[0,T]}$ the set of all possible behaviours of the interface variables of area 2, an external stability domain of area 2 is a subset $F_2 \subset y_{2,1}^{[0,T]}$ such that

$$P(\text{Area}_2 \text{ is stable} | y_{2,1}(0:T) \in F_2) \geq 1 - \epsilon.$$

The description of F_2 must be such that it is easy to check whether a certain trajectory belongs to it.

2) Learning stability domain descriptions: Suppose that TSO_2 is careful and that initially he has no idea about the external stability domain of his system. Thus, he will use as first guess $F_2(0) = \emptyset$ and he will receive at this first cycle from TSO_1 the signals $y_{2,1}(0:T)$ for every contingency simulated by TSO_1. He will analyse these signals, and can thereby construct a sample of signals each one being labelled as stable or unstable. Using this sample, he can use supervised learning methods, such as decision tree induction [21], in order to build a classifier that can be considered as a new description $F_2(1)$ and send it to TSO_1. At the next step, he will thus receive from TSO_1 only those signals which do not belong to the set $F_2(1)$. He will analyse these signals and add them to the sample of known signals and compute $F_2(2)$, and so on.

If at some cycle there is a significant change in his system which might impact its stability domain, he would have to re-run simulations over the whole sample of trajectories to refresh their stability classification before retraining F_2.

Notice that the external stability domain construction is not used by TSO_2 to check whether his internal contingencies are potentially dangerous. Indeed, this stability domain is valid and useful only for predicting the effects of external disturbances (it is built under the assumption that $u_2 = 0$).

External stability domain descriptions could be expressed as the convex hull of the signals found to be stable in the past. Assuming that the exact external stability domain is indeed a convex set, this would guarantee that

$$P(\text{Area}_2 \text{ is stable} | y_{2,1}(0:T) \in F_2(c)) = 1, \forall c.$$

Automatic learning can be used in order to derive an approximation of this convex hull that can be described (and tested) in a sufficiently simple manner.

IV. Discussion and Conclusion

This paper has introduced a collaborative framework for multi-area security assessment. This framework relies on the willingness of TSOs to exchange two main pieces of information about the dynamic performance of their system.

The first piece is what we have called a dynamic equivalent model, and is defined to be an information set that is sufficiently rich to enable the computation by other TSOs of their internal response and that of the interface variables of the whole interconnection (e.g. tie-line currents and boundary node voltages) in the post-contingency regimes caused by contingencies originating in their system. Quite obviously, a particular case of a dynamic "equivalent" which satisfies this condition is the full detailed model. However, using more compact dynamic equivalents (at least for a significant part of the system) would lead to a more efficient and viable approach. Hence we encourage research on the systematic construction of dynamic equivalents.

The second piece of information is what we have called in the beginning a contingency filter and later on an external stability domain description. This is a piece of information which allows any TSO to predict whether a contingency that he has simulated could lead to instabilities in the area from which the filter has been received. The filter should be such that the probability of missing dangerous contingencies is very low. Again a trivial (and useless) solution to this problem would be to provide a filter which doesn't filter at all. We argue that supervised learning can be used in order to build up good filters from the information that each TSO has anyhow to generate during his analyses.

As a general conclusion, we can say that collaborative multi-area dynamic security assessment is indeed feasible, useful and hence desirable. In addition, we have explained how automatic learning would allow to post-process the results of real-time dynamic security analyses done in such a framework, so as to progressively improve the quality of dynamic equivalent models and the precision of the contingency filters. In this way, each TSO could progressively run more and more contingency analyses without saturating his computation budget or his communication bandwidth.

Furthermore, we would like to stress that the proposed framework does not rely on the use of the same software package by all TSOs. It relies however on the agreement among the TSOs on a common language that they will use to exchange dynamic equivalent models and contingency filters. We also believe that the collaborative framework that we have described will help to increase the awareness of all TSOs about the main weaknesses of the interconnection, and thus improve security coordination.

Our future work will have to go deeper in the questions of learning from simulations in the context of this framework. At a higher level, we would like also to address multi-area optimization and control in a similar framework and study the properties of information sharing schemes appropriate in these contexts of control.

Acknowledgments

DE and MG were supported by the FNRS (Belgian National Fund for Scientific Research).

References

[1] US-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", http://www.pserc.wisc.edu, April 2004.

[2] UCTE Report, "Final Report of the Investigation Committee on the 28 September, 2003 Blackout in Italy", [Online], Available: http://www.ucte.org/news/e-default.asp, April 2004.

[3] UCTE Report, "Final Report: System Disturbance on 4 November, 2006", [Online], Available: http://www.ucte.org/news/e-default.asp, 2007.

[4] A. Calvaer, F. Denis, J. P. Piret, "Exchange of equivalent circuits between control centres of interconnected systems", CIGRE General Session, Paper 32-04, Paris, France, Aug./Sept. 1978.

[5] A. Diu, L. Wehenkel, "EXaMINE - Experimentation of a monitoring and control system for managing vulnerabilities of the European infrastructure for electric power exchange", In Proc. of IEEE PES 2002 Summer Meeting, Chicago, Illinois, USA, June 2002.

[6] T. Dy-Liacco, N. Singh, M. Pavella, "Congestion management in large interconnected networks: needs and methods", CIGRE Shanghai Symposium, Paper 440-14, Shaghai, China, 2003.

[7] L. Min, A. Abur, "Total transfer capability computation for multi-area power systems", IEEE Trans. on Power Systems, vol. 21, no. 3, pp. 1141-1147, Aug. 2006.

[8] W. Jiang, V. Vittal, G. T. Heydt, "A distributed state estimator utilizing synchronized phasor measurements", To appear in IEEE Tarns. on Power Systems, [Online], Available: http://ieeexplore.ieee.org, 2007.

[9] L. Wehenkel, M. Glavic, D. Ernst, "On multi-area security assessment of large interconnected power systems", 2nd Carnegie Mellon Electricity Conference, Pittsburgh, USA, Jan. 2006.

[10] L. Wehenkel, M. Glavic, D. Ernst, "Multi-area security assessment: results using efficient bounding method", In Proceedings of 38th North American Power Symposium, Carbondale, Illinois, USA, Sept. 2006.

[11] J.W. Polderman, J.C. Willems, *Introduction to mathematical systems theory: a behavioral approach*, Springer Texts In Applied Mathematics Series, 1997.

[12] R. Podmore, "Identification of coherent generator dynamic equivalents", IEEE Trans. Power App. Syst., vol. PAS-97, pp. 1344-1354, July/Aug. 1978.

[13] S. Geeves, "A modal-coherency technique for deriving dynamic equivalents", IEEE Trans. on Power Systems., vol. 3, no. 1, pp. 44-51, Feb. 1988.

[14] L. Wang, M. Klein, S. Yirga, P. Kundur, "Dynamic reduction of large power systems for stability studies", IEEE Trans. on Power Systems., vol. 12, no. 2, pp. 889-895, May 1997.

[15] J. M. Undrill, A. E. Turner, "Construction of power system electromechanical equivalents by modal analysis", IEEE Trans. Power App. Syst., vol PAS-90, pp. 2049-2059, Sept./Oct. 1971.

[16] S. T. Y. Lee, F. C. Schweppe, "Distance measures and coherency recognition for transient stability equivalents", IEEE Trans. Power App. Syst., vol. PAS-92, no. 5, pp. 1550-1557, Sept./Oct 1973.

[17] J. R. Winkelman, J. H. Chow, B. C. Bowler, B. Avramovic, P. V. Kokotovic, "An analysis of interarea dynamics of multi-machine systems", IEEE Trans. Power App. Syst., vol. PAS-100, pp. 754-763, Feb. 1981.

[18] A. M. Stankovic, A. T. Saric, M. Milosevic, "Identification of Non-parametric Dynamic Power System Equivalents With Artificial Neural Networks", IEEE Trans. on Power Systems, vol. 18, no. 4, pp. 1478-1486, Nov. 2003.

[19] A. M. Stankovic, A. T. Saric, "Transient Power System Analysis With Measurement-Based Gray Box and Hybrid Dynamic Equivalents", IEEE Trans. on Power Systems, vol. 19, no. 1, pp. 455-462, Feb. 2004.

[20] E. De Tuglie, L. Guida, F. Torelli, D. Lucarella, M. Pozzi, G. Vimercati, "Identification of Dynamic Voltage-Current Power System Equivalents through Artificial Neural Networks", In Proceedings of Bulk Power System Dynamics and Control, VI, Cortina d'Ampezzo, Italy, pp. 220-226, August 2004.

[21] L. Wehenkel, *Automatic Learning Techniques in Power Systems*, Kluwer Academic Publisher, 1998.