Paper accepted for presentation at 2009 IEEE Bucharest Power Tech Conference, June 28th - July 2nd, Bucharest, Romania

Security Assessment by Multiple Transmission System Operators Exchanging Sensitivity and Tie-Line Power Flow Information

D. Fabozzi, M. Glavic, *Senior Member, IEEE*, L. Wehenkel, *Member, IEEE*, T. Van Cutsem, *Fellow, IEEE*

***Abstract*—This paper considers a procedure for multi-area static security assessment of large interconnected power systems operated by a team of Transmission System Operators (TSOs). In this procedure, each TSO provides the other TSOs with his own equivalent model as well as the detailed effects of contingencies in his control area on all tie-line flows. The paper deals with the implementation of sensitivity-based equivalents suitable for static security assessment. Accuracy with respect to the unreduced model and computational efficiency are considered in evaluating the proposed approach. The relevance of the procedure in the context of recent UCTE operational security policy recommendations is also stressed. The procedure has been implemented in an AC power flow program and tested on a three-area variant of the IEEE 118-bus test system.**

***Index Terms*—Power system equivalents, sensitivity analysis, static security assessment, multiple transmission system operators**

I. Introduction

Reorganization of power systems towards a market-based environment has led the Transmission System Operators (TSOs) to operate with lower security margins. According to the present practice, each TSO is responsible for the security assessment of his own area, but a higher level of awareness and coordination among the TSOs is desirable to improve the security of the whole interconnection, as stressed by some of the blackouts experienced over the recent years [1], [2].

In North America the effort has been to create Regional Transmission system Operators, which are higher-level operational entities responsible for the coordination of TSOs. This approach, however, does not seem currently feasible in Europe. As a matter of fact, European directives provide general objectives, guidelines and principles only but, at the bottom level, the coordination of the different TSOs is based on multi-lateral negotiations and collaborations. There are some initiatives such as a coordination center being currently put in operation jointly by France and Belgium.

Carrying out a complete and detailed security analysis over the whole European interconnection in a central point may not be desirable or even feasible in the coming years. Indeed centralized large-scale computations might become intractable from the computational point of view and the knowledge by each individual TSO of his own system could be somewhat lost [3]. As an alternative, a coordination center might serve as a hub for the information exchange discussed in this paper.

This paper reports on static security assessment within the collaborative framework proposed in [4]. In this context, each TSO is committed to:

- computing and making available an equivalent model of his system, to be included by other TSOs in their external system model;
- determining for each contingency originating in his system relevant quantities allowing the other TSOs to compute its impact on their own systems.

The second aspect, usually ignored in today's security assessment, may involve the communication among TSOs of tie-line power flow changes under the effect of contingencies.

The derivation of external equivalents has been largely investigated in the power system literature [3], [5], [6], [7], [8], [9], [10], [11]. Reference [7] provides a comprehensive review of external network modeling approaches with the emphasis on Ward and REI type equivalents as well as their variants.

In this paper, a sensitivity-based equivalent is proposed. This equivalent assumes exchange of sensitivity and tie-line power flow information between the TSOs and is equally applicable for branch as well as generator outages. The quality of this equivalent is judged by how well it represents the effects of the external systems on the internal system for the evaluation of contingencies appearing in the internal system. Computational efficiency is also considered, in terms of the amount of data required and the computational burden added with respect to a standard power flow computation to generate and exploit the equivalent.

The paper is organized as follows. Section II reviews present practice and some recent activities at the European level within the context of power system operational security. Section III outlines a general multi-area security assessment framework. The proposed sensitivity-based equivalent is presented in Section IV. Implementation of this equivalent is considered in Section V while the results using the IEEE 118-bus test system are given in Section VI. Section VII offer some conclusions.

II. Present practice and recent activities at the European level

At the European level, security assessment is usually handled in a distributed way, where each TSO focuses on his own power system, and receives accurate and updated information only about a relatively small part of the external subsystem (typically neighboring substations).

The authors are with the Dept. of Electrical Engineering and Computer Science (Montefiore Institute) of the University of Liège, Sart Tilman B37, B-4000 Liège, Belgium. Email: fabozzi@montefiore.ulg.ac.be, glavic@montefiore.ulg.ac.be, L.Wehenkel@ulg.ac.be, t.vancutsem@ulg.ac.be

978-1-4244-2235-7/09/$25.00 ©2009 IEEE

Each TSO maintains a real-time model of his system based on real-time measurements, planned and forecasted quantities, and off-line data. The latter may include some external equivalents provided by the neighboring TSOs.

From the European power system perspective, efforts have been made towards the standardization of operational policies and practices. These efforts are summarized in the UCTE Operation Handbook [12]. One section of this handbook focuses on information exchange between the TSOs.

The TSOs yearly provide each other with a provisional data-set including network, generation, load and exchange programmes for the preparation of a reference case, the so-called UCTE base case. Moreover, the TSOs yearly provide each other with data sets for a full representation of their network in real-time conditions (the so-called snapshots) [12].

Recent activities at the European level are summarized in the additions [13], [14] to the Operation Handbook [12]. Both documents are dedicated to Policy 3 (Operational Security). The need for a regional approach to security assessment and control is clearly identified in these documents. The documents provide definitions, standards, and guidelines for a regional approach to the N-1 security rule in the context of operational planning and real-time operation.

Some important definitions, directly related to the topic of this paper, are the following [13], [14]:

- *Responsibility area.* The TSO is responsible for the secure operation (N-1 principle) of its own grid and all the interconnection tie-lines to adjacent TSOs. The equipment making up this network is called responsibility area.
- *Influence factor,* is a numerical value used to quantify the highest effect of the outage of an external network element on any internal network branch.
- *Contingency influence threshold,* is a numerical limit value against which the influence factor must be checked.The outage of an external element with an influence factor higher than this threshold is considered having a significant impact on the responsibility area.
- *External contingency list.* External elements with a contingency influence factor higher than the contingency influence threshold are considered as part of the external contingency list.

Furthermore, the documents define that each TSO, at any operational planning stage or in real-time, simulates the risk coming from outside based on the external contingency list, and informs its neighbors of the risk of cascading from outside to inside [13], [14].

The objectives of the work presented in this paper is to illustrate one aspect of the general multi-area security assessment and control framework introduced in [4]. In the authors' opinion this framework fits well the regional security assessment and control problem discussed in the UCTE documents. The specific aspect of this framework considered in the present paper is the implementation of the sensitivity-based equivalents of the TSO responsibility areas.

III. Multi-area security assessment framework

The general multi-area security assessment and control framework introduced in [4] is outlined in Fig. 1. Although introduced in the context of dynamic security assessment and control, the framework is equally applicable in the context of static security, as considered in this paper.

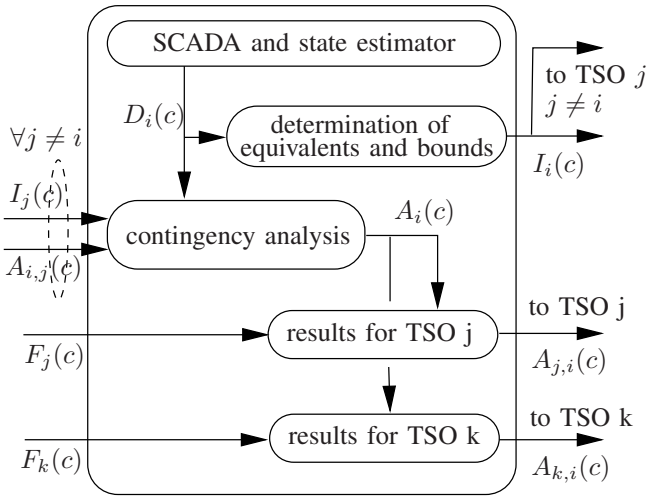

Fig. 1. Computations and data flow for TSO_i

This framework defines a common information exchange scheme and the way to coordinate preventive and corrective actions among the TSOs. The common information exchange allows each TSO not only to run his own security assessment locally, but also to appreciate the security level of the whole interconnection. The framework 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.

We shortly present the main features of the framework (for more details, the reader is invited to refer to [4]). Let $D_i(c)$ denotes the real-time data about the system of TSO_i (SCADA, state-estimator output, contingency lists, etc.) that this TSO obtains from his EMS system at some security assessment cycle c. The following tasks are performed (see Fig. 1):

- TSO_i computes from $D_i(c)$ the information $I_i(c)$ about his subsystem that he will communicate to all other TSOs. $I_i(c)$ is composed of an equivalent of area i and possibly safety bounds which indicate the changes of injections into area i which can be safely discarded as yielding no risk of violations inside area i;
- TSO_i broadcasts $I_i(c)$ to all other TSOs. At the same time, he collects the information $I_j(c)$, $\forall j \neq i$ broadcasted by them;
- TSO_i computes the consequences of all plausible contingencies originating in his area. He uses to this purpose $D_i(c)$ and $I_j(c)$, $\forall j \neq i$. Let us denote the results of this assessment by $A_i(c)$;
- For each $j \neq i$, TSO_i determines 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 of these contingencies in his system. This information is denoted as $A_{j,i}(c)$;
- 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 to him by TSO_j;

- 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 labeled as potentially dangerous for his area by at least one of the TSOs.

In the particular implementation presented in this paper, each TSO_i reduces the information $I_i(c)$, that he broadcasts to all the others, to a static sensitivity-based equivalent model of his system. Furthermore, for each contingency that he evaluates, he sends to TSO_j ($\forall j \neq i$) the information $A_{j,i}$ in the form of variations of tie-line power flows (under the effect of contingencies).

The objective is to exchange the minimal amount of information with minimal loss of accuracy of the results. So, instead of using detailed data-consuming models, equivalents are used.

It is expected that the computational effort and the amount of data required to use the equivalents will be small with respect to those required by an unreduced model.

This paper does not consider the idea proposed in [4] to reduce the information flow by exploiting safety bounds provided by each TSO so as to filter the amount of post-contingency power flow sets that need to be exchanged. Instead, it is assumed that each TSO determines which variation of tie-line power lows have a significant impact on his system and hence require a more detailed analysis.

IV. Sensitivity-based equivalents

In this work, the equivalents take on the form of sensitivity matrices that are easily computed and incorporated to power flow computations.

A feature of the approach presented in this paper is the use of a comprehensive sensitivity formula to represent the effect of an area on the remaining of the system. The latter can be written as:

$$\begin{bmatrix} \mathbf{P}^{eq} \\ \mathbf{Q}^{eq} \end{bmatrix} = \begin{bmatrix} \mathbf{P}^0 \\ \mathbf{Q}^0 \end{bmatrix} + \mathbf{S} \begin{bmatrix} \boldsymbol{\theta} - \boldsymbol{\theta}^0 \\ \mathbf{V} - \mathbf{V}^0 \end{bmatrix} + \mathbf{h}\, \Delta P_d, \quad (1)$$

where $(\mathbf{P}^0, \mathbf{Q}^0, \boldsymbol{\theta}^0, \mathbf{V}^0)$ are base case powers and voltage phase angles and magnitudes at the boundary buses, $(\mathbf{P}^{eq}, \mathbf{Q}^{eq})$ are equivalent active and reactive power injections in boundary buses, $\mathbf{S}$ is a sensitivity matrix linking changes in boundary bus power injections to changes in boundary bus voltage magnitudes and phase angles.

Vector $\mathbf{h}$ links changes in active and reactive power injections at boundary buses to changes in generations in the equivalenced system. More precisely, assuming a power imbalance ΔP_d (caused typically by a generator outage) outside the equivalenced system, $(\mathbf{h}\, \Delta P_d)$ represents the variation in boundary bus injections under the effect of speed governor responses (primary frequency control) in the equivalenced system. Both $\mathbf{S}$ and $\mathbf{h}$ are determined using a well-known sensitivity formula (e.g. [15]) applied to the power flow equations relative to the equivalenced network only.

Let us denote by $\mathbf{f}(\mathbf{x}, \mathbf{p}) = \mathbf{0}$ the power flow equations in compact form, where $\mathbf{x}$ is the vector of bus voltage magnitudes and phase angles and $\mathbf{p}$ a vector of parameters. Let us also denote by $\eta(\mathbf{x}, \mathbf{p})$ a quantity of interest, function of $\mathbf{x}$ and $\mathbf{p}$. The sensitivity of η to $\mathbf{p}$ is given by:

$$\mathbf{s}_{\eta\mathbf{p}} = -\left(\frac{\partial \mathbf{f}}{\partial \mathbf{p}}\right)^{\mathbf{T}} \left[\left(\frac{\partial \mathbf{f}}{\partial \mathbf{x}}\right)^{\mathbf{T}}\right]^{-\mathbf{1}} \frac{\partial \eta}{\partial \mathbf{x}} + \frac{\partial \eta}{\partial \mathbf{p}}, \quad (2)$$

where $\frac{\partial \mathbf{f}}{\partial \mathbf{x}}$ denotes the Jacobian of $\mathbf{f}$ with respect to $\mathbf{x}$, and similarly for the other matrices and vectors. $\mathbf{S}$ is obtained by:

- attaching a fictitious generator with constant voltage magnitude and phase angle to each boundary bus;
- setting η to either the active or the reactive power injected by one of these fictitious generators;
- taking for $\mathbf{p}$ the voltage magnitudes and phase angles of the fictitious generators;
- using (2) transposed to obtain the row vector of $\mathbf{S}$ relative to the selected power.

Similarly, $\mathbf{h}$ is obtained by (assuming g generators inside the TSO):

$$\mathbf{h} = \mathbf{S}_h \begin{bmatrix} pf_1 \\ pf_2 \\ ... \\ pf_g \end{bmatrix} \quad (3)$$

where the sensitivity matrix $\mathbf{S}_h$ is obtained by the same procedure as for $\mathbf{S}$ with the only difference that for $\mathbf{p}$ the active power generations of the generators inside the TSO are taken. Participation factors $pf_1, pf_2, ..., pf_g$ are determined from the permanent speed droop characteristic of each individual generator.

The computation of $\mathbf{S}$ and $\mathbf{h}$ only involves solving linear systems based on the sparse Jacobian matrix. Indeed $\mathbf{s}_{\eta\mathbf{p}}$ is obtained by first solving,

$$\left(\frac{\partial \mathbf{f}}{\partial \mathbf{x}}\right)^{T} \mathbf{y} = \frac{\partial \eta}{\partial \mathbf{x}}, \quad (4)$$

and substituting $\mathbf{y}$ into (2). To this purpose, the already available factors of $\frac{\partial \mathbf{f}}{\partial \mathbf{x}}$ are re-used.

Thus, for each boundary bus, the following data are needed:

- the base case solution $(P^0, Q^0, \theta^0, V^0)$;
- the sensitivities of P^{eq}, Q^{eq} with respect to θ, V of every fictitious generator;
- the two components of $\mathbf{h}$.

For N_b boundary buses, the total number of data is $N_b(4 + 4N_b + 2) = 4N_b^2 + 6N_b$.

The second term in the right-hand side of (1) has some similarities with the Jacobian equivalent concept in Ref. [10] but different in as far as it is based on the sensitivities calculated using the already factored Jacobian matrix. At the same time, the sensitivity-based equivalent retains some nice properties of the Jacobian concept such as correct incremental performance [10].

The third term in the right-hand side of (1) bears some similarity with the equivalent shown in [9], which models the steady-state MW response to a generator outages of the external system, after primary speed control action. Thus, the sensitivity-based equivalent is applicable for branch as well as generator outages.

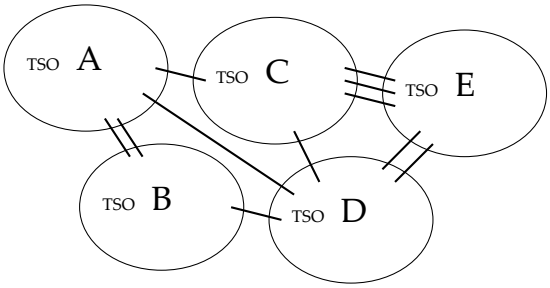

Fig. 2. A hypothetical 5-TSO system

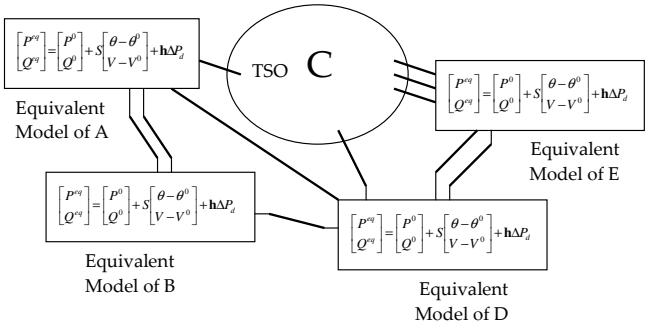

Fig. 3. System model to evaluate an internal contingency in C

The main advantages of the sensitivity-based equivalents are: accuracy, $P - V$ and $Q - \theta$ coupling not neglected (hence the compromise explained in [7] is not required), use of already available factors of $\frac{\partial \mathbf{f}}{\partial \mathbf{x}}$.

The fact that the equivalent is linear as well as the need to slightly modify standard power flow programs in order to embed the sensitivity matrix $\mathbf{S}$ into the Jacobian, are the main limitations of the proposed technique.

V. Implementation of the sensitivity-based equivalent

Figure 2 shows a hypothetical 5-TSO system to demonstrate how the sensitivity-based equivalent would be used within the general framework given in Section III.

In the first step of the procedure, contingencies are simulated. To this purpose, each TSO will use the detailed model of his network and all tie-lines and will attach the equivalent model of the other TSO's network.

For instance, if we consider security assessment by TSO C, Fig. 3 shows the replacement of the external system by sensitivity relationships, using one set of eqns. (1) per area, and preserving tie-lines. When a TSO computes the sensitivity-based equivalent for other TSOs it switches his slack bus to the PV type with all boundary buses become $V - \theta$ buses. This resolves the problem of having sensitivities computed with respect to different slack buses. Note also that the "identity" of each external TSO is retained (each external TSO is considered as a "super node"). This preserves sparsity since in practice a TSO is connected to other TSOs through a small number of tie-lines only. The computational burden added to a standard power flow computation is just that of:

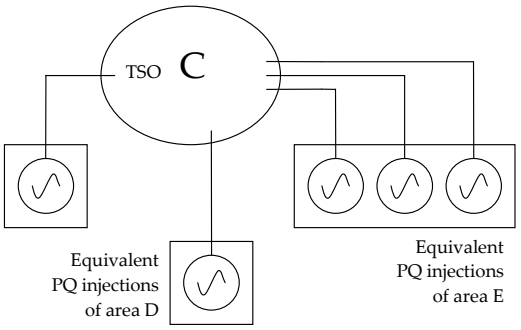

Fig. 4. System model to evaluate an external contingency in C

- adding to the Jacobian the elements of the sensitivity matrix, and
- updating boundary bus (active and reactive) powers according to the power imbalance ΔP_d caused by the contingency.

inserting in the Jacobian a few elements, updating the Jacobian itself with the addition of the elements of the sensitivity matrix and considering in the first iteration the power deficit in the computation of the active and reactive power injections at the boundary buses.

In the second step of the procedure, for each internal contingency considered, each TSO informs the others on the likelihood of the contingency, whether it is internally harmful or harmless and the post-contingency active and reactive power flows in tie-lines.

Using this information, each TSO will assess the impact on his system of external contingencies. To this purpose, he uses the detailed model of his area and tie-lines, and attaches equivalent PQ generators at the boundary buses forcing the active and reactive power flows computed by the TSO in which this external contingency has taken place. For instance, Fig. 4 shows how the impact on area C of a contingency located outside this area is going to be evaluated by the TSO of area C.

Finally, for each external contingency considered, each TSO informs the others whether it is internally harmful or harmless.

The only information that each TSO is requested to publish are the equivalent model of his area and the results of his own security assessment including the changes in tie-line power flows.

It must be stressed that the information about all the tie-lines are considered common information and that the outage of each tie-line is computed by each TSO. Hence, the resulting post-contingency tie-line flows are computed and published several times (once by each TSO, each one using a detailed model of his system and the equivalent models provided by the others). All these values will be coherent if all the equivalent models are of good quality and the computations of individual TSOs are sufficiently well synchronized. Thus, all TSOs could detect potential inconsistencies in the models they use and such inconsistencies may be exploited to trigger procedures for improving the quality of the exchanged information for reducing the cycle time of information exchange or for better synchronization of the individual computations.

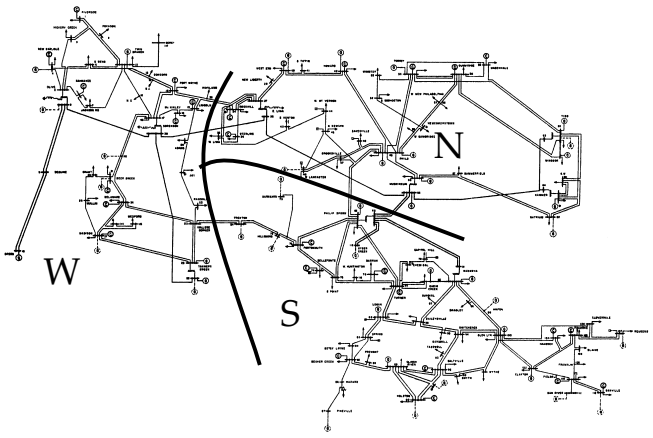

Fig. 5. The partition of the IEEE-118 network

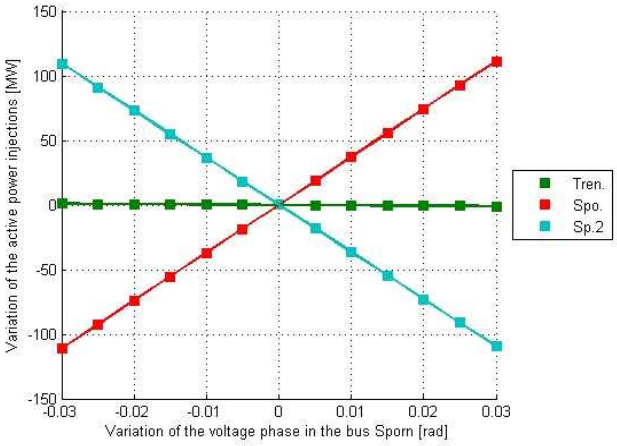

Fig. 6. Variation of the voltage phase in the bus Sporn

The procedure provides some incentives for the TSOs to publish good quality equivalents and to keep them updated in real-time. Indeed, providing good equivalents to the other TSOs is necessary for being able to predict correctly the impact of external contingencies on one's area, while receiving good equivalents from the others is sufficient for being able to predict correctly the internal consequences of internal contingencies and the other TSOs to compute the effects on their system of these contingencies.

In principle, the proposed procedure obliges each TSO to compute the effects on his system of all the contingencies (including the external contingency list as defined in [13], [14]) analyzed and published by any TSO.

In the worst case, each TSO thus has to compute the detailed impact of all internal and external contingencies, but on a network considerably smaller than the original one. Moreover, each TSO is committed to maintaining and monitoring only his part of the system.

VI. Test system and results

The approach has been tested on the IEEE 118-bus system (see Fig. 5). The system has been decomposed into 3 areas, referred to as Northern (N), Western (W), and Southern (S), respectively.

The bus and line data used are slightly different from the original one [16], since the system has been stressed in order to increase possible overload effects of contingencies.

To create harmful situations, the MVA limits of all lines have been decreased to 75 % of their initial values.

A. Validation of the equivalent model

In order to validate the sensitivity-based equivalent, several tests were performed in the area N, with the areas S and W replaced by their respective equivalents. The validation was performed through comparison of results for base case and for variations of system parameters around the base case.

First, the equivalent has been tested by replacing the (non-linear) power flow equations in areas W and S by their linear approximation (1) and solving the base case. No significant differences were found in the results when compared to the base case solution of the unreduced model. A few differences occurred in the voltage magnitudes and phase angles but they were below 10^{-4} pu and 10^{-4} rad. Mismatches on boundary bus powers were all within the given tolerances (0.1 MW, 0.1 Mvar).

Next, the sensitivities were tested for small variations around the base case solution. The tests consisted in forcing small variations of one parameter at a time and observing the changes produced in the variables of interest. The results shown in Fig. 6 refer to variations of the active power injections with respect to variations of the voltage phase angle at the boundary bus Sporn.

In Fig. 6 the lines correspond to the linear approximation, while the dots have been obtained by treating all boundary buses as $V-\theta$ buses in the original, unreduced model, and imposing a change in voltage phase angle at one of those buses only. As can be seen no significant difference can be identified in the results. The variations of the voltage phase angle were between -0.03 and 0.03 rad, leading to significant changes of the active power flowing in the tie-lines of more than 200 MW.

The tests performed with variations in the active power generation pattern (in the range 0-300 MW), assuming an active power generation surplus in area S, as well as with small variations in voltage magnitudes, revealed some differences in reactive power flow injections with the largest error of 5.7 (Mvar) and 2.6 (Mvar), respectively, at bus Sporn. These differences are acceptable, particularly having in mind that the variations in active power generation were not small.

B. Representative security assessment results

The security assessment in the N area is considered here, while the S and the W are replaced by their respective sensitivity-based equivalents. The set of contingencies include internal branch outages, internal generator outages and tie-line branch trippings.

The detailed effects of the area N set of contingencies on the S and W areas are computed on these networks with PQ generators attached at their boundary buses, forcing the active and reactive tie-line power flows resulting from the contingencies computed in area N. For the purpose of accuracy

checking, all contingencies have been also analyzed on the unreduced model of the system.

The set of contingencies considered in N area security assessment includes: 21 internal branches, 9 tie-lines, and 6 generators. For each contingency the variations of tie-line power flows are passed on to the S and W areas.

Out of the above 21 internal contingencies, 2 revealed to be harmful for other areas: the outage of the line "LEast-Lim2Muskngum" (for S area) and the outage of the transformer "TEastLim2EastLima" (for W area). The first produces the worst effects. This contingency trips one circuit of a 345-kV line carrying 380.7 MW and 30.8 Mvar. This causes four lines and a transformer to be overloaded in the N area. Two interconnection tie-lines are also overloaded.

The base case power flows in the tie-lines as well their variations under the effect of the above contingency are listed in Table I.

TABLE I
TIE-LINE POWER FLOWS AND THEIR VARIATIONS AFTER THE WORST BRANCH CONTINGENCY IN AREA N.

Areas	$P(MW)$	$\Delta P(MW)$	$Q(Mvar)$	$\Delta Q(Mvar)$
S-W	-168.7	-81.1	31.2	10.8
S-W	-168.7	-81.1	31.2	10.8
S-N	-131.7	-17.8	-7.2	-12.1
S-N	-97.8	-12.8	5.3	-9.3
S-N	-19.8	115.8	16.9	-2.0
S-N	-19.8	115.8	16.9	-2.0
W-N	44.2	-8.7	-21.0	-10.8
W-N	93.9	-9.5	-17.6	-9.8
W-N	-1.2	-132.1	-70.3	-15.5
W-S	160.1	74.7	-60.1	-33.9
W-S	160.1	74.7	-60.1	-33.9

This specific contingency causes five lines in the S area (checked by the TSO of area S using the equivalent PQ injections provided by the TSO of area N) to be overloaded with the highest overload of 47.5 % above the MVA limit on the interconnection tie-line "Lsporn2Portsmth".

One generator outage (generator "GMuskngum") in area N revealed to be harmful for area W. This contingency trips a generator producing 350.0 MW and 272.3 Mvar. This causes a line to be overloaded in the N area. No overload was found on the interconnection tie-lines.

The base case power flows in the tie-lines as well their variations under the effect of the above contingency are listed in Table II.

TABLE II
TIE-LINE POWER FLOWS AND THEIR VARIATIONS AFTER THE WORST GENERATOR CONTINGENCY IN AREA N.

Areas	$P(MW)$	$\Delta P(MW)$	$Q(Mvar)$	$\Delta Q(Mvar)$
S-W	-78.3	9.3	18.2	-2.2
S-W	-78.3	9.3	18.2	-2.2
S-N	-118.0	-4.1	5.2	0.3
S-N	-89.7	-4.7	15.2	0.6
S-N	-219.5	-83.9	1.8	-17.1
S-N	-219.5	83.9	1.8	-17.1
W-N	42.1	-10.8	-3.8	6.4
W-N	92.9	-10.5	-2.2	5.6
W-N	63.4	-67.5	-34.7	20.1
W-S	76.5	-8.9	-22.3	3.9
W-S	76.5	-8.9	-22.3	3.9

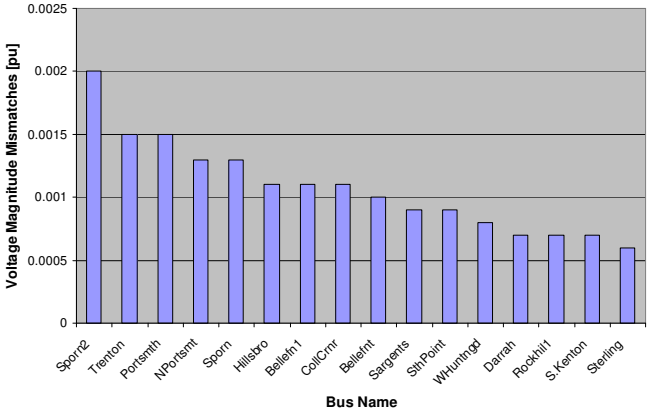

Fig. 7. The biggest mismatches in voltage magnitudes (branch contingency)

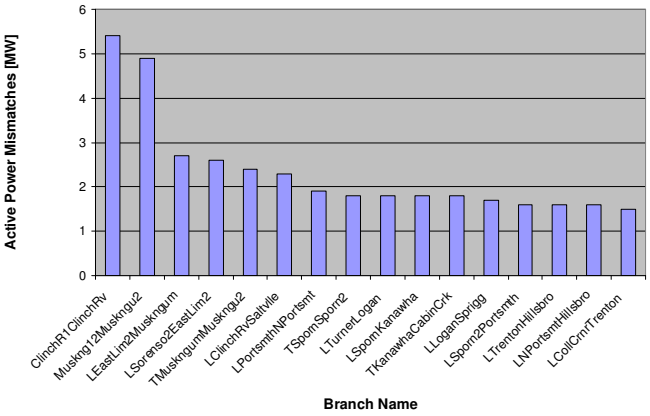

Fig. 8. The biggest mismatches in active power flows (branch contingency)

This specific contingency causes one line in the area W to be overloaded (checked by the TSO of S using the PQ injections provided by the TSO of area N) with the line "LCollCrnrTanrskCk1" being loaded a little above its MVA limit.

C. Accuracy of the equivalent model in case of a branch contingency

Next, the accuracy of the equivalencing procedure with respect to the unreduced system model is shown for the worst branch (out of all internal and interconnection lines) outage contingency.

Figures 7, 8 and 9 show the results of the worst contingency, in terms of biggest mismatches on the boundary bus voltage magnitudes as well as active and reactive power flows in the tie-lines.

More precisely, the figures show the discrepancies between the solutions obtained, on one hand, with a standard contingency evaluation performed on the whole, unreduced model and, on the other hand, with the proposed two-step procedure.

The errors observed on voltage magnitudes are within 0.002 pu. The errors experienced on tie-line power flows are within 6 MW and 3 Mvar, respectively. The branch with the worst results is the double circuit tie-line "LMuskngumSporn".

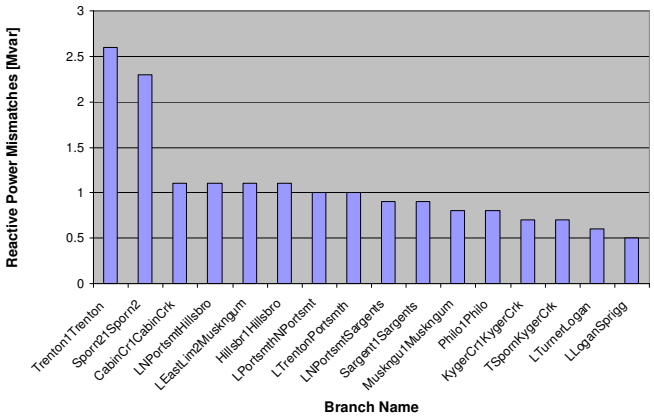

Fig. 9. The biggest mismatches in reactive power flows (branch contingency)

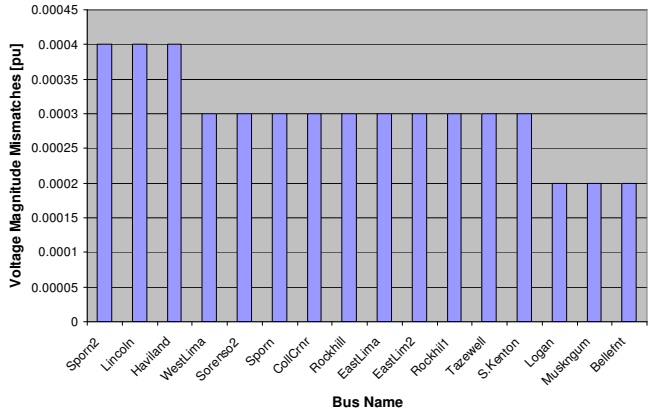

Fig. 10. The biggest mismatches in voltage magnitudes (generator contingency)

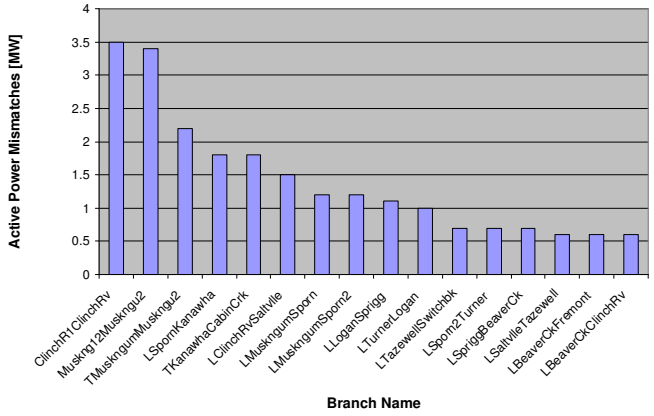

Fig. 11. The biggest mismatches in active power flows (generator contingency)

D. Accuracy of the equivalent model in case of a generator contingency

Finally, the results similar to those of the previous section are shown for the worst generator outage contingency.

Figures 10, 11 and 12 illustrate the accuracy of the equivalent model for the worst generator contingency in area N (generator "GMuskngum"). The shown results are of the same type as for the branch outage.

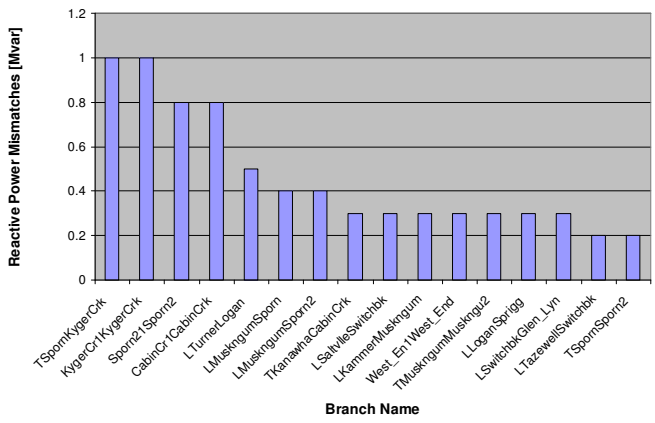

Fig. 12. The biggest mismatches in reactive power flows (generator contingency)

The errors observed on voltage magnitudes are within 0.0004 pu. The errors experienced on tie-line power flows are within 3.5 MW and 1 Mvar, respectively. These results, together with those of previous subsection, show that the accuracy of the procedure is quite satisfactory for practical applications.

E. Discussion

In our simulations we did not consider the possibility for some generators hitting active or their reactive power limits. The problem of hitting active power limits could be handled by properly re-computing vector $\mathbf{h}$. A similar procedure would be very difficult for reactive power limits. However, to the authors' knowledge, reactive power limits are not handled in external system equivalents.

It could be also envisaged to have the active power rescheduling managed in an iterative way, avoiding to leave the slack bus of the particular TSO network model on the variation of losses.

Besides the equivalents, the proposed approach can be improved and extended in several directions. Natural extensions would deal with a filtering or bounding as well as static security control aspects. In particular a bounding method [17], especially the complete bounding one [18], would strengthen the approach presented in this paper by defining influence factors and appropriate thresholds [13], [14].

It would be also interesting to extend this work to dynamic security assessment, based on either a full dynamic model or a Quasi Steady-State approximation [15]. While the multi-area security assessment framework would still be valid the equivalents should be extended to dynamic equivalents, in which the dynamics of the active and reactive power injections can be computed from the knowledge of the dynamics of voltage magnitudes and phases.

VII. Conclusion

This paper has described a procedure relying on sensitivity-based equivalent for the multi-area static security assessment of large interconnected power systems operated by a team of TSOs.

The relevance of this equivalent in the context of general multi-area security assessment framework and recent activities at European level (UCTE recommendations on operational security policy), has been stressed and discussed in the paper.

The equivalent has been validated by the comparison of the results for base case with respect to the unreduced model and by variation of system parameters around the base case solution.

The proposed sensitivity-based equivalent model, tested on the IEEE-118 network, proved to be a good compromise between computational speed and accuracy of the security assessment computations. The validation and accuracy checking revealed that the proposed procedure is a viable approach for security assessment of large interconnections operated by multiple TSOs.

ACKNOWLEDGMENTS

M. Glavic acknowledges FNRS (Belgian National Fund for Scientific Research) for supporting his research stays at the University of Liège through a visiting professor grant. Thierry Van Cutsem is a research director of FNRS. This paper presents research results pertaining to Belgian Network DYSCO (Dynamical Systems, Control, and Optimization), funded by the Interuniversity Attraction Poles Programme, initiated by the Belgian State, Science Policy Office. The scientific responsibility rests with its authors.

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," [Online], Available: http://www.pserc.wisc.edu, April 2004.

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

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

[4] L. Wehenkel, M. Glavic, and D. Ernst, "A collaborative framework for multi-area dynamic security assessment of large scale system," *in Proc. 2007 IEEE Power Eng. Soc. PowerTech Conference*, Laussane, Switzerland, Jul. 2007.

[5] A. Calvaer and P. L. Boulanger, "Application of External Equivalents in the Case of Machine Outages in the Study System," *in Proc. 1980 IFAC Symposium on Automatic Contrl in Power Generation, Distribution, and Protection*, Pretoria, RSA, Sept. 1980.

[6] A. S. Debs, *Modern power systems control and operation*, Springer, 1983.

[7] F. F. Wu and A. Monticelli, "Critical review of external network modelling for online security analysis," *International Journal of Electric Power and Energy Systems*, vol. 5, no. 4, pp. 222-235, Oct. 1983.

[8] A. Bose, "Modelling of external networks for on-line security analysis," *IEEE Trans. on Power App. and Syst.*, vol. PAS-103, no. 8, pp. 2117-2125, Aug. 1984.

[9] F. C. Aschmoneit and J. F. Verstege,"An External System Equivalent for On-Line Steady-State Generator Outage Simulation," *IEEE Trans. on Power App. and Syst.*, vol. PAS-97, no. 3, pp. 770-779, May/Jun. 1979.

[10] F. L. Alvarado,"Determination of External System Topology Errors," *IEEE Trans. on Power App. and Syst.*, vol. PAS-100, no. 11, pp. 4553-4561, Nov. 1981.

[11] K. Kato (Chairman),"External Network Modeling - Recent Practical Experience," *IEEE Trans. on Power Syst.*, vol. 9, no. 1, pp. 216-228, Feb. 1994.

[12] UCTE Document, "UCTE Operation Handbook," [Online], Available: http://www.ucte.org/resources/publications/ophandbook/.

[13] UCTE Document, "UCTE OH-Policy 3: Operational Security," [Online], Available: http://www.ucte.org/activities/.

[14] UCTE Document, "UCTE Appendix-OH-Policy 3: Operational Security," [Online], Available: http://www.ucte.org/activities/.

[15] T. Van Cutsem, C. Vournas, *Voltage Stability of Electric Power Systems*, Springer (previously Kluwer Academic Publishers), 1998.

[16] R. D. Christie, "Power systems test case archive. 118 Bus Power Flow Test Case," University of Washington, Department of Electrical Engineering, [Online], Available: www.ee.washington.edu/research/pstca/pf118/pg_tca118bus.htm.

[17] L. Wehenkel, M. Glavic, and D. Ernst, "Multi-Area Security Assessment: Results using Efficient Bounding Method", *in Proc. 2006 38th North American Power Symposium (NAPS)*, Carbondale, IL, Sept. 2006.

[18] V. Brandwajn and M. G. Lauby,"Complete Bounding Method for AC Contingency Screening," *IEEE Trans. on Power Syst.*, vol. 4, no. 2, pp. 724-729, May 1989.