Multi-Area Security Assessment: Results using Efficient Bounding Method

Louis Wehenkel, *Member, IEEE*, Mevludin Glavic, *Member, IEEE*, Damien Ernst, *Member, IEEE*

***Abstract*— We present our recent results on using previously introduced framework for multi-area security assessment in large interconnections. The basic idea of the framework is exchanging just enough information so that each operator can evaluate the impact in his control area of contingencies both internal and external to his area. We provide illustrations based on a localization concept known as efficient bounding method and recently introduced approximate DC model of the European interconnected system. In this paper we focus on four transmission system operators (within the approximate DC model): Belgium, France, Germany, and Netherlands (for both Summer and Winter-peak load conditions).**

***Index Terms*— Security assessment, information exchange, multi-area large interconnection, black-box equivalent.**

I. Introduction

LARGE interconnected power systems are usually decomposed into areas based on various criteria and the operation and control of the whole interconnection is shared by Transmission Systems Operators (TSOs) responsible for their respective areas. To keep the security of the whole interconnection on desired level, a higher level of coordination among TSOs is required [1]-[3]. Efficient coordination among TSOs requires an efficient information exchange. Different approaches have been considered or are under consideration aiming to a higher level of coordination among different TSOs.

In North America the approach is to create higher level operational entities (RTOs or Mega-RTOs) that act as the coordinator of the lower level TSOs over very large geographical areas [1]-[3].

From the European perspective it is not (at least presently and in near future) possible to set up a transnational security coordinator that would have authority to handle security assessment over the whole or part of the European interconnection.

There is a strong impediment towards information exchange among different actors of the European energy sector. Indeed, for several reasons, the European electric power industries have traditionally been very cautious in terms of confidentiality and security of technical information about their system. Nevertheless, there are some ongoing efforts towards the standardization of operation policies and practices summarized in UCTE Operation Handbook [4].

In our previous work [5] we introduced a framework for information exchange and security analysis suitable for distributed multi-area security assessment and control in large interconnections operated by a team of TSOs. In this framework, each TSO is committed to compute the effect of his internal contingencies on line flows and voltages in his area and on current flows in all the interconnections between all control areas of the system. Each TSO is also committed to provide to all other TSOs an up to date equivalent model of its internal area that allows one to compute voltages at the terminal buses of all its interconnections from current injections in these latter. Furthermore, each TSO is committed to use the detailed model of his area so as to compute the internal state of its area when subjected to the post-contingency flows in the interconnections as they are computed by the other TSOs for their own internal contingencies, and to inform the other TSOs of any internal violations due to external contingencies.

The rest of the paper is organized as follows: Section II briefly presents the multi-area security assessment framework; Section III presents the results obtained using efficient bounding method and approximate (DC) model of the European Interconnection and Section IV offers some conclusions.

II. Multi-area security assessement framework

The framework was introduced and discussed in [5]. To make this text self-contained we repeat main features of the framework. The framework defines an information exchange scheme to allow each area to: carry out security assessment locally and appreciate security level of whole interconnection.

When a TSO runs his static security assessment package, say to simulate the tripping of one of his lines (including his interconnections with his neighbors), the detailed results concerning his own system will be displayed to him only. If the contingency leads to internal violations, he should however inform the other TSOs that there is a problem. On the other hand, if this contingency creates violations on interconnection lines, all the operators should be aware about the detailed consequences. Furthermore, if the contingency creates problems inside any other area, these should also be detected and analyzed in detail. In this case also, all TSOs should be aware of the fact that there is a problem whose solution needs cooperation between the operators. A theoretical solution to this problem is to share completely all real-time SCADA information and power system models, and to oblige each TSO to run its security assessment package by using the complete model of the whole interconnection when analyzing the effects of his internal contingencies and interconnection losses. However,

The authors are with the Electrical Engineering and Computer Science Department, the University of Liège, Sart Tilman B28, 4000 Liège, BELGIUM. E-mails: {lwh, glavic, ernst}@montefiore.ulg.ac.be

1-4244-0228-X/06/$20.00 ©2006 IEEE

this solution is technically expensive if not impossible and hindered by confidentiality issues.

The framework relies on the exchange of minimal amounts of information, while still achieves the above requirements. Therefore, instead of using detailed models requiring detailed data exchange, it is based on the exchange of equivalent models. For the purpose of static security assessment, an equivalent model of an area is a black-box model of the voltage-current relationship at the receiving ends of the interconnections of that area, which can be plugged into a power flow computation.

The good quality equivalent models can in principle be computed in real-time by each area TSO, using the SCADA measurements, topology processor and state-estimation software available in his EMS platform, and that in principle it can also be packaged in such a way that no detailed information about the area is exchanged, other than what is strictly required from a physical points of view to model voltage/current relationships at the terminals.

The framework provides incentives for good quality equivalents, since:

- each TSO has the possibility to check quality of equivalents, by plugging his detailed model, computing interconnection currents, and comparing with “equivalent” information published by others;
- providing a good quality equivalent of one’s area to other TSOs is a necessary and sufficient condition for being able to predict correctly the impact of external contingencies on one’s area.

The TSOs can collect information about the interface (to other subsystems) variables and they could also enrich these measurements by providing measurements corresponding to a richer set of simulated conditions. Using such datasets, it would in principle be possible to construct, by supervised learning, synthetic input-output models relating the steady-state of input signals to those of outputs.

A. *Security assessment decomposition*

From the viewpoint of each particular TSO there are three types of *contingencies*:

- Internal contingency in its own area (loss of line or generator, etc.)
- External contingency to its area (a contingency internal to another area)
- Outage of an interconnection line (anywhere in the overall system, i.e. not just those directly connected to the particular area)

There are two types of *effects*:

- Internal effects (currents and voltages in particular area, subsequent to contingency occurrence)
- External effects (active/reactive current flows through all the interconnections, subsequent to contingency occurrence)

Computation of effects (within the framework) is as follows:

- **Internal contingency or interconnection trip**: use detailed model of own area and interconnections plus equivalent models of other areas.
- **External contingency**: use detailed model of own area plus post-contingency interconnection currents computed by area of origin of this external contingency.

B. *Information exchange protocol*

The TSO of each area posts on the “Web”:

1. An equivalent model of his area,
2. Results of his own security analysis:
   - For each internal contingency considered:
     - likelihood of the contingency,
     - summary of internal effects (e.g. harmless vs. harmful)
     - detailed external effects (i.e. post-contingency currents in all the interface lines of the whole interconnection)
   - For each external contingency considered:
     - summary of internal effects (e.g. harmless vs. harmful)
   - For each interconnection contingency considered:
     - Detailed external effects and summary of internal effects

All information that has changed since the last update must be posted as soon as possible. Computations must be done to respond to new information (internal or external) within deadline. All information about all interconnections (measured or computed) should be considered as common information inside the team of TSOs. Actually, each TSO should be committed to compute the effect of the tripping of any interconnection using the detailed model of his own area and the equivalent models provided by the other areas. This means that the contingencies related to the loss of interconnections are computed several times and that the resulting post-contingency flows over the remaining interconnections are shared information. All TSOs could anticipate any problem that could appear on any interconnection, and if the equivalent models are of good quality, the information computed by all the TSOs about all the interconnections will be coherent.

III. Results using efficient bounding method

Since many contingencies present rather localized effects, the above scheme would lead to many useless computations. In order to exploit the local nature of many contingencies each TSO could publish “safe bounds” on his area. All TSOs would then publish only those external effects that fall outside of the “safe bounds” of at least one other area. This would allow a significant reduction of the computational burden related to the computation by each area of internal effects of external contingencies and the amount of information to share.

In the worst case, each TSO has to compute the detailed impact on his system of all contingencies internal or external, and in the worst case the computational burden for each such computation is equivalent to using a complete detailed model. If necessary, parallel computations can be used to speed up response times, e.g. by running several contingency sets in parallel. However, from the maintenance and monitoring point of view this is concerned by the details of only this system.

We provide illustrations based on a localization concept known as bounding [6,7]. Bounding methods are based on engineering observation that many power system contingencies have a local impact. This was first recognized and efforts undertaken to take advantage of this fact in [8] where the concept of concentric relaxation was introduced. Next, powerful concept of bound estimates was presented in [9]. These concepts were further extended in [6,7]. We suggest and use the bounding method within the framework for several reasons and main being:

- The localization is inherent to the proposed framework and the bounding method fits well to it,
- Bounding method will further ease computational burden within the framework,
- We determine the upper bounds for individual TSOs based on the idea of bounding technique [6].

To make this text self-contained a brief description of the efficient bounding technique [6] (for the case of a single branch outage) is given below.

A. *Efficient Bounding method*

The bounding methods [6,7] have important attributes that render this approach, in contingency analysis, superior with respect to others. The method is very efficient for detecting line MW flow violations and is based on DC (linear incremental) power flow model that is expressed (for a system with n buses) by the following matrix equation,

$$B'\Delta\theta = \Delta P \tag{1}$$

where ΔP is n-dimensional vector of changes in real power injections, $\Delta\theta$ is n-dimensional vector of changes in bus angle, and B' is $n\times n$ susceptance matrix. The effect of each contingency on MW flows can be found by solving for $\Delta\theta$, and calculating the resulting changes in line flows as (for the line km) [6],

$$\Delta P_{km} = (\Delta\theta_k - \Delta\theta_m)/x_{km} \tag{2}$$

where x_{km} is the reactance of the line km. The total post-contingency power flow is computed as (for the line km),

$$P_{km} = P_{km}^0 + \Delta P_{km} \tag{3}$$

where P_{km}^0 is pre-contingency MW flow.

As illustrated in Fig. 5, the entire network is divided into three sub-networks: N1, N2, and N3.

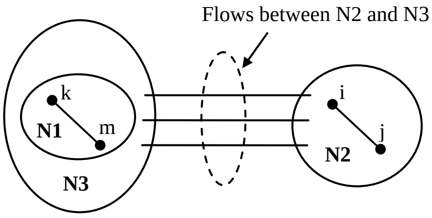

Fig. 1 A network partition in bounding method

During the procedure the N1 sub-network, which initially contains only the terminal buses of the outaged branch (*k* and *m*), is progressively extended by including nodes from N3; on the other hand N3 is always composed of the boundary buses that separate the sub-network N1 from the remainder of the system model contained in N2. The iterative procedure building up the three sub-networks ends as soon as it is possible to ensure that no flow violation outside N3 may occur. The effects of the branch outage are modeled by a pair of equal but opposite injections at buses *k* and *m*. The efficient bounding method is based on incremental flow criterion [6]:

The maximum incremental active power flow in any branch in N2 cannot exceed the incremental flow entering that sub-network,

or incremental angle criterion [6]:

The incremental angular spread across any branch in N2 cannot exceed the maximum incremental spread between the boundary buses.

The incremental angle criterion has several advantages over incremental flow criterion [6] and we use it in our illustrations. The main advantage in using this criterion is the fact it can be diminished, unlike incremental flow criterion, by expanding N1 even if the expansion does not add any closed loops to N1 [6]. The central idea of efficient bounding technique is to expand sub-network N1 and diminish incremental angle criterion until it becomes less than minimal angular spread over the lines in sub-network N2 (set of endangered lines in N2 is empty). In this way the sub-network (N1+N3) that is affected by particular line outage and that should be analyzed with more scrutiny is identified.

The effect of branch outage in efficient bounding method is modeled by a pair of appropriately scaled injections at the buses at the both ends of the line. It can be shown rigorously that [6], within assumptions of the linearized (DC) model, the maximum incremental flow in any line in particular sub-network cannot exceed the incremental flow entering or leaving that sub-network. Consequently, the flows have to be calculated only for branches endangered by the boundary flow [6]. This is the main argument around which the efficient bounding method is built. We use the same argument to define the upper bounds for every sub-system in the network, as discussed in next sub-section.

B. *Results*

We take advantage of the availability of the IEEE Common Data Format (CDF) [10] for the recently introduced approximate model of European interconnected system [11].

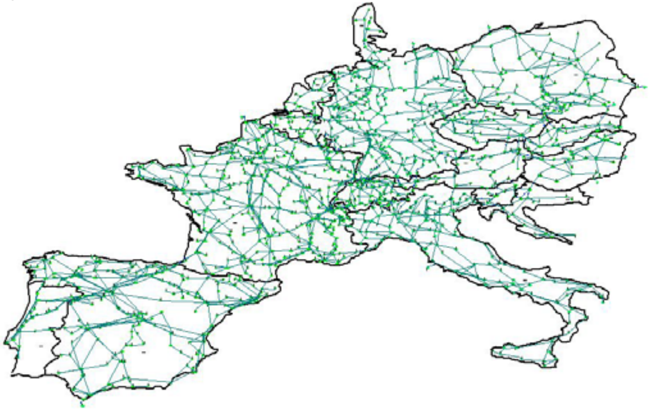

Fig. 2 European Interconnected System

The system is shown in Fig. 2. and includes 1254 buses, 378 generators, 17 areas (TSOs) , and 28 cross-border interfaces.

In our illustrations we suppose that every individual TSO uses efficient bounding technique in order to ease computational burden. Two CDF files [10,11] are used for the system corresponding to Summer 2002 and Winter-peak 2002 loading conditions. Available DC model has been particularly tailored for the study of cross-border trades and consequently considerable work had to be done in order to make this model useful for security assessment. The limits of the lines are not available in any of CDF files used (except for the tie-lines, however some of the tie-lines were already tuned to be congested). First effort undertaken was to put a reasonable MW limit for all lines with main goal of having feasible system conditions in base-case and reasonable values of safe bounds in every sub-system (in this paper we focus on four TSOs: Belgium, France, Germany, Netherlands) for both Summer and Winter-peak load conditions. After having the feasible system state for both Summer and Winter-peak load conditions the safe bounds are calculated for each of the sub-systems of interest. Safe bounds of each sub-system are calculated as,

$$\underset{l\in N_l}{Min}\left\{\left(P_l^{\max}-\left|P_l^0\right|\right)\cdot x_l\right\} \qquad (4)$$

where $P_l^{\max}$ is the MW flow limit on the line l, P_l^0 the flow on the same line in base-case (pre-contingency), x_l is line reactance, and N_l is the number of the lines in the sub-system. This safe bound corresponds to the minimum changes in phase difference across the lines in the system and for the line l (between the buses p and q) holds,

$$\left(\Delta\theta_p-\Delta\theta_q\right)^{\max}=\left(P_{pq}^{\max}-P_{pq}^0\right)\cdot x_{pq} \qquad (5)$$

The results of safe bounds determination are summarized in Table I.

TABLE I
SAFE BOUNDS

Load conditions	Belgium	France	Germany	Netherlands
Summer	0.0271	0.0277	0.0187	0.0173
Winter-peak	0.0153	0.0123	0.0116	0.0142

Following the same reasoning and argument of the efficient bounding method [6], the upper bound (maximal angular spread) for every sub-system in the network can be determined as maximal angular spread over boundary buses of the sub-system (see illustration in Fig. 3 and equation (6)). Fig. 3 illustrates how (as an example) Netherlands TSO performs security assessment in its own system and how determines for each particular contingency the upper bound in changes of phase angles for German TSO. This upper bound is determined as maxumum change of phase angles among all buses (within Germany) through which German system is connected with the rest of the whole system (bulleted buses in Fig. 3).

For each contingency inside Netherlands internal effects as well as upper bound for German TSO are calculated. The upper bound is calculated as,

$$UB=\left|\Delta\theta_i^{\max}-\Delta\theta_j^{\min}\right| \qquad (6)$$

where UB stands for upper bound, $\Delta\theta_i^{\max}$ is maximum angle change (with respect to the base-case value) among all buses connecting German TSO to the rest of the system (supposed in the equation to happen at bus i) and $\Delta\theta_j^{\min}$ is minimum angle change (with respect to the base-case value) among all buses connecting German TSO to the rest of the system (supposed in the equation to happen at bus j). Each contingency for which upper bound exceeds posted safe bound of German TSO is declared as potentially externally harmful.

The results of contingency assessment for all four TSOs of interest are summarized in Tables II and III. Table II gives total number of contingencies, those declared as internally harmless and harmful as well as those declared potentially harmful for other TSOs for both Summer and Winter-peak load conditions. External equivalent for each TSO is taken as the exact DC model of all other TSOs in the system. Table III presents the results of assessment of each contingency declared as potentially externally harmful by every TSO performed by every TSO to which the contingencies are declared as potentially harmful.

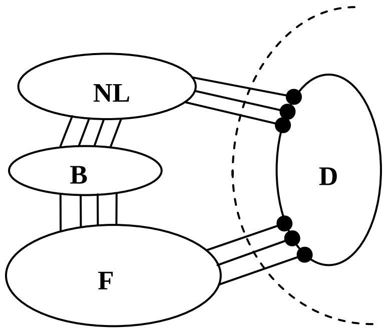

Fig. 3 Illustration of upper bound determination

TABLE II
CONTINGENCIES SUMARY (SUMMER/WINTER-PEAK)

Contingencies	Belgium	France	Germany	Netherlands
Total	32/32	546/546	334/334	35/35
Internally harmless	6/4	112/101	83/74	4/3
Internally harmful	20/22	427/438	243/252	24/25
Potentially externally harmful	22/24	25/29	28/39	29/29

TABLE III
POTENTIALLY EXTERNAL HARMFUL CONTINGENCIES AS ASSESSED BY OTHER TSO

-	Belgium	France	Germany	Netherlands
Belgium	-	16/10 (17/10)	14/10 (15/12)	16/14 (18/15)
France	15/10 (17/13)	-	21/16 (24/19)	118/12 (20/13)
Germany	20/15 (21/16)	24/19 (34/25)	-	21/18 (27/22)
Netherlands	24/17 (24/17)	25/18 (26/19)	24/23 (24/23)	-

Observe that all line outages within every TSO are considered as contingencies augmented by all interconnection lines in the system not directly connected to a particular TSO (numbers of these interconnection lines are: 6 for Belgium (interconnection lines between Germany and Netherlands and Germany and France, see Fig. 3), 7 for France, 8 for Germany, and 7 for Netherlands.

The results in Table III are in the following format: Potentially harmful/Harmful (no brackets correspond to Summer and within brackets to Winter-peak load conditions).

It is interesting to note that most of internal contingencies in Belgian and Dutch TSO are also potentially externally harmful to other TSOs. This is even intuitively clear since both of the sub-systems are relatively small as compared to French or German system. Also, by inspection of the data in available CDF files [10,11] it is clear that Dutch system is heavily loaded (with high flows on the lines) even during Summer conditions. Similar observation holds for Belgian TSO. Contrary to this, small fractions of contingencies within French and German TSOs are declared as potentially externally harmful. Note also, that most of contingencies inside Belgian or Dutch TSO are also declared finally as harmful by other TSOs but this is not the case with French and German TSOs.

For each contingency declared as externally potentially harmful, a TSO that computes effect of such a contingency does not need the model of the TSO declared the contingency potentially harmful. In this case, the TSO just adjust inputs from other TSO based on the posted violation of its safe bounds calculated by other TSO.

C. *Discussion*

Static security assessment is considered in this paper together with efficient bounding method. In principle, other bounding concepts that permit consideration of other system limits then line MW (e.g., complete bounding method [12]) could be also used within the framework. The idea can also be extended to dynamic security assessment by replacing the external equivalents by dynamic equivalents and posting post-contingency dynamics of interconnection flows rather than steady state values. In this context a dynamic equivalent is a black-box model of an area which allows one to compute dynamics of voltages from dynamics of current injections (or vice versa) and which can be plugged into a dynamic security assessment package. Notice that the idea of safe bounds also carries over in principle to the dynamic case. While static equivalents can in principle be computed in real-time with present technology, the issue of computing good quality dynamic equivalents deserves further research. Some research considerations in constructing the dynamic equivalents through artificial neural networks are reported in [13,14].

We intend to use supervised learning to synthesize input-output models relating the steady-state (or dynamics) of input signals to those of outputs, in our future research.

IV. Conclusions

The results of using efficient bounding method within recently introduced multi-area security assessment framework, are presented in this paper. In this paper it is demonstrated using approximate model (DC) of the European Interconnected System. The choice of efficient bounding method is based on the observation that this localization concept fits well into the framework, while the choice of the European Interconnected System is based on the fact that the framework is perfectly coherent with actual collaborative nature of system wide operation in Europe, needs only a minimal amount of information sharing and is not very demanding in terms of communication infrastructures. We also believe that the framework together with efficient bounding method could also be considered as an approach to handle security assessment in North-American Mega-RTOs, where it could help to circumvent problems of scalability of algorithms and maintainability of data by distributing them over the TSOs under the authority of the Mega-RTO [15].

Acknowledgment

M. Glavic and D. Ernst gratefully acknowledge the support from Belgian National Fund for Scientific Research (FNRS).

References

[1] P. Hirsch, S. Lee, “Security Applications and Architectures for an Open Market”, *IEEE Computer Applications in Power*, pp. 26-31, July 1999.

[2] M. Kezunovic, A. Abur, A. Edris, D. Sobajic, “Data integration/exchange, Part 1: existing technical and business opportunities”, *IEEE Power and Energy Magazine*, pp. 14-19, March/April 2004.

[3] K. Morison, L. Wang, P. Kundur, “Power System Security Assessment”, *IEEE Power and Energy Magazine*, pp. 30-39, September/October 2004.

[4] "UCTE Operation Handbook”, [Online] Available: http://www.ucte.org/ohb.

[5] L. Wehenkel, M. Glavic, D. Ernst, “On multi-area security assessment of large interconnected power systems”, *Second Carnegie Mellon Conference in Electric Power Systems*, Pittsburg, PA, Jan. 2006.

[6] V. Brandwajn, “Efficient Bounding Method for Linear Contingency Analysis”, *IEEE Transactions on Power Systems*, vol. 3, no. 1, pp. 38-43, Feb. 1988.

[7] V. Brandwajn, “Localization Concepts in (In)-Security Analysis”, *IEEE Athens PowerTech*, Paper APT IS-322, pp. 10-15, Athens, Greece, Sept. 1993.

[8] J. Zaborzsky, K. W. Whang, K. Prasad, “Fast Contingency Evaluation using Concentric Relaxation”, *IEEE Transactions on PAS*, vol. PAS-99, pp. 28-36, 1980.

[9] F. D. Galiana, “Bound Estimates on the Severity of Line Outages in Power System Contingency Selection of Overloads”, *IEEE Transactions on PAS*, vol. PAS-103, pp. 2612-2624, 1984.

[10] “Common Data Format of European Interconnected System”, [Online]Available:http://webdb.ucs.ed.ac.uk/see/staff/staff.cfm?person=jbialek.

[11] Q. Zhou, J. W. Bialek, “Approximate Model of European Interconnected System as a Benchmark System to Study Effects of Cross-Border Trades”, IEEE Transactions on Power Systems, vol. 20, no. 2, pp. 782-788, May 2005.

[12] V. Bradwajn, M. G. Lauby, “Complete bounding method for AC contingency screening”, IEEE Trans. on Power Systems, vol. 4, no. 2, pp. 724-729, May 1989.

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

[14] 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.

[15] R. Thompson, V. Brandwajn, “Functional aspects of scaling to a large RTO”, *In Proceedings of IEEE PES Winter Meeting 2002*, p. 42, New York, USA, 2002.