On multi-area security assessment of large interconnected power systems

Louis Wehenkel, Mevludin Glavic, Damien Ernst

***Abstract*— The paper introduces a framework for information exchange and coordination of security assessment suitable for distributed multi-area control in large interconnections operated by a team of transmission system operators. The basic idea of the proposed framework consists of 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. The framework has been thought out with the European perspective in mind where it is presently not possible to set up a transnational security coordinator that would have authority to handle security control over the whole or part of the European interconnection. Nevertheless, it can also be considered as an approach to handle security control 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 RTO.**

***Index Terms*— Security assessment, information exchange, security control, congestion management.**

I. Introduction

THE electric power sector, all around the World, is undergoing a series of very important changes which have strong impact on power systems security. Among these changes, the most well known one is due to the restructuring of the electrical power sector towards a market-based environment. Competition in the electric market forces generating companies as well as system operators to operate the system with lower security margins, the first in order to remain competitive with other electricity suppliers, the second in order to allow this competition to take place over a wide region. This tendency, which is already quite advanced, will continue to change power flow patterns, increase uncertainties, and reduce security if care is not taken. The intimate role that electricity plays in today's societies implies that the power system security is to remain the most important aspect of power system operation which cannot be compromised in a market-driven environment [1].

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 at a desired level, a higher level of coordination among TSOs is required [2]-[4]. 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 [2]-[4]. Most notable work in this field is done by EPRI [2] through the development of Common Information Model (CIM) data format. CIM has the data structure that is common to almost all Energy Management Systems (EMS) proprietary systems and is now a standard structure to convert proprietary EMS formats.

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. A very important specificity of Europe is the way the interconnection is organized and regulated. Essentially, the European Union has no structure nor any legal power to enforce a common way of organizing the whole business. On the top level, the European Directives provide common objectives, general guidelines and principles. On the bottom level, the precise implementation of these guidelines is sub-contracted to each country, where the rules and laws are created in order to comply with the European Directives and, above all, to fit into the local system, political organization and economic context. Also, there is no transnational body playing a role such as FERC does in the US, and the model adopted for the coordination of the different TSOs is essentially based on multi-lateral negotiation and cooperation through gentlemen's agreements.

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. These reasons are technical (insufficient communication infrastructure, different data formats, etc.) or non-technical (conflicts in commercial and social interests or in regulatory frames) ones. Nevertheless, there are some ongoing efforts towards the standardization of operation policies and practices which are summarized in UCTE Operation Handbook [5].

The paper introduces 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. The concepts

The paper is based on a presentation that was made at the Electric power control centers workshop organized by Tom Dy Liacco in June 2005 in Diablerets (Switzerland).

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

that are introduced are general in the sense that they apply as well to dynamic as static security assessment. However, the paper focuses on static security assessment. The basic idea of the proposed framework consists of exchanging just enough information so that each TSO can evaluate the impact in his control area of contingencies both internal and external to his area. To this end each TSO is committed to compute the effect of its 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 which 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 effect of the framework on better transparency and coordination of security control in multi-area systems is discussed and policies for handling multi-area congestion management are suggested.

This framework fits to the collaborative European organization but it could also be considered as an approach to handle security control 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 RTO.

The rest of the paper is organized as follows: Section II briefly discusses present practice of security assessment in multi-area systems like Europe; Section III presents the proposed framework and Section IV provides an illustration of the presented ideas.

II. Present practice and ongoing activities

A. Present practice

Present practice (from the European perspective) is as follows. Each TSO maintains a physical model (in real-time, and also in the operation planning environment) of his own power system. These models are based on a combination of three types of information [6]:

- Off-line data and first-principles from physics: the elementary state equations of the different physical devices and the measured parameters (impedances, inertias, standard deviations of measurement errors, etc.), and the external equivalents provided by the neighbor TSOs or by central agency such as UCTE.

- Real-time measurements provided by the conventional SCADA function every few seconds.

- The forecasted and planned quantities (weather, load, maintenance schedules, etc.)

The basic tool for exploiting this information in the TSO environment is the power flow software, and its extended versions (the state estimator and static security assessment package), which are used in order to determine whether or not forecasted or actual network state in a given context should be accepted or rejected. The basic criterion for rejecting a network state is the capacity of the network state to meet the security criteria. These criteria are normally based on the analysis of the actual or forecasted operating state and under all the contingencies with a certain level of probability to occur. This leads to the following decision rule: a state is rejected by a particular TSO if it would lead, or if it would lead potentially under some contingency in the system of the TSO, to an unacceptable operating state (voltages or flows out of their limits) of the system controlled and supervised by this TSO.

At the European level, security assessment and control is thus handled in a distributed way, where each TSO essentially focuses on his own power system, and uses accurate and up-to-date information only about his own system. Clearly, it would be better to provide to all TSOs a coherent and complete real-time model of the whole interconnection. The question is how this can be achieved in the most cost-effective way, while complying with the confidentiality and safety requirements of data exchange among TSOs. The framework introduced in this paper tries to answer this question.

B. Ongoing activities

The UCTE Operation Handbook [5] summarizes ongoing efforts towards the standardization of operation policies and practices for the European interconnected power system. Most relevant standards to this paper are those concerned with information exchange between TSOs for operation. The Handbook defines the following information exchange for power system computation (relevant to the problem considered in the paper):

- Each TSO provides, on a yearly basis, to all other TSOs a provisional data set (network, generation, loads, and exchange programs) for the preparation of a reference case (so called UCTE base case) that serve to calculate Net Transfer Capacities [5]. Two data sets are to be provided (one for winter and one for summer).

- Each TSO provides, on yearly basis, to all other TSOs data sets (snapshots) for a full representation of their network in real time conditions. Two snapshots are to be provided (winter, and summer) but other snapshots can be exchanged when deemed necessary. Snapshots are more detailed with respect to the data sets used for the preparation of UCTE base case.

The document also defines Electronic Highway (EH), the communication network of European Transmission System Operators (ETSO). The EH is a private network dedicated to the data exchange between TSOs, and its primary scope is the real time data exchange that enhances the security of interconnected system operation. It has been pointed out

that the data exchanged through EH are intended to be used by security related applications within an EMS (power flow, optimal power flow) and are not recommended to be used in real time control applications of EMS (such as load-frequency control). Security-related data to be exchanged in real time include: switch status, MW and Mvar flow, voltages, tap changer position of transformers alarms, generation unit status and MW and Mvar generations. Data exchange has to be agreed among the involved TSOs.

III. MULTI-AREA SECURITY ASSESSEMENT FRAMEWORK

A. Framework objectives

The main objectives of the framework are as follows:

- Define an information exchange scheme to allow each area to:
  - carry out security assessment locally,
  - appreciate security level of whole interconnection.
- Coordinate preventive and emergency control among TSOs

A multi-area interconnected power system is illustrated in Fig. 1. Let us adopt the viewpoint of TSO 1. When TSO 1 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.

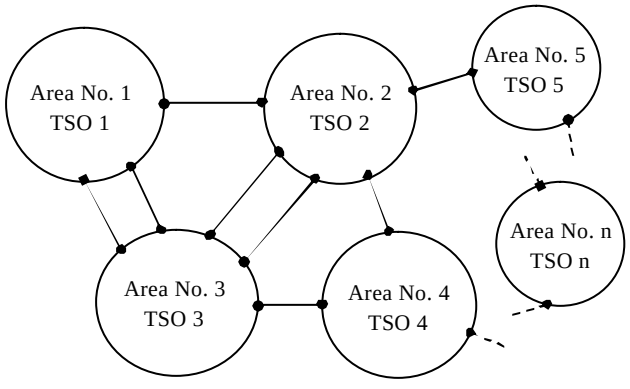

Fig. 1 A multi-area interconnected power system

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

The objective of the proposed framework is to rely on the exchange of minimal amounts of information, while still achieving 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 (Fig. 2).

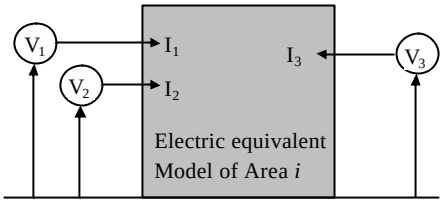

Fig. 2 A black-box model of an area

We will come back to the issue of equivalent models in later section. For time being it is sufficient to know that 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.

B. Security assessment decomposition

From the viewpoint of TSO 1 there are three types of *contingencies*:

- Internal contingency in area 1 (loss of line or generator, etc., in area 1)
- External contingency to area 1 (a contingency internal to another area)
- Outage of an interconnection line (anywhere in the overall system, i.e. not just those directly connected to area 1)

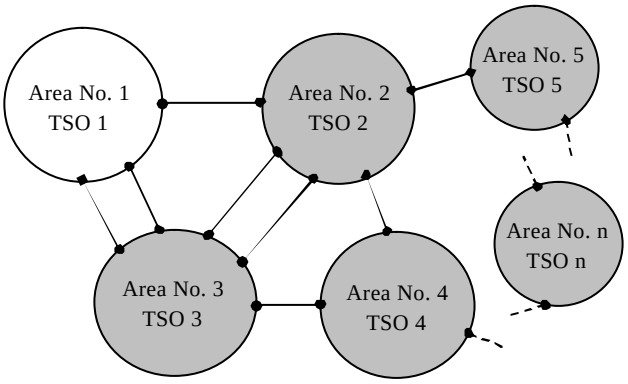

Fig. 3 The viewpoint of the TSO 1

There are two types of *effects* from the viewpoint of TSO 1:

- Internal effects (currents and voltages in area 1, subsequent to contingency occurrence)
- External effects (active/reactive current flows through all the interconnections, subsequent to contingency occurrence)

Proposal for the computation of effects:

- **Internal contingency or interconnection trip**: use detailed model of area 1 and interconnections plus equivalent models of other areas.
- **External contingency**: use detailed model of area 1 plus post-contingency interconnection currents computed by area of origin of this external contingency.

C. 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.

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.

D. Security control issues

Responsibility of TSO1 to handle harmful contingencies:

- In preventive mode:
  - Contingencies leading to internal violations in area 1,
  - Contingencies internal to area 1,
  - Outages of all interconnecting lines
- In emergency mode:
  - All violations internal to area 1,
  - All violations at the interconnections to area 1.

Negotiation/coordination among TSOs is thus required if a contingency or a violation affects several TSOs.

E. Extension to dynamic security assessment

In principle, the framework can 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 would be 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.

Nevertheless, 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.

F. Computational aspects

In principle, the framework obliges every TSO to compute the internal effects in his area of all contingencies analyzed by all other TSOs and for which they publish the resulting post contingency flows in the interconnections. In the worst case, each TSO thus 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.

Thus, if necessary, parallel computations could 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 each area TSO is concerned by the details of only this system.

IV. AN ILLUSTRATION USING SAFE BOUNDS

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, a refinement of the framework would consist of allowing each TSO to publish "safe bounds" on his area (e.g. bounds on the interconnection flows into his area within which he can guarantee that no internal violation will appear) which can be exploited by other TSOs in order to identify the contingencies internal to their area which are potentially harmful for the other areas. 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.

Since, throughout of the paper it is emphasized that the framework development is motivated by the European perspective, we take advantage of the availability of the IEEE Common Data Format (CDF) [7] for the recently introduced approximate model of European interconnected system [8] in order to fix ideas. The available model is tuned to study effects of cross-border trades and indeed much more work is needed to make this DC power flow model of the European interconnection suitable for contingency analysis. In this paper we just use it to illustrate some initial results obtained in developing the framework. We consider this model as a UCTE base case in this paper.

The whole UCTE network is shown in Fig. 4 (we use winter peak CF data from [7]). The network includes 17 areas (TSOs) and 28 cross-border interfaces. For the countries outside the UCTE, fictitious generator/load buses were put at the borders to simulate the power imports/exports.

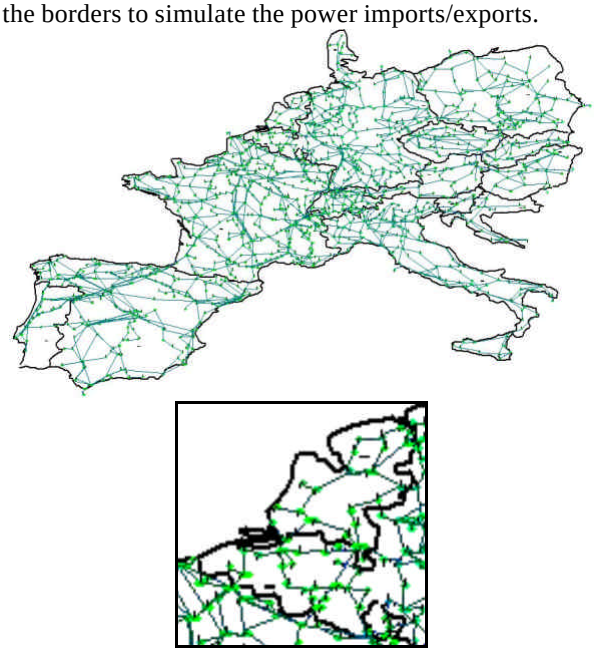

Fig. 4 UCTE network and zoom on Belgian and Netherlands TSO systems

We provide a simple illustration that is based on a localization concept known as bounding [9], [10]. 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 [11] where the concept of concentric relaxation was introduced. Next, powerful concept of bound estimates was presented in [12]. These concepts were further extended by Vladimir Brandwajn [9], [10]. We use the bounding method to illustrate how the framework works for two main reasons:

- The localization is inherent to the proposed framework and the bounding method fits well to it, and
- Our future research efforts will be focused on a variant of bounding method that can be used in conjunction with proposed framework.

To make this text self-contained a brief description of the efficient bounding technique [9] (for the case of a single branch outage) is given below.

A. Bounding method

The bounding methods [9]-[10] have important attributes that render this approach, in contingency analysis, superior with respect to others. Among many of these attributes we enumerate just few [9]: fast adaptability to any type of sustained topological changes in the system, flexibility to model any type and number of contingencies including multiple bus splits, flexibility to adjust the contingency list on-line, ability to modify on-line the list of monitored branches, fast contingency analysis under all conditions and no off-line setup needed. As illustrated in Fig. 4, the entire network is divided into three sub-networks: N1, N2, and N3. 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.

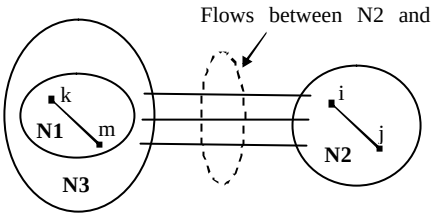

Fig. 4 A network partition in bounding method

The effects of the branch outage are modeled by a pair of equal but opposite injections at buses *k* and *m*. The bounding method is based on boundary flow criteria that can be stated as [9]:

- The maximum incremental active power flow in any branch in N2 cannot exceed the incremental flow entering that sub-network.
- The incremental angular spread across any branch in N2 cannot exceed the maximum incremental spread between the boundary buses.

B. Belgian TSO point of view

We now adopt the Belgian TSO point of view. The Belgian system, within the interconnection, (Fig. 4) is modeled by 22 buses (400 kV); 23 internal lines, and 7 interconnection lines (3 with France, 3 with Netherlands, and 1 with Luxembourg). To illustrate the framework we extracted data corresponding to Belgian and the Netherlands systems and built DC equivalents for both. For both systems, instead of putting arbitrary values for line thermal limits we rather calculated these values by finding "point-to-point" maximum transfers using a variant of continuation power flows [13] (the limits are not provided in CDF data file available [7]). The contingency evaluation has been performed as follows:

- The Belgian TSO is informed by the TSO from Netherlands about the minimum flow margin of all internal lines inside Netherlands, and receives also an equivalent model from the Netherlands internal part.
- The Belgian TSO uses his detailed internal model,

information about the interconnections and the Netherlands equivalent system to compute for each contingency the post-contingency flows inside Belgium and on the interconnections.

- The Belgian TSO uses the efficient bounding method for each contingency in order to assess whether it is internally harmful, or whether it is potentially harmful inside the Netherlands.
- As long as sub-networks N1 and N3 remain within the Belgian system the contingency is declared harmless for the Netherlands and internally harmful or harmless depending of the consequences in terms of active power flow limits of the lines.
- If N3 spreads over the interconnection lines, the TSO of Netherlands is informed that there is potentially an internal problem in his area and the corresponding post-contingency power flow increments on the interconnections are sent to him.

The Netherlands TSO is then able to access its internal impact of these contingencies by using the incremental power flows provided for each such contingency, and by using its internal detailed model.

In our simulations we have considered the tripping of each line inside Belgium incident to the interconnection lines buses (inside Belgium) towards the Netherlands. The results are summarized in Table I (MVA base is set to 100). We borrow the names of buses as they are defined in [7].

TABLE I
SUMMARY OF THE CONTINGENCY SELECTION

BELGIUM		**THE NETHERLANDS**	
Outaged line (from-to)	*Harmful/ Harmless*	*Maximum incremental power flow (p.u.) in N3*	*Harmful/ Harmless*
B_Zandvl –B-2	Harmful	2.2868	Harmful
B-2-B-4	Harmless	-	-
B-5-B_meerho	Harmful (internal)	-	-
B_15-B_Achene	Harmful	0.403	Harmless
B-16-B_15	Harmful	1.1494	Harmless
B-17-B-16	Harmful	11.1137	Harmful

In Table I the second column shows for each contingency the status with respect to internal violations in Belgium. The third column provides the maximum incremental flow in the interconnections in the case the N3 sub-network contains these latter, and the fourth column provides the status of violations inside the Netherlands.

Obviously, the procedure works in a symmetric way to assess the effect of contingencies internal to the Netherlands.

V. CONCLUSIONS

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 is presented in this paper. The strength of the proposal comes from the fact that it 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. At the same time we believe it can also be considered as an approach to handle security control 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 RTO.

We have also illustrated the possibility to use bounding methods to reduce the amount of computations and information exchange needed to implement the framework. It remains to be shown that from a mathematical, numerical and technical point of view this extension is indeed sound in general.

ACKNOWLEDGMENTS

Damien Ernst and Pierre Geurts acknowledge the support of the Belgian FNRS (Fonds National de la Recherche Scientifique) where they are post-doctoral researchers.

REFERENCES

[1] M. Shahidehpour, W. F. Tinney, Y. Fu, “Impact of Security on Power Sistems Operation”, *Proceedings of the IEEE*, vol. 93, no. 11, pp 2013-2025, Nov. 2005.

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

[3] 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.

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

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

[6] A Diu, L. Wehenkel, “EXaMINE – Experimentation pf a Monitoring and Control System for Managing Vulnerabilities of the European Infrastructure for Electric Power Exchange”, *IEEE Summer Meeting 2002*, Chicago, USA. [Online} Available: http://www.examine.ree.es/free/papers/paper1.pdf

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

[8] 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.

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

[10] V. Brandwajn, M. Lauby, “Complete Bounding Method for AC Contingency Screening”, *IEEE Transactions on Power Systems*, vol. 4, no. 2, pp. 724-729, 1989.

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

[12] 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.

[13] M. Glavic, F. L. Alvarado, “Interaction among limits during maximum loadability and transfer capability determination”, PSERC paper, Cornell University, USA, May, 2001, [Online] Available: http://www.pserc.cornell.edu/tcc/info.html