Operating in the Fog

By Patrick Panciatici, Gabriel Bareux, and Louis Wehenkel

Security Management Under Uncertainty

OVER THE LAST TEN YEARS, WE HAVE HEARD SO OFTEN IN CONFERENCES, seminars, and workshops that the power system will soon be operated very near to its limits that this statement has become a cliché. Unfortunately, it is no longer possible to comply with the classical preventive N-1 security standards during all of the hours in a year. The system is indeed no longer able to survive all single faults without postfault actions. More and more corrective (i.e., postfault) actions are defined and prepared by operators, and the "cliché" is now a reality, as a matter of fact. To be more precise, it is no longer possible to maintain the N-1 security of the system at all moments by using only preventive actions, and the number of hours during which the system requires corrective actions to be secure is increasing. More and more, new special protection schemes (SPSs) are deployed to implement some of these corrective actions automatically. Devices such as phase-shifting transformers (PSTs) and static var compensators (SVCs) are added in the system to increase its controllability. As a result, the system becomes more and more complex.

This state of affairs has various causes that will not disappear in the near future. One is that it is more difficult than ever to build new overhead lines because of the "not in my backyard" (NIMBY) attitude. People are more and more afraid of hypothetical electromagnetic effects, or they just don't like to see big towers in the landscape. This is particularly the case in protected areas, which are becoming more and more numerous around Europe. It is very difficult to explain the need for new interconnection lines to people who already have access to electricity at a reasonable price and with high availability. An increase in European social welfare with a positive feedback for the European economy and hopefully for all European citizens is a concept that is too theoretical compared with the negative local impact. Alternative solutions are technically complex, costly, and need even more time to be deployed.

The second main reason is the massive integration of renewable but generally intermittent generation in the system. Power flows in the grid are created by difference in location between power sinks and sources. With a significant amount of intermittent power generation, the predictability of the sources (location and levels of power injections) decreases and strongly affects the predictability of power flows. Furthermore, these new power plants are generally

Digital Object Identifier 10.1109/MPE.2012.2205318
Date of publication: 16 August 2012

1540-7977/12/$31.00©2012 IEEE

small units connected to the distribution grid. Transmission system operators (TSOs) therefore have difficulty observing these power injections, and they have no direct control over them. Another factor is the inconsistency between the relatively short time needed to build new wind farms (two or three years) or install photovoltaic panels (months) and the time it takes to go through all the administrative procedures required to build new lines (more than five years). Some TSOs have proposed that their regulators implement mechanisms that encourage the installation of these new generators in areas where the grid has enough spare capacity to accommodate the new injections. Unfortunately, changing the regulatory framework is difficult. Such mechanisms could only take the form of incentives, and each producer must find the optimal balance between the cost of accessing the grid and the cost of the primary energy. In addition, these mechanisms would only solve some local problems. At the European level, the best locations for wind farms are mostly along the coasts and offshore, while for photovoltaic generation they are in the south of Europe. Since these locations do not generally match those of the large load centers, a transmission network is still required, and this network will still have to cope with the variability of the power flows.

The third reason is linked to the liberalization of the electricity markets. Generators, retailers, and consumers view the transmission system as a public resource to which they should have unlimited access. This approach has the desirable effect of pushing the system toward maximization of the social welfare and an optimal utilization of the assets. This optimization is limited by security considerations, however, because large blackouts are unacceptable in our modern societies due to their huge economic and social costs. Since TSOs are responsible for maintaining the security of the supply, they must therefore define the security limits that should be respected. As in any constrained optimization problem, the optimal solution toward which the market evolves tends to be limited by these security constraints. The stakeholders therefore perceive them as constraining their activities and reducing European social welfare. A transparent definition and assessment of the distance to these security limits thus becomes of paramount importance.

To maintain the security of the supply in this context, TSOs must adapt the architecture of their transmission systems by considering the following technologies:

- ✔ long-distance HVac underground cables with large reactive compensators
- ✔ HVdc underground cables in parallel with the ac grid with smart controls of the ac/dc converters
- ✔ HVdc grids, first to connect offshore wind farms efficiently and then to provide cheaper interconnections between distant areas.

Meanwhile, TSOs will try to optimize the existing systems by adding more and more special devices such as the PSTs and SVCs mentioned above, along with advanced controls and protection schemes. While demand response could offer new ways to control the system, this flexibility will require a rethinking of current operating practices; TSOs will have to assume that part of the generation is an uncontrollable exogenous stochastic variable while part of the load is controllable.

The Need for New Methods and Tools

The previous section suggests that the complexity of transmission system management will continue to increase. In this context, defining security limits and measuring the distance between an operating point and the nearest security limit become more and more difficult. In this article, we present some ideas about new methods and tools that can reliably assess the security of the pan-European transmission network as its complexity increases.

The basic functional needs for these tools are:

- ✔ the ability to obtain or construct realistic pictures of the state of the system over different time frames (in real time, intraday, a day ahead, and so on)
- ✔ the ability to define reliability criteria and security limits
- ✔ the ability to assess the security of the system by running time domain simulations.

Probabilistic methods (e.g., Monte Carlo methods) could be applied to define these limits because they can deal with the complexity of a system that is nonlinear, nonconvex, and discontinuous. The fast algorithms that will build base cases and run time domain simulations could be at the core of these Monte Carlo methods.

As previously mentioned, the complexity of the system is increasing, and we want to have a more robust and accurate assessment of the security margins. Some of the approximations used in the standard methods and some of the tools used to assess security should therefore be reviewed. We have identified three main categories, which we discuss below.

Description of the Neighboring Systems

The operational tools used by each TSO rely on rather poor descriptions of the neighboring systems, in particular for the estimation of the state of the systems and of their security in real time. In the past, these descriptions were sufficiently accurate because the variability of the external systems was very low and because it was therefore possible to define time-invariant equivalent models that gave sufficiently accurate results when assessing security. Moreover, the system was operated most of the time with security margins that were large enough to ensure that some inaccuracies in the state estimation were of no consequence. But this is no longer the case: the optimization of the resources utilization produced by the liberalized electricity markets causes much larger power transfers over longer distances, and these interchanges make the national systems much more interdependent. Electric phenomena no longer stop at administrative borders.

Today, TSOs are trying to improve their state estimators by incorporating larger and larger parts of neighboring

In this article, we have proposed an overall approach to deal with the security management of electric power systems from two days ahead to real-time operation.

networks in their real-time IT systems, both for the supervisory control and data acquisition (SCADA) system and the energy management system (EMS). In the medium to long term, this approach is not very realistic. It is indeed nearly impossible, even with a large amount of manpower, to maintain a valid model of the neighboring systems because of all the maintenance and upgrade activities taking place in these systems. Certain alternative solutions that use the concept of a hierarchical state estimator should be more efficient and more robust.

Forecast States

For the day-ahead and intraday security assessments, TSOs must build base cases from which they can run "what if" analyses. The standard method for developing these base cases relies on forecasts of load and generation at each bus of the network. A power flow combined with a contingency analysis is then run on the basis of these forecast injections. Potential corrective actions are difficult to take into account with this approach, however. For example, the contingency analysis usually does not take into account the optimal redispatch of the generations after a contingency to suppress an overload. The forecast of generations is generally done using a very poor model based on a static merit order. With more and more active intraday electrical markets, producers maximize their profits by playing on the short-term market, making the schedules of power plants across Europe more difficult to predict a day in advance. Moreover, wind power injections are difficult to forecast accurately more than a few hours ahead. With massive integration of wind power in Europe, conventional generators have to be adjusted to balance the system. Each individual generation node thus becomes more volatile. We propose to discuss how to use advanced optimization methods to build realistic base cases, in particular using mixed-integer programming to deal with discrete variables such as the status of generating units. We will not only propose more accurate models for devices such as capacitor banks and on-load tap changers but also ones that take into account possible remedial actions such as topology changes.

Model Accuracy

In static security assessment, a power flow computation gives the stabilized postcontingency state, and the assessment of security is done on the basis of that state. The underlying assumption is that a stable trajectory exists between the initial state and the stabilized postcontingency state. This means that all dynamics are stable and can be neglected. In several countries, however, the dynamic behavior of the system can no longer be neglected. When operating the system close to its limits, unstable dynamic phenomena can appear after a contingency before the static overload problems that are more "easily" manageable using remedial actions. A robust security assessment should check that dynamic phenomena are acceptable. Moreover, when many dynamic devices with complex controllers (dead band, limiters, and so on) interact, it is nearly impossible to predict the stabilized postcontingency state without running a time domain simulation. The proposal is therefore to use time domain simulations to assess security and—if needed from a computational point of view—to use simplified time domain simulations rather than purely static approaches.

For detailed time domain simulations, the challenge is to find the right balance among different objectives for very large power systems. The first objective is *simulation fidelity*. The time domain simulation method must simulate accurately the system described by a set of differential algebraic equations. In particular, numerical integration methods that approximate unstable dynamics by stable ones are not acceptable.

The second objective is *computational speed*. The time domain simulation must run as quickly as possible. Some parallelism in numerical methods should be found in order to use the new multicore computers efficiently. Improving computational performance is a prerequisite for the following applications:

- ✔ using detailed time domain simulation for dynamic security assessment in real time
- ✔ making possible probabilistic approaches to the definition of the security limits.

The third objective is to offer *modeling flexibility*. As mentioned above, more and more special devices (such as PSTs, SVCs, and HVdc devices) are being installed in the European power system along with advanced controllers and protection schemes. The model for each piece of equipment can be very specific. The only possible approach, therefore, is to give users the capability to define these models themselves. A review of the modeling requirements will need to be done, and a method of exchanging detailed models in a standard framework will have to be prototyped.

These three objectives are clearly in conflict. Depending on the application, particular tradeoffs may have to be made.

The New Approach to TSO Decision Making

In power system operation, some actions must be decided in advance because the means to implement these actions must be reserved ahead of the actual operation. For instance, the time needed to start up a thermal power plant is often several hours. Likewise, planning for the maintenance of overhead lines and substations must usually be scheduled several days in advance so as to leave enough room to optimize the deployment of maintenance teams. Certain decisions must therefore be made from a few days to a few hours ahead of the moment when the corresponding actions are actually launched. In order to make these decisions, the TSO must analyze the security of the anticipated steady state of the system at the time when these actions must be implemented. To this end, the TSO takes into account uncertainties about exogenous factors (and their correlations) that may influence the future system state as well as all possible preventive and corrective actions that could be applied in the meantime in order to adapt the system state to these exogenous factors.

The problem formulation proposed to handle this issue is a generalization of the current practice of certain European TSOs, such as RTE in France and ELIA in Belgium. Because most of the preventive actions are costly and irreversible for the TSO (e.g., keeping must-run generators operating, generation rescheduling, activation of demand-side responses, postponing of maintenance, and so on), the basic rationale of the proposed formulation consists in postponing for as long as possible the moment a particular decision must be made so as to take advantage of all the information that can be collected in the meantime. The additional information will help reduce the level of uncertainty about the system state at the moment the action is applied. The decision-making process is no longer a two-step process (making day-ahead and then real-time decisions) but more and more a continuous, multistage process with a number of different time slots (i.e., intraday) available for deciding and/or applying different possible actions, depending on the market and on regulatory rules. The whole framework is actually applied "indefinitely," with a receding horizon of analysis corresponding to the longest delay of action implementation relevant for the TSO.

A Functional Architecture for the Proposed Approach

We propose the integration of these various computational engines and data management tools into a unified "toolbox" for performing static and dynamic security assessments of the European transmission network.

The security assessment requires a definition of reliability criteria. The proposed implementation clearly uses a probabilistic approach, the most demanding type from the computational and modeling points of view. We propose to use screening methods based on the integration of various computational engines to address this very complex problem.

We propose a risk-based approach that takes into account the probabilities of faults and of other events' influencing the possible states of the system, the estimation of the associated impacts of faults when applied to system states, and a catalog of possible corrective and preventive actions.

The Overall Toolbox Architecture

We propose to have a layer of data management tools to provide inputs to the computational toolbox (see Figure 1), including a pan-European state estimation and data-mining features. The toolbox itself is composed of four main parts:

- ✔ online security assessment
- ✔ off-line definition of security rules
- ✔ off-line validation of dynamic models
- ✔ off-line defense plan and restoration plan design and assessment.

Online Security Assessment

Our proposal is to develop a screening method based on a worst-case state (WCS) approach as suggested by the Pan-European Grid Advanced Simulation and State Estimation (PEGASE) project (www.fp7-pegase.eu). This approach relies on the construction and analysis of the worst states for each contingency. The main objective is to minimize the costly preventive actions by taking into account all possible corrective actions. The first stage is a static "conservative" security assessment based on security rules. For unacceptable cases, a less conservative simplified dynamic security assessment is performed. If corrective actions are not sufficient to ensure security, we must find the minimal preventive actions for this contingency. Then we have to find a common set of preventive actions for all the contingencies requiring preventive actions.

The online security assessment does not only address real-time security assessment. It is a sliding process that starts from two days ahead and ends in real time. On the one hand certain actions must be anticipated (e.g., the start-up of a thermal power plant), whereas on the other hand the level of uncertainty decreases as we approach the real-time context.

The period from two days ahead to real time will be divided into various time horizons. The exact splitting of this period will depend heavily on a precise definition of the "last time to decide" principle for every preventive action.

Real-Time Security Assessment

Our main assumption is that real-time security assessment is based on snapshots, and we don't take into account any uncertainties. Our approach is a rather classical one. It uses a conservative load flow that computes, for every contingency to be considered (low-probability contingencies may be forgotten at this stage and will be taken care of in the defense plan), the postcontingency state of the grid, taking into account all possible corrective actions. For each

In power system operation, some actions must be decided in advance because the means to implement these actions must be reserved ahead of the actual operation.

contingency where the conservative load flow doesn't find any solution—or if there are remaining constraints after the use of corrective actions or if corrective actions are not fast enough—a less conservative simplified dynamic simulation is performed to analyze whether or not the grid situation is secure. After this step, if the grid situation is deemed insecure, drastic actions (e.g., load shedding) may be needed.

An alternative to this first approach would be to skip the static security assessment and to rely only on a simplified dynamic security assessment. This approach is realistic if we have

- ✔ access to high-performance computing facilities, e.g., 10,000 cores (one for each contingency)
- ✔ a reliable and sufficiently simple dynamic model.

Forecasting-Mode Security Assessment

In the real-time security assessment just described, the actions of the operators are limited to corrective actions. Those actions may not be sufficient to ensure the security of the grid, and therefore drastic actions such as load shedding may be needed to avoid dramatic consequences like blackouts. TSOs are not limited to this online security assessment, however. They can also rely on forecast security assessments, so as to take advantage of possible preventive actions to ensure the security of the grid.

After predicting what the uncertainties that could affect the system are, the TSO may seek answers to the following questions:

- ✔ What is the WCS for each postulated contingency?
- ✔ Are postcontingency corrective actions sufficient to satisfy the postcontingency operational limits in the WCS?
- ✔ If not, what are the optimal preventive actions, taking into account the corrective actions available to deal with contingencies in the WCS?

For one time horizon, the whole process can be schematized as shown in Figure 2.

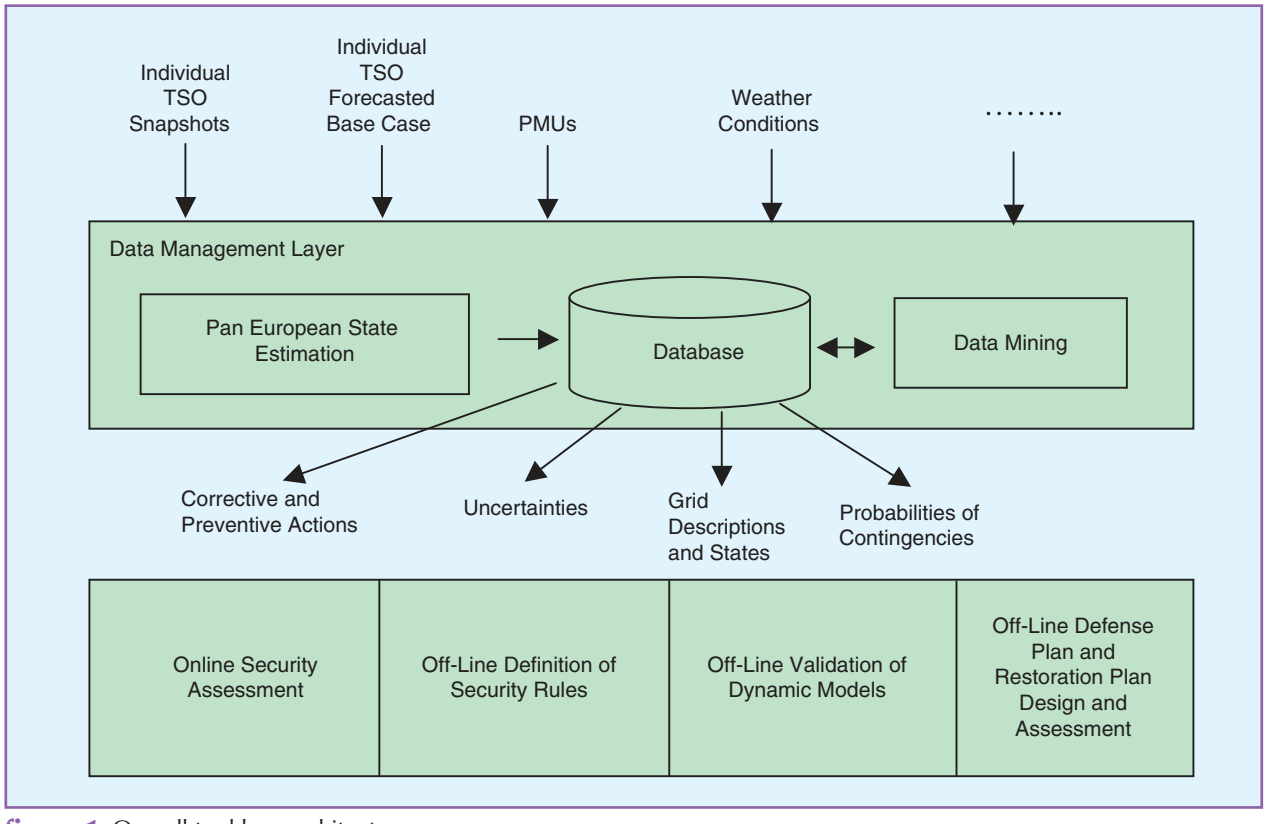

figure 1. Overall tool box architecture.

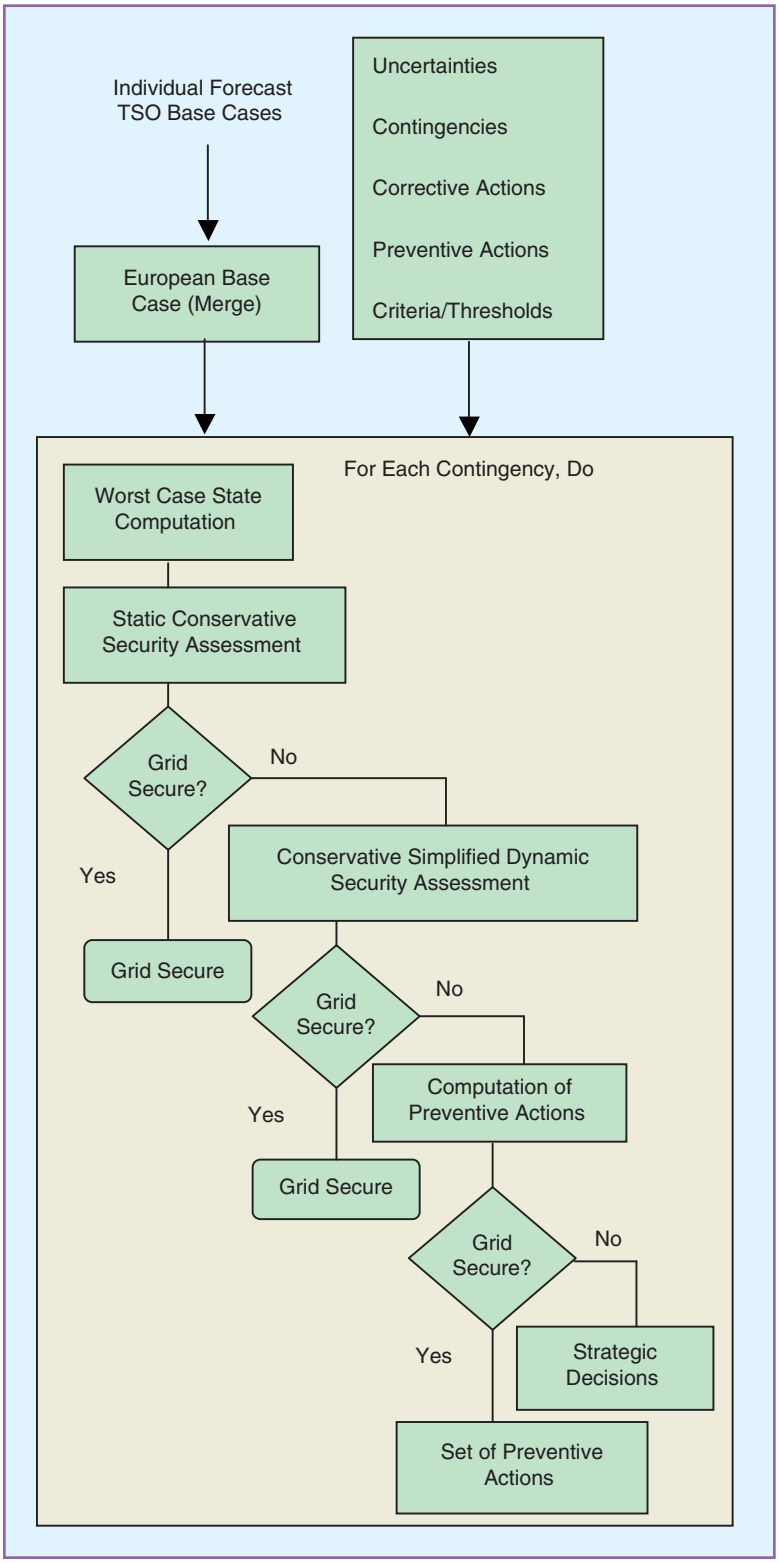

figure 2. Security assessment process.

Off-Line Definition of Security Criteria and Thresholds

The online security assessment described above will require inputs such as the probability of occurrence of a fault, the definition of complex uncertainties, and simplified conservative criteria and thresholds that can be assessed using static or dynamic computation. The efficiency of the online security assessment will clearly depend on the accuracy of these inputs. We propose the use of enhanced Monte Carlo techniques such as importance sampling to make extensive use of the data sets archived in our system. The archived grid data will be patched in order to represent all the uncertainties (load patterns, generation patterns, and so on) and all the contingencies. We will then use optimal power flow computations in order to construct the resulting anticipated states of the grid. All these grid situations will be assessed using high-fidelity time domain simulations. The results of these simulations will then be processed using machine-learning algorithms (for example, decision tree–based methods) so as to obtain simple static conservative criteria and thresholds (e.g., bounds on the generation balance in a zone) sufficient to ensure reliable operation of the grid. These rules will be given to the optimization engines of the online security assessment tools as constraints of the optimization problem they are intended to solve. It is an elegant pragmatic means of taking into account dynamic security in extended static security assessment. This procedure represents a generalization of ideas proposed in the past by Dy-Liacco (1997) and Wehenkel et al. (1994) and developed in the European Seventh Framework Program (FP7) Twenties project as the Netflex work package for interarea oscillations, in which the objective is to derive security rules for operators through PMU measurements.

Validation of Dynamic Models

Dynamic models are tremendously complex and their validation can be a very intensive task requiring a very high level of expertise. Nevertheless, the secure operation of the grid depends heavily on the accuracy of the dynamic models used. These models therefore need to be reassessed on a regular basis. We propose to provide tools to help operators evaluate the models. Based on accurate PMU records of the significant events on the grid (e.g., loss of a significant power plant), these new tools will identify the inaccuracies of the models and point out to operators the parameters responsible for these discrepancies. They will

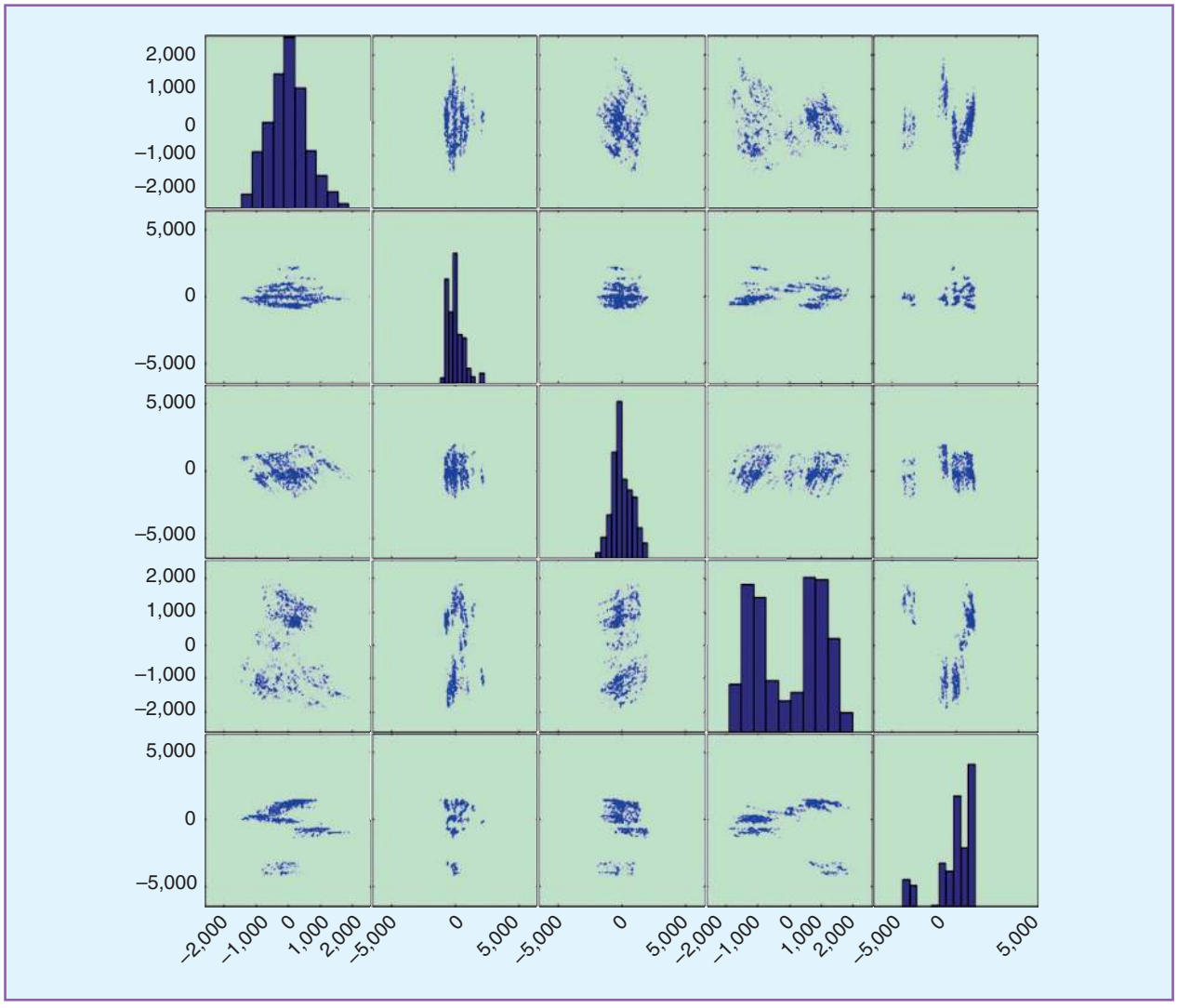

figure 3. Scatter plots for actual data.

provide distance indicators that will highlight discrepancies between the results of the simulation and the measurements.

Data Management

All the main functions described above rely on the availability of

- ✔ detailed and accurate grid descriptions and states
- ✔ precise definitions and levels for the uncertainties that need to be taken into account
- ✔ accurate probabilities of the contingencies taken into account
- ✔ a catalog of possible corrective and preventive actions associated with a constraint or contingency.

The grid descriptions will come from pan-European state estimation for real-time snapshots and from the optimal merging of individual TSO forecast base cases from two days ahead to one hour ahead. The PEGASE project has already demonstrated the feasibility of a hierarchical state estimator and identified the possible advantages of using PMU data to improve the pan-European estimated state.

Online security assessment depends heavily on the definition and the levels of uncertainties that our system will have to face. One challenge is to build realistic forecast states of the grid that capture the uncertainties associated with individual and collective forecast errors of loads and generations. Building up accurate and realistic probability density functions using the huge database available from the TSOs and efficiently sampling from them could enable robust and—hopefully—useful Monte Carlo approaches for power system reliability assessment. Standard methods exist to address such issues, but they can't handle problems of such a large size; the power grids consist of tens of thousands of nodes. To address this, we have developed a pragmatic approach. It consists of an initial dimension reduction stage using principal and independent component analysis (PCA and ICA) and classification techniques. These were obviously suggested by the existing

The increasing level of uncertainties due to intermittent generation leads to reconsider the decision making process on most-likely future states to a more probabilistic approach.

links among electrical nodes (wind generation in a given area, urban load similarities, and so on) that highlight the valuable generation and load patterns. We then use multivariable probability density function estimation on the reduced space, first trying a conventional kernel method and quickly adopting a copulas and pair-copulas decomposition approach for their analytical properties and their associated efficient sampling techniques. We have performed visual appreciation of the estimation methods through comparative scatter plots of initial and generated samples, first using simulated data (a mix of Gaussians and others) and then data from the French SCADA system for the 2010–2011 winter (compare Figures 3 and 4 for an idea of the differences between the initial data and the generated data from the French system for the 2010–2011 winter).

We have also tried to test a quantitative measure to test the goodness of fit of our samples based on an attempt to generalize to a higher dimension the classical Kolmogorov-Smirnov test (in dimension 1). After several attempts, we found that the additional computational burden introduced by ICA is not compensated for by sufficient gains in the quality of the estimation. The conclusions of these tests made us choose an algorithm (labeled "Algorithm #3" in Figure 5) that uses first a PCA and then an estimation of parameters based on pair-copulas for every class identified, along with efficient sampling associated with these pair-copulas.

The probabilities of each contingency are also important inputs of the proposed risk-based approach. For example, events whose probability is too low will be disregarded,

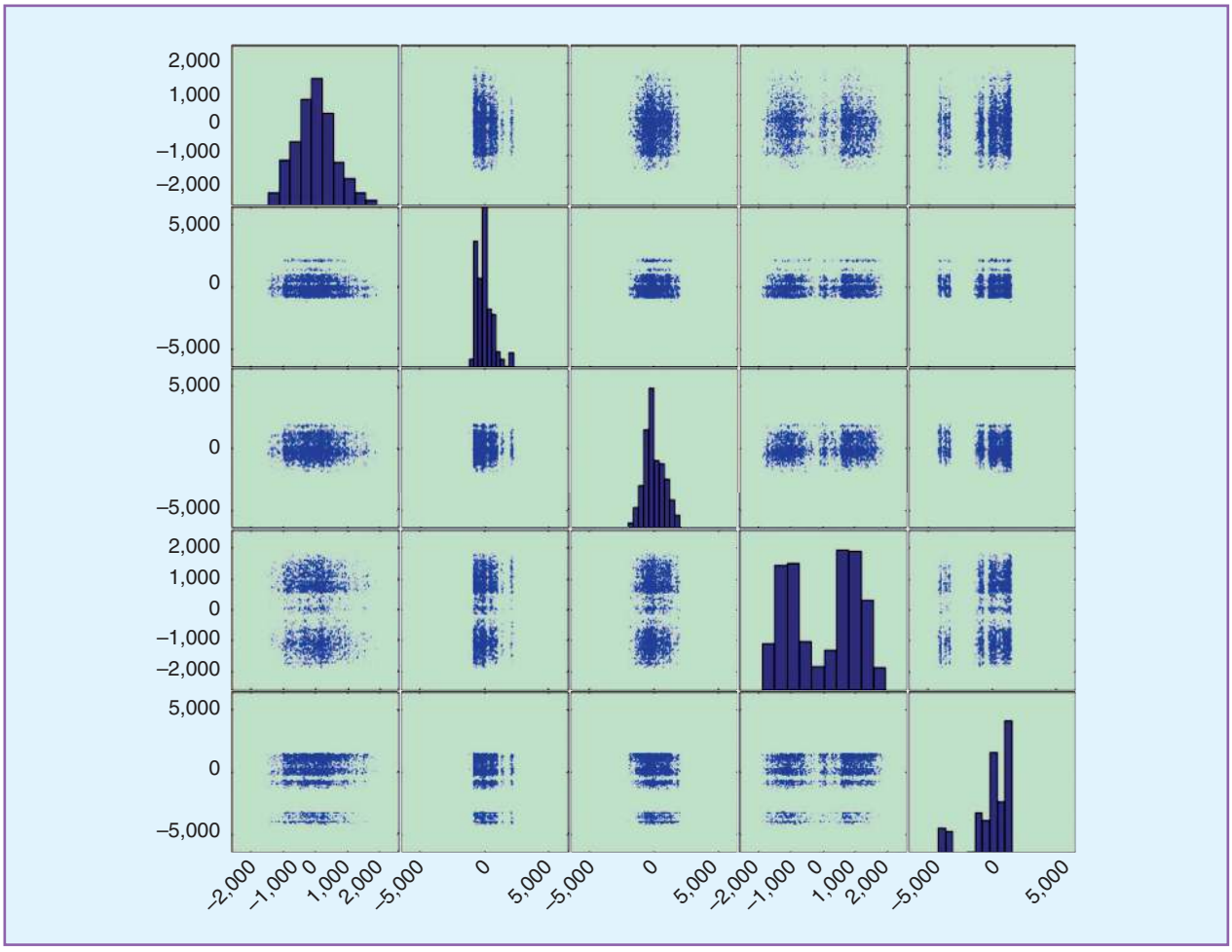

figure 4. Scatter plots: generated data.

Our proposal is to move in this direction, implementing realistic solutions through screening methods based on a worst-case state approach and data mining techniques.

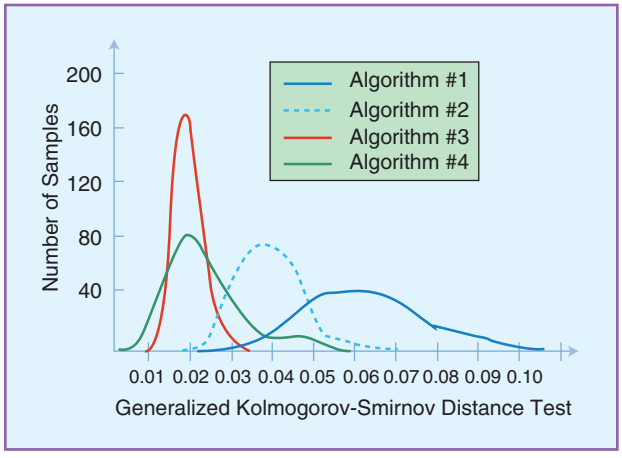

figure 5. Fitting indices.

on the assumption that even in the case of a high impact, defense plans are in place to minimize the most dramatic consequences. Our goal is to use relevant probabilities that take into account several phenomena and their possible correlations (e.g., weather conditions, technology, age of components, and so on).

TSO operators have at their disposal a catalog of possible corrective and preventive actions to relieve constraints. These remedial actions should be shared at the European level to optimize their use and assess their pan-European efficiency. We think that the definition of a framework to exchange this information is required, perhaps in the form of a Common Information Model (CIM) extension. As the probability of failure of remedial actions could become an important factor in the assessment of the risk, some estimated value of these probabilities is also required.

Defense and Restoration Plan Design and Assessment

As mentioned above, certain low-probability contingencies will be discarded from our proposed online security assessment, under the assumption that even in cases of high impact, defense plans are in place to prevent excessively dramatic consequences. The restoration process after a blackout is a complex problem, and the dynamic behavior of the system is a critical factor for the success of the restoration process. The process becomes very complex indeed when a blackout affects areas controlled by more than one TSO. We are proposing tools that will help to design and assess pan-European defense and restoration plans. One of our main ideas is that defense and restoration plans are rather difficult to design and assess; we will therefore try to avoid overly complex designs that may prove to be insufficiently reliable.

Conclusions

In this article, we have proposed an overall approach to deal with the security management of electric power systems from two days ahead to real-time operation. We have described all the basic functional needs for this new approach and proposed innovative yet pragmatic ways to implement them. We believe that this new approach will permit a systematic security assessment of the grid from operational planning to real time. Substantial work remains on the actual implementations of the four identified blocks, but this article may pave the way for the work that still needs to be done.

Acknowledgments

This article presents ideas developed in the European FP7 projects PEGASE and Innovative Tools for Electrical System Security Within Large Areas (iTESLA). Scientific responsibility rests with the authors.

For Further Reading

T. E. Dy-Liacco, "Enhancing power system security control," *IEEE Computer Applications in Power*, vol. 10, no. 3, pp. 38–41, July 1997.

L. Wehenkel, M. Pavella, E. Euxibie, and B. Heilbronn, "Decision tree based transient stability method a case study," *IEEE Trans. on Power Syst.*, vol. 9, no. 1, pp. 459–469, Feb. 1994.

P. Panciatici, Y. Hassaine, S. Fliscounakis, L. Platbrood, M. A. Ortega-Vasquez, J. L. Martinez-Ramos, and L. Wehenkel, "Security management under uncertainty: From day-ahead planning to intraday operation," in *Bulk Power System Dynamics and Control (IREP)—VIII, 2010 IREP Symp.*, Rio de Janeiro, Brazil, 1-6 Aug. 2010, pp. 1–8.

F. C. Schweppe, "Power systems '2000': Hierarchical control strategies," *IEEE Spectrum*, vol. 15, no. 7, pp. 42–47, July 1978.

Biographies

Patrick Panciatici is with RTE (French TSO), Versailles, France.

Gabriel Bareux is in with RTE (French TSO), Versailles, France.

Louis Wehenkel is with the University of Liège, Belgium.