



PS2 – S8-02



Dynamic Network Security Assessment – Ranking of System Contingencies

Edwin LERCH, Chris O. HEYDE, Rainer KREBS, Olaf RUHLE
Siemens AG
Germany
edwin.lerch@siemens.com

KEYWORDS

System performance, dynamic security, visualization, performance indices.

ABSTRACT

The growth and loading of today's power system needs more elaborated tools to monitor the system security in order to find countermeasures in case of system insecurity and instability. Studying system security refers to analysis of system voltage, transient and small signal stability. The paper will combine a set of indexes for the overall system behavior ranking small system behavior, transient stability, voltage behavior and system performance using a fuzzy logic to monitor the system state. Indexes for monitoring the system loading of each node and approximation of collapse power is introduced, too. The indexes allow the definition of absolute nodal loading and nodal voltage state. With these indexes the actual situation, increase in loading and nodal voltage state over a time-period to show the trend of the system behavior can be analyzed and monitored in a suitable way.

1 INTRODUCTION

Over past decades many techniques and tools capable of fast (real time) analysis of power systems have been developed. However, despite the intensive research, the large majority of them have hardly moved from the research laboratories to the industrial world and, as a matter of fact, the very large majority of today's control centers does not make any use of any real-time stability software [1]. Still, the increasing number of incidents that led to large system failures or even blackouts has forced some power system operators to reconsider the established strategies for determining the security limits of their systems and to look for techniques and tools that would help them in identifying the actual limits of a system during its operations.

Without doubt, these goals imply intense computational and study effort. In computations, aspects of security relating to different stability forms need to be considered: voltage, frequency, small signal and transient stability are the ones most commonly referred to. By addressing these aspects over-all system performance can be determined; by knowing the over-all system performance, the operator can develop a feel about the severity of a condition, and estimate the magnitude of remedial actions required for its improvement. Collecting information on the system security can be, however, a time consuming process, since it involves individual consideration of the security aspects. In exceptional cases, e.g. under severe time restrictions, it would be therefore welcome to have a sort of support methodology facilitating the process.

At the present time there is no widely accepted methodology to handle this issue. There are many techniques tailored to the physical phenomena under evaluation, but only few shell frameworks exist for combining the evaluation results into an over-all security indicator. In this paper, a security assessment concept is discussed addressing this subject. The concept has been successfully

incorporated into well established simulation domain and by proper visualization it delivers a promising solution for fast dynamic security investigations.

2 TYPICAL REQUIREMENTS

The main components of a security assessment framework are shown in Fig. 1. The security assessment system takes measurements of the actual system condition and performs security analysis in (near) real-time and passes information to the operator or directly on to control systems. The fundamental role of each component is described in detail in [2].

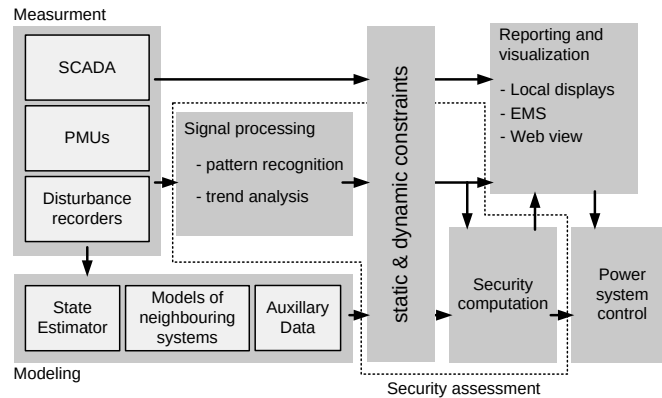


Fig. 1: The components of an online security assessment system

Here, the framework is considered from the perspective of the security assessment process only. Of concern are the typical requirements that have to be taken into account when implementing such process into an existing environment, defined by data sources, such as the system state estimator, PMUs and SCADA system, on one side, and system control assets on the other. In particular, the common requirements put forward by the operators Australian National Electricity Market Management Company (NEMMCO), Long Island Power Authority (LIPA), Independent System Operator in Bosnia and Herzegovina (NOS-BiH), and Office National de l'Electricité Morocco (ONE), which are outlined in [3]-[5] respectively are given a special attention. The following is their summary.

2.1 Computational Technique

As in case of NEMMCO [3], the operators are rather conservative when choosing the computational techniques and tools for security calculations. They preferably adhere to the well established solutions, in particular to the ones with which they are familiar with and are widely accepted amongst other operators and the associated industry.

The technique providing a level of confidence is conventional time domain simulation. It is one of the main tools in network planning and system operation research. It is accurate and has a superb modeling capability. The system trajectories are calculated by integrating the system differential equations step by step, and solving of the system feasibility and stability problem is possible. Moreover, it is also compatible with other computational domains. For example, hybrid time-domain direct methods are used to combine the functionalities of both, time-domain and direct methods, and further, to extend them. And last but not least, the cost of computers and technology for easy parallel computations, made it also more or less straightforward to carry out time domain simulations in real-time, even for large-scale networks.

2.2 Security Aspects, Constraints, and Analysis

The system operators have the responsibility for the secure system operation under the provisions of grid code rules; the rules are subject to equality (power flow) and inequality (limits on the variables) constraints, restraining system quantities in a steady state, or following a disturbance or contingency. In security analyses, $N-1$, voltage, transient, small signal, and frequency security are commonly evaluated regarding these constraints. The calculations are carried out off-line and/or online, whereas the derived limits are applied in the dispatch solution to ensure secure power system operation.

N-1 security is concerned with the amount of power flowing through system branches. It gives the limits for the MW flows on the branches with respect to their thermal rating and the system required transmission reserve, for ensuring continuity of supply in case of line or corridor outages. Constraints to limit post-contingency branch flows are normally formulated off-line, by performing load flow calculation. Online, they can be recalculated and applied in the market dispatch engine, so the appropriate limits are enforced on the actual branch flows.

Voltage security refers to voltage stability and is concerned with the ability of a power system to maintain steady state voltages at all buses in the system under normal operating conditions, and after being subjected to a disturbance. Within the voltage security considerations steady-state and transient security limits are commonly formulated. The former give the permissible band for voltage deviation in the normal operation, while the latter give the ride through requirements in case of faults. Both types of limits are normally developed off-line. Online, they are being used for voltage restraining.

Transient security refers to solving the transient stability problem of a power system. The problem is concerned with synchronous operation of the system generators; if following a fault the generator rotor angles advance beyond a certain limit the synchronism is lost and instability occurs. To determine the transient security of a power system, operators are dependent on model validation of their systems and computations. Since direct methods are still treated with suspicion, largely because of the importance of control system limit action and other non-linearities in calculations, predominantly time domain simulations are used for the purpose. The main aim of the transient security studies is to determine the fault critical clearing time and the margin to instability.

Small signal security is concerned with whether there is sufficient damping in a power system for oscillations triggered by a disturbance to die away; if the damping is poor the system may experience system-wide security problem. To aid management of these problems online, tools for damping estimation in real-time are being increasingly adopted by the operators. These tools have the feature of estimating the damping instantly. When a sufficiently low degree is detected, security constraints are being enabled in the dispatch engine to limit power transfers across problematic interfaces. To produce the security constraints the operators are reliant on off-line studies.

Frequency security is concerned with whether there is sufficient rotating reserve in a power system to maintain the system frequency within the frequency standards in case of imbalances between the system generation and load. To keep it stable, the operators use ancillary services of different characteristics and qualities: primary and secondary frequency control, load shedding etc. The application of these services is subject to the grid code rules. The limits implying their activation are developed off-line and with respect to admissible frequency deviations that the grid users can withstand without suffering any consequences. Typically, frequency gradient, maximum drop and post-contingency steady-state deviation are addressed within the scope of the security analysis.

2.3 Credible Contingencies

In general, the state of a power system is determined based on its ability to perform its intended function under different contingency levels. A reliable way of judging the impact of contingencies on the system operation is to perform the contingency analysis. Current practice to perform the analysis is in two phases: contingency screening and contingency evaluation (ranking). The contingency screening phase is usually performed off-line and with the objective to screen a number of possible contingencies down to the most credible ones; it gives the list of potentially severe cases that are most probable to occur and are expected to cause security violations. In the contingency evaluation phase, full analysis of these credible contingencies is performed.

In the system operation, the analysis of the credible contingencies assists operators to control the system at a secure operating point. They are examined online on a periodic basis or after a change in the operation; day ahead runs are also common. The final list of contingencies to be checked is subject to the system condition in a state and operator's experience. Typically, the ones to be examined are defined as the loss of a single item or plant due to phase to earth faults or other adverse situations.

2.4 Performance requirements

Online security assessment aims at determining the state of a power system as it operates. The credible contingencies are evaluated after system changes, periodically, or on demand. The time

settings used by the operators [3]-[5] are as follows: contingency and short circuit analysis are performed every 5 minutes, transient stability calculation every 2 to 3 minutes, $N-1$ security is examined on a 5 minute cycle, and every time after a valid state estimation becomes available voltage security is calculated.

2.5 Incorporation into system control

The security assessment can be integrated into the control environment in many ways. Normally, it is added to the existing SCADA/EMS architecture in form of modules that are compatible with other integrated subsystems. A loose solution, which has also been adopted by ONE Morocco, is illustrated in Fig. 2. The solution requires minimum structure adjustments and allows for incorporation of any number of sub-processes. For instance, the SINAUT Spectrum SCADA/EMS system installed at ONE control center did not contain a module for transient stability assessment (TSA). This missing functionality was recently added to the existing configuration via installation of a PC based workstation running the TSA on basis of a data snapshot from the system state estimator. Obviously, the same concept can be used when incorporating multi-processor computing strategies.

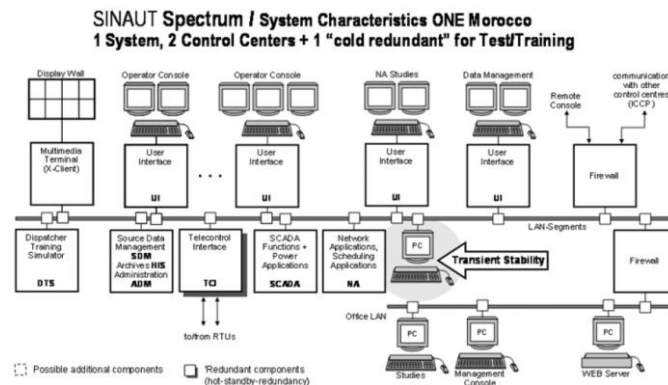


Fig. 2: Conceptual system configuration of ONE National Control Center (reproduced from [5])

2.6 Power System Security Visualization

In visualizing power system security it is important to report on key issues. This implies use of various visualization techniques, which can be arranged into two general classes: common techniques, such as for visualization in two dimensional diagrams and charts of any kind, and advanced techniques, such as for two- or three-dimensional animated representations.

Good visualizations improve the efficiency of operator response to power system problems. They are helpful in focusing attention on particular elements or problematic areas, and for displaying bus voltage magnitude information and transmission line/ transformer flow information. The desirable functionalities of the visualizations include showing the overall system security status, showing the severity levels of the contingencies in terms of their associated limit violations, and showing the geographic connection between the violated elements and the contingent elements.

The operators are aware of the fact that the sophisticated visualization can play a crucial role in reducing the risk of future blackouts. Clear and meaningful graphical representation of the system status can help them to quickly assess a potentially rapidly changing system state and to formulate corrective control actions.

3 DYNAMIC SECURITY

To deal with some of the requirements given in the previous section and to establish a sort of synergy between academic ideas and 'real world' challenges, a dynamic security inference solution has been established, relaying completely on conventional time domain simulation. The aim of the inference process is to collect the information on the system behavior and to deliver its overall performance by means of an over-all security indicator.

Evaluation of dynamic security of a power system refers to analyzing system dynamic behavior under a set of credible disturbances (contingencies) for a range of feasible operating conditions.

Obviously, system security can be evaluated regarding different criteria: system physical limits, operating constraints, custom criteria etc; but in practical terms, it is reasonable to make the

assessment regarding grid code rules and absolute stability limits; by using this approach a general impression of the system's performance under different contingency levels is easily established.

By considering the grid code rules and absolute stability limits from slightly different perspective one can see that for the assessment, besides the deterministic approach in its conventional fashion, also the one involving estimation of relation between the actual and limiting values of the system quantities (variables) is possible; the conventional deterministic approach delivers if system limits are violated or not which can be represented by logical statements 0 or 1, while the one based on a relative formulation gives a relative distance to the limits by ranging from 0 to 1, where 0 denotes full compliance with the limits, 1 denotes a violation, and the values in between deliver performance variation.

The derived relations are further in the paper referred to as performance indices; since their algorithmic and theoretical definition is given in full extent in references [6]-[8] reproducing them within the scope of this paper is intentionally omitted; but the readers are strongly encouraged to consider the references in order to fully comprehend the background of herein discussed approach.

The indices have been successfully incorporated into PSS[®]NETOMAC, which is a well established time domain simulator. Three independent calculation runs are required for their calculation. In the first run, the energy margin index is derived (see [6]). It is calculated by inserting three phase fault of a specific duration into the network and delivers the transient energy the system is still able to absorb without going unstable. The second simulation run delivers the small signal stability index (see [7]). The index quantifies susceptibility of the post-fault network to perturbations and reports if damping of low frequency oscillations initiated by the perturbations is insufficient. In the third simulation run, dynamic performance of the system in its transition from pre-fault to post-fault network condition is quantified. The quantification is made by calculating analytical expressions proposed in [8]. Quantified are voltage, frequency and generator dynamics, and post-fault steady state magnitude of some network quantities.

The simplified computational strategy is illustrated in Fig. 3. It is designed for a single processor execution. In addition to simulation algorithm, the other main components are contingency builder, which allows for building of contingencies and scenarios, the security inference system, and graphical output for providing the results. Obviously, the algorithm runs in a sequence, calculating study cases one after another.

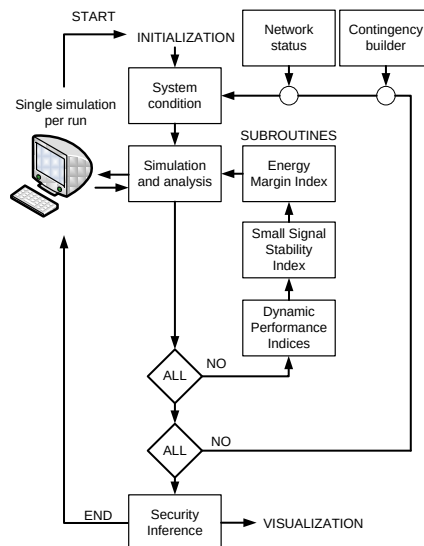


Fig. 3: Computational strategy

3.1 Dynamic security inference system

Evaluation of various security aspects by a number of performance indices yields an amount of data requiring further processing if an over-all index is to be delivered. There are many approaches for combining the indices into a single one, but none of them seems to be more adequate than the one based on fuzzy logic. By fuzzification and defuzzification of the indices equally distributed along the interval 0 to 1, a multi-stage Fuzzy Inference System (FIS) sufficiently composes an over-all dynamic performance index. An example of the inference algorithm is well described in [8], whereas in our

work, instead of three-level membership functions, five-level fuzzy membership functions are used (Fig. 4). The structure of the three stage FIS employed is illustrated in Fig. 5 and delivers Fuzzy Dynamic Security Index (FDSI).

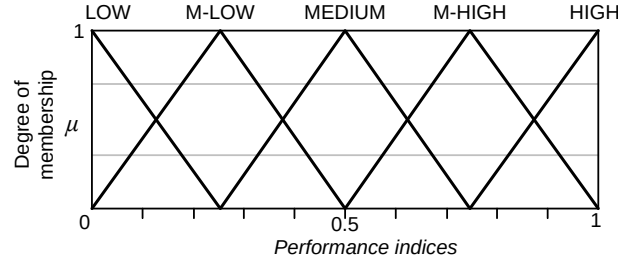


Fig. 4: Membership function for fuzzification and defuzzification of the performance indices

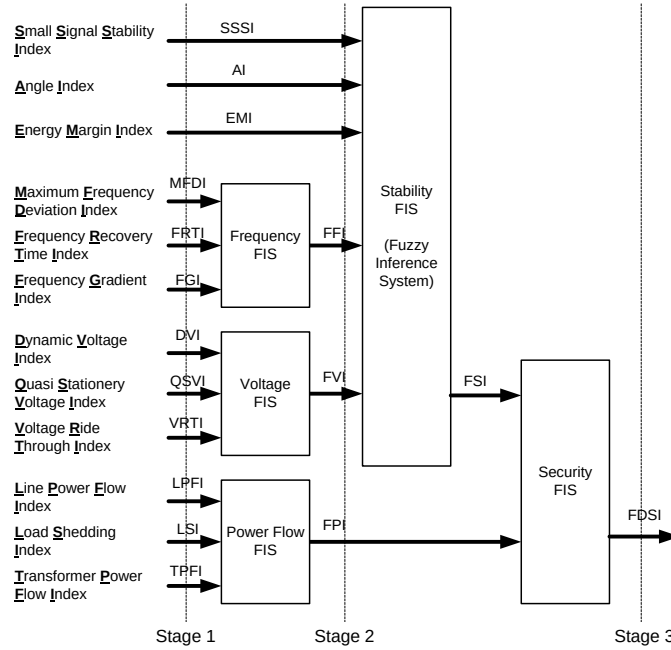


Fig. 5: Three stage fuzzy inference system

3.2 Visualization

For controlling the capabilities of the constructed computational algorithm a graphical interface is required. The screenshots of a conceptual solution are shown in Fig. 7 to 10. The main relations among user interface windows are depicted in Fig. 6. Note that the interface is still under development, so some routines are not discussed here. The main window (Fig. 7) is divided into two sides. On the left side, panels for visualization of system trajectories are located. The trajectories can be acquired in real time or from recordings. The idea behind is to select a point on a trajectory (with time reference) and tune the system model accordingly until the chosen condition is reproduced. Then time domain simulation is used to evaluate if in this condition the system can withstand a set of contingencies.

Typical and custom contingencies are easily built by using functionalities of contingency builder (Fig. 8). The contingency builder automatically reads input data and establishes lists of network elements, sorted by name and type, which can be involved in system manipulations. To facilitate the process, in addition, the network topology is visualized.

Through “index selection” window selection of indices to be calculated is possible. An index is activated by checking an associated checkbox. The index selection directly affects the computational strategy: removing the indices from the list speeds up the computations, whereas activating them poses an additional computational burden. Moreover, each selection implies re-adjustment of the fuzzy inference system. Fuzzy rules have to be re-established, so accurate calculation of over-all index is ensured.

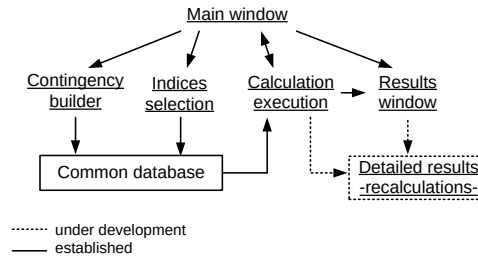


Fig. 6: System structure

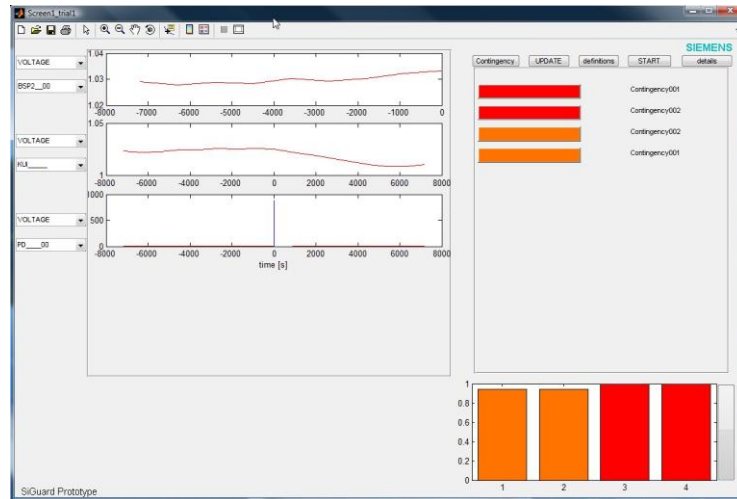


Fig. 7: User interface –main window

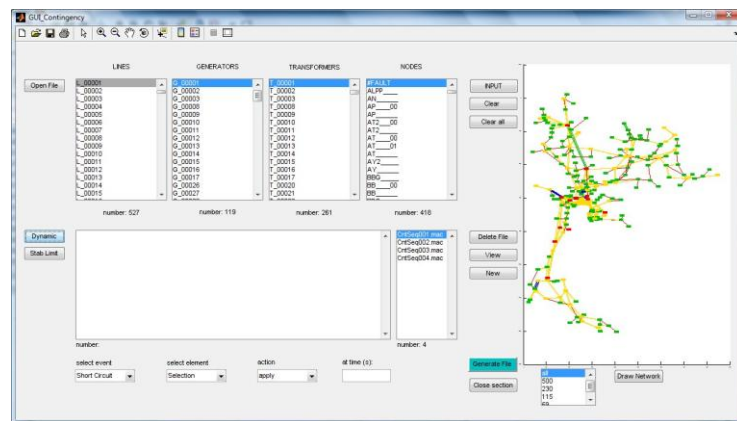


Fig. 8: User interface - contingency builder

On the right side of the main window, a notification display is implemented. The display is in a matrix format of $n \times 1$ in size, where n is the number of matrix lines corresponding to the number of contingencies; or in other words, each cell refers to a contingency. The matrix is for communicating the over-all performance index (FDSI) by means of indicative colors. Although any colour scale is adequate for the purpose, the most obvious is to use green and red for denoting the absolute secure and insecure system condition and a colour-mix in between for security variation. With a single view of the display, one can immediately get an impression of the system performance under different contingencies. The cases needing further attention are clearly indicated and can be dealt with further by going into investigation details.

Closer look is possible via the “results window” (Fig. 10). Similar as the main window, this one is also fictively divided. On the left side, diagram panels are located enabling visualization of simulation results, one can select among trajectories of different network quantities, whereas on the right side, again, a visualization matrix is placed, however this time of $n \times 6$ in size. Note that both visualization matrices, one in the main window and one in the results window, are associated with

third and second stage of the FIS respectively (see Fig. 5). Number of lines n is contingency related, while cells in a line refer to 6 security aspects: small signal stability, transient stability, generator dynamics, frequency behavior, voltage deviation, and power fluctuations. Once again the color scheme is used to communicate insufficient performance. Security aspects colored red require further consideration.

Going even further into details is possible by activating “detailed results window”. This window is associated with stage 1 of the FIS and delivers the performance indices in their original fashion. Critical network elements are clearly indicated and can be easily identified; for example, if voltage performance is poor, nodes with insufficient voltage are outlined.

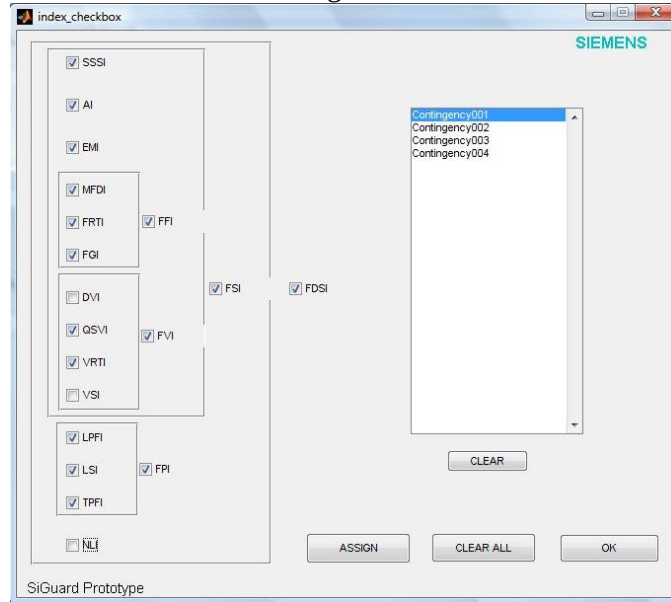


Fig. 9: User interface – indices selection

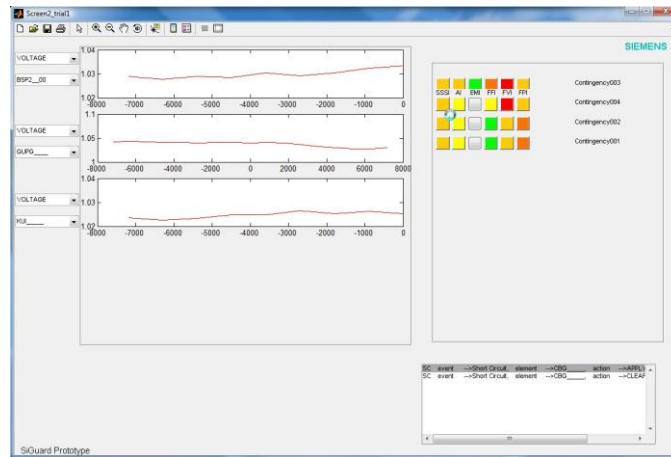


Fig. 10: User interface – results window

4 STUDY CASE

A model of a large power system is used to test the performance of the computational strategy. The main characteristics of the model are: 500-, 230-, 115 kV and lower voltage levels, 259 transformers, 119 generators, and 515 transmission lines. The main 500- and 230 kV transmission network is shown in Fig. 11.

Evaluated is a set of 4 contingencies: spontaneous 500kV line outage (A), spontaneous generator outage (B), a self clearing three phase fault (C), and a three phase fault followed by a tripping of parallel 500kV lines (D). Contingencies A, B and D are evaluated for small signal stability and dynamic performance, whereas case C is evaluated for all of the security aspects. The visualization of results via the graphical interface is given in section III (see Fig. 7 to Fig. 10). Case A

is ranked as conditionally secure (last position in the visualization matrix); however, it can be easily escalated to an insecure case. If following the outage the remaining line is tripped, the system breaks into two areas and loses its stability. The conditions are shown in Fig. 12 and Fig. 13.

4.1 CPU Performance

The total execution time consists of two times: calculation time and time required for post-computation data processing, such as data reading, fuzzy inference, writing of results files etc. The average time for small signal stability calculation is 6.69 second per case, for transient stability calculation is 9.52 seconds per case, and for dynamic performance calculation is 13.52 seconds per case. The post-calculation processing takes about 5 to 6 seconds per case. In average, the total execution time for calculating of all aspects of security is 35 seconds per case. Clearly such performance is in line with typical requirements outlined in section II and is thus considered sufficient.

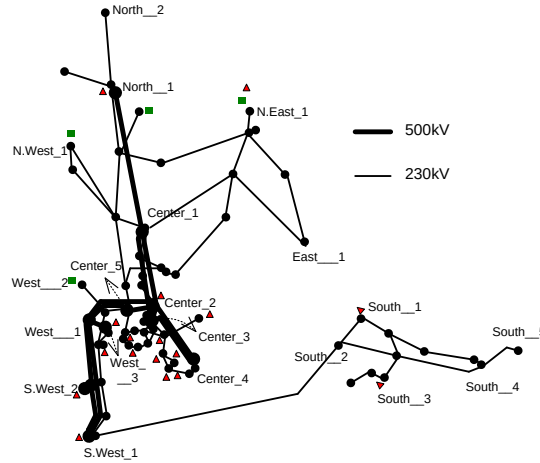


Fig. 11: 500- and 230 kV networks of the test system

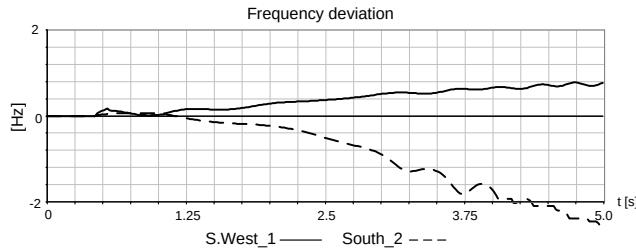


Fig. 12: Frequency deviation following a corridor outage

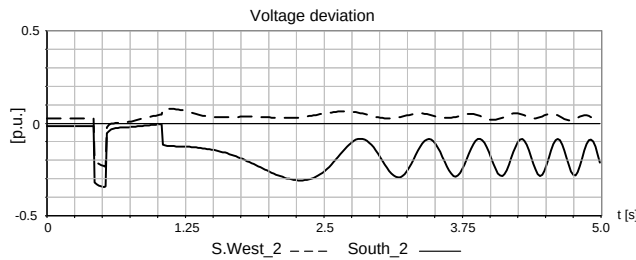


Fig. 13: Voltage deviation following a corridor outage

5 CONCLUSION

In this paper a conceptual solution is presented enabling fast dynamic security inference of power systems. The solution is based on application of system performance indices and meaningful visualization. By using the graphical interface a user can define contingencies and scenarios, and activate/ deactivate computational strategies for evaluation of different security aspects. As shown by the study case the investigation results are delivered in a sufficient time, so besides off-line applications, there is also a potential for on-line employments.

REFERENCES

- [1] D. Ernst, L. Wehenkel, M. Pavella, “What is the likely future of real-time transient stability”, in *Proce. of IEEE Power Systems Conference & Exposition*, 15-18 March, Seattle, 2009
- [2] K. Morison, L. Wang, P. Kundur, “Power System Security Assessment”, IEEE power & energy magazine, September/ October 2004
- [3] S. Boroczky, E. Gentle, “Real-Time Transient Security Assessment in Australia at NEMMCO”, in *Proce. of IEEE Power Systems Conference & Exposition*, 15-18 March, Seattle, 2009
- [4] L.E. Arnold, J. Hajagos, ”LIPA Implementation of Real-Time Stability Monitoring in a CIM Compliant Environment“, in *Proce. of Power Systems Conference & Exposition*, 15-18 March, Seattle, 2009
- [5] E. Lerch, O. Ruhle, D. Vickovic, “Real-Time Stability Assessment in the Control Centers of the ISO of Bosnia and Herzegovina and a National Dispatching System in North Africa”, in *Proce. of Power Systems Conference & Exposition*, 15-18 March, Seattle, 2009
- [6] C.K. Tang, C.E. Graham, M. El-Kady, R.T.H. Alden, “Transient Stability Index from Conventional Time domain Simulation”, IEEE Transactions on Power Systems, Vol. 9, No. 3, August 1994
- [7] U. Kerin, E. Lerch, G. Bizjak, “Small Signal Security Quantification of Highly Loaded Power Systems”, in *Proce. of IEEE Power Systems General meeting*, 26 – 30 July, Calgary, 2009
- [8] J.M. Gimenez and P.E. Mercado, "A new approach for power system online DSA using distributed processing and fuzzy logic", *Electric Power System Research* 77 (2007), pp. 106 – 118
- [9] L. A. Zadeh, “Fuzzy sets. Information and Control”, 8:338–353, 1965