Scientific
Research

Online Stability Assessment in Control Room Environment

R. Krebs[1], C. Heyde[1], X.-P. Liang[2]

[1]Siemens AG, Erlangen, Germany
[2]Siemens Ltd., Shanghai, China
Email: rainer.krebs@siemens.com, renate.butterhof@siemens.com

Abstract

Power transmission systems are being operated closer to their stability limits compared to twenty years ago. As a result, an increasing risk of blackouts combined with extremely high costs economically and socially is observed. To reduce this risk the personnel in the control rooms of the transmission system operators have to be assisted by a system, which assesses the dynamic state of security online. The system presented in this paper is designed to investigate the security with regards to voltage stability, transient stability and small signal oscillatory stability. New technologies of visualizing the degree of stability to non dynamic stability experts are used as well as integration in existing SCADA/EMS systems are realized. The performance of the system is sufficiently high to be employed in the online environment of the control room.

1. Introduction

The increase of the consumption of electric energy during the last decades led to an extension and a spatial expansion of synchronous operated AC systems as well as higher voltage levels. In Europe, technical and economical advantages of combined operation caused the interconnection of adjoining networks. So, the synchronous operated combined network of UCTE with an installed generation capacity of currently more than 860GW was created. Today, as an organization, the UCTE is integrated in ENTSO-E (European Network of Transmission System Operators for Electricity) (www.entsoe.eu).

The development in the field of off-shore wind energy in the northern waters of Europe will cause the introduction of HVDC connections between the off-shore wind farms and on-shore locations. Even multiterminal HVDC grids are currently under discussion [1] in order to cope with the huge amount of wind energy.

In the course of deregulation, privatization and trading of electrical energy, the loading in special network areas is extremely increasing. This results in transportation bottlenecks and deterioration in reliability. With a view to global warming and the very necessary reduction of CO_2-emissions, there will be additionally a significant change in used resources and the energy mix. As the transmission and distribution network structures were de-

veloped in accordance with the generation and load structures of the past, significant structural and operational changes of the networks are now required.

Large-area outages and blackouts in America and Europe have confirmed that the interconnection of adjoining networks is beneficial in terms of operation and economy, but it also bears the risk of uncontrollable, cascading outages. Especially when those networks are operated close to their thermal limits in certain areas, stability and protection problems will occur.

In the paper, a system for the assessment of the dynamic network security is introduced.

2. Transmission Network Changes in Europe

In Europe, the generation of energy undergoes a change including three significant tendencies according partly to **Figure 1**.

1) An increase in generation from renewable resources near the point of consumption, feeding directly medium and low voltage distribution networks.

2) An increase in resources-orientated centralized generation, such as onshore and offshore wind farms, solar parks and coal-fired power plants, feeding the high-voltage transmission network. Introduction of highly dynamic system elements like HVDC stations (see **Figure 3**).

3) A shutdown of nuclear power plants in load centres (in Germany).

In the future, these changes will lead to spatial separation of generation and consumption in the European transmission network. This causes longer transmission ways in a network, which was not designed for this. It is expected that steady-state bottlenecks, dynamic oscillations and protection problems will occur, which have to be detected in advance, and against which, countermeasures have to be determined and verified online [2].

3. Assessment and Improvement of Network Security with SIGUARD®

3.1. Time Scales of System Analyses

The measures for the assessing and improving the network security can generally be divided in three time periods, referring to **Figure 2**.
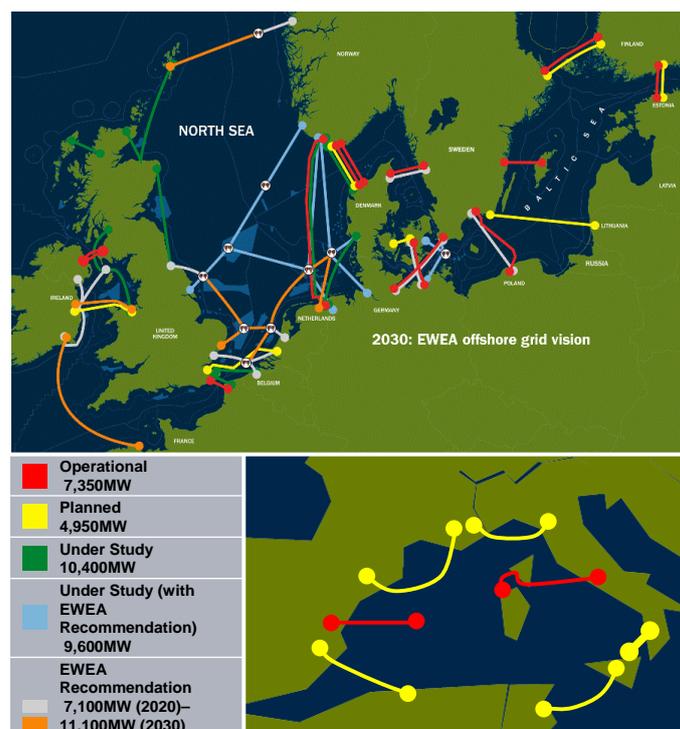
Figure 1. Offshore grid development in Europe as shown in the EWEA offshore grid vision for 2030 [3].
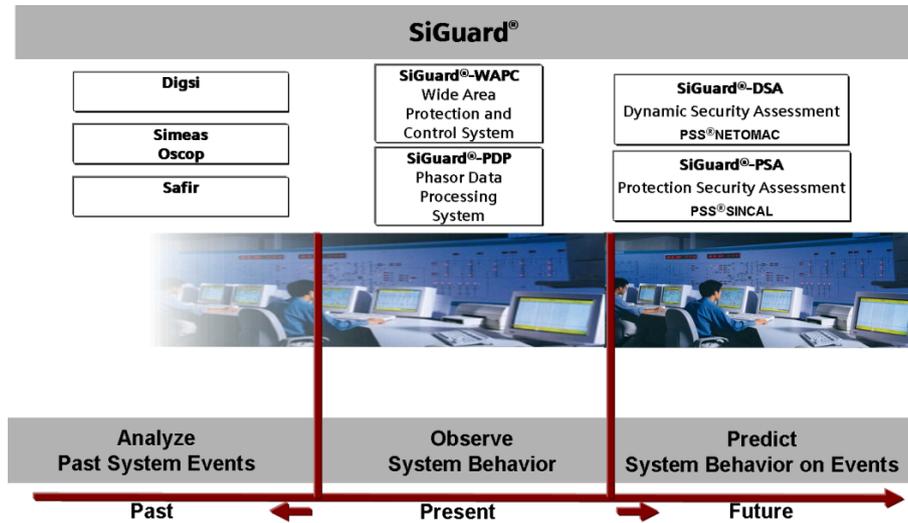
Figure 2. Measures for assessing and improving the system stability.

Past:

The analysis of already occurred disturbances on the basis of disturbance and fault records allows us to identify weak points as well as wrong protection concepts and settings and to improve them in the future. A wide range of usable software tools is available on the market [4].

The disadvantage here is, that disturbances must have occurred at least once in order to identify a weak point.

Present:

Today, so-called Phasor Measurement Units (PMUs) are available, which are able to carry out time-synchronized and time-stamped measurements of the voltage and current phasors in the range of 20 - 100 ms, using GPS, the Global Positioning System. The transmitted phasors will be collected and archived in Phasor Data Processors and are then available for online monitoring of the electromechanical behaviour of the system. This is called "Wide Area Monitoring". The Siemens Phasor Data Processor is the SIGUARD® PDP which is also able to provide further analysis of the phasor measurements.

On the basis of this higher observability, it is possible to design a "Wide Area Protection and Control System" in the future, provided that sufficient fast power electronics equipment (FACTS and HVDC) are available to close the loop.

Future:

With the performance of up-to-date computers, nationwide networks can be dynamically simulated and analyzed with sufficient speed. Hereby, the actual state-estimator results, the actual switching state and the state of the protection system will be used as initial conditions.

So it is possible to receive a foresighted assessment of the network stability in case of disturbances and contingencies, before these disturbances even occur. This also allows us to determine and verify countermeasures, which can be proposed to the operator [5]-[7]. It is the first small step towards an "Autopilot" for network operation.

3.2. Dynamic Security Assessment with SIGUARD® DSA

Network disturbances such as short-circuits, equipment and generator failures as well as sudden network changes, caused by switching, create electro-mechanical transients [8] [9]. Whether these events do not only endanger the steady-state but also the transient stability must be analyzed beforehand using a so-called "Dynamic Security Assessment, DSA". To do so, all passive equipment (wires, cables, transformers, …) as well as all active, switched or controlled equipment (generators, capacitor banks, FACTS, …) including their controllers must be modelled appropriately.

In order to consider the influences and limits caused by the protection system, e.g. in case of overload or power oscillations, the dynamic simulation software must be able to simulate the protection devices of many different manufacturers including all their characteristics and communications. Also out-of-step protection relays and vector-jump relays must be considered. This is indispensable as the relays have direct impact on the

switching condition of the network through the circuit breakers they are assigned to. That is the only way, the danger of cascading outages, as occurred at beginning blackouts, can be identified. A DSA-system, for example the Siemens system SIGUARD® DSA, must be able to not only assess the dynamic state of the system, but also to determine, rate and visualize the margins to critical states of the system [10]. To do so, an interconnection to existing control systems is essential, in order to provide continuous snapshots of the actual, quasi-steady-state condition of the system as a basis for the dynamic security assessment [11].

These snapshots can either represent the current status of the power system and/or the near future, based on generation (wind, solar, market, etc) and load forecasts. The snapshots are taken as the starting point of dynamic time domain contingency simulations. Stability indices, calculated during the simulation process, give information about the stability status while the power system progresses from pre- to post-contingency state. These indices reflect all kinds of local and global instability phenomena (e.g. voltage stability, angle stability, small signal stability, etc.) as well as operational constraints and protection behaviour. The stability assessment is done fully automatic. The user does not have to analyse time curves or tables in order to recognize a stability problem. However, these information are available for further investigations regarding remedial or preventive measures.

If network outages are simulated and possible dynamically critical conditions are found, the online DSA-system should be able to find measures and solutions that will keep the system, or bring it back in a stable and secure mode. Some examples for such measures are:
- Blocking of transformer tap changers (OLTCs)
- Switching of available reactive power components
- Islanding
- Load shedding
- Generation shedding

The Siemens SIGUARD® DSA is using the well established simulation software PSS®NETOMAC [12] as engine. With PSS®NETOMAC it is possible to carry out dynamic contingency simulations faster than in real-time, using a standard PC.

Analyses of past blackouts showed that there is always a time period of 20 - 30 minutes between the first critical network outage and the following cascading disconnections. The typical snapshot time step of 15 minutes or less is therefore completely sufficient to identify critical network conditions, to propose countermeasures and therefore to prevent blackouts.

At an exemplary project for a nationwide transmission network in North Africa [13] [14], where the Siemens SIGUARD® DSA-system is already in use, it could be shown, that a 20 seconds transient stability contingency simulation takes about 8 seconds for simulation. Within 15 minutes (900 sec) this system is able to run more than 100 contingency simulations on a single simulation core. Depending on the number of contingencies, which are required to be simulated, the computation power must be scaled. If, for example, 4000 contingencies have to be simulated each 15 minute cycle, than 40 simulations processes must run in parallel. This means that only four 12-core servers had do be employed in order to meet this requirement.

4. Typical DSA Setup for Control Room Implementation

An online DSA system must be seamlessly integrated in existing control room applications. Therefore it must provide, among others, the following functionalities:
- multi-user capabilities,
- web applicability,
- operating independency of user clients,
- customizable user interfaces,
- hot redundancy,
- disaster recovery capability.

Traditional SCADA EMS systems satisfy extremely high reliability requirements. Such systems are installed at two distant sites in order to remain in control even during and after catastrophic situations. One site (backup site) is usually in down state while the databases are continuously updated. Additionally, an offline system with the same functionalities is installed for training purposes. A typical system setup is shown in **Figure 3**.

From the setup, shown in **Figure 3**, it becomes obvious, that the DSA software must have a distributed architecture. The advantage of such software architecture is that the system is highly scalable. If, for example, the
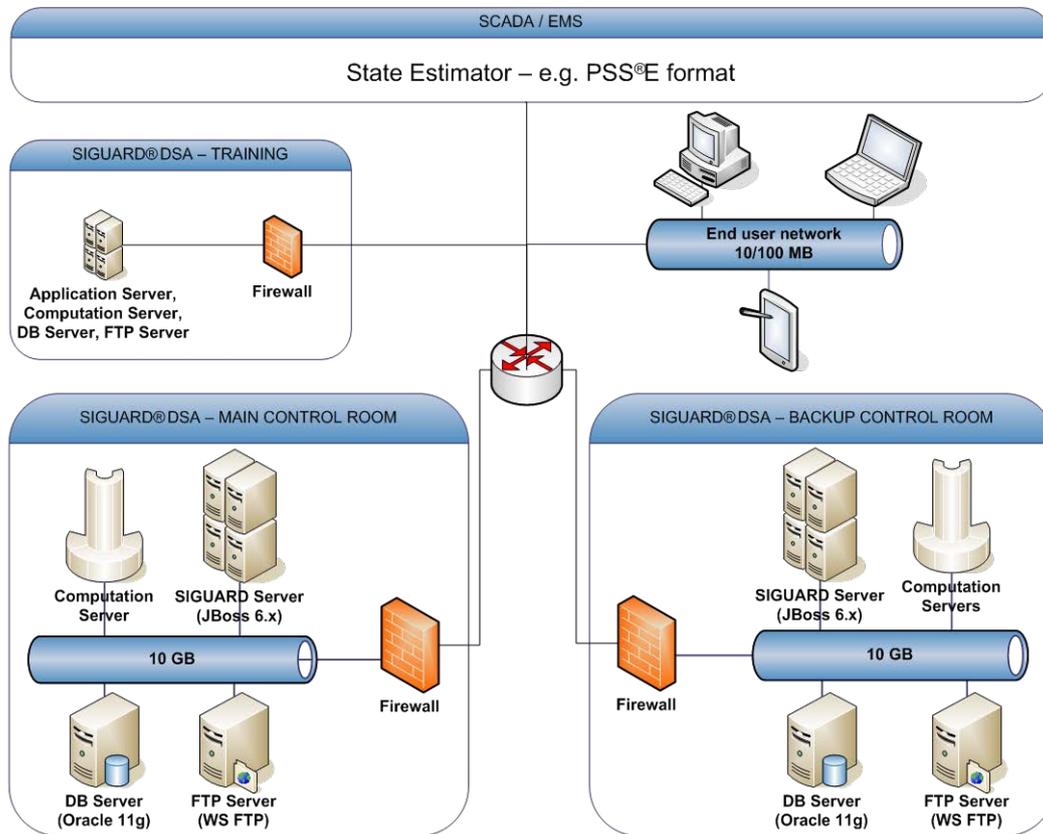
Figure 3. Typical control room integrated setup of DSA system.

size of the system model increases and demands for more computational power, the number of computation servers can be increased without any changes in the rest of the system.

5. Summary

The increasing number of blackouts emphasizes the need for new dynamic security assessment systems (DSA). Stability limits are often reached before thermal and operational limits because of new system equipment (e.g. high temperature overhead line etc.) and highly dynamic system elements like HVDC links. This has been recognized by many utilities and regulators, and online DSA systems are being installed in more and more power system control rooms. The presented SIGUARD® DSA system is the most modern system, which copes with all kinds of dynamic stability threats, including protection behaviour, of today's power systems. It is capable of being easily implemented in existing and new SCADA/EMS systems for power systems of any complexity and size. Its flexibility regarding software and computation hardware extensions (e.g. for wide area monitoring and control applications) are highly appreciated by several European TSOs.

References

[1]   3E, Dena, EWEA, For Wind, IEO, NTUA, Senergy, SINTEF (2011) Offshore Electricity Grid Infrastructure in Europe, Final Report.

[2]   Buchholz, B.-M., Krebs, R., Rudion, Z. and Sassnick, Y. (2008) Vision 2020—Security of Network Operation Today and in Future. *German Experiences*, IEEE PES, Pittsburgh.

[3]   EWEA (2009) Oceans of Opportunity. Report by the European Wind Energy Association EWEA.

[4]   PSS®SINCAL: Utility and Industry System Analysis. www.siemens.com/power-technologies

[5]   Jaeger, J., Krebs, R. and Lund, P. (2009) Network Security Assessment—An Important Task in Distribution Systems with Dispersed Generation. CIRED, Prague.

[6]   Jaeger, J. and Krebs, R. (2008) Protection Security Assessment in Nationwide Power Transmission Systems. GCC-CIGRE, Bahrain.

[7]   Balasiu, F., Balaurescu, R. and Lazar, F. (2009) Defence Plan against Major Disturbances of the Romanian EPS. *IEEE GM*, Calgary.

[8]   van Cutsem, T. and Vournas, C. (1994) Voltage Stability of Electric Power Systems. *Power Electronics and Power System Series*.

[9]   Kundur, P. and Balu, N.-J. (1998) Power System Stability and Control. McGraw-Hill Inc., New York.

[10] Kerin, U., Bizjak, G., Krebs, R., Lerch, E. and Ruhle, O. (2009) Faster than Real Time: Dynamic Security Assessment for Foresighted Control Actions. *IEEE-Powertech*, Bucharest, 29 June-2 July 2009.

[11] Heyde, C. and Styczynski, Z. (2009) Voltage Stability Analysis as Part of an Online DSA System. *IEEE GM*, Calgary.

[12] PSS®NETOMAC: Dynamic System Analysis. www.siemens.com\power-technologies

[13] Lerch, E. and Ruhle, O. (2009) Ranking of System Contingencies in DSA Systems. APSCOM, Hong Kong.

[14] Lerch, E., Ruhle, O. and Vickovic, D. (2009) Real-Time Stability Assessment in the Control Center of Bosnia and Herzegovina and a National Dispatching System in Noeth Africa. *IEEE PES*, Seattle.