© JUL 2022 | IRE Journals | Volume 6 Issue 1 | ISSN: 2456-8880

Power System Security Assessment

HARSHDEEP[1], VISHAL V. MEHTRE[2]

[1, 2] *Department of Electrical Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India*

Abstract- A broad overview of on-line power system security analysis is provided, with the intent of identifying areas needing additional research and development. Current approaches to state estimation are reviewed and areas needing improvement, such as external system modelling, are discussed. On-line contingency selection has become practical, particularly for static security. Additional work is necessary to identify better indices of power system stress to be used in on-line screening filters for both static and dynamic security analysis. Near interruptions (emergencies) without interruption of customer service. It is related to system robustness in nearby disturbances, therefore, depending on the operating system and the potential for interference.

Historically, ensuring safe operation has been a key factor in the safe and economical operation of energy systems. If the system has an insufficient level of security, it becomes extremely dangerous and, in some cases, catastrophic, systemic failures of the most recently observed species on various power grids around the world, events with significant economic costs and potentially even losses. of life.

Indexed Terms- Power System Security Assessment, Security Control SCADA, Dynamic Security Assessment

I. INTRODUCTION

In times of controlled and integrated energy systems, systems tend to be more secure for several reasons. First, as the grids were designed, built, and operated by private companies (usually public bodies and public services), integrated planning ensured that the production and transmission facilities were accompanied by increased load, thus preventing overload and equipment failures that could lead to system disruption. The maintenance programs were, in general, strong. From a practical point of view, the conditions of the forecasting system were simple because they were few in transit owners and generations and operated in a carefully planned and collaborative manner. As a result, the systems were exposed to the smallest possible disruption, were most effective in responding to potential disturbances, and were highly predictable in their operational patterns.

However, the emergence of the electric power market in open markets over the past decade has introduced many factors that have increased potential sources of systemic disruption, reduced system robustness, and reduced performance

forecasts. Some of these factors are described in Table 1. To ensure that the energy system is reliable enough, that there is an acceptable chance of it operating efficiently over time, the system must 1) be properly designed.

with security as a primary consideration and 2) monitored during operation to ensure that the safety limit is always present (as actual working conditions or emergencies may differ from those planned). Success in achieving these goals depends largely on the use of good engineering, which includes growing confidence in the use of energy analysis tools. The changes that have taken place in the new environment both have increased the need to test the security of the robust energy system and changed the skills requirements of the power system analysis tools.

- Security in System Operations

The DSA refers to the analysis required to determine whether a power system can meet the specified reliability and safety conditions in both temporary and stable times in all trusted emergencies. In the workplace, a secure system is one in which the working conditions are respected in the pre- and post-emergency situations. This means that analysis should be performed to assess all aspects of safety, including thermal loading of system components, power and frequency variations (both solid and transient), and all types of stability. The statistics required to accurately assess the security of the defined system state are technically strong and require considerable effort. As a result, security tests have historically been performed in an offline performance planning environment where the stable and flexible performance of predictable near-term system conditions is completely determined using tools such as power flow and time simulation simulation. As a result of the engineering and calculation efforts required for the complex tests, which are required to assess stability, it was necessary to calculate the system performance limits in advance of what was expected to happen. In this way, all planned and emergency situations had to be assessed although many would not really be possible.

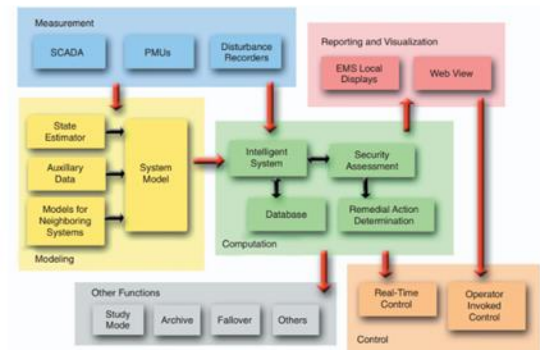
In a new competitive environment, the uncertainty of predicting future working conditions has created the need for a new security assessment method: the online DSA. In this way, the stability of the current operating system is calculated as it happens and with sufficient speed to activate the automatic control action or to allow the operator time to respond when an emergency is shown to be too great. it is likely that such an examination will provide the operator with early indications of a waiting problem and provide an opportunity to take remedial action. In fact, the final report of the U.S.-Canada Power System Outage Task Force dated August 14, 2003 closed includes a number of recommendations (particularly Recommendations 13 and 22) related to research, testing, and familiarity with tools related to reliability and technology, targeted. in establishing real-time operational tools guidelines.

- Components of the online DSA Program

Online DSA takes measurements of the real state of the system and performs security analysis in a timely manner and transmits the information to the operator or directly to system control. The main components are shown in Figure 1.

Ratings

System measurements can be obtained from a number of sources, including standard SCADA systems, PMUs (usually the data is first transferred to a data connector for pre-processing), and interference monitors. The measurements obtained are used for four main purposes, as follows:



- input to state estimation from which system models will be developed (SCADA or PMs).
- direct input to security computation engines (SCADAor PMs)
- benchmarking of state estimation results or computa- tional results (PMs or disturbance recorders)
- arming or triggering SPSs (SCADA or PMs).

As all power systems have existing SCADA systems, thisremains the primary source of data to be used as input to DSA systems. SCADA systems also offer a rich range of measured parameters and are updated at a relatively fast rate.On the other hand, PM systems have substantial advantages in that they can provide fast, accurate, continuous, and time-synchronized data for both magnitudes and phases of virtual- ly any quantities in the system. This helps improve the models for the DSA applications.

- Modelling

If a detailed analysis is to be done at an online DSA, high-quality connected system models are required. In fact, since all analysis depends on the quality of the system model, it may be the most important part of the DSA system. This is especially true if testing will be done using statistics based on fully defined system models. Common state estimates are the main source of power flow models, which must then be supplemented with other information such as dynamic mathematical models. Many of the main problems are associated with modelling, including model size, model details, variable representation, model accuracy and model validation, including model size, model details, dynamics representation, and model accuracy and validation.

- Model Size

Some connected electrical systems have grown significantly in size, and as a result, their "full simulation" models have grown exponentially in size. The NERC planning model for the eastern North American network, for example, now has about 45,000 buses, and some regional measurement models (intended to measure the full system representation) in this region are closer to 20,000 buses. In general, it is necessary to model large components of the power system in DSA online systems because some of the limiting events, especially small signal stability, may involve wider system areas. SCADA data (or other system measurement sources) and the result of state measurement output, on the other hand, may be limited to a specific location (such as part of a linked system, usually associated with a control area.). It is therefore necessary to enter the representation of the external system (possibly in an equitable manner) before performing the analysis. This can be achieved by installing a national measurement model with an advanced “offline” external presentation or by integrating a few regional measurement models from different parts of the connected system.

- Model Detail

The level of detail contained in the model is also important. For example, representing the key features of the distribution system is important in the analysis of the dynamics of electrical energy. Many power flow models based on regional measurement models include load models in which all distribution components have been integrated into a single load representing half active force (P) and half active force (Q). In order to analyze the dynamics of electrical energy, it is often necessary to remove the load component representing the key components, such as distribution transformers, distribution capacitors and reactors, and induction motors. Similarly, details of the active power of a generator and the maximum power that can be sent are important in the calculation of genetic stability genes in specified system conditions and functions.

- Dynamics Representation

The power flow model from the world scale is matched to the dynamic models of all the important devices in the system. In this case, it is also important that all the important dynamics are represented correctly and appropriately. Special controls, such as generator overexcitation, as well as SPS, sophisticated equipment, such as high voltage dc (HVDC) and FACTS, and new flexible devices, such as wind generators, may need to be incorporated into DSA systems. In some cases, it is important to determine the status of flexible devices (such as PSS) in the model to ensure statistical accuracy.

- Model Accuracy and Validation

In order to have confidence in the results of the analysis, the models used must be verified with accuracy. Although this is a major challenge, it can be divided into three categories.

The first type of verification confirmation can also be achieved using advanced measurement technology (such as PM), best measurement, and a high-level measurement algorithm.

The second type of device model authentication can also be achieved by generating location generators and loading. For example, after a power outage in 1996 in a system connected to western North America, the WECC authorized a generator test and model verification function. This process exposed a wide range of errors and inaccuracies in the original WECC model library and resulted in the full validation of dynamic models of generators and controls. Modeling loading is a major challenge, and due to the natural variability of load over time, field testing has met with limited success. Other methods, such as the integration of models from survey data with online diagnostic models, may be more effective.

The third type of system model validation. This includes ensuring that all simulation model responses are consistent with the actual system performance. As it is possible to test only a limited system in this regard, a great source to ensure complete repetition of the actual system bugs. Such efforts have been made in the wake of numerous major disruptions, including the 1996 WECC shutdown and the most recent blackouts in the Northeast.

Data obtained from disruption monitors or PMUs may be useful in these efforts.

- Computation

The types of methods used for DSA are widely varied and can be considered as spanning into two extremes.

Deterministic evaluation using analytical solutions: This is the most complex of approaches in which the response of the power system is assessed using detailed models of the steady-state and dynamic characteristics of the system. Contingencies are applied and the responses computed using techniques such as time-domain simulations.

Direct inference from measurements: This is the simplest of approaches in which the security of the power system is inferred from direct quantities measured from the grid; using the difference in two PMs to establish transient security, for example.

In between these two extremes are a plethora of methods differing in computational complexity and that may include hybrid approaches combining simulation with some direct or measurement-based methods. The selection of a suitable computational method is based on a balance of the require- ments described below.

Comprehensive and Accurate Computation Capabilities
What you need to know about the operator at any time
1) How secure is the current state of the system,
2) How secure the system will be when it is directed, in the next few minutes, from the current state to another state.
3) If the security level of the system is not acceptable, what steps can be taken to make it acceptable?

In fact, the biggest challenge is to ensure the security of the current situation and to find a safe place where the system can be directed. This protected region can be visualized in nomograms, as shown in Figure 2 (full nomogram), and is defined by the set parameters with respect to the limits. representing various security criteria, including:

- thermal overloading of transmission elements
- steady-state voltage and frequency excursions
- transient voltage dip/rise
- transient stability
- small-signal stability
- voltage stability
- frequency stability
- other.

The limitations associated with these items can be done using full simulations or using limited methods. Examples of complete simulation methods include a complete PV curve power solution, temporary safety simulation simulation, and eigenvalue analysis for small signal stability. Limited methods include techniques such as sensitivity methods to assess electrical safety and direct power methods to assess temporary stability. While limited methods may offer some speed benefits, full simulation methods provide more accurate safety assessments.

- Speed of Computations

Although detailed simulation is recognized as providing the most accurate security tests, computational speed remains a challenge especially with the complex models required for analyzing large connected systems. Simple or straightforward methods can play a role in completeness, especially in emergency examinations. A typical online system calculation cycle is 5 to 15 minutes, which means that a complete security check should be completed within 5 to 15 minutes from the time the summary is taken from the system to the time the results are made available. Since safety assessments should determine the safety of emergencies, and as it is generally unreasonable to research all emergencies in detail, one key factor on the DSA's online site is to assess emergencies; the ability to select emergencies that need to be analyzed in detail. Although many methods have been proposed and have been used for this purpose, there is still a balance between speed and accuracy. Thermal fluctuations or power outages may be easier to use than stable ones, where complex and indirect flexibility of the system may make simplified testing methods unreliable. However, research in this field is still ongoing.

One way to deal with the problem of speed calculators is to increase the computer power of the DSA internet system by distributing statistics between multiple servers. This can easily be achieved as DSA problems are inherently related, at least at the level of emergencies and analysis.

Distributing DSA analysis enables the computer performance of the DSA system to increase the number of servers used, thereby increasing the DSA processing capacity of larger system models.

- Automation and Reliability

DSA online systems must be highly automatic and able to complete all tasks, repeatedly, under different conditions without human intervention. This requires not only high standards in DSA software but also with some ingenuity to provide the required results. For example, determining appropriate remedial measures may require additional emergency assessments or system conditions depending on the results of the safety assessment. Honesty is another important aspect of the online DSA program. As indicated on the cancellation of 14 August 2003, the potential consequences of non-availability of critical software applications can be very dangerous. In addition to ensuring the deployment of high-quality software and hardware for the DSA online system, strategies such as downtime and livelihoods should be considered in order to meet the requirements of reliability.

- Graphical Format

It shows the results of the analysis of small signals displayed on the location map. Such observations clearly show the regions (and some generators) involved in interarea movement following the unfavorable situation. It shows the secure circuit nomogram for electrical safety safety analysis. The circuit is bound to violate the conditions of thermal conductivity, voltage stability, power outage, and active energy sources. With this display, the operator is free to direct the system to the green area without encountering security breaches. Combining nomenclature of this type to protect electrical power, temporary safety, and small signal analysis creates the image display shown at the beginning of

The above demonstration of the security test result can be associated with other types of displays in order to have a complete understanding of system performance under taught conditions. For example, the critical system status placed on the map transfer system may help to identify the worst operating system regions. A history defense margin chart can be used to predict and interpret system security.

Another practice of viewing results is to provide complete security test results to the local EMS console and to broadcast them in real time on the web, which can be viewed from any remote location by authorized personnel. This can facilitate the exchange of security information between control centers so that preventive measures can be taken as soon as security checks are performed.

- Control

If the DSA online system determines whether a particular emergency or system situation may lead to an unsafe situation, remedial measures should be taken. Remedial measures can be preventive or remedial measures and may include actions such as switching off the capacitor, changing the capacitor, rearranging the generator, pressing the transformer, or installing special protection systems, such as generation resistance or power switch. These controls may be operated by the operator as recommended by the DSA system or by the automatic operation of the DSA system. In this way, the DSA system can be an integral part of special security systems.

- Other Functions

A number of other important requirements for an online DSAsystem include the following:

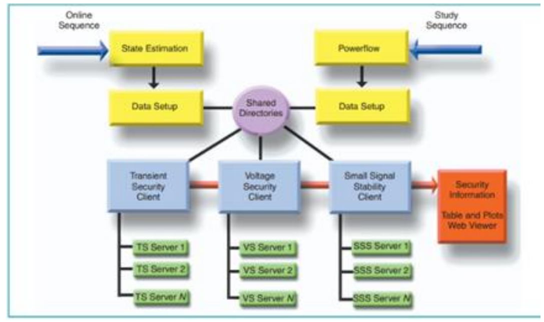
- *Study mode:* The system should allow the operators orengineers to study any scenario of interest in an offline“study mode” environment using base data taken fromthe live system (or archive).
- *Archive:* The DSA system should be able to periodical-ly and selectively store cases studied and correspondingoutput results for use in the study mode or for post- mortem analyses.
- *System monitoring, diagnostics, and maintenance func- tions:* As a component of the real-time applications, it isimportant that the performance of the DSA system is monitored continuously and any indication of opera- tional irregularity should be detected and reported for diagnostics and maintenance.

- Architecture of an IntegratedOnline DSA System

The basic structures used in the implementation of the online DSA system are shown in Figure 6. The tools work in both the learning mode and the real-time sequence of the EMS system with the basic network model obtained from the state analyst. The bus-breaker model used in the EMS system has been delayed by a nodal model that has direct access to the DSA system. Similarly, emergency data, dynamic data, and other system data are mapped for use in the DSA system. Assist data, such as control files, can be set using the EMS console or terminals assigned and transferred, as well as all other data, to the DSA system. DSA applications (including power flow, time zone simulation, and modular analysis) complete the abstract image test provided by the state measure. Each DSA system system operates on a client (backup) connected to a number of servers where it is calculated and a Web server to be displayed to users and other stakeholders. The reliability of the DSA system ensures client and server copies are automatically changed when required.

- Where We Are Today in DSA

Significant improvements have been made in recent years regarding the use of DSA technology as described in previous sections. The development of sophisticated, highly automated, and reliable software tools, combined with seemingly endless improvements in computer performance, has led to the installation of DSA on many sites around the world. In North America, a large number of transport system operators are also moving to the DSA online, including the Electric Reliability Council of Texas (ERCOT), which has eliminated the installation of electrical safety and temporary security devices that operate in real-time sequence. of EMS. This system calculates the basic case security and security limits for the number of specified functions. In another example, Guangxi Electric Power Company (China) has installed a DSA system that spans every five minutes and includes a comprehensive set of safety conditions that include temporary stability, wetting, short-term power flow and frequency travel, and post-mergence steady-state volt. - age profiles (addition of small signal stability test shared. Once the statistics are complete, critical results are compiled and returned to the EMS console associated violated criteria for each point on the boundary of the secure region.



it is a configured developer). Reliable emergencies can be screened for any security measures and displayed to system users. If an emergency is identified as unsafe, the online DSA will re-evaluate available emergency control actions and recommend to operators the appropriate regulatory action. Additionally, important system conditions and DSA results are sent to the company intranet, allowing authorized users to view such information in real time using a web browser from anywhere within the intranet.

Today, the tools available for basic DSA are quite matureand the focus is moving to issues such as ease of connectivity to the EMS, improved remedial action determination, direct control of special protection systems, the use of new technologies such as PMs, and advanced visualization.

- Looking Forward: Intelligent Systems

DSA's advanced online tools often rely heavily on prescribed calculation methods and should therefore fully evaluate the many possible scenarios and seek security limits using a robust approach. Although this method provides the most accurate results available (and certainly higher than methods based on simplified indices), it is statistically burdensome and, as a result, time consuming. To address the complexity of the system, these methods may make certain models easier and speculate about the most important emergencies. To overcome these shortcomings, these applications can be linked to an intelligence system (IS) that can use the pre-collected statistical information (stored on the site), apply the rules set by experts, and consider based on system conditions. . In this way, security (and security restrictions) can be achieved quickly without extensive simulation, and the whole system can read automatically. IS can be connected in conjunction with the DSA simulation engine so that simulation can proceed as it seems necessary in the system. The IS can also be used to determine the best control measures to be taken based on the security situation. The structure of such a system is shown in Figure 7. System parameters are applied directly to the IS which has access to both the knowledge base and the determining tools. To date, some value has been applied to the use of this technology in subcontracting systems. One such development, based on the use of temporary stability test trees [see “Smart Dynamic Safety Assessment Program” in the “Continuous Learning” section], uses a software framework to provide several old jobs and automatically update decision trees. The framework consists of a few sections described below:

- Data Builder

This module includes a scenario generator, which allows the user to define a set of conditions that will be used to create a large IS database, which will be used to build decision trees. The case generator generates a control file that then uses the full domain simulation and determines the stability status of all defined conditions. Prior to using the time domain simulation, the developer attribute selector can be used to determine which output values (such as bus volumes or generator output power) should be removed or stored. This helps to reduce the size of the outgoing site. Output data builder is a large database of objects (a few thousand) each that includes a number of elements (several hundred objects such as voltages and currents) and a target element that shows the stability status of that particular object.

- IS Builder

This module includes a web browser that allows the user to perform statistical analysis on a website and select or reject items or attributes. This module also connects to tree tree building software. Trees are built from a large website and are released as a viable system that can be run over time in real-time EMS sequences.

- Online IS Controller

This module connects to a live EMS system and takes the form of a system from the state coordinator and creates an object that can be dropped from the created resolution trees. This module also links to DSA analytics engines (time domain simulations), KNN software (nearby neighbor), and standard viewing tables (if available). The output of the IS controller is a system stability (stable or unstable) or a real limit of stability when using a processing loop that sets the limit repeatedly.

CONCLUSION

Ensuring security in a new environment requires the use of advanced energy system analytics tools that can fully assess safety with due regard to practical operating conditions. These tools should be able to model the system efficiently, calculate safety limits in the form of fast and accurate measurements, and provide reasonable indicators to system operators. The technology is currently available to achieve these goals and is being used on many sites around the world. The systems are relatively inexpensive and easy to use as EMS vendors take the initiative to integrate such tools into their native products. Online dynamics safety tests can provide a first line of defense against widespread system disruption by quickly scanning the system for potential problems and providing operators with possible results. With the development of emerging technologies, such as PMs and ISs in a wider area, the online DSA is expected to be a powerful weapon against system shutdown.

REFERENCES

[1] *CIGRE Tech. Brochure*, no. 231, 2003. U.S.-Canada Power System Outage Task Force, “Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations,” Apr. 2004.

[2] K. Morison, L. Wang, P. Kundur, X. Lin, W. Gao, C. He, F. Xue, J. Xu, T. Xu, and Y. Xue, “Critical requirements for successful online security assessment,” *presented at the IEEEPES PSC&E Conf.*, New York, Oct. 10–13, 2004.

[3] R. Avila-Rosales, A. Sadjadpour, M. Gibescu, K. Morison,H. Hamadani, and L. Wang, “ERCOT’s implementation of online dynamic security assessment,” presented at the PanelSession of the *IEEE PES 2003 General Meeting*, Toronto, Ont., Canada, July 13–17, 2003.

[4] K. Morison, "Future directions: Online dynamic security assessment using intelligent systems," presented at the Panel Session on Power System Security in the New Market Environ-ment, *IEEE PES Summer Power Meeting*, New York, July 2002.

[5] J.A. Huang, A. Valette, M. Beaudoin, K. Morison, A. Moshref, M. Provencher, and J. Sun, "An intelligent sys-tem for advanced dynamic security assessment," in *Proc. PowerCon 2002*, Kunming, China, Oct. 2002 [CD-ROM].

[6] K. Morison, H. Hamadani, and L. Wang, "Practical issues in load modeling for voltage stability studies," presented at the Panel Session of the *IEEE PES 2003 General Meeting*, Toronto, Ont., Canada, July 13–17, 2003.

[7] Rocco, C.M.; Ramirez-Marquez, J.E.; Salazar, D.E.; Yajure, C. Assessing the Vulnerability of a Power System Through a Multiple Objective Contingency Screening Approach. IEEE Trans. Reliab. 2011, 60, 394–403.

[8] Ding, T.; Li, C.; Yan, C.; Li, F.; Bie, Z. A Bilevel Optimization Model for Risk Assessment and Contingency Ranking in Transmission System Reliability Evaluation. IEEE Trans. Power Syst. 2017, 32, 3803–3813.

[9] Street, A.; Oliveira, F.; Arroyo, J.M. Contingency-Constrained Unit Commitment with n–K Security Criterion: A Robust Optimization Approach. IEEE Trans. Power Syst. 2011, 26, 1581–1590.

[10] Wang, Q.; Watson, J.; Guan, Y. Two-stage robust optimization for N-k contingency-constrained unit commitment. IEEE Trans. Power Syst. 2013, 28, 2366–2375.

[11] Levitin, G. Optimal Defense Strategy Against Intentional Attacks. IEEE Trans. Reliab. 2007, 56, 148–157.

[12] Levitin, G.; Hausken, K. Redundancy vs. Protection vs. False Targets for Systems Under Attack. IEEE Trans. Reliab. 2009, 58, 58–68.

[13] Ejebe, G.C.; Wollenberg, B.F. Automatic Contingency Selection. IEEE Trans. Power Appar. Syst. 1979, PAS-98, 97–109.