A Study on Dynamic Security Assessment and Early and Reliable Identification of The Critical Machine Cluster

[1]Ankamma Rao Jonnalagadda (IEEE member) and [2]Dr. Sardar Ali

[1]Student, Pursuing PhD in Sri Satya Sai University, Bhopal, https://orcid.org/0000-0001-9008-695X
[2]Professor and head of EEE department at Deccan College of Engineering & Technology, Hyderabad-Telangana

ARTICLE DETAILS

Article History
Published Online: 15 March 2019

Keywords
dynamic, security, assessment, thermal, generator

ABSTRACT

In this paper, we have focused on dynamic security assessment and identification of the critical machine cluster. In the operating environment, a secure system is one in which the operating criteria are regarded at pre-and post-contingency conditions. This infers that investigations must be performed to evaluate all aspects of security, including the thermal loading of system components, voltage and frequency variations (both steady state and transient) and all types of stability. In this paper, another technique is proposed to recognize the CMC, which uses productive algorithms from chart theory. For that reason, a novel coupling coefficient is inferred, which speaks to the coupling strength between pairs of generators.

1. Introduction

So as to improve situation awareness of the system operator, it is critical to know stability of the power system in its current condition as for a number of credible contingencies. Dynamic security assessment (DSA) tools are tending to this need. DSA is characterized in as follows: "DSA alludes to the analysis needed to decide if a power system can meet indicated unwavering quality and security criteria in both transient and steady-state time outlines for every credible contingency." In systems with conventional generation, power system operators relied intensely upon the security assessment results from off-line operation analysis to guarantee a secure and solid everyday operation. Today's power systems are more perplexing, because of open business sectors and integration of more renewable energies. Henceforth, the consistency of power system operation is decreased and depending entirely on off-line DSA results is illogical or may even be infeasible. Therefore, the utilization of and the demand for on-line DSA is becoming around the world

In a structure for an on-line DSA was proposed as appeared in Fig. 1. In the accompanying a short description of the various components of an on-line DSA will be introduced

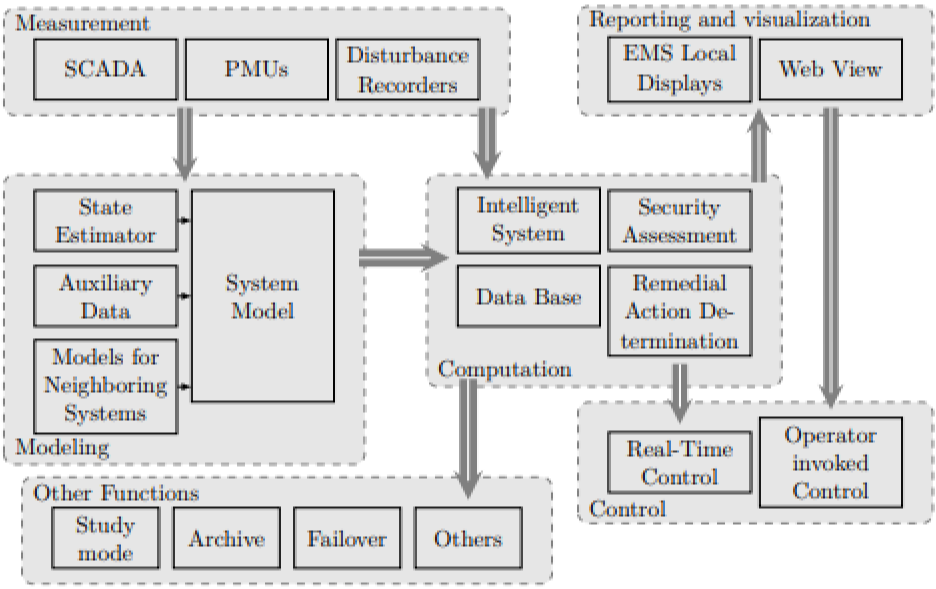


Figure 1: Components of a DSA and their interaction

- **Measurement:** Estimations can be gotten, for example from SCADA systems or PMUs. The decision is relying upon the estimation necessities, for example, exactness, examining rate, and so on. The estimations are then utilized as input to a state estimator or may legitimately be utilized in the security assessment tools.
- **Modeling:** Accurate modeling of the power system and its components might be the most significant and critical part of an on-line DSA. Right off the bat, since the pattern is towards larger and larger interconnected

systems, it is a challenge to decide the necessary size of the pre-owned model and the satisfactory representation of external systems. Secondly, another critical issue is to distinguish, the required detail of the model representation, for example model representation of distribution grids. Thirdly, so as to do dynamic assessments and simulations, the system components must be spoken to by dynamic models reasonable for the picked time outline. At last, the models should be approved with for example measurements, field tests or comparison of simulations with recorded measurements of events.

- **Computation:** In order to determine security of the system, a wide range of methods has been developed, which may be split into two extreme groups.
- **Deterministic evaluation using analytical solutions:** Most complex; requires detailed models; techniques such as detailed time-domain simulation
- **Direct inference from measurements:** Simplest approach; security inferred directly from measurements (e.g. comparison of phasor angles)

2. Research on On-Line Dynamic Security Assessment

In the creators portray the further evolved functions of the online DSA system utilized in Brazil – ONS. As mentioned before the DSA system utilizes a combination of nitty gritty time-domain simulation and direct strategies. The assessment of stability utilizing exclusively time-domain simulation requires visual inspection of the results. The creators trade the requirement for inspection by utilizing numerical energy functions and a changed version of the SIME strategy to register stability edges, recognize instability and empower early termination of the simulations. The further advancement of the DSA functions is for the most part concerning the transient stability assessment approach, where the first SIME strategy was altered. The altered version of SIME improves the speed and the precision of the computation of stability edges for stable cases. The focal thought was to gauge the Pe − δ normal for the single machine comparable or rather the one machine infinite bus system (OMIB) by the accompanying equation

$$P_e(\delta) = \frac{E_m(\delta)E_\infty}{X_e}\sin\delta + P_0 \qquad (1)$$

This equation communicates the electric power of the OMIB as a function of the comparable machine voltage behind the transient reactance E_m, the voltage at the infinite bus E_∞, the proportionate machine rotor angle δ and a local power P_0, which is resolved to fit a particular operating point. The creators propose figuring the parameters E_m (δ) and E_∞ as the normal of the generators' voltages behind the synchronous reactance in the critical and non-critical generator group. Also, X_e is resolved as the weighted normal of the external impedance seen by every generator in the critical group. The Pe − δ normal for the OMIB would then be able to be utilized to decide the stability margin of a case when the greatest motor energy is known. The ongoing accomplishments in research on-line DSA systems utilizing the transient energy function. The creators present a report on the on-line DSA system actualized at TEPCO in Japan. The introduced DSA system exists of two significant blocks. The main block does a dynamic contingency screening given a system state and a rundown of contingencies. The contingencies are ordered and the very stable cases are filtered out. The unstable and/or uncertain cases are sent to the second block, which does nitty gritty time-domain analysis.

3. Off-Line Vs On-Line DSA

In the operating environment, a secure system is one in which the operating criteria are regarded at pre-and post-contingency conditions. This infers that investigations must be performed to evaluate all aspects of security, including the thermal loading of system components, voltage and frequency variations (both steady-state and transient) and all types of stability. The computations expected to accurately evaluate the security of a single characterized system condition are in fact thorough and require considerable exertion. As a result, security assessment has been historically conducted in an off-line arranging environment in which the steady-state and dynamic execution of the close term estimated system conditions are thoroughly decided utilizing tools, for example, power flow and time-domain simulations. Due to the designing and computational endeavors required for the more unpredictable assessments, for example, required for stability assessment, it was important to register system operating limits well ahead of time of the time in which they were relied upon to happen. In this approach, the most critical conditions and contingencies must be inspected despite the fact that most could never really happen. Be that as it may, the operating limits processed off-line for a proposed situation don't really apply to all other power system operating conditions. This is on the grounds that the stability limit is a local property of the system state vector. For each new solution of the system of equations that depict the system state there is another stability limit. Essentially stated, the stability limits are not fixed and change with the system's loading, voltages and topology.

4. Requirements for On-Line DSA

There are a number of prerequisites that must be met for an effective on-line DSA implementation. These consist of auxiliary necessities, (counting such things as basic system components and data connections) and functional prerequisites (depicting such things as what the system must do and how fast it must perform). This Chapter gives an overall description of these prerequisites. The fundamental functions of an On-line DSA system incorporates the accompanying essential steps,

- Take a snapshot of the power system condition
- Develop a suitable network model
- Combine any additional dynamic data and contingency data required to perform the assessment
- Perform the analysis
- Report on results of analysis
- Raise alarms when security issues are detected.
- Identify security issues and make recommendations on how to alleviate them. (This function is not always achievable).

Although there are a variety of on-line DSA architectures that can achieve these functions, most on-line DSA systems can be divided into the components as shown in Figure 2

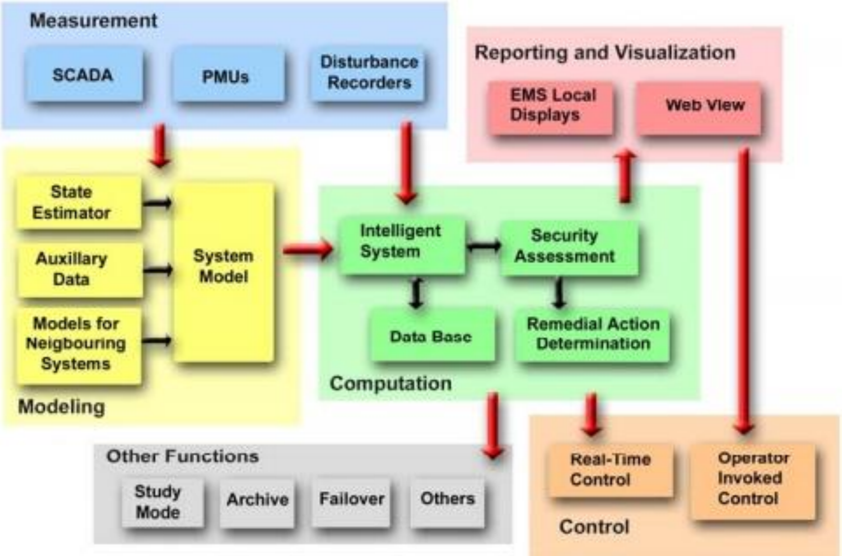


Figure 2 - The components of an on-line dynamic security assessment system

5. Measurements for On-Line DSA

On-line DSA systems rely heavily on the breadth and quality of measured data taken from the power system. The measurements obtained are used for four primary purposes,

- Input to state estimation (SE) tools from which system network and contingency models will be developed. This is the most common approach in which SCADA measurements are used as input to SE which in turn produce network (power flow) model suitable for use with security assessment tools. Other inputs, such as those from phasor measurement units (PMUs) may be used to augment the SCADA data set in an effort to produce a more accurate system model.
- Direct input to security computation tools. Examples include use of measured quantities to assess system damping, or use of PMU data (such as angle spread across a system) to infer stability.
- Benchmarking of system models or security assessment results. Examples include (i) use of PMU measurements to verify quantities in models produced by state estimators or (ii) use of disturbance monitors to benchmark system responses predicted from the on-line DSA system.
- Arming or triggering of Special Protection Systems. An example is the arming of generation rejection schemes directly from PMU measurements. This assumes that either off-line or on-line studies have provided a relationship between the measured value and the required arming.
- System measurements can be obtained from a number of sources including traditional Supervisory Control and Data Acquisition (SCADA) systems, phasor measurement (PM) units and disturbance monitors.

6. Performance for On-Line DSA

Albeit point by point simulations are perceived as giving the most accurate security assessments, speed of computation stays a challenge particularly with the unpredictable models required in breaking down large interconnected systems. Improved or direct techniques can assume a corresponding role with full simulation, particularly in contingency screening. The common computation cycle for an on-line system is 5 to an hour, in other words that a total security assessment must be finished inside 5 to an hour from the time the preview is taken from the system to the time the results are made accessible. Since security assessment must decide the security for critical contingencies, and since it is commonly unfeasible to concentrate all contingencies in detail, one principle component in on-line DSA is contingency screening. Contingency screening is the capacity to choose, from a broad rundown, the significant contingencies which must be broke down in detail. While various techniques have been proposed and applied for this task, it stays a harmony among speed and precision. Screening techniques for thermal overloading or voltage declines might be a lot simpler to apply than those for stability, in which complex dynamics and nonlinearities of the system may deliver streamlined screening strategies questionable. Nonetheless, research in this field is on-going. Another approach in managing computation speed issue is to build the processing power of an on-line DSA system by dispersing computations among multiple servers. This can be handily accomplished since the DSA issues are equal in nature, at any rate at the contingency and analysis situation levels. Dispersing DSA examinations makes the computational exhibition of a DSA system versatile with the number of servers utilized, thereby expanding the DSA handling power for large system models.

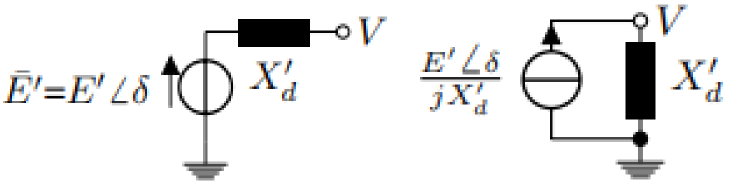
7. Automation and Reliability For on-Line DSA

On-line DSA systems should run continuously on a scheduled cycle, be set off by indicated system changes, or summoned physically. The system must be highly automated and be fit for finishing all tasks, drearily, under fluctuating conditions with practically zero human intervention. This demands high standards for the DSA software as well as functionalities with certain insight so as to give the necessary results. For instance, determination of suitable remedial actions may require the assessment of additional contingencies and/or system situations relying upon the security assessment results.

Dependability is another significant issue for an on-line DSA system. As represented in late power outages, the possible consequences of the inaccessibility of mission-critical software applications can be pulverizing. In addition to guaranteeing the organization of high quality software and equipment for an on-line DSA system, techniques, for example, repetition and self-recuperating ought to be considered to meet the dependability necessities.

8. Critical machine cluster identification using the equal area criterion

Stable and secure gracefully of electric energy is a crucial necessity of modern culture. So as to guarantee operation of the power system inside stability and security limits, the system operator is reliant on tools and techniques, which give situational awareness. Analysis that decide whether a system can stay inside the stability and security limits for a given arrangement of credible contingencies are alluded to as dynamic security assessment (DSA). A productive transient stability assessment (TSA) strategy is a significant part of a DSA toolbox. So as to arrive at real-time execution in TSA, approaches utilizing purported direct strategies are engaging. A large number of these strategies are utilizing the transient energy function, for example, the BCU technique, or the equal area criterion (EAC, for example, the EEAC strategy and the SIME strategy. The mentioned techniques utilizing the EAC are necessitating that the generators in the system are part into a group of critical generators likewise called critical machine cluster (CMC), which is the group prone to lose synchronism, and a group of non-critical generators. This stems from the assumption that regardless of how complex a system is the transient stability issue emerges from the separation of two generator groups. An early and dependable identification of the CMC is pivotal to empower right stability assessment. It is proposed to extrapolate the individual rotor angle trajectories utilizing a lot of measurements and for example Taylor arrangement expansion. The extrapolations are utilized to anticipate the individual rotor angles some time ahead. The anticipated rotor angles are arranged sliding and the holes between sections are evaluated. The generators are part into the critical and the non-critical group as indicated by the greatest angular hole. A list for grouping the generators, which is called angle increase it is a measure of the overall rotor angle change of an individual generator since fault clearance and concerning the normal difference in the rotor angles of all generators. In this paper another technique is proposed to recognize the CMC, which uses productive algorithms from chart theory. For that reason, a novel coupling coefficient is inferred, which speaks to the coupling strength between pairs of generators.



(a) Thevenin Equivalent **(b) Norton Equivalent**

Fig. 3Thevenin and Norton equivalents of generator

A new method is proposed to identify the CMC, which utilizes efficient algorithms from graph theory. For that purpose, a novel coupling coefficient is derived, which represents the coupling strength between pairs of generators.

Results for CMC Identification

- **Test system and scenario**

The power system model, utilized to test the introduced technique, is the New England and New York system. It consists of 68 buses and 16 generators. The loads are modeled as constant impedances and the generators are spoken to by a 6th request model in the time-domain simulation. All generators have a basic excitation and voltage regulation system just as a thermal turbine/governor model. Also all generators, however GEN 7 and GEN 14, are furnished with a power system stabilizer. To test the proposed technique three-phase short circuits on individual transmission lines were considered, which keep going for 250 ms and are cleared by opening of the breakers at the two finishes of the particular transmission line.

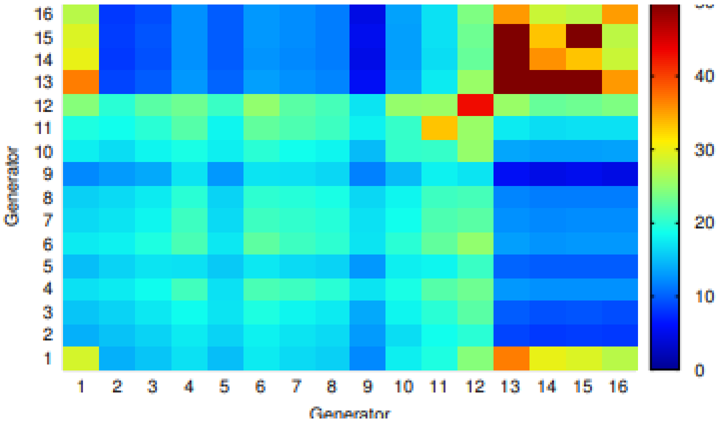


Fig. 4Coupling matrix computed in steady state initial conditions

- **Coupling strength at initial conditions**

In the accompanying the coupling strength matrix is figured for the pre-fault steady state conditions with the equations, the results are utilized to show the clear correlation of the proposed coupling coefficients and the structure of the power system. The coupling matrix in the underlying conditions is appeared in Fig. 3.12 The got coupling coefficients of the generators are contrasted with one another generally, where more prominent values, for example over 25, demonstrate a stronger coupling, while lower values, for example under 20, correspond to a more vulnerable coupling. Visual inspection of the chart permits recognizing designs, which may demonstrate a stronger coupling between specific generators. The coupling coefficients between the generators GEN 1 and 13−16 may recommend a tight coupling. In the one-line graph, which can be found in for example, it tends to be seen that the generators GEN 14 − 16 are close and very much connected. Besides, generator GEN 1 is strongly connected with two transmission lines to the area, which may disclose the strong coupling to this generator group. The generators GEN 4−8 and 10−11 appear to be firmly coupled also. The coupling strength of generator GEN 12 gives off an impression of being moderately high concerning all generators yet generator GEN 9. This could demonstrate that generator GEN 12 large affects all generators, which may likewise be clarified by its central location in the system. GEN 9 seems to have more vulnerable coupling to the other generators. This might be clarified by its remote location and the couple of lines connecting it to the remainder of the system.

9. Conclusion

The PAPER concerned the improvement of tools and strategies reasonable for a future on-line dynamic security assessment system. For that reason, the assumptions were the accessibility of a database, which contains definite models of the system components, and system previews, which give full discernibleness at a high testing rate, for example given from a quick state estimator or PMUs. Furthermore, it was accepted that because of the change in perspective in power system operation and the decreased consistency of generation and load designs, approaches dependent on large case and simulation databases, which are periodically produced off-line, are ominous. The ambition of the PhD project was to create on-line stability and security assessment techniques, which are free of such case databases. Therefore, approaches, which exclusively use on-line estimations and parameters, were picked or created. The consequences of the paper are techniques and tools, which birthplace from inside and out investigations of the hidden instability components. The attention was on first-swing transient stability. Critical machine cluster identification: In request to further improve the exhibition of the contingency screening and on-line TSA technique, another approach for ahead of schedule and precisely distinguishing the critical machine cluster was created. For that reason, a coupling coefficient was created, which is a proportion of the coupling quality between two generators.

References

1. JefBeerten& Ronnie Belmans 2013, ‘Analysis of Power Sharing and Voltage Deviations in Droop-Controlled DC Grids’, IEEE Transactions on Power Systems, vol. 28, no. 4, pp.4588-4597.
2. Wang Feng, Le Anh Tuan, Lina BertlingTjernberg, Anders Mannikoff& Anders Bergman 2013, ‘Cost Benefit Analysis of a Multi Terminal VSC-HVDC System using a proposed mixed AC/DC optimal Power flow’, 10th International conference on European Energy Market, pp. 1-8.
3. Priyank Srivastava, RashmiPardhi / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 3, May-Jun 2013
4. Stijn Cole ,Beerten, J &Belmans, R 2012 ‘Generalized Steady-State VSC MTDC Model for Sequential AC/DC Power Flow Algorithms’ IEEE Transactions on Power Systems, vol. 27, no.2 pp. 821 – 829
5. Aragüés-Peñalba, M, Egea-Àlvarez, A, Gomis-Bellmunt, O &Sumper, A 2012, ‘Optimum voltage control for loss minimization in HVDCmulti-terminal transmission systems for large offshore wind farms’, Electric Power Syst. Res., vol. 89, pp. 54-63.
6. Egea-Alvarez, A, Bianchi, F, Bellmunt, OG, Junyent-Ferre, A& Gross, G 2012, ‘Voltage control of multiterminal VSC-HVDC transmission systems for offshore wind power plants: Design and implementation in a scaled platform’,IEEE Trans. Ind. Electron., vol. 60, no. 6, pp.2381- 2391.
7. Bilal Hussain, Muhammad Usman, Affan Ahsan, Ahmad Talha and FarhanMahmood, “Improvement of Small Signal Performance of Multi-Machine Power System using SMIB based PSS and STATCOM Designs”, Emerging Trends and Applications in Information Communication Technologies, Communications in Computer and Information Science, Vol. 281, No. 3, pp. 188-199, 2012.
8. Vakula, V.S. and Sudha, K.R. “Design of Differential Evolution Algorithm-based Robust Fuzzy Logic Power System Stabilizer using Minimum Rule Base”, IET Generation Transmission Distribution, Vol. 6, Issue 6, pp. 121-132, 2012.
9. Komla A. Folly, “Population based Incremental with Adaptive Learning Rate Strategy”, Advances in Swarm Intelligence Lecture Notes in Computer Science, Vol. 7331, No.2, pp. 11-20, 2012.
10. Bera, P., Das, D. and Basu, T.K. “Analysis of Dynamic Stability of Power System using Thyristor Controlled Phase Shifter”, IEEE India Conference, Vol. 1, No. 3, pp. 102-109, 2012