Vulnerability Analysis and PMUs as Next Generation Protection System in Smart Grid

Kaveri Bhuyan
Department of Electric Power Engineering
Norwegian University of Science and Technology
Tondheim, Norway
kaveri.bhuyan@ntnu.no

Saibal Chatterjee
Department of Electrical Engineering
North Eastern Regional Institute of Science and Technology, Nirjuli-791109, Arunachal Pradesh, India
saibalda@ieee.org

Abstract—Vulnerability analysis in modern power systems is essential to mitigate cascading failures. This assumes prominence in the wake of permeation of information and communication technologies in the operation of power systems. Most research works have focused on vulnerability analysis of either general interdependent infrastructure systems or power systems. As a part of this work, it will be of interest to identify the existing approaches in vulnerability analysis in power systems as well as ICT infrastructures. Phasor Measurement Units (PMUs) are typically used in Wide Area Measurement (WAM) systems to predict and prevent cascading failures. The role of PMUs in preventing cascading failures because of interaction between ICT and the power grid in future Smart Grid is reviewed.

Keywords—Cascading failures; ICT; Protection system; Smart grid; Wide area monitoring; Vulnerability

I. INTRODUCTION

Our future electrical power grid is Smart grid. It is smart in the sense that traditional power grids will have digital technology with upgraded energy infrastructure. Smart grid is defined by IEC strategic group SG3, in [1] as “the concept of modernizing the electric grid. The Smart Grid is integrating the electrical and information technologies in between any point of generation and any point of consumption”. Power systems will interact with advanced technologies such as information technology, wireless and mobile devices, sensor and control systems, etc. to provide more flexible, smart, self-healing, resilient, and efficient power grid. Interdisciplinary interdependence and interoperability are the key domain areas in smart grid.

Such a complex interdisciplinary network consisting of millions of interconnections are exposed to many security risks and vulnerabilities. Majority of the disruptions or outages in power grids occurs when failure in one infrastructure amplifies and worsens the severity of failure in terms of restoration time etc. or when multiple infrastructures are disrupted simultaneously or due to geographic interdependency or natural disaster. It is observed that in the event of cascading failure, failure of nodes in one network can lead to failure of dependent nodes in other networks and the system reliabilities could decline as much as 95% [2]. Few examples of cascading events are line tripping due to loss of synchronism, generator tripping due to abnormal voltage and frequency system condition, and under frequency or under voltage load shedding etc. Owing to extremely catastrophic, unpredictable nature, and high probability of occurrence, the study of effect of cascading failures in the risk and reliability assessment of complex infrastructure systems is only taken into account in this work. The motivation for the work presented in this paper is to gain knowledge of vulnerability analysis within combined ICT and power systems. This can form the basis to investigate the possibility of new types of security risks and threats in the complete interconnected complex grid. The main objective of this work is to understand the interactions and interdependencies of ICT and power systems and create a framework for the dependability and reliability analysis.

This study has been organized as follows: Section II presents a survey of the most relevant scientific studies investigating the vulnerability analysis concerning power systems and ICT. Further, section III describes the Phasor Measurement Units (PMUs) typically used in Wide Area Measurement (WAM) systems to predict and prevent cascading failures. An important aspect of this investigation is to understand the role of PMUs in preventing cascading failures because of interaction between ICT and the power grid in future Smart Grid. Section IV discusses standards very briefly followed by conclusions on the study with future research needs in section V.

II. VULNERABILITY ASSESSMENT

Vulnerability can be caused by the internal and external sources to the infrastructure like natural disasters, system instability or equipment failures. Customer security, greater number of intelligent devices, physical security, lifetime of power systems, using Internet Protocol (IP) and commercial off-the-shelf hardware and software, more stakeholders etc. are some of the most common types of vulnerabilities in smart grids [3].

Cascading failures in power system networks are an important cause of blackouts. Vulnerability is an essential indication of a system prone to cascading failures [4]. To prevent or reduce catastrophic failures, it is of utmost importance to identify the cause of failure instantly and initiate
The classical way of determining the cascading failures in power system permits only local, control actions based on network topology and measurements at the substation equipment or transmission lines. The network structure defines the topology and their attributes while operative state of the network defines the load flow. Most of the recent research on vulnerability analysis is based on classical and detailed physical models. It ignores the essence of electric power flow or operative states. A new topological approach with net-ability and entropic degree is proposed in [5]. The proposed metric takes into account the structural and operative states of power grids. Generally, Power flow analysis using N-x contingency analysis, graph analysis and probability analysis are performed on (quasi-) steady-state model of the power system for assessing the vulnerability and analyzing the cascading nature of the events [6]. The key challenge in using N-x contingency analysis is to apply modern computing techniques and hardware to investigate multiple simultaneous contingencies within the time constraint.

Southern company has developed an industrial tool named TRELSS (Transmission Reliability Evaluation of Large-Scale Systems) to identify cascading failure problems and evaluate the transmission reliability of large scale systems [7]. It has the advantages of providing both ac and dc network models, screening multiple initiating contingencies, simulating the cascading process, evaluating the system impacts, ranking the cascading scenarios based on their severity and likelihood, and identifying the tap contingencies that require primarily attention.

The effects of blackouts can be catastrophic. Cascading failure in a dynamic transmission system model was examined by Carreras et al. [8]. They analyzed the different transitions namely, limited generator capacity and transmission line flow limits and the characteristic properties of the distribution function of the blackouts near the critical points. This was essential for modeling the power transmission systems and analyzing the cascading failures.

Nedic et al. [9] examined the critical transition phase for a 1000 bus network with an AC blackout model. The blackout model represented the behavior a power systems against disturbances like cascade and sympathetic tripping of transmission lines, heuristic representation of generator instability, under frequency load shedding, emergency load shedding etc. They demonstrated considering critical loading as a reference point for assessing risk of cascading failure. The main contribution from their risk analysis was obtaining the probability distribution of blackout size. The security margins calculated using deterministic criteria sometimes give incorrect results under some operating conditions. To determine accurately the margin of security, probabilistic analysis should be performed. Monte Carlo simulation was used to model Time Dependent Phenomea (TDP), such as cascade and sympathetic tripping, transient stability, and weather effect in the computation value of security [10]. Hidden failures in power system are known to inhibit the proper operation of relay against the disturbances. These failures remain inactive during normal operation but become active during system disturbances. Tamronglak et al. [11] modeled hidden failures of protection systems using a probabilistic approach. They were successful to identify the vulnerable regions within which the hidden failures may be active. The sensitivity of power-law behavior against system loading level, hidden failure probability, spinning reserve capacity and control strategy and the corresponding blackout mitigation are investigated using WSCC 179-bus equivalent system and the IEEE 118-bus test system in [12]. Another probabilistic model was proposed by Dobson et al. [13] to study the effect of system loading on cascading failures. Strategic Power Infrastructure Defense (SPID) system was proposed in [14]. SPID could capture essential information in real time, assess system vulnerability quickly, and perform timely self-healing and adaptive reconfiguration actions based on system-wide analysis. A probabilistic model of cascading failures called CASCADE was proposed in [15]. This model described the cascading failure in components that fail when their loads exceed a threshold. Another model of loading dependent cascading failure was proposed by Carreras et al. [16]. The model results showed how system loading can influence the risk of cascading failure.

According to it, the power grid is a complex network in which electricity is exchanged between nodes through the shortest or most efficient path. In 1998, Watts et al. [17] proposed the "Small-world network". After this discovery, using metrics and complex network (CN) theory for the structural analysis of transmission grids against vulnerabilities was accelerated [5]. Vulnerable lines in a power network were identified using complex network theory in [18]. They have proposed a new index called "Betweenness" based on their position in the network and the power flow analysis of the transmission lines to detect vulnerable lines in IEEE 39 Bus and IEEE 118 Bus systems. Effective Graph Resistance approach was employed to investigate vulnerable lines in [19]. The effective graph resistance method was successfully used to identify the critical transmission lines in IEEE 118 buses power system. Based on complex networks theory, a dynamic model of cascading failures in the power grid was developed [20]. They have proposed a metric (RCF) to assess the robustness of power grid considering the effects of both structural properties as well as operative state. Complex network theory has provided a new direction to vulnerability analysis of power grids. Zhang et al. [21] proposed a practical model of power grid based on complex networks theory considering the active and reactive power loads with the locally preferential load redistribution rule. Sachjen et al. [22] proposed a power transmission model which provides insight into the nature and probability distribution of disturbances in a real complex power system. Wei et al. [23] proposed a cascading model under a load preferential redistribution rule (LLPRR). In this rule, the load on the failed node is redistributed to its neighboring preferential nodes according to the preferential probability, namely, among these neighboring nodes, the one with a higher degree undertakes more shared load [21].

Failure in the system occurs when the service does not implement the system function. A detailed taxonomy of failure modes is presented in [24]. They have described fault-error-failure model to understand the various threats that may affect a system. Few other potential effects that may confer
vulnerability to the interdependent ICT system are identified in [25] namely:

1. Catastrophic effects: They affect the monitoring or control systems leading to cascading failures. There will be interaction between the ICT and the current carrying part.
2. Degrading effects: They are responsible for degrading the system performance by inefficient utilization of resources. This failure would only degrade the ability of the system to make maximum use of the current carrying part.
3. Local effects: There area of influence is local in nature and are limited both in duration as well as impact.

Depending on the response, [26] has classified failures into passive and active types.

1. Passive failure: The device does not respond spontaneously when required.
2. Active failure: The device starts malfunctioning and does not work as intended.

These failures are not always independent but are correlated and occur as simultaneous or/and combinational failures. Thus, in order to understand the risk of failures, it is utmost important to analyze the interdependencies. The role of ICT in intelligent monitoring and control system to increase system reliability and security is highly impactful. Apart from failures in power systems and ICT infrastructures, malicious attacks and threats in ICT infrastructure and their consequences should also be analyzed for vulnerability assessment.

Most of the proposed reliability analysis models did not take into account the interactions and interdependencies between the power systems and the ICT infrastructures. However, few recent studies done like by Kirschen et al. [27] have considered the influence of ICT on the overall dependability of power systems. They proposed a framework for analyzing the effect of failures in the information infrastructure on the quality and reliability of the electricity supply. Laprie et al. [28] described and analyzed the behavior of ICT and power systems taking into account the effect of failures of each infrastructure on the other one using qualitative models. Their model also considered accidental failures and malicious attacks in ICT infrastructure. Smart grid dependencies have been studied using structural models like reliability block diagrams and dynamic models like Markov models [29]. An overall reliability and security assessment process for the electric power communication network using a three-level hierarchical architecture is proposed in [30]. The assessment results showed better protection and regulation in ICT and the power systems. A meta-model for identifying interdependencies and failure types in combined power systems and ICTs has been proposed in [26]. Vanfretti et al. [31] have proposed an open modeling equation-based approach 'Modelica' to solve the inconsistencies while using the dynamic models and time-domain simulation for power systems across different simulation platforms.

The cyber-physical nature of the smart grid places greater demand to model future vulnerabilities for power system operation and management. The review of state-of-the-art of vulnerability analysis emphasizes the importance of analyzing the power systems and ICT together in a single model for overall assessment of reliability and quality. Thus, addressing the dependability issues in the ICT infrastructure, the power systems and their interactions is crucial for failure analysis in both systems operating with close interactions in the smart grid.

III. ROLE OF PHASOR MEASUREMENT UNITS (PMUS) IN PREVENTING CASCADING FAILURES

SCADA (supervisory control and data acquisition) systems are implemented to monitor and control electrical power grids in present power grids. To improve wide area observability and controllability, many emerging technologies like PMUs, advanced visualization, high-performance computing (HPC), and data mining has been proposed [6]. This section reviews the role of Phasor Measurement Units (PMUs) in preventing vulnerabilities.

Wide area monitoring, protection and control systems (WAMPACs) based on time synchronized phasor measurements provide real time measurement data to monitor and provide control. Real time data visualization provides a clear picture of the current status of the system and based on the real time measurement information, remedial action schemes to improve the power system security can be directly incorporated and implemented.

Even though the PMU is in its development stage, its technology is maturing. Several countries like Brazil, Baltic, China, France, Japan, Korea, Mexico, Norway, the United States etc. have installed PMUs on their electrical systems [32]. The basic building block of a WAM system is the Phasor Measurement Unit (PMU). It measures time synchronized voltage and current phasors at any location in the power system through Global Positioning System, GPS time stamping. The synchrophasors of PMU measurements are collected, processed or stored in Phasor Data Concentrators (PDCs) for further use in protection and control systems. By installing PMUs in strategic points, we can have an overview of the system frequency, power oscillation and voltage stability monitoring over a wide area. Monitoring the synchronized phasor data at multiple locations in a transmission system can help to identify potential cascading failures.

Sun et al. [33] proposed a scheme based on phase-space visualization and pattern recognition to predict potential instability or cascading failures. The proposed scheme monitors PMUs measurements and analyzes the dynamic patterns using the knowledge obtained through offline learning. PMUs have been extensively used for analyzing dynamic phenomena like voltage stability and the damping of power oscillations over wide geographical areas. The PMUs are embedded in the system protection terminals (SPT) and used for long-term voltage stability prediction [34].

PMUs have been used to improve the overall stability of the Hydro-Quebec’s transmission system through
supplementary modulation of voltage regulators [35]. Kjetil et al. [36] applied PMU measurements to detect power oscillations in terms of amplitude, frequency and damping of the dominant modes in the Nordic transmission system. Robustness of the PMU measurements was evaluated for 420 kV Norwegian bulk transmission grid by Leirbukt et al. [37].

In another application, PMUs have been used for improving selectivity of the generator dropping controls at the Colstrip power plant - Acceleration Trend Relay (ATR) [35]. The main purpose of this study was to evaluate the potential benefits and feasibility of phasor measurements for the Colstrip stability controls. State estimation in power grids is about estimating voltage phasors at all nodes, and thus providing a valid power flow solution. PMU directly measures voltage phasors and overcomes the task of state estimation. Another promising application of PMU is detection of impending instability during transients. PMU control has been demonstrated in [38] to detect and trigger remedial actions against the transients.

IV. STANDARDS

There is a need for standardization of smart grid for interoperability, transmission, distribution, metering, connecting consumers and cyber security. Recently initiatives have been taken around the world by International Society of Automation (ISA), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), and NIST (US National Institute of Standards and Technology) etc. to define the standards and write guidelines on how the smart grid should operate using the latest technology in power engineering, control, communications, and information technology. IEC has identified more than 100 standards related to the field of power generation, distribution, control, protection, information and communication technology etc. [39]. For example IEC 61850 is a standard for the design of electrical substation automation. It consists of several parts and provides guidance on how systems for monitoring, protection and control are designed, operated and maintained. The IEC Common Information Model (CIM) is recognized as a core standard, supporting electricity transmission system interoperability [40]. There is a huge need for interoperability standards that will allow equipments to work with each other at every level. Cyber-security threats have been a matter of concern as these can exploit the increased complexity and connectivity of critical infrastructure systems, and posing risk to the entire network. Manufacturers and utilities should be well aware of the mature standards, best practices and regulatory guidelines while designing and applying to smart grid systems. The risk-based cybersecurity framework have been developed to address the involved threats and risks and apply the principles and best practices of risk management by assembling international standards, guidelines and practices [41]. With the smart grid standard mapping online tool (www.smartgridstandardsmap.com), it is possible to identify instantly any given standard in relation to its role within the Smart Grid.

V. CONCLUSION

The current situation exhibits a number of major challenges in smart grid networks. Considerable research effort are needed to study the new types of threats and failures, online analysis tools, wide-area monitoring, measurement and control, design new security solutions, better protection and regulation of power systems, improve stability, etc. are needed to improve reliability of the power networks. This work has presented an insight into the analysis of vulnerability assessment in interconnected and interdependent infrastructures concerning power systems and ICT. The knowledge of existing approaches for vulnerability analysis and their modeling are important to develop better tools for planning, operation and control of the power system dynamics at various voltage levels in Smart Grids. It is concluded that PMUs can significantly improve the observability and controllability of the power system dynamics. Applications of PMUs are emerging and more efforts are needed to develop methods to identify, filter, extract, and aggregate useful information from the PMU data. Future work will focus to develop methods which can consider these factors in cascading failure analysis. Attempts will be made to investigate interactions and interdependencies and propose a model for evaluating the reliability of Smart Grids. The developed model will define preventive and corrective actions taking into account the overall system structure, interaction of systems, dependability, information security and dependability, and system dynamics.

Acknowledgment

This work was carried out during the tenure of an ERCIM Alian Bensoussan Fellowship Programme.

REFERENCES


