View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Online Research Database In Technology

Technical University of Denmark

A Review of Cyber-Physical Energy System Security Assessment

Rasmussen, Theis Bo; Yang, Guangya; Nielsen, Arne Hejde; Dong, Zhaoyang

Published in:
Proceedings of 12th IEEE Power and Energy Society PowerTech Conference

Link to article, DOI:
10.1109/PTC.2017.7980942

Publication date:
2017

Document Version
Peer reviewed version

Link back to DTU Orbit

Citation (APA):
Rasmussen, T. B., Yang, G., Nielsen, A. H., & Dong, Z. (2017). A Review of Cyber-Physical Energy System Security Assessment. In Proceedings of 12th IEEE Power and Energy Society PowerTech Conference IEEE. DOI: 10.1109/PTC.2017.7980942

DTU Library
Technical Information Center of Denmark

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

A Review of Cyber-Physical Energy System Security Assessment

Theis B. Rasmussen,
Guangya Yang, Arne H. Nielsen
Department of Electrical Engineering
The Technical University of Denmark
Kongens Lyngby, Denmark
thras@elektro.dtu.dk

Zhaoyang Dong
School of Electrical and Information Engineering
The University of Sydney
Sydney, New South Wales, Australia

***Abstract*—Increasing penetration of renewable energy resources (RES) and electrification of services by implementing distributed energy resources (DER) has caused a paradigm shift in the operation of the power system. The controllability of the power system is predicted to be shifted from the generation side to the consumption side. This transition entails that the future power system evolves into a complex cyber-physical energy system (CPES) with strong interactions between the power, communication and neighboring energy systems. Current power system security assessment methods are based on centralized computation and N-1 contingencies, while these risks should still be considered in the future CPES, additional factors are affecting the system security. This paper serves as a review of the challenges entailed by transforming the power system into a CPES from a security assessment perspective. It gives an indication of theoretical solutions to CPES challenges and proposes a new framework for security assessment in CPES.**

***Index Terms*—Communication system, cyber-physical systems, distributed power generation, power system security, security assessment.**

I. Introduction

The recent increase in implementation of generation based on renewable energy sources (RES) such as wind and solar, together with an increased focus on mitigating emission of greenhouse gasses in services such as transportation, through electric vehicles (EVs), and domestic heating through heat pumps (HPs), have led to a complex layout of the future power system [1]. Integrating these technologies into the power system changes its topology from being centralized with a few large controllable synchronous generators to being decentralized with numerous distributed generating (DGs) units based on intermittent energy sources [2]. In order to manage the decentralization of the power system, smarter monitoring and control techniques are required. This issue is addressed by implementing an advanced metering infrastructure (AMI) through smart meters and phasor measurement units (PMUs), as well as a further utilization of information and communication technologies (ICT).

ICT helps improve the visibility of current power system operation and enhances the possibilities of advanced control processes [1]. The ICT network build around the power system becomes more and more integrated and the whole system is transitioning into a complex cyber-physical energy system (CPES) [3]. The strong interactions across systems in a CPES entails new challenges in maintaining a high security of supply, as new factors can affect the general security of the power system. Such factors include cybersecurity, behavior and constraints of neighboring energy systems, and the dynamics of interactions between the different systems [4]. In order to acknowledge security threats from ICT and neighboring energy systems, a revisit of current power system operation methods is necessary.

Power system security assessment plays a central role in maintaining a high security of supply. However, it is based on a centralized power system and does not consider the threats entailed by the transition towards a CPES. The aim of this paper is to review the power system security assessment method from a CPES perspective. This review includes a description of the current security assessment method, a presentation of operational factors of CPES to be considered, a discussion of challenges of the current security assessment method entailed by CPES, and propose a new framework for future CPES security assessment.

Section II introduces the current power system security assessment method and the three key factors, safety, security and sustainability, of cyber-physical system (CPS) operation. Section III discusses CPES challenges of the current security assessment method, section IV presents a new framework for CPES security assessment based on the discussion in section III and emerging methods and philosophies. Section V concludes.

II. CPES Transition

Kundur et al. [5] have defined power system security as the degree of risk in its ability to survive imminent disturbances without interruption of customer service. In order to ensure a high level of supply security, power system operators need to verify operational properties in its continuous operation and in the event of a disturbance that can change the operational environment. If a disturbance is expected to interrupt or limit the supply, the power system operators are required to change the operation of the power system in order to secure the system from such a disturbance [6].

A. Power System Security Assessment

The starting point of the continuous process of security assessment is the monitoring phase as shown in Fig. 1. Depending on the measuring devices, a supervisory control and data acquisition (SCADA) network, PMUs or a combination of both, measurements are taken and send to the control center every few second or millisecond. The measurements include physical properties such as system frequency, bus voltages, equipment thermal loading and generator rotor angle displacement as well as load and generation levels [6]. After measurements are received by the control center, operational constraints are verified. This process takes place in the alarm-phase shown in Fig. 1, where a few constraint examples are listed [6].

Every few minutes, the measured data are used by the power system operators to perform the contingency analysis shown in Fig. 1. The contingency analysis is based on the N-1 criterion and involves simulating a model of the power system, where one component is taken out of operation, through a load flow calculation to see how the power system reacts to such a disturbance. Ideally, power system operators should simulate all possible contingencies in order to ensure power system security. However, the computational burden of simulating the power system model is too extensive. Therefore, power system operators identify and simulate the most critical contingencies and assume the remaining possible contingencies have limited effect on the power system [7].

As shown in Fig 1, the results from the contingency analysis are used to check power system operation in case of a disturbance. This check is performed in the alarm-phase of Fig. 1, where operational values are compared to power system constraints. If either current operation or a disturbance can cause operational constraints to be violated, power system operators need to perform preventive control [6]. Power system operators can perform different actions in order to satisfy operational constraints, some of them are listed in Fig. 1.

The current security assessment displayed in Fig. 1 is highly dependent on valid measurements and accurate computations in comparing operational limits and calculating load flow. In this way, the power system already has strong relations to the operation of the ICT network and depends on the reliable operation of the CPES as a whole.

B. CPS Safety, Security and Sustainability

In recent years the classification of CPS has emerged in different technologies such as health care, smart energy and industrial control systems [8], [9]. In CPS, there is a general understanding of three key factors that has to be preserved in order for CPS to function as intended. These factors are referred to as S3, and consist of safety, security and sustainability. The complexity of the power system transition towards a CPES is illustrated in Fig. 2. First of all, CPS safety is characterized as avoidance of hazards that can interrupt the CPS operation [3]. These hazards are the result of different interactions within the CPS symbolized by the blue dobble arrows in Fig. 2.

In CPS there are intended and unintended interactions between the different systems, where intended interactions are created to improve the CPS operation and unintended interactions are caused by changes in the different system environment that can have a harmful effect on the system operation [3]. Furthermore, researchers distinguish between three different types of interactions, inter-physical, cyber-physical and inter-cyber interactions. Each of these types can have both intended and unintended interactions [3]. As the power system transits towards a CPES with numerous interactions, the reliability of electricity supply depends on CPS safety in avoiding all serious hazards.

CPS security is characterized as assurance of integrity, authenticity, and confidentiality of information, which can be understood as ensuring the cybersecurity of the ICT system in the CPES from unauthorized access [3]. As the future power system will rely on a complicated ICT system to monitor and control the operation of future CPES, the security and validity of the data transmitted in the communication network and processed in the information network becomes an important factor to consider [10]. In Fig. 2, the security of the CPES is represented by a cyber-perimeter which objective is to block hackers who try to access the CPES.

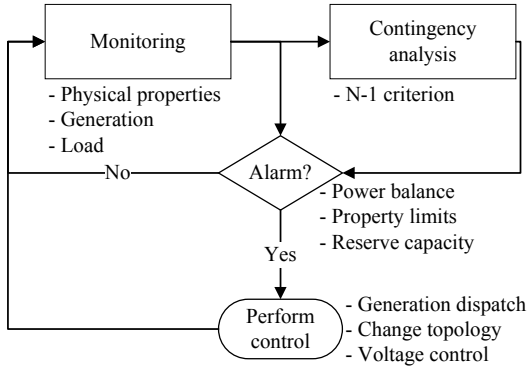

Fig. 1. Flowchart of current power system security assessment method.

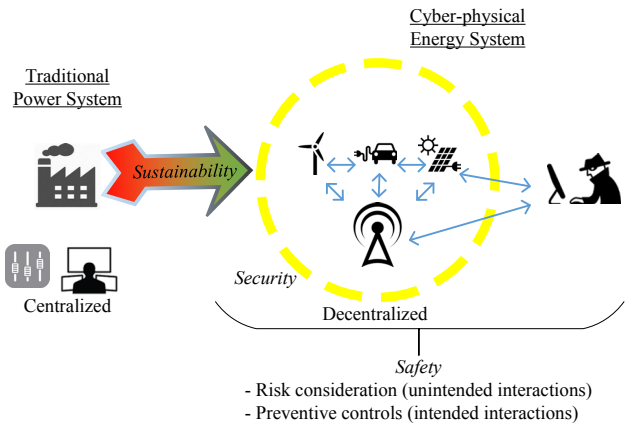

Fig. 2. Power system transition towards a cyber-physical energy system.

The last of the entities in S3, required for ensuring intended operation of CPS, is sustainability which is characterized as maintenance of long-term operation of CPS using environmental friendly sources of energy [3]. From a power system perspective, the motivation for transitioning the power system into a CPES is to enable an efficient integration of RES into the generation part and environmental friendly alternatives to services into the consumption part of the power system. Therefore, you could say that sustainability is an inherent part of the future power system through the decentralization of generating units, which is illustrated by the arrow in Fig. 2. In order to ensure CPES sustainability, the power system needs intelligent control and monitoring processes from the ICT system because of the intermittent nature of distributed energy resources (DERs).

III. Security Assessment Challenges

The main challenge of the current security assessment method is the decentralization of generating units and interactions between the power system and an ICT network, which changes the landscape of the modern power system. This change affects the requirements of power system operational methods that help operators maintain a high security of supply illustrated by the transition in Fig. 2. From the characterization of a CPES based on S3, it is apparent that each phase of the current security assessment method in Fig. 1 becomes insufficient, as a method of securing the electricity supply in the future.

A. Monitoring

In section II the monitoring phase of security assessment is described as providing the power system operators with the visibility of the current operational status. In this way ensuring the validity of the acquired data is extremely important in operating power systems. With the transition towards a CPES, monitoring the current power system operation becomes increasingly challenging. In recent years, researchers have investigated the possibility of ICT cyberattacks with false data injection into a CPES, that can result in an inaccurate picture of power system operation [1], [11], [12].

In [11] the authors concluded that the current practice of bad data detection (BDD) to ensure data validity is insufficient as knowledgeable attackers can inject data which evades BDDs. Additional cyber-attacks, such as replay attacks and denial of service (DoS) attacks, that can affect the visibility of the power system are described in [13].

The DoS attacks are not the only challenge that can cause congestion of communication channels [14]. As more and more electronic devices have communication capabilities as an inherent part of their design, a larger amount of data is communicated and bottlenecks in the ICT network can occur.

By considering the power system as a dynamic physical system, communication latency and interruptions can affect the validity of the current power system operation shown at the control center. Additional challenges are entailed by the increase in the amount of data, which puts additional performance requirements for control center computers to process the data and give relevant and valid information of current power system operation in a timely fashion [1].

B. Contingency Analysis

The contingency analysis in security assessment serves to increase the security of supply by acknowledging possible disturbances that can affect the power system dynamics. As described in section II, the current practice is to investigate possible power system equipment outages that have the largest impact on the continuous operation [5], [6]. In the CPES, the power system will have strong interactions with neighboring energy systems such as the transportation, waste treatment and domestic heating system [15].

These systems operate in ever changing environments which complicate the contingency analysis by increasing the number of possible disturbances with unknown severity. The uncertainty lies in the operational environment of neighboring energy systems, which indirectly affects the operation of the power system. The operation of neighboring energy systems are limited by a set of technical, environmental and governmental constraints. Reaching these limits during operation can disturb the CPES by limiting its controllability.

As more end-user services are electrified, the CPES has more interactions with energy systems affected by end-user irrational behavior. Even though power system engineers are trying to implement control of end-user consumption, there is no certainty that end-users will behave rational and always remember to plug-in EVs as an example. Additional uncertainty is introduced as more intermittent DGs are installed. Thereby the power system becomes more dependent on the weather system, which increases the operational uncertainty further.

In the CPES, the power system and the ICT network are interdependent, meaning a loss of power supply at a substation or load bus affects the ICT equipment and when the ICT network fails control, computation and monitoring actions becomes disabled. This cascading behavior has previously been the cause of a major blackout which happened in Italy in 2003 [16]. From this interdependence the complexity of determining possible contingencies increases further. Not only physical power system equipment failure can cause disturbances, but also failure of ICT network equipment.

The increasing interactions between ICT and the power system was visualized in December 2015 when hackers gained access of a part of the Ukrainian power system control center and caused a region wide blackout [18]. Such an extreme interference raise new questions to the security of the future power system as a CPES [4], [10], [19] and adds an additional contingency to the contingency analysis pool in the form of outages of region wide SCADA networks.

Additional risk is present in the power system control equipment, as a large number of the distributed units, have autonomous control abilities. If hackers gain access to them, they can change the control of these equipment to perform harmful instead of helpful actions [9], [17]. These contingencies apply a whole new level of risk and complexity in the

security assessment not considered in the current formulation of the method.

From this short discussion of contingencies introduced by the transition towards a CPES, the sheer number and variety of possible contingencies is evident. The current contingency analysis is based on the N-1 criterion, but with the increasing number of interactions between systems in the CPES, predicting the possible contingencies and their impact becomes even more complicated than previously.

C. Preventive Control Actions

As the power system have previously been a centralized physical system based on large generating units, the protective actions have been performed by performing a constrained economic dispatch where contingency impacts are considered [5], [6]. However, due to the decentralization, a growing interest in the research community has focused on the paradigm shift where regulating actions are shifted from the generation side to the consumption side.

This paradigm shift has resulted in numerous possible control actions performed by distributed equipment that help improve the operational status of the power system in a continuous fashion. Examples of these include static VAR compensators, inverters with droop control and active power storage devices. However, as previously described, these devices are vulnerable to unauthorized access where either the control methods can be altered or false data can cause internal control loops to perform undesirable control actions. Besides the risk of cyber-attacks, the autonomous control capabilities can also misbehave due to non-considered events as has been seen on November 4, 2006, where a major European blackout occurred. When the frequency increased beyond the safe operation range of the wind farms in the Northeastern part of Germany, they disconnected. When the operators managed to improve the operational status of the power system and lowered the frequency, the wind farms reconnected and forced a recurring increase of system frequency [20].

In the consumption side of the power system, new methods for controlling consumption have emerged. Most popular is the demand response (DR) method, where household appliances and electrified services can be controlled to change consumption to balance the power system [21]. However, compared to the traditional economic dispatch, where a relative few number of units have to be coordinated, the DR method includes controlling thousands, if not millions, of distributed units. Therefore, the complexity of performing protection actions of power systems increases rapidly [1], [15].

Furthermore, when all these distributed units are capable of providing control which should help ensuring the security of supply, further cyber security risk can be considered as unauthorized personal can enforce protective control actions when not required. An example is in the case of smart meters, which are predicted to be distributed to all households in most countries to enable real time pricing. These smart meters are equipped with a control capability which allows the utility company to disconnect the households from the grid, this method is known as load shedding. If hackers gained access to such a control mechanism, the protective nature of load shedding could be turned into a disruptive action instead [22].

IV. CPES Security Assessment

From the discussion of challenges and limitations of the current security assessment method in section III it is apparent that a revisit of the traditional method is needed when considering the transition towards a CPES shown in Fig. 2. An updated security assessment method for CPES should consider both interactions between the power system and neighboring energy systems as well as the ICT network and the risk of cyber-attacks.

A summary of all challenges described in section III are divided into each phase of the security assessment shown in Fig. 1 and are shown in Table I. In this section a description of different technologies and methods that could help transform the security assessment method and make it useful in the future CPES. In this way, the aim of the current security assessment will stay the same, but the means of achieving this aim will change. Following the Ukraine blackout in December, 2015, cybersecurity of power systems has been a hot topic for both ICT and power system researchers [18]. The research focus is further emphasized after the North American Electric Reliability Corp. (NERC) has announced an update of their grid codes from July 2016. The updated grid codes demand that power system operators change the current methodology of creating a cyber-perimeter to avoid unauthorized access, to actively perform intrusion detection and prevention [23].

TABLE I
Challenges for power system security assessment

Phase	Challenge	Solutions
Monitoring	Cyber-attacks	IDS
	Communication congestion	DI
	Large data quantity	Big data
Contingency analysis	Neighboring system constraints	RMP
	Neighboring system uncertainty	RMP
	Interdependence	IA
	Unauthorized control	IDS
	SCADA outage	RMP
	Determining worst case	DC
Preventive control actions	Recurring autonomous control	Coordination
	Cyber-attacks	IDS
	Large-scale economic dispatch	DO

Already at the time of writing, there exists numerous different intrusion detection systems (IDS), some of which are explained in [9]. By implementing IDS into the CPES security assessment method as additional cyber security measures, the general CPS security increases as the monitoring and communication network is less vulnerable to unauthorized access. As seen in Table I, the implementation of IDS could help counteract challenges in all phases of the security assessment method.

In [1] the possibility of distributing calculations and decisions making in the ICT network is introduced. The authors propose utilization of the increased computational capacity of integrated electronic devices (IEDs) to decentralize parts of the control and computation responsibilities. By implementing distributed intelligence (DI) into parts of the CPES, additional challenges in Table I can be solved. In the monitoring phase, DI can help analyze and filter data to limit the communication channel congestion.

In the preventive control phase of security assessment, distributed optimization (DO) can help by locally calculate the required control actions that help balance the power system in its current operation and against disturbances. By utilizing DO, the number of units in the large-scale economic dispatch decreases which increases the computational speed. Furthermore, in the contingency analysis phase, the determination of worst case scenarios could be partially solved as the combined computational power would increase when utilizing distributed computation (DC). This means that a larger number of contingency situations can be investigated.

In recent years researchers have looked into the Internet of Things (IoT) and the concept of big data [24]. The utilization of these technologies is widespread and could potentially be applicable to the power system. As more and more data is generated and available, a number of big data computational tools have been developed which can help scientists in processing large scale data. In the monitoring phase of security assessment, a challenge is the large amount of available data and how to process it safely without losing important signals or alarms. Therefore the authors propose an investigation of big data computational tools, such as machine learning and clustering, applied to SCADA and PMU data [24]. The aim is to improve the visibility and ease the preventive action decision process.

The power system is not the only large scale system that is facing problems and threats through strong interconnections with ICT. For several years, industrial control systems have recognized the risk of unauthorized personnel access due to the growing digitalization of monitoring and actuating devices. The common practice of industrial cyber security starts by consultants performing a risk assessment (RA) of the current control system. From this point security measures such as encryption and certification of programmable logical controllers (PLCs) are implemented [25].

In industrial control systems, the scale is somewhat small compared to the power system. In the CPES, new devices are implemented continuously and their sheer number is too large for encrypting the whole network. Therefore RA in the power system should be implemented as a continuous process as part of a risk management process (RMP) [25].

The RMP contains different steps where the context of the system is analyzed to provide an overview of intended operation. After a context establishment, RA is performed which consists of a risk identification, risk analysis and risk evaluation process. These processes give an overview of the current security threats and their impact. If such a RMP could be done in a continuous fashion for the cyber risk in the CPES, the SCADA outage challenge in the contingency analysis in Table I could be treated.

A RMP can also be developed to analyze the threats posed by neighboring energy systems and their changing environment. For example an identification of possible changes in the neighboring energy system environments could be performed utilizing system specific techniques such as weather forecasts, seasonal or daily variations in transport requirements etc.. The impact of these risk can then be analyzed and evaluated in a similar fashion as cyber risk, which could be useful for treating the neighboring energy system constraints and uncertainty challenges of the contingency analysis parts of Table I.

The topic of interdependency have previously been covered by [16] and [12]. In the latter, the effects of having backup power supply to control centers in the ICT network is investigated. The process of a interdependency analysis (IA) in the CPES can be applied in the CPES security assessment method and give indications of large scale contingencies and their combined impact in the power system and the ICT network. The integration of such an analytical tool could solve the interdependence challenge in the contingency analysis in Table I.

In case of a fault in the power system or unsustainable operating conditions, autonomous control units can help providing fast regulating actions. However, as mentioned earlier they can also worsen the problem due to build-in control action constraints. In order to ensure fast recovery from a fault, it would make sense to analyze the behavior of autonomous control units in normal and abnormal operating conditions and coordinate the control of these units in case of abnormal operating conditions, the implementation of fault coordination is shown in Table I for the recurring autonomous control challenge in the preventive control action phase.

A. Proposed framework

The discussion on problems faced by the current security assessment method in Section III. and the possible theoretical solutions presented in Section IV. is used as the base of a framework for CPES security assessment presented in the following. The general idea of the new security assessment framework is to distribute the process of monitoring, contingency analysis and preventive actions decision to the distribution level.

In the CPES, the distribution network is diverse and ranges from substations connected to distributed generation such as wind farms, to substations connecting residential areas with both generation and consumption. The CPES security assessment method is based on an implementation of IEDs at a substation level. At this level, the IEDs will perform the tasks presented in Fig. 3. In Fig. 3 the monitoring task is preceded by an intrusion detection task, the type of IDS at each substation can vary according to the operational environment. After the signals measured in each substation area is validated by the IDS, the IED observes whether the measured values are within operational limits. By performing this verification

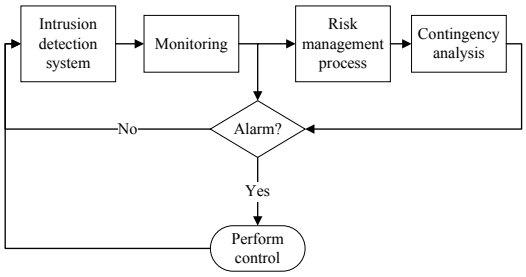

Fig. 3. Proposed framework of security assessment of future cyber-physical energy system.

on a substation level, less data is being transferred to the main control centers and the risk of communication channel congestion is lower.

As in the original security assessment method, the IEDs will assess the security of the system by including faults and disturbances, that can happen in each distinctive area, in the contingency analysis task of Fig. 3. Prior to the contingency analysis, the IEDs will utilize knowledge about their respective area to predict the worst case scenarios based on the risks and uncertainties in their part of the CPES, including interactions between physical and cyber systems.

In the case where a preventive actions is needed, the IEDs will evaluate the distributed control of their area and coordinate and perform the optimal control. If the system is unable to perform a suitable preventive action, the required information about needed control are send to the transmission level control center, which will act as an additional layer of security,

The transmission system control center will perform a security assessment of similar to the one shown in Fig. 3 and will handle the overall operation of the system by including central power plant operation points and interdependence analysis in the contingency analysis.

V. Conclusion

In this paper, the power system security assessment is analyzed in a CPES with strong interconnections between the power system, ICT network and neighboring energy systems. From the analysis of CPS safety, security and sustainability in the future CPES, a number of challenges are listed for each of the three phases in the traditional security assessment method. Based on the challenges, a new framework for CPES security assessment is proposed, which adds new solutions, such as IDS and RMP, on top of the traditional power system security assessment method.

Topics of further research include investigation of IDSs, distributed optimization, intelligence and computation, analysis of utilizing big data computational tools to improve visibility and development of a RMP that can cover all risks in a CPES.

References

[1] X. Yu and Y. Xue, "Smart Grids: A CyberPhysical Systems Perspective," *Proc. of the IEEE*, vol. 104, no. 5, pp. 1058-1070, May 2016.

[2] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18-28, Jan.-Feb. 2010.

[3] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber-Physical Systems," *Proc. of the IEEE*, vol. 100, no. 1, pp. 283-299, Jan. 2012.

[4] X. Shi, Y. Li, Y. Cao and Y. Tan, "Cyber-physical electrical energy systems: challenges and issues," *CSEE Journal of Power and Energy Systems*, vol. 1, no. 2, pp. 36-42, June 2015.

[5] P. Kundur et al., "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1387-1401, Aug. 2004.

[6] A. J. Wood, B. F. Wollenberg and G. B. Shebl, Power system security, in *Power generation, operation, and control*, 3rd ed. New York, Wiley, 2013, ch. 7, pp. 296-349.

[7] K. Morison, L. Wang and P. Kundur, "Power system security assessment," *IEEE Power and Energy Magazine*, vol. 2, no. 5, pp. 30-39, Sept.-Oct. 2004.

[8] S. Huang, C. Zhou, S. Yang and Y. Qin, "Cyber-physical System Security for Networked Industrial Processes," *International Journal of Automation and Computing*, vol. 12, no. 6, pp. 567-578, Dec. 2015.

[9] R. Mitchell III, "Design and Analysis of Intrusion Detection Protocols in Cyber Physical Systems," Ph.D. dissertation, Dept. Computer Sciencem, Virginia Polytechnic Institute and State University, Falls Church, VA, 2013.

[10] G. N. Ericsson, "Cyber Security and Power System CommunicationEssential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501-1507, Jul. 2010.

[11] Y. Liu, P. Ning and M. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," *ACM CCS*, pp. 21-32, Nov. 2009.

[12] L. Liu, J. Ma, Z. Dong, G. Chen and K. Wong, "Influence of enhanced interconnecting links on cascading failures in smart grid," *IEEE Power & Energy Society General Meeting*, Denver, CO, 2015, pp. 1-5.

[13] A. Teixeira, H. Sou, H. Sandberg and K. Johansson, "Secure Control Systems," *IEEE Control Systems Magazine*, pp. 24-45, Feb. 2015.

[14] National Institute of Standards and Technology, "Guidelines for Smart Grid Cybersecurity," National Institute of Standards and Technology Interagency Report 7628 Rev. 1, Vol. 1, Sep. 2014.

[15] R. C. Green, L. Wang and M. Alam, "Applications and Trends of High Performance Computing for Electric Power Systems: Focusing on Smart Grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 922-931, Jun. 2013.

[16] S. Buldyrev, R. Parshani, G. Paul, H. Stanley and S. Havlin, Catastrophic cascade of failures in interdependen networks, *Nature*, vol. 464, pp. 1025-1028, Apr. 15 2010.

[17] C. Ten, C. Liu, G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Transaction on Poer Systems*, vol. 23, No. 4, pp. 1836-1846, Nov. 2008.

[18] K. Zetter. (2016, January 20). *Everything we know about Ukraines power plant hack (1st ed.)* [Online]. Available: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

[19] Y. Mo et al., "CyberPhysical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012.

[20] Union for the co-ordination of transmission of electricity, System disturbance on 4 November 2006, UCTE, Final report, 2007.

[21] J. Mathieu, T. Rasmussen, M. Sørensen, H. Jó hannsson and G. Andersson, "Technical resource potential of non-disruptive residential demand response in Denmark," in *IEEE PES General Meeting Conf. & Expo.*, National Harbor, MD, 2014, pp. 1-5.

[22] S. Sridhar, A. Hahn and M. Govindarasu, "CyberPhysical System Security for the Electric Power Grid," *Proc. of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012.

[23] P. Fairley. (2016, April 20). *Upgrade coming to grid cybersecurity in U.S. (1st ed.)* [Online]. Available: http://spectrum.ieee.org/energy/the-smarter-grid/upgrade-coming-to-grid-cybersecurity-in-us

[24] J. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet of Things Journal*, Vol. 1, No. 1, pp. 3-9, Jan 2014.

[25] Y. Cherdantseva et al., "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," *Elsevier Journal in Computers and Security*, Vol. 56, pp. 1-27, Oct. 2015.