Survey of Cyber Security Challenges and Solutions in Smart Grids

Lindah Kotut and Luay A. Wahsheh
Computer Science Department
Norfolk State University
Norfolk, VA
Email: l.kotut@spartans.nsu.edu; law@nsu.edu

***Abstract*—The smart grid is the new iteration of the power grid that merges communication technology amongst other technological advances, with the aim of providing reliable and efficient services. With the known and potential risks associated with communication networks, and with the potential catastrophic effects of the grid failure, assured security of the smart grid is at the forefront of cyber security research. We present a survey of recent advances and discussions on smart grid cyber security. The main focus of our survey is on the entire grid instead of specific components, as we aim at painting the big picture as to the state-of-the-art on cyber security of the smart grid. Our survey identifies both successfully adopted solutions and shortfalls that remain to be addressed. The approach taken by this paper is an important step towards developing secure solutions for the smart grid.**

Keywords-component; Smart Grid, Cyber Security, Security Management.

I. INTRODUCTION

The smart grid is a result of the modernization of electricity power infrastructure, that in addition to allowing for the integration of renewable sources of energy, it leverages the integration of advanced computing and communication technology [20]. This allows for two-way communication between the power source and consumer, and thus allowing for better energy management and distribution in addition to improved control, efficiency, transparency, and safety, all this in the aim of reducing costs, increasing reliability, efficiency, and transparency of this infrastructure [21].

The advantages brought about by providing two-way communication to the power grid cannot be overstated: By leveraging the communication technology, it becomes possible to incorporate other renewable sources of energy into the grid in order to supplement, and in some cases replace, traditional and mostly non-renewable sources of energy. Increasing cost of production in the non-renewable sector of energy coupled with the market forces dictating the move towards cleaner energy are other major influences. To add to this, the attraction of dynamic pricing of electricity use – where a consumer is charged a different rate for electricity use during either peak or off-peak hours are just a tip of the iceberg of the many incalculable advantages to be had by the widespread adoption of the smart grid.

The health and fidelity of the grid is of the utmost importance, as failures in it could be catastrophic. Examples include the North American blackout of 2003, a 4-day event triggered by a relatively small failure, which ended up costing the United States (U.S.) between $4 and $10 billion [22], the South Australian massive blackout of September 2016 [30], where a cascading failure impacted the entire state's power grid and affected close to 1.7 million residents - the resulting incurred loss still being determined by the conclusion of this paper, and the December 2015 Ukrainian blackout being the first confirmed case of power loss directly attributed to the increasing incidence of cyber-attacks [28].

Smart grids have a promise of mitigating, if not completely halting such events, owing to its inherent decentralized architecture and protocols that provide for power-flow control, reliability, security, fault tolerance, and self-healing. As such, its adoption is highly encouraged, highly anticipated, and deeply studied.

With the health of the smart grid as a whole being the focus of our survey, we are able to categorize cyber security challenges ranging from lack of communication due to factors such as classified information, trust laws, and non-disclosure agreements to lack of proper regulations in the field. We further examine proposed solutions and ongoing studies against field applications and determine whether they have been successful or not, and in the case of the latter outcome, what alternate remedies have been used and if they can be replicated across the grid. Based on these collected facts, we then propose courses of action which we deem to be of more practical use; ranging from the recommendation of the adoption of known secure central platforms used to collect reported data on security breaches, to proposing methods of disseminating critical information such as security patches.

The remainder of this paper is organized as follows: Smart grid architecture and policies are discussed in section II, together with its security objectives, and resulting requirements. In section III, the current challenges beleaguering the grid are discussed, while attacks, threats and consequences are presented in section IV. In section V, actual, and proposed recommendations as well as in-progress solutions are discussed after which the paper concludes in section VI with a discussion and provides proposals to be implemented as future work.

978-1-5090-5771-9/16 $31.00 © 2016 IEEE
DOI 10.1109/CYBERSEC.2016.18

II. ARCHITECTURE, POLICIES, AND SECURITY REQUIREMENTS

With continued and inevitable trend in the pervasiveness of the communication technology into every imaginable sector, it was only a matter of time before this was also true of the power grid. But the sheer vastness and complexity of the smart grid, not to mention the interconnectedness with other critical infrastructures, make the development of common standards necessary if not compulsory. Having a set of rules makes it easier to incorporate the ever increasing stakeholders of this infrastructure.

With this in mind, there is legislation in place mandating the transitioning of the U.S. power infrastructure into the Smart Grid [21]. Coupled with this, and in an effort to provide proactive security to the smart grid, President Obama in 2013 signed an executive order mandating the National Institute of Standards and Technology (NIST) to develop a framework to guide the smart grid cyber security standards [17]. The resulting framework, named NIST Interagency Report (NISTIR 7628) [10] provides comprehensive guidelines for smart grid security. Our survey uses these guidelines as a baseline for studying not only the advances made in compliance with NIST's recommendations, but also the challenges and shortfalls preventing a complete system-wide adoption of the standards and/or where the standards fall short of expectations.

A. Smart Grid Architecture

NIST's framework describes a conceptual model as shown in Figure 1, consisting of seven logical domains: Bulk Generation describes the transmission and storage of electricity in bulk; Transmission regards the carriage of electricity over long distances; Distribution concerns the supply of power to the Customer – who is the end user. These four domains have two-way power and communication flows, while Markets consisting of operators and participants, Service Providers that provide services to customers and utilities, and Operations – the managers of the movement of electricity domains involve information collection and power management.

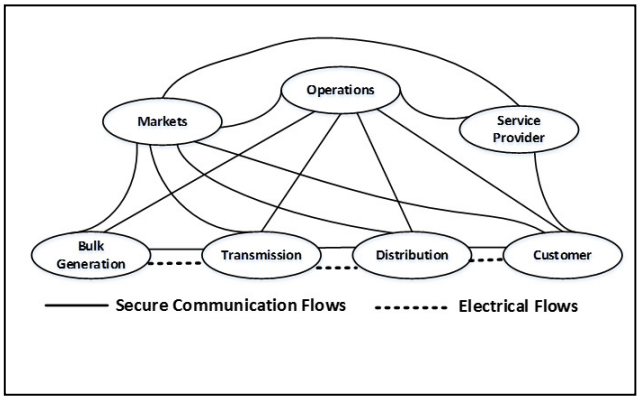

Figure 1. NIST Smart Grid Framework.

Detailed discussions regarding the NISTIR 7628 architecture has been done, including an analysis of the effectiveness of the framework by [5], weaknesses and loopholes highlighted by [2], risk assessments for different smart grid stakeholders performed by [1], and a comparison with Smart Grid Architecture Model (SGAM) – the European standard model studied by [24].

B. Security Objectives and Requirements

The smart grid high-level security requirements listed by [10] are no different than that of any system employing the communication network: *Confidentiality* prevents unauthorized access to private information; *Integrity* ensures the fidelity of information; while *Availability* provides a guarantee of service. Unlike traditional communication networks however, the importance of the requirements is in reverse arrangement: Availability, integrity, and confidentiality in that order.

The cyber security requirements are aimed at ensuring that the grid is robust, resilient to attacks and secure. As such, the grid should have the following strategies: Be able to detect attacks and mount a response, have provision for access-control mechanisms to prevent unauthorized access, and describe protocols to ensure secure communication.

III. CHALLENGES

Except for exceptional circumstances such as the 2015 Ukrainian blackout [28], confirmed instances of successful cyber-attacks and methods have generally been proprietary or classified; owing to either its sensitivity, or potential repercussions such as stock market price drop concerns. The decentralized aspect of the smart grid means that there are diverse stakeholders in charge of different (still proprietary) sections of the grid, and thus information sharing amongst and between all of them presents a challenge. The Department of Homeland Security, through its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a public alert dashboard with threat alerts and advisories that is curated from stakeholders ranging from the government to the private sector, to provide security-related incidents and mitigation measures [23]. The limitations to this tool however, are as stated above: Most cyber-attacks and attempts are proprietary information and as such cannot be listed on ICS-CERT.

A. Confidentiality, Privacy, and Anti-Trust Laws

Dissemination of information regarding attack information and/or patches to discovered security holes are not only governed by the potential financial repercussions of revealing such information as noted earlier, but the employees and companies are more often held back by confidentiality/non-disclosure agreements and anti-trust laws. Even if released in good faith, any proprietary information released by an individual in a company is subject to such laws. Ghansah [4] studied the classification of data and information flowing through the grid and categorized them into either confidential or non-

confidential, and proposed best-practices on dealing with sharing of each category of information. Their main argument however, is whether a lot of the information passing through the grid really ought to be marked as classified, rather than providing a mechanism on how to share the information across domains.

The Cybersecurity Information Sharing Act (CISA) [8] originally introduced to congress in 2013 and passed into law in 2015, aims to provide a secure platform for companies to share cyber threat information with the government, where the government in return provides legal immunity against anti-trust laws. However, CISA acts more of a reporting platform rather than a sharing platform – infomation flows only one way. It neither provides for a secure space for all stakeholders to share information, nor does it address the responsible or permissible use of private information collected. Therefore, until solutions are found to address these concerns, the number of companies willing to participate will be affected.

B. Regulations and Resources

The glaring lack in regulations, is that the adoption of the NISTIR 7628 framework is considered voluntary in the private sector. NISTIR 7628 recommendations are simply suggestions, and are not enforceable. With no guarantee of complete adoption, it becomes difficult to determine whether the system is/will be properly adopted or not. And if adopted, whether it was done according to specifications. Clear requirements, especially implemented by members of the Industrial Control Systems Information Sharing and Analysis Center (ICS-ISAC) – to which the smart grid stakeholders are members of; with at the very least, a running list of the compliant players, are the baseline we recommend, to provide assurance to other compliant stakeholders and interested consumers.

C. User Awareness and User Error

For the purposes of our survey, we associate user awareness with the customer domain, and user error with the operations domain. The two-way communication adopted by the smart grid opens the way for feedback from meters and by extension, the users. Data obtained from the meter can predict the activity of the users and this can be used to form a pattern and create a profile about each user [7]. Coupled with the fact that of the three security objectives, confidentiality is ranked third, understandably concerns arise about the integrity and confidentiality of data obtained from the user: If it is secured, and in case of a breach, if it is anonymized enough to at least provide a measure of protection to the users. With those protections in place, educating the consumer regarding the various aspects of the smart grid would go a long way not only in ensuring that dynamic pricing is maximized by the user, but also the customer may serve as a spotter in case of unusual activity, or in reporting cases of vandalism.

Our survey found many large-scale power outages that were caused by human error, or a combination with technical errors. A recent case, the Turkish blackout of March 2015 [3] – initially feared to be a case of successful cyber-attack, was found to be the caused by human error. Add this to the magnitude of loss – whether monetary or otherwise, and there is reason to aim for the mitigation of human error by implementing automation and setting aside human intervention for needed cases.

IV. THREATS AND CONSEQUENCES

The integration of communication network, while allowing for significant advantages, also brings with it risks and challenges in securing and managing the resulting network. The rising cases of successful data breaches impacting millions of people have served to underscore the catastrophic nature of increased internetworking, while the cascade failures as evidenced in the U.S. in 2003 [22] and in Australia in 2016 [30] point to the fallacy of continued reliance on the centralized power grid. Therefore, the threats from each side leaves the smart grid to strike a delicate balance between the two – in providing enough internetworking to create redundancies that ensure that cascades would be an impossibility, while ensuring data security.

We categorize threats, known and potential attacks into broad classifications in keeping with the objectives discussed earlier in section II, and discuss both known and inferred potential consequences.

A. System Failure

Apart from human errors, many failures on the current grid can be attributed to equipment failures, as were the cases with the North American, the Swiss/Italian [15], the London/West Midlands [12], the Turkish [3] and the South Australian blackouts [30]. The North American Blackout triggered research into detection mechanisms of events that potentially could lead to cascade failures [14]. Factors such as power oscillations and power surges have been considered, with proposed measured to be used in case of an imminent natural disasters tabled.

B. Targeted Attacks

There are many motives that could be attributed to attacks on the grid including cybercrime, hacktivism, and more recently, cyberespionage and cyberwarfare. The malware Stuxnet [9], is the most notorious example of a cyber weapon. Its attack vectors encompass different sectors of the grid: From the physical to the data. Stuxnet was designed to target specific Supervisory Control and Data Acquisition (SCADA) systems that amongst other things, caused a destruction of over a thousand Iranian nuclear centrifuges [9]. The stealth and success of the malware has raised a lot of questions regarding the security of such systems. Havex [31] is another known malware developed to target industrial control systems (ICSs) and the trojan BlackEnergy [28] was discovered in the computer networks post Ukrainian blackout and is suspected to have played a major role in the event. Unlike most occurrences where SCADA systems are isolated and mostly offline, not all of which are involved in the grid will be so. Therefore, there is

increased focus on the threat in itself, and also in devising strategies of defense against such similar attacks.

C. Physical Threats

While purely physical attacks on the grid are beyond the scope of this survey, we do place into consideration the fact that physical attacks may have consequences on the cyber realm and vice versa. Such attacks may be attempted on the actual power lines as well as transformers and substations, although these may be unlikely given the risks. Physical attacks on soft entry points into the smart grid however are more likely. Such include smart meters, which we consider as soft targets due to their accessibility and profusion. Until tamper proof, or tamper evident design becomes the norm, there is a need to ensure that security of data and information on the systems to be of paramount importance. Yan et al. [26] considered this hostile environment and discussed possible attacks to such meters, and potential integrity and confidentiality loss especially regarding the consumer.

Harder, but by no means impossible targets are the SCADA systems. These systems are responsible for measuring data such as power flows and passing them to the state estimator to estimate the power and network states. As revealed by the success of the Stuxnet malware, these systems are by no means immune to attack, a phenomenon also studied by [7] – who also noted that SCADA's connection to the communication network exposes its vulnerabilities to a wider base of attacks.

D. Hybrid Attacks

As there are attacks leveraged either purely on the cyber realm or on the physical realm as referenced in section IV part C, there are attacks that can be leveraged on both realms. These hybrid attacks present unique challenges in not only mounting defenses, but also in defining protocols. Defense against these attacks are understandably complex as an attack could involve any mix of the different components of the smart grid.

V. RECOMMENDATIONS

Due to the sheer magnitude of the smart grid, the proposed solutions aimed at specific sections of the architecture are a legion. With the increased adoption of NIST's recommendations, it is reasonable to assume that most of these solutions will not be disparate in nature, and thus compatible with other offered solutions. In the same manner that a human body cannot be referred to as healthy if only one organ is observed as fully functional, is the same way that the overall health of the entire grid cannot be determined by focusing on a certain section of the grid. This section – as does our main theme, focuses on known and proposed solutions that cover the smart grid security in its entirety.

A. Information Sharing

Timely and accurate information sharing is vital in decision making, regardless of whether the information is used as a means of determining and defending against threats, or in establishing the health of the grid. Therefore, the collection, and most importantly the sharing of information across all the stakeholders is vital. We determine that information sharing can be subcategorized into three items: Data, information, and intelligence. Data involves specifics about individual components that make up the grid; information deals with aggregated details on collected data; while intelligence involves sharing of observations gleaned from both the data and information.

As the smart grid falls under the realm of critical infrastructure, it is a given that the government, in collaboration with the private sector stakeholders will be involved in determining the best course of action in sharing data across domains. Table 1 gives a brief overview of policies, directives, and executive orders that have been put in place by the government, in an effort to facilitate a streamlined process in collecting and sharing information. Of note, are the Executive Orders (EOs): EO 13526 prescribes a uniform system of classifying, safeguarding, and declassifying national security information in an effort to provide guidelines on how to handle declassified information from the federal government [18]; EO 13636 sets the mandate for NIST to develop the framework that has been used as the basis of this survey [17], while EO 13691 was given to encourage the voluntary formation of Information Sharing and Analysis Organizations (ISAOs) that are structured to provide platforms for sharing information related to cyber security risks and incidents, as well as to mount response or defense in as close to real time as possible [15].

TABLE I. SMART GRID POLICIES

Year	Title	Description
1998	Presidential Decision Directive (PPD) 63	Development of sector-specific Information Sharing and Analysis Centers (ISACs) [19]
2003	Homeland Security Presidential Directive (HSPD) 7	Critical Infrastructure Identification, Prioritization, and Protection (involvement of the private sector in sharing cyber security information) [6]
2009	EO 13526	Classified National Security Information [18]
2013	EO 13636	Improving Critical Infrastructure Cyber Security [17]
2015	EO 13691	Promoting Private Sector Cyber Security Information Sharing [16]
2015	S.2588	Cyber Security Information Sharing Act [8]

There are disparate systems that allow for central information gathering and threat analysis, most of which unsurprisingly are state sponsored; such as the Public Regional Information Security Event Management (PRISEM) system [11] localized in the state of Washington. The need with these systems are two-fold – and fulfils our recommendation standard: Provide secure location for sharing data, and a standard framework for collecting and analyzing threats.

A collaborative framework for sharing information on cyber infrastructure was proposed by [25] to fill the gap between information collected and disseminated at the federal level such as PRISEM, and those provided at the community level such as the Community Cyber Security Maturity Model (CCSMM) – which was also discussed in the proposal. Framework requirements and proposed system-wide threat levels were given to provide uniformity and coherence in the information collected.

To the best of our knowledge, there is currently no completed research work on secure platforms that would implement the proposed frameworks and allow for information sharing. There is research work in progress however, led most notably by the Pacific North-West National Laboratory's (PNNL) Cyber-security Risk Information Sharing Program (CRISP) [13,32], whose aim is to provide the secure platforms for both the government intelligence and private utilities to share threat information. The collation of data in a central location would allow for proper identification of threats; development of signatures; and the dissemination of new information, threat alerts, and threat mitigation strategies system-wide.

B. Soft Targets

Easily accessible components of the grid include the smart meters which have a critical and inescapable role to play in facilitating communication between the consumer and the power source. As such, they need to have robust protocols in order to mitigate breach attempts if possible, and if not, a way to alert for breach attempts, or turn passive if breach is suspected. With this in mind, [26] for example proposed an efficient security protocol for the Advanced Meter Infrastructure (AMI) implemented by the smart meters with the help of a third party authentication protocols. A comprehensive study has also been done by [7] as to the security concerns regarding the smart meters.

C. Multi-Domain Defense Strategies

Apart from, and including solutions brought about by information sharing, defense strategies that focus on the entire complex infrastructure are important. While NISTIR 7628 presents a base of reference regarding amongst other things, a guide to develop secure systems, it is by no means exhaustive – as outlined by [1]. Therefore, there is further need to develop in-depth defense strategies that take into account the complex nature of the grid and formulate custom solutions, or incorporate existing solutions that fit the model described in the defense strategy. This gap is especially evident when considering hybrid attacks referenced in section IV. Mo et al. [27] address this phenomenon and present a theory so named cyber-physical security (CPS) – a combination of system theory (that focuses on physical systems) and cyber security that could be applied to the smart grid.

VI. CONCLUSION AND FUTURE WORK

A first line of defense in ensuring a secure infrastructure is the development and use of a common framework that provides references to define new protocols and modify older protocols to ensure cohesion of the different components system-wide. Employing the NISTIR 7628 framework meets this goal, in presenting a good possibility that it will be adopted in future developments and implemented as a baseline especially in establishing security protocols.

Developing secure solutions to the smart grid will be an ongoing process in tandem with advances in technology, as the right strides have been taken in developing security parameters from inception. The need for cohesive sets of standards and measurement has also been addressed in part by NISTIR 7628, and further adoption of the proposals would go a long way in developing standard-based solutions.

We presented our recommendations with a specific focus on information sharing across the domain. We offered examples of proposed and working platforms that we deem to have the qualities that can be adopted for a system aimed at the entire grid.

We conclude with a determination that a robust system of information sharing would be an invaluable, and dare we say – inevitable step regarding cyber security of the smart grid, and as such, it offers an exciting glimpse of what the future of cyber security of the smart grid would entail.

REFERENCES

[1] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz and A. Mili, "Risk assessment methodology based on the NISTIR 7628 guidelines," System Sciences (HICSS), 2013 46th Hawaii International Conference on, Wailea, HI, USA, 2013, pp. 1802-1811. doi: 10.1109/HICSS.2013.466

[2] A. C. F. Chan and J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," in IEEE Communications Magazine, vol. 51, no. 1, pp. 58-65, January 2013. doi: 10.1109/MCOM.2013.6400439

[3] "Head of Turkish grid operator resigns after blackout," *Deutsche Welle*. June 4, 2015. Online: http://www.dw.com/en/head-of-turkish-grid-operator-resigns-after-blackout/a-18363453

[4] I. Ghansah, "Categorizing research and development issues for cyber security in the smart grid into confidential and non-confidential". 2010. California Energy Commission. Publication No. CEC-500-2014-051

[5] M. Harvey, D. Long and K. Reinhard, "Visualizing NISTIR 7628, guidelines for smart grid cyber security," Power and Energy Conference at Illinois (PECI), 2014, Champaign, IL, 2014, pp. 1-8. doi: 10.1109/PECI.2014.6804566

[6] Homeland Security, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection,"

December 17, 2003. Online: https://www.dhs.gov/homeland-security-presidential-directive-7

[7] N. Komninos, E. Philippou and A. Pitsillides, "Survey in smart grid and smart home security: issues, challenges and countermeasures," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014. doi: 10.1109/COMST.2014.2320093

[8] Library of Congress, D. Feinstein, "S.2588 – Cyber Security Information Sharing Act of 2014," 2014. Online: https://www.congress.gov/bill/113th-congress/senate-bill/2588

[9] N. Falliere, L. Murchu, and Chien, E.,"W32.Stuxnet Dossier, Version 1.4" February 2011. Online: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[10] The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee, "Volume 1 – smart grid cybersecurity strategy, architecture, and high-level requirements," National Institutes of Standards and Technology, 2014. doi:10.6028/NIST.IR.7628r1

[11] Office of the Chief Information Officer, "The Public Regional Information Security Event Management (PRISEM) system," 2014. Online: https://ocio.wa.gov/news/prisem

[12] PB Power, "OFGEM Report on Support Investigations into Recent Blackouts in London and West Midlands," February 2004. Online: https://www.ofgem.gov.uk/ofgem-publications/37665/sectoralinvestigations-18.pdf

[13] Pacific Northwest National Laboratory, "Success Stories," October 10, 2014. Online:http://www.pnnl.gov/about/literature/PDF/11_2013_EED_Success_Stories_Booklet.pdf

[14] S. Ruj and A. Pal, "Analyzing cascading failures in smart grids under random and targeted attacks," 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Victoria, BC, 2014, pp. 226-233. doi: 10.1109/AINA.2014.32

[15] Swiss Federal Office of Energy, "Report on the blackout in Italy on 28 September 2003," November, 2003. Online: http://www.bfe.admin.ch/php/modules/publikationen/stream.php?extlang=en&name=en_109363212.pdf

[16] The White House, *Executive Order – Promoting Private Sector Cybersecurity Information Sharing*. February 13, 2015. Online: https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[17] The White House, *Executive Order – Improving Critical Infrastructure Cybersecurity.* 2013. Online: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[18] The White House, *Executive Order 13526 – Classified National Security Information*. 2009. Online: https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

[19] The White House, *Presidential Decision Directive NSC-63*. May 22, 1998. Online: http://fas.org/irp/offdocs/pdd/pdd-63.htm

[20] U.S. Department of Energy, "Smart grid." 2014. Online: http://energy.gov/oe/services/technology-development/smart-grid

[21] U.S. Department of Energy, *Title XII Section 1301 – Statement of Policy on Modernization of the Electricity Grid*. 2008. Online: http://energy.gov/oe/downloads/title-xiii-smart-grid-sec-1301-1308-statement-policy-modernization-electricity-grid

[22] 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," 2004. Online: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

[23] U.S. Department of Homeland Security, "Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)," Online: https://ics-cert.use-cert.gov.

[24] M. Uslar, C. Rosinger and S. Schlegel, "Security by design for the smart grid: Combining the SGAM and NISTIR 7628," Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International, Vasteras, 2014, pp. 110-115. doi: 10.1109/COMPSACW.2014.23

[25] W. Zhao and G. White, "A collaborative information sharing framework for Community Cyber Security," Homeland Security (HST), 2012 IEEE Conference on Technologies for, Waltham, MA, 2012, pp. 457-462. doi: 10.1109/THS.2012.6459892

[26] Y. Yan, R. Q. Hu, S. K. Das, H. Sharif and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," in IEEE Network, vol. 27, no. 4, pp. 64-71, July-August 2013. doi: 10.1109/MNET.2013.6574667

[27] Y. Mo et al., "Cyber–physical security of a smart grid infrastructure," in Proceedings of the IEEE, vol. 100, no. 1, pp. 195-209, Jan. 2012. doi: 10.1109/JPROC.2011.2161428

[28] ICS-CERT, "Cyber-attack against Ukrainian critical infrastructure," Feb. 25, 2016. Online: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. [Accessed: October 6, 2016].

[29] ICS-CERT, "Ongoing sophisticated malware campaign compromising ics (Update E)," March 02, 2016. Online: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[30] "The South Australia blackout: Once in 50-year storm lashes state", *The Sydney Morning Herald,* September 28, 2016. Online: http://www.smh.com.au/national/south-australia-blackout-once-in-50year-storm-lashes-state-20160928-grqpks.html

[31] ICS-CERT, "ICS focused malware (Update A)," June 27, 2014. Online: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

[32] S. Ashby, "PNNL research is enhancing cybersecurity," *Tri-City Herald,* May 15, 2016. Online: http://www.tri-cityherald.com/news/local/pacific-northwest-national-lab/article77790282.html