Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources

Preprint

Ricardo Siqueira de Carvalho and Danish Saleem

National Renewable Energy Laboratory

Presented at Resilience Week 2019
San Antonio, Texas
November 4–7, 2019

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-74895
December 2019

Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources

Preprint

Ricardo Siqueira de Carvalho and Danish Saleem

National Renewable Energy Laboratory

Suggested Citation
Siqueira de Carvalho, Ricardo and Danish Saleem. 2019. *Examining the Net Revenue and Downstream Flow Impact Trade-Offs for a Network of Cascading, Small-Scale Hydropower Facilities: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5R00-74895. nrel.gov/docs/fy20osti/74895.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-74895
December 2019

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources

Ricardo Siqueira de Carvalho
Energy, Security & Resiliency Center
National Renewable Energy Laboratory
Golden, USA
ricardo.siqueiradecarvalho@nrel.gov

Danish Saleem
Energy, Security & Resiliency Center
National Renewable Energy Laboratory
Golden, USA
danish.saleem@nrel.gov

***Abstract*—The current electric grid is transitioning through increasing penetration of distributed energy resources (DERs), which include intermittent renewable generation resources on the distribution side. Both the monitoring and control of DERs require extensive data-exchange and communication networks. These networks lead to cyber vulnerabilities and risks of new kinds of cyberattacks that may be extremely destructive for power system operations. Although current standards, such as IEEE Std. 1547-2018, do not discuss cybersecurity measures for DERs, cybersecurity controls should be developed for securing DER systems at the device level, communications level, and applications level. This paper discusses the current industry's best practices related to DER cybersecurity and proposes recommended functionalities for improving the cybersecurity posture of DERs, specifically at the device/distribution level. These practical recommendations have been discussed and verified with the industry through a DER cybersecurity working group.**

Keywords—distributed energy resource, renewable energy, cybersecurity, smart grid, communication, standards.

I. Introduction

The legacy electric grid was designed for unidirectional power flow from large electric machine-based generators located far from load centers. This grid was not designed to handle multiple sources of distributed energy resources (DERs), such as photovoltaic, storage, and wind power. Increased implementation of these DERs is transitioning the modern grid into accommodating a bidirectional power flow [1]. Figure 1 depicts the main trends in modern distribution systems, including increased penetration of DERs. Monitoring and control of such DERs require data and communication to integrate DERs with the modern grid, but this oversight also makes DERs vulnerable to cyberattacks, which can have destructive impacts on a power distribution system because of lacking built-in security controls [2–3]. Recent cyberattacks targeting the Ukrainian electric grid [4], shown in Table I, are a prime example of this lack of built-in security controls.

Although the greater electric grid has been modernized, its function remains to provide safe, secure, and reliable electricity to consumers. To continue meeting this objective, adequate security must be added to these newly installed and constantly growing DERs [5]. Overall, cyber vulnerabilities can be found at either the generation, transmission, or distribution level, though this paper focuses on mitigating vulnerabilities at the distribution level.

TABLE I. Recent Cyberattacks, Modified from [6]

Year	Target	Source of Attack	Consequence
2014	Monitoring and control systems of several utilities in United States and Europe	Spear phishing, Havex malware for watering hole attack	Espionage to map devices on utilities' computer network [7]
2015	Ukrainian grid-control centers	BlackEnergy3 malware	Power outage to 220,000+ customers [4]
2016	Pivnichna substation control systems, Ukraine	Industroyer or Crash Override malware	Power outage to one-fifth of Kiev [8]
2015–2017	Western energy sector (United States)	Dragonfly 2.0 (US-CERT 2018)	Spear phishing, Trojan-ware, watering hole attacks, and data theft [9]
2018	Ukraine's chlorine plant	VPN Filter malware (prevented successfully)	Data exfiltration and espionage [10]

Table 1 shows some recent cyber and physical attacks on the electric grid's industrial control systems and speaks to the urgency of securing all aspects of this critical infrastructure. To make the electric grid better prepared against cyber and physical threats, several industry standards and guidelines for cybersecurity have been developed and established. Existing cybersecurity frameworks address some issues related to the electric grid as whole, but sufficient guidelines and procedures do not exist to help vendors, utilities, aggregators, government institutions, and other partners adopt and implement procedures to secure the data and communications of DERs [6].

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding was provided by the DOE Office of Energy Efficiency and Renewable Energy (EERE) under Solar Energy Technologies Office (SETO) Agreement No. 34216. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

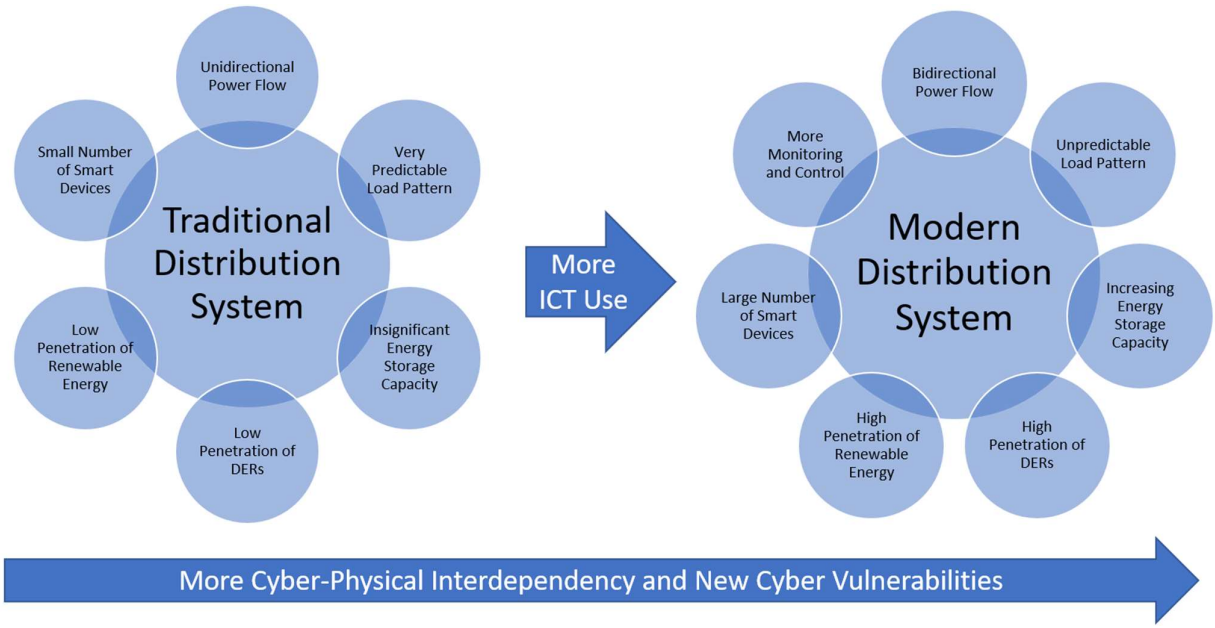

Fig. 1. Trends in modern distribution systems, including increases of Information and Communication Technology (ICT), cyber-physical interdependency, and new vulnerabilities.

Further, attackers are constantly evolving and finding new exploitable vulnerabilities for inflicting cyberattacks. Thus, there is a critical need to create an effective and efficient way of securing next-generation DERs that will be connected to the distribution grid [11–12].

This paper focuses on: (**1**) a summary of DER advanced functionalities required by IEEE Std. 1547-2018 for interconnection of DERs to the grid; (**2**) a literature review on the commonly known and existing cyber vulnerabilities of DERs and their possible impact in smart distribution grid operation; and (**3**) a succinct set of recommended DER cybersecurity functionalities that can be incorporated to improve device-level cybersecurity of a DER. These recommendations are based on a consensus developed after a year-long discussion with the SunSpec/Sandia DER cybersecurity working group and in partnership with utilities, vendors, manufacturers, and researchers.

II. Modern DER Functionalities and Cyber-Physical Impact

IEEE Std. 1547-2018 is the current standard for interconnection and interoperability of DERs [13]. The modern distribution grid with DERs is a cyber-physical system, and the impact of cyberattacks targeting DERs can have a cyber-physical impact. The main objective of traditional DERs was to inject active power into the grid, whereas modern DERs have several new operating modes to improve the overall system operation and efficacy by dispatching active and reactive power [14]. If those advanced modes of DERs are compromised, the impact on the electric grid can be devastating [15–16]. It is important to identify the functionalities of a modern DER and know the possible impacts if such modes either malfunction or become a target of a cyberattack. Following are key operation modes of a DER and the possible impact of loss of data integrity for such control systems:

- **Constant power factor mode:** A DER operates at a constant power factor value. With appropriate access, an attacker could change the power factor to an inductive or capacitive one that could potentially increase system losses, create problems with voltage regulation, and reduce the overall power quality of the electric system.
- **Limit active power mode:** The amount of active power that can be injected by a DER is limited to a set point determined by the operator. An attacker could reduce the set point of this mode to zero watts. This would reduce the amount of active power injected into the grid, therefore impacting grid operation.
- **Constant reactive power mode:** Similar to the active power mode, a DER injects a constant amount of reactive power defined by a set point. By changing the set point, an attacker potentially could set DERs to inject or absorb reactive power into the electric grid to cause undervoltage or overvoltage at the point of common coupling.
- **Voltage-reactive power mode (volt-var):** A DER is designed to inject or absorb reactive power, depending on the voltage level at the point of common coupling, and to maintain the voltage limit within the prescribed boundaries. An attacker could change the voltage-reactive droop curve to affect the grid voltage, potentially creating problems with the voltage control application.
- **Active power-reactive power mode (watt-var):** In this mode, a DER actively controls the reactive power output as a function of the active power output, following a linear active power-reactive power characteristic curve. An attacker could change this characteristic curve to create problems with both voltage levels and power flows into the grid.
- **Voltage-active mode (volt-watt):** DERs increase or decrease the amount of active power injected in the grid, depending on the voltage level at the point of common coupling. An attacker could change the setting of this mode to cause undervoltage and/or overvoltage at the points of common coupling.

- **Frequency droop mode (frequency-watt):** A DER helps to control grid frequency by increasing or decreasing the amount of active power injected by itself. An attacker could potentially change the DER droop curve and affect the electric grid system frequency. In a worst-case scenario, it could lead to a system frequency collapse, similar to a cyberattack targeting large generators in a power system.

Figure 2 summarizes how attackers could inflict multiple types of damage on the distribution system and its operation through a cyberattack. It is important to emphasize that an attacker could seize control over just one DER or multiple DERs, and the number and size of the hacked DERs in a given attack could limit the impact of the consequences from such cyberattacks [6]. Further, the opponent could potentially use the DERs for malicious lateral movement to map the cyber-physical electric grid. Although some investigative studies have been published that measure the physical impacts on smart grids from cyberattacks, many opportunities remain for further research in this area [11].

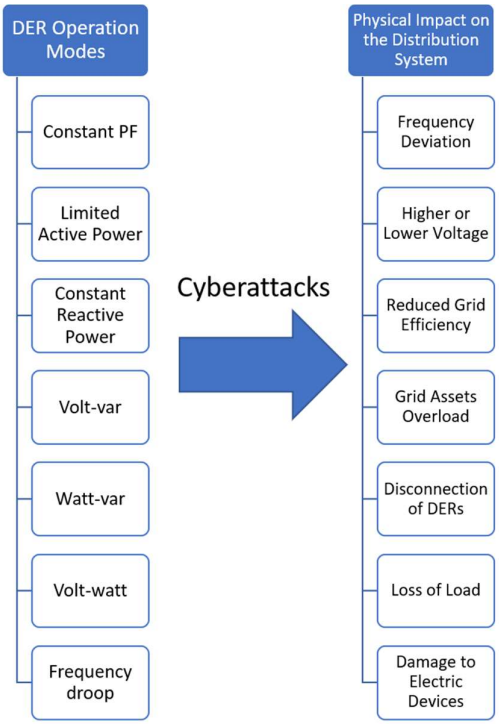

Fig. 2. Potential physical impacts on the distribution systems resulting from a data-integrity attack targeting DERs.

III. DER Common Vulnerabilities and Cyberattacks

The key security objectives to make a cyber-physical system safer are integrity, availability, and confidentiality of system data and services [17]. An attacker looks for system vulnerabilities and makes a deliberate attempt to evade security services to gain unauthorized access to system information and control of system services. It is difficult to identify all possible vulnerabilities of a system, but it is a good practice to use security mechanisms to detect, prevent, and recover from commonly known threats and vulnerabilities [18]. Recent research has identified several security breaches and cyber vulnerabilities for DERs. Based on our literature review [3], [5–6], [11], [12], [15], [19–23], the following are the most commonly known vulnerabilities.

- **Man-in-the-middle (MITM):** In a MITM attack, an opponent gains access over communication systems to manipulate the data exchanged between two devices in the system. If the attack is successful, the opponent could delete, modify, or add data.
- **Replay:** The objective of this attack is to acquire and repeat, or delay, valid data from the system to cause malfunctions.
- **Eavesdropping:** In this passive attack, the opponent tries to acquire valid data and information about the system. Once information has been acquired, the opponent could use it for other malicious purposes or even other cyberattacks.
- **Spoofing through security certificates:** Security certificates are used to prove ownership of public keys and also to authenticate a client so he or she can use services from a server. An attacker with unauthorized access to public key certificates could potentially gain unauthorized access to system monitoring and control and perform a data-modification attack later.
- **Denial of service (DoS):** In this type of attack, the objective is to overload the communication network to limit system availability and therefore prevent authorized users from having access to the grid monitoring and control functions. Because control of DERs is centralized, a DoS attack targeting a distribution utility controller may leave all DERs of a feeder unreachable, which could lead to voltage and frequency disruptions.
- **Least privilege violation:** An authorized system user should only have access to the information and functionalities necessary for a specific task. In this type of attack, an opponent tries to access unauthorized services to view and manipulate system data. Once the least privilege principle is violated, the attacker can perform a data-modification attack.
- **Brute force credentials:** In this attack, either software or a human attacker continually attempts to guess the password or a key on a cyphertext. This attack can be time consuming. If the password is weak or if the cryptography has a small key, however, then the attacker has a better chance of succeeding. If the brute-force credentials attack is successful, then the attacker could perform a data-modification attack.

Although this list of vulnerabilities includes the most common cyberattack threats, it is not exhaustive. Cybersecurity researchers continue to identify new vulnerabilities and find novel approaches to secure DERs.

IV. Recommended Device-Level Functionalities for Securing DERs

To increase the electric grid's cybersecurity effectiveness, several industry standards and guidelines for cybersecurity have been developed and established. The North American Electric Reliability Corporation has developed cybersecurity

TABLE II. VULNERABILITIES OF DER COMMUNICATION PROTOCOLS

Protocol	MITM	Replay	DoS	Eavesdropping	Spoofing	Data Modification
SunSpec Modbus	X	X	X	X	X	X
IEEE 1815 (DNP3)	X	X	X	X	X	X
IEEE 2030.5 (SEP2)			X			X

requirements for critical infrastructure protection. These requirements, however, apply only to issues of the bulk power system and are not applicable to DERs [24]. Similar, the National Institute of Standards and Technology has developed a cybersecurity framework, which suggests ways that organizations can develop processes to manage system cyber risks; however, it does not address cybersecurity risks of DERs [25].

In addition to the aforementioned efforts, other organizations have developed security standards and guidelines for power systems, including: (a) IEC Std. 62351, which provides security for information exchange in power systems [26] and is widely used in Europe; (b) the U.S. Department of Energy, which developed the Cybersecurity Capability Maturity Model to provide cybersecurity benchmarks and guidance for utilities on effective risk-management processes that consider specific organizational requirements and constraints [27]; and (c) IEEE Std. C37.240-2014, which provides cybersecurity requirements for substation automation, protection, and control systems [28–29].

These security standards and guidelines are all designed to address the bulk energy system, and although these principles help improve DER security, they do not address the particularities of DERs. Attackers are constantly evolving and finding new breaches for inflicting cyberattacks. IEEE Std. 1547-2018 [13] is the most widely used standard in the United States for interconnection and operability of DERs, and this standard requires specific communication protocols. Thus, this paper considers only those communication protocols, namely, IEEE Std. 1815 (DNP3), SunSpec Modbus, and IEEE Std. 2030.5 (SEP2)/Common Smart Inverter Profile (CSIP).

Previous research has identified vulnerabilities for many different communication protocols. Table II summarizes some (but not all) known vulnerabilities for such protocols [30–32]. In Table II, the least privilege violation and brute force credentials attack have been combined into "data modification" attack, a broader attack category that includes those two specific categories. Regarding the protocols, SunSpec Modbus is the simplest of the three and has no security measures. DNP3 has a few security measures, such as authentication and message integrity check. The IEEE Std. 2030.5 (SEP2) is the only communication protocol from Table II that requires and implements cryptography [32], and although this protocol is resilient against most of the cyber threats listed in Table II, it is not a complete solution for known vulnerabilities [23].

In related work, several recent research papers have detailed strategies to help create an effective and efficient way of securing next-generation DERs that will be connected to the distribution grid [5], [6], [20], [21], [23], [33–36]. This paper specifically focuses on practical cybersecurity functionalities for DERs, based on a year-long discussion with personnel from utilities, vendors, manufacturers, and researchers. These functionalities have been verified with the subgroup "DER Devices & Servers" within the SunSpec/Sandia DER Cybersecurity Working Group [37], [38]. Outcomes of this research effort include the following recommended cybersecurity functionalities at the device level for DERs; if implemented, these solutions will help protect DERs from the vulnerabilities listed in Section III.

Hardened operating system: Distribution management systems at a control center can be connected to other computer networks and are vulnerable to several types of cyber threats. Outdated software and lack of antiviruses put the system at risk of additional vulnerabilities. Using up-to-date firmware and operating systems, together with security services and software from the control center to DERs and communication systems, is a necessary procedure to harden the whole Information and Communication Technology (ICT) system. In addition, it is good practice to scan the whole communication network of the smart distribution system to detect connected devices and identify the firmware and software status of all DERs. If the software or firmware of the DER is not up to date, then it should be updated to the latest and most secure version. This measure helps to protect from least privilege violation and DoS attacks.

Roll-back firmware update: Firmware is the driving software of the DER, and—as is the case for most software—it can be updated to newer and improved versions. New firmware versions, however, can also have vulnerabilities or other security issues. In such cases, the DER should have a quick and effective roll-back firmware feature in place, so the system can rapidly revert to the previous working firmware to limit any possible cyber-physical impact on the electric grid.

Authentication: This is the process to verify a user's identity, based on known information. Users are granted different privileges for accessing system services, based upon their authentication. In the DER scenario, this security service is extremely important for ensuring that utility personnel, customers, and vendors have different privileges for accessing the DER monitoring and control systems. This measure helps protect DERs from least privilege violation.

Password management: If a cyber-physical system does not enforce use of strong passwords, then the system is highly vulnerable to brute force attacks. Thus, a password-management system can be used as a tool to ensure that all users have strong passwords. Another important feature is to restrict access from a user that has consecutive failed log-in attempts. This measure helps to protect the distribution grid from brute force credential attacks and least privilege violations.

Transport layer security (TLS): Transport layer security focuses on ensuring secure and reliable communication between two hosts in a network. The TLS protocol begins with a start request from the client to the server, then continues with the exchange of a specific set of messages, known as the "TLS handshake." After the handshake, the two hosts can exchange encrypted data. There are many cipher suites available for

TLS cryptography, and future research will provide recommended suites for DERs. This security protocol ensures encryption, authentication, and integrity of data in the transport layer. TLS version 1.2 or 1.3 should be included in DERs. This measure helps to protect the DER against MITM, eavesdropping, replay, and spoofing cyberattacks.

Certificate revocation list: Certificate revocation is a security mechanism that uses public key infrastructure and provides a list of a user certificate status. It indicates whether the certificate has been revoked and thus should not be trusted. In the DER scenario, this security service is important to identify and keep track of devices and users that are no longer authorized to access system services. This measure helps to protect DERs from least privilege violation, MITM, eavesdropping, replay, and spoofing attacks.

Expired certificate: When a DER is deployed in the field for the first time, it receives a certificate that lists the lifespan of the device, so it can authenticate its connection with the distribution system control center. If the DER becomes compromised, this lifetime certificate adds vulnerabilities. To avoid these vulnerabilities, the DER main certificate should have an expiration date and should be replaced at a specific given frequency. This measure helps to protect DERs from least privilege violation, MITM, eavesdropping, replay, and spoofing attacks.

Session renegotiation: When a client requests a TLS session after a previous session has been established, the standard TLS protocol uses stored information from previous sessions to skip some steps of the TLS handshake and to make the renegotiation of the session faster. This feature, however, introduces vulnerabilities to cyber threats. To overcome such exposure, we recommend that if a TLS session has been active for longer than the maximum period permitted, then it should be renegotiated. Session identification resumption is a feature that can be used to protect against this type of breach and should be a feature of the TLS protocol used for DER applications. This measure helps protect DERs from MITM, eavesdropping, and spoofing attacks.

Supply chain: DERs typically incorporate components from multiple vendors, creating a complex supply chain. In such scenarios, if a single internal device or component is compromised, then the whole DER could also be compromised. To avoid such security breaches, the entire supply chain should be carefully studied, and each component and device used for manufacturing DERs should come from trustworthy vendors and organizations. This measure helps to protect DERs from eavesdropping and least privilege violation.

Another important aspect of cybersecurity for distribution systems is a trade-off between high cybersecurity levels and smooth electric system operation. When grid operation becomes more complex, there is a possibility of false-positive lockups affecting a healthy DER, which could negatively impact system operation. Consequently, some utilities choose to turn off some DER security functions for the sake of simple system operation, but this practice creates vulnerabilities to cyberattacks. Finally, it is important to note that even when all the cybersecurity functionalities discussed herein are implemented, it is impossible to guarantee zero vulnerabilities. Rather, these functionalities simply help limit vulnerabilities and their cyber-physical impact on DERs and distribution systems.

V. Conclusion

The electric grid is shifting toward a high penetration level of DERs, including sources of renewable energy. This trend requires an innovative method of distribution system operation. The recent IEEE Std. 1547-2018 allows for the dispatch of active and reactive power and is the most widely used standard in the United States for interconnection and operability of DERs. The communication protocols recommended by this standard are Modbus, DNP3, and SEP2. These ICT standards all have security vulnerabilities, but the current version of IEEE Std. 1547-2018 does not yet include cybersecurity recommendations.

This paper summarizes some of the common known cyberattacks targeting DERs and the potential impact of such attacks on smart grid operation. It also recommends a succinct set of DER cybersecurity functionalities that can be incorporated to improve device-level cybersecurity of DERs. These recommendations are based on a joint effort that was developed after a year-long discussion among utilities, vendors, manufacturers, and researchers. As a final note, vulnerabilities for DERs are related to the communication protocols and control features of DERs only. Because the communication protocols at transmission level may be different, these recommendations are limited to DERs only.

Acknowledgements

The authors would like to thank Cedric Carter and all the other contributors from the SunSpec/Sandia Distributed Energy Resource Cybersecurity Working Group [37] and National Electrical Manufacturers Association who provided their valuable comments and feedback on the recommended functionalities. The authors would also like to thank Professor Pankaj Kumar Sen (PK) for his extended paper review. Ricardo Siqueira de Carvalho received a scholarship from CAPES—Brazilian Federal Agency for Support and Evaluation of Graduate Education within the Ministry of Education of Brazil (scholarship number 99999.013282/2013-01).

References

[1] B. Kroposki, B. Johnson, Y. Zhang, V. Gevorgian, P, Denholm, B. M. Hodge, and B. Hannegan, "Achieving a 100% Renewable Grid: Operating Electric Power Energy Systems with Extremely High Levels of Variable Renewable," *IEEE Power and Energy Magazine*, vol. 15, no. 2, pp. 61–73, 2017.

[2] R. Siqueira de Carvalho and S. Mohagheghi, "Analyzing Impact of Communication Network Topologies on Reconfiguration of Networked Microgrids, Impact of Communication System on Smart Grid Reliability, Security and Operation," *2016 North American Power Symposium (NAPS)*, Denver, Colorado, United States, pp. 1–6, 2016.

[3] A. Sundararajan, T. Khan, A. Moghadasi, and A. I. Sarwat, "Survey on Synchrophasor Data Quality and Cybersecurity Challenges, and Evaluation of their Interdependencies," *Journal of Modern Power Systems and Clean Energy,* vol. 7, No. 3, pp. 449–467, 2018.

[4] Electricity Information Sharing and Analysis Center (E-ISAC), "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," Mar. 2016.

[5] A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security," *Energies,* vol. 11, pp. 1996–1073, 2018.

[6] D. Saleem, A. Sundararajan, A. Sanghvi, J. Rivera, A. Sarwat, and B. Kroposki, "A Multidimensional Holistic Framework for the Security of Distributed Energy and Control Systems," in *IEEE Systems Journal* (forthcoming).

[7] SANS, "The Impact of Dragonfly Malware on Industrial Control Systems," SANS Institute InfoSec Reading Room Technical Report, 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/paper/36672.

[8] R. M. Lee, M. J. Assante, and T. Conway, "Crashoverride: Analysis of the Threat to Electric Grid Operations," *Dragos Technical Report*, 2016. [Online]. Available: https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.

[9] US-CERT, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *US Computer Emergency Readiness Team (CERT) Alert* (TA18-074A), 2018. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA18-074A

[10] K. Higgins, "Ukraine Security Service Stops VPNFilter Attack at Chlorine Station," Dark Reading Online Article [Online]. Available: https://www.darkreading.com/attacksbreaches/ukraine-security-service-stops-vpnfilter-attack-at-chlorine-station/d/d-id/1332282.

[11] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in Distributed Power Systems," in *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[12] D. J. Sebastian and A. Hahn, "Exploring Emerging Cybersecurity Risks from Network-Connected DER Devices," *2017 North American Power Symposium (NAPS)*, Morgantown, West Virginia, United States, pp. 1–6, 2017.

[13] IEEE, "IEEE Std. 1547-2018—IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," 2018.

[14] Y. Xue, M. Starke, J. Dong, M. Olama, T. Kuruganti, J. Taft, and M. Shankar, "On a Future for Smart Inverters with Integrated System Functions," *2018 9th IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Charlotte, North Carolina, United States, pp. 1–8, 2018.

[15] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," in *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012..

[16] P. Kaster and P. K. Sen, "Cybersecurity and Rural Electric Power Systems: Considering Competing Requirements for Implementing a Protection Plan," in *IEEE Industry Applications Magazine,* vol. 23, no. 5, pp. 14–20, Sept.–Oct. 2017.

[17] W. Stallins, *Criptography and Network Security*, 7th edition, London: Pearson Education, 2018.

[18] The MITRE Corporation, "Common Vulnerabilities and Exposures (CVE)" [Online]. Available: https://cve.mitre.org/ [Accessed Jun. 12, 2019].

[19] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, (2017). "Cyber Security Assessment of Distributed Energy Resources," *2017 IEEE Photovoltaic Specialists Conference*, Washington. D.C., United States, June 2017.

[20] S. Gholami, S. Saha, and M. Aldeen, "A Cyber Attack Resilient Control for Distributed Energy Resources," *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Turin, Italy, pp. 1–6, 2017.

[21] J. Qi, A. Hahn, X. Lu, J. Wang, and C. Liu, "Cybersecurity for Distributed Energy Resources and Smart Inverters," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016.

[22] B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andren, C. Seitl, F. Kupzog, and T. Strasser, "Investigating Cyber-Physical Attacks Against IEC 61850 Photovoltaic Inverter Installations," *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Luxembourg, pp. 1–8, 2015.

[23] N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, C. Lai, P. Cordeiro, A. Hasandka, M. Martin, and C. Howerter, "Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources," *2019 IEEE Power and Energy Conference at Illinois (PECI)*, Champaign, Illinois, United States, 2019, pp. 1–8.

[24] North American Electric Reliability Corporation (NERC), "Critical Infrastructure Protection (CIP) Standards" [Online]. Available: https://www.nerc.com/pa/Stand/pages/cipstandards.aspx [Accessed June 13, 2019].

[25] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity" [Online]. Available: https://www.nist.gov/cyberframework/framework [Accessed June 13, 2019].

[26] IEC, "IEC Standard 62351—Power Systems Management and Associated Information Exchange—Data and Communications Security," 2018.

[27] U.S. Department of Energy, "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)" [Online]. Available: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1 [Accessed Jun. 13, 2019].

[28] IEEE, "IEEE Standard C37.240-2014—IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems," 2014.

[29] R. Siqueira-de-Carvalho, P. K. Sen, Y. N. Velaga, L. F. Ramos, and L. N. Canha, "Communication System Design for an Advanced Metering Infrastructure," *Sensors*, Vol. 18, 2018.

[30] R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 Broadcast Communications in SCADA Systems," in *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474–1485, Aug. 2016.

[31] A. Shahzad, M. Lee, Y. K. Lee, S. Kim, N. N. Xiong, J. Y. Choi, and Y. H. Cho, "Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information," *Symmetry*, vol. 7, 2015.

[32] IEEE, "IEEE 2030.5-2018—IEEE Standard for Smart Energy Profile Application Protocol," 2018.

[33] A. Veichtlbauer, O. Langthaler, D. Engel, C. Kasberger, F. Pröstl Andrén, and T. Strasser, "Towards Applied Security-by-Design for DER Units," *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Berlin, Germany, pp. 1–4, 2016.

[34] G. Dondossola, F. Garrone, G. Proserpio, and C. Tornelli, "Impact of DER Integration on the Cybersecurity of SCADA Systems—The Medium Voltage Regulation Case Study," *CIRED 2012 Workshop: Integration of Renewables into the Distribution Grid*, Lisbon, Portugal, 2012, pp. 1–4.

[35] F. Kargl, R. W. van der Heijden, H. König, A. Valdes and M. C. Dacier, "Insights on the Security and Dependability of Industrial Control Systems," in *IEEE Security & Privacy*, vol. 12, no. 6, pp. 75–78, 2014.

[36] V. Kounev, D. Tipper, A. A. Yavuz, B. M. Grainger, and G. F. Reed, "A Secure Communication Architecture for Distributed Microgrid Control," in *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2484–2492, Sept. 2015.

[37] Sunspec Alliance, and Sandia National Laboratories, "SunSpec/Sandia Distributed Energy Resource Cybersecurity Workgroup" [Online]. Available: https://sunspec.org/sunspec-cybersecurity-workgroup/ [Accessed Jun. 19, 2019].

[38] D. Saleem, and C. Carter. 2019. "Certification Procedures for Data and Communication Security of Distributed Energy Resources." Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-73628. https://www.nrel.gov/docs/fy19osti/73628.pdf