Vulnerability Detection Methodology for a Digital Signal Processor Micro-Controller at Edge Level Distributed Energy Resource Controller

Pankaj Bhowmik
Electrical Energy Systems Integration Group
Oak Ridge National Laboratory
Oak Ridge, Tennessee
bhowmikp@ornl.gov

Michael Starke
Electrical Energy Systems Integration Group
Oak Ridge National Laboratory
Oak Ridge, Tennessee
starkemr@ornl.gov

Ben Dean
University of Tennessee
Knoxville, Tennessee
bdean7@vols.utk.edu

Madhu Chinthavali
Electrical Energy Systems Integration Group
Oak Ridge National Laboratory
Oak Ridge, Tennessee
chinthavalim@ornl.gov

***Abstract*—Integration of renewable energy and energy storage based Distributed Energy Resource (DER) assets to the grid has seen an upsurge over the past few decades. Traditionally, energy would be generated at a thermal or nuclear power plant and then transmitted over long distance through the transmission grid and then supply to the customers at the distribution grid. Modern renewable energy based DER assets have brought energy production at the edge of distribution grid, which has made the grid vulnerable to cyber intrusion as the power flow controllers for such DER assets are now distributed across the grid from distribution level to transmission level. This paper discusses the vulnerability posed by such power flow controllers of DER assets and demonstrates a detection methodology for unauthorized access and manipulation of system configuration for Digital Signal Processor based Microcontrollers. Experimental results proving efficacy of the methodology have been shown in paper.**

Keywords— Vulnerability, Digital Signal Processor, Interrupt Service Routine, Clocking, Edge Level Controller

I. INTRODUCTION

With increasing DER penetration right from distribution grid to transmission grid, there has been higher demand for grid automation and control. But increased grid smartness also serves as a double-edged sword as it also makes it more vulnerable to unauthorized access because of the involvement of many layers of software and hardware integration with multiple Industrial Control Systems (ICS) associated with physical Intelligent Electronic Devices (IEDs) [1]. The key aspects of such vulnerability are:

- Multiple access points for unauthorized access
- Increasing ICS with DER integration
- Greater coordination and real time data exchange between utilities, market operators and customers.
- Greater and faster connectivity with high speed communication, as for instance, 4-G LTE networks.
- Distributed generation and energy storage spread across the distribution and transmission grid

The National Cybersecurity and Communications Integration Center has published its findings [2], wherein it reports out of 245 total reported incidents, about 79% of FY2014 incidents of threats and attempts to unauthorized access being reported by energy sector.

The reliance of the power grid on Supervisory Control and Data Acquisition (SCADA) has led to exploitable vulnerabilities in its infrastructure, and multiple cyber-attacks have occurred that target these ICSs. These incidents include Stuxnet (2010), Havex (2013), Blackenergy (2015), CrashOverride (2016), and Triton (2017) [3]. All these incidents were on energy companies or on utility distribution companies. The impacts were serious as it created power outages for a part of city with thousands of customers. An electric utility in the United States was impacted by a malware in recent years (2019) where the internet-based communications for the utility was disrupted [4]. Such incidents demonstrate the fact that with growth of renewables and increased grid smartness in terms of generation and loads, we ought to carefully identify the vulnerabilities and protect the grid.

It may be worth mentioning that DER installation has grown tenfold in the past decade in the USA, including both solar installations and utility scale battery installations [5]-[6]. These solar installations all include potentially vulnerable inverters. The US Energy Information Agency reports that the energy storage installation capacity in the states would be reaching about 2.4 GW by 2021 as compared to 1.25 GW in 2019 [5]. DER systems now play a role in grid support during disturbances, instead of simply disconnecting, which requires a higher level of integration with utility SCADA control. This poses a higher risk with increasing DER adoption [7]. The impact of these cyber-attacks on the power grid can have major consequences. These include financial loss, deteriorated services, and physical damage, such as the loss of equipment [8]. Ref. [3] demonstrates the effect of Crash Override on the power grid, and the resulting load shedding required as one or more remote terminal units were compromised. Having adequate cyber security protection on the power grid helps ensure that these situations can be avoided.

978-1-7281-9591-9/20/$31.00 ©2020 IEEE

As the number of consumer-owned DER devices on the power grid grows, these devices will require a high level of interoperability, as they are commonly tied into preexisting networks with vastly different security levels [9]. The current operation modes of DER inverters lend themselves to inherent flaws [10]. The potential impact on power grid due to control schemes of inverters is shown in Fig.1.

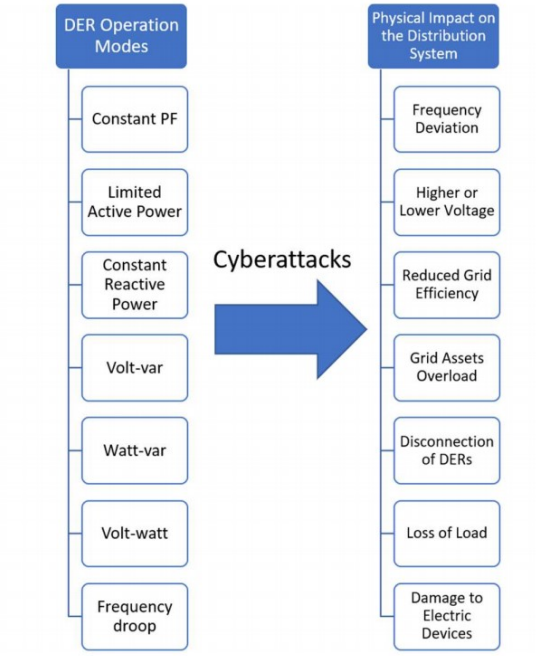

Fig. 1. Potential impact of DERs result from cyber attacks [9]

A proper amalgamation of the best practices from all domains that coalesce to integrate a DER to the grid can be utilized to make the grid more resilient and secure [4]. This amalgamation of best practices is shown in Fig. 2.

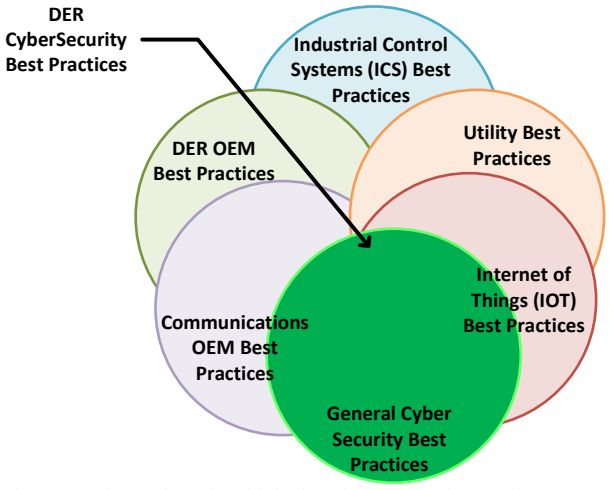

Fig. 2. Amalgamation of multiple domain best practices to form DER Security best practice

II. Vulnerability posed by Digital Signal Processing Microcontroller (DSP MC) in Edge Level Controller (ELC)

This section discusses the vulnerability of DERs with regards to Digital Signal Processing Microcontroller (DSP µC) at Edge-Level Controller (ELC). The system architecture demonstrating flow of control command and power flow for a DER is shown in Fig. 3.

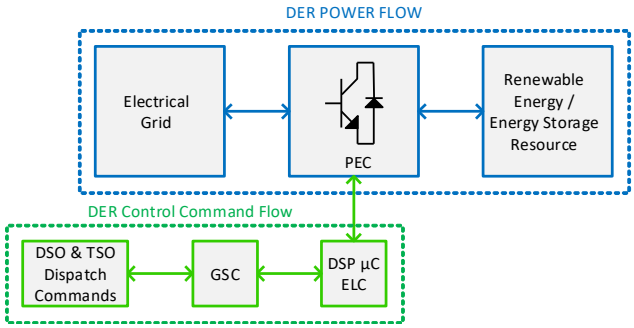

Fig. 3: System Architecture showing flow of Control Command from DSO & TSO level to ELC and flow of Electrical Power from/to Grid through PEC to/from Renewable Energy / Energy Storage Resource

It may be seen that DER at its core comprises of power semiconductor devices-based Power Electronic Converters (PECs), which may be utilized to regulate the voltage, current and power factor at the either source or grid side of the PECs. The various control operation modes of a DER, as shown in Fig. 1, are performed by the Edge Level Controller (ELC). The ELC comprises of a Digital Signal Processor (DSP) Microcontroller (µC), which serves as the brain of the ELC. The ELC is commanded to perform the grid support functions by the Grid Support Controller (GSC) via communication channels, which may be viewed as a potential vulnerability in terms of cyber-security. The GSC may be operated based on control commands dispatched to it, via communication networks, by the energy distribution network operators, viz. Distribution System Operators (DSOs) or Transmission System Operators (TSOs). This dispatch commands may also be viewed as a potential cyber-security issue. This paper only discusses the cyber security vulnerability posed by DSP µC sitting at the core of Edge Level Controller (ELC).

A. ELC Memory Architecture

In DER ELCs, the input to DSP µC is the real-time measurement data from voltage and current sensor at source and grid side, which is then converted to digital format using Analog to Digital Converter (ADC). The control algorithms reside in the flash memory of DSP µC, which analyzes the data and provides real time digital outputs which are then converted to analog signals using Digital to Analog Converter (DAC). The memory architecture of any DSP µC may be classified into two types, viz.

1. Von Neumann Architecture – CISC (Complex Instruction Set Computer) µCs
2. Harvard Architecture – RISC (Reduced Instruction Set Computer) µCs

The data flow diagram for both architectures are shown in Figs. 4 and 5. It may be seen that the Von Neumann Architecture shares a common signal and storage bus for data and instructions, whereas Harvard Architecture has separate signal and storage bus for data and instructions. Typically, DSP µCs used in PECs are RISC µCs. The program resides in Flash Memory, which is a non-volatile memory. Once the code is running, some functions residing in flash may also be run in the RAM, a volatile memory. As soon as the sensor data is digitized by the ADC, the control algorithms performed on the data on an assembly level is a combination of basic mathematical operations, viz. addition, subtraction, multiplication and division. The data is stored in registers, as they are the fastest and most time synchronized memory element available. All of these assembly opcodes are performed on the registers at each instruction cycle, which is synchronized via system clock. The system clock is synchronized from a physical piezo-electric quartz crystal oscillator, which resonates at the system clock frequency. Thus, it may be noted that the crystal oscillator is the most sensitive device for reliable operation of the DSP µC.

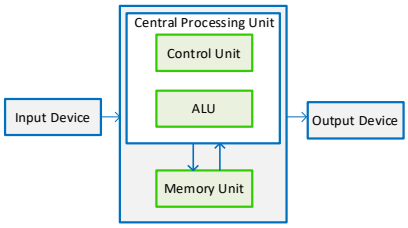

Fig. 4: Von Neumann Architecture: CISC µC

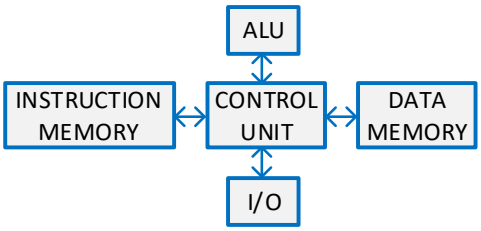

Fig. 5: Harvard Architecture: RISC µC

The power for the crystal oscillator and all the execution of assembly level instructions at the registry level is derived from the external power supply to the DSP µC. Now, the oscillator frequency may be increased or decreased via µC settings registries, which generally resides in Flash Memory, which may be altered by the programmer. This accessibility poses a huge cyber security threat to DSP µCs, thereby making the DER PEC not resilient anymore. Now, the accessibility may be gained by physical access to the hardware or during Over the Air (OTA) updates to the DSP µCs. There are derived clocks from the actual oscillator clock pulses which synchronize various control opcodes being executed in the µC. As the µC oscillator frequency is set to a lower frequency, the reliability of control operation performed by the overall DSP µC fails as the operations would not be performed in a time synchronized manner and there is high possibility of undesired data being pushed off DAC of the µC. In the contrary, if the µC oscillator frequency is set to a higher frequency than rated operation frequency, the crystal oscillator's performance would deteriorate, and the clock synchronization pulses might be erroneous. This would again result in failure of the execution of instruction opcodes in a timely synchronized manner. This decrease or increase in oscillator frequency may be termed as Under-Clocking or Over-Clocking. Therefore, it may be concluded that accessibility to µC system clock oscillator poses a major vulnerability in DSP µCs at Edge Level Controllers (ELCs).

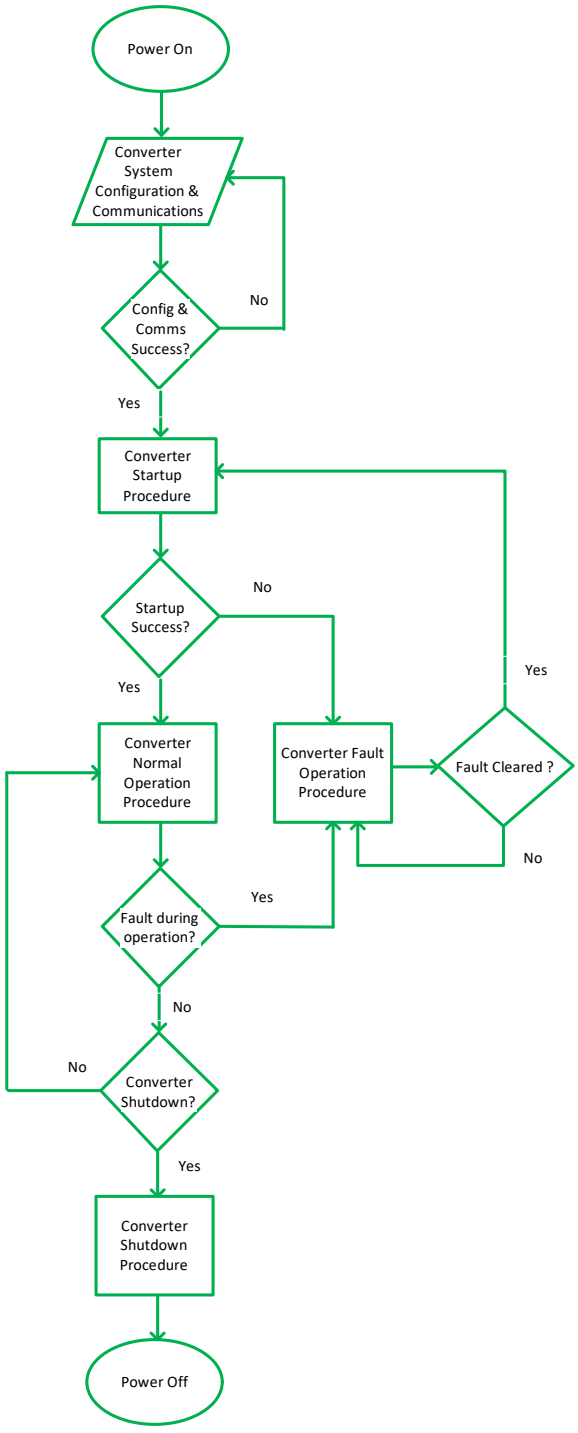

Fig. 6. DSP µC Operational Flow Diagram

B. *ELC Vulnerability Example*

A typical operational flow chart for a DSP µC based ELC is shown in Fig. 6. One instance of the control modes of operation of a Battery Energy Storage based DER ELC is active power control. In a situation where the ELC is under-clocked or over-clocked, the Interrupt Service Routine (ISR) time period for a DSP µC would vary as it is a derivative of the Phase Locked Loop (PLL) which generates the system clock frequency. It may be noted that the code for the Operational Flow Diagram resides inside this interrupt sub-routine program. Now, this code processes incoming analog measurements from the PEC and outgoing digital signals to the PEC. Based on the measurements, active power setpoint commands and active power control algorithm, it locks with the grid frequency, goes through multiple PI loops and generates the Digital Signals required to operate the semiconductor devices in a PEC. Since the active power processed by the PEC is computed from analog measurements inside this ISR, the computed value would vary as the computation is dependent on the number of samples of analog measurement data. Even the control loops have integrators which are a function of the interrupt service routine. An example of a 1-ϕ DER PEC Edge Level Control algorithm is shown in Figs. 7, 8 and 9.

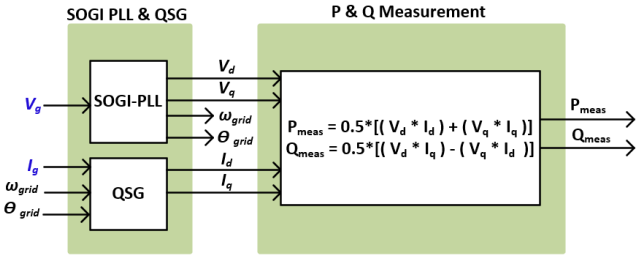

Fig. 7. Signal flow diagram for analog measurements from converters and utilization to derive synchronous frame reference voltage, current and power

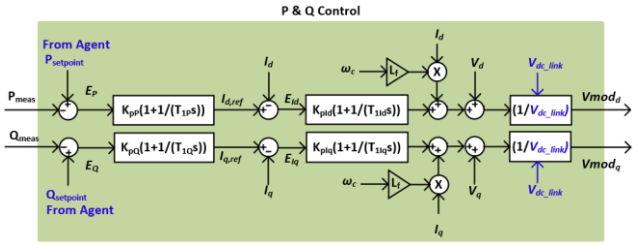

Fig. 8 Signal flow diagram for P-Q Control of energy storage inverter in synchronous control frame of reference

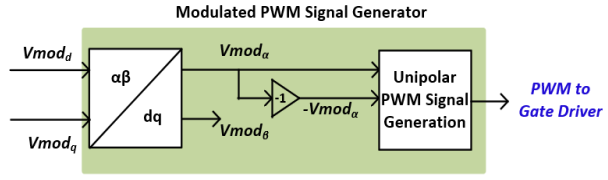

Fig. 9. Signal Flow Diagram for generation of PWM Signals from synchronous frame modulation indices

Any variation in ISR frequency of the control algorithm implementation in DSP would go undetected and undesired active power flow would happen between DER and grid, which in turn can be detrimental to the grid voltage quality. The scale of impact would depend upon the DER capacity and location of the DER at the utility grid. The next section presents the detection methodology for such vulnerability in a DSP µC.

III. Vulnerability Detection Methodology of DSP µC Threat at ELC

A DSP µC utilizes external power supply for its operation. During variation in ISR frequency, power demands of a DSP µC would vary from normal operation. This power demand may be monitored to trigger a security alarm based on the abnormal power demanded by the DSP µC and if the demand varies outside acceptable limits, the whole DER PEC may be identified as a potentially compromised DER asset and DER system would be taken offline and shutdown, thereby avoiding any potentially catastrophic failure. The implementation of such security would greatly enhance the reliability, resiliency and security of any DER PEC.

In order to evaluate the detection methodology discussed above, an experimental setup with TI F28379D DSP µC Evaluation Kit Board has been designed. The TI F28379D DSP µC board receives the analog measurements from a C-HIL (Controller-Hardware in Loop) setup, where a single-phase inverter with a battery source is modelled. It sends digital signal to the HIL hardware to perform real time control of the HIL inverter model. All these signal conversion and processing for inverter are performed in the normal operation procedure, and the entire instruction flow diagram inside DSP µC is already shown in Figs. 6-9. As discussed earlier in previous section, the code runs in an ISR whose frequency may be altered. As part of our testing, the ISR frequency has been changed and the resultant Voltage, Current, Power as well as Capacity requirements by DSP µC are logged. The DSP µC is powered through usb port from a regular computer usb port. The usb power wire passes through a meter which logs the measurement of Instantaneous Voltage, Current and Power, as well as Capacity up to three significant figures, as desired by DSP µC.

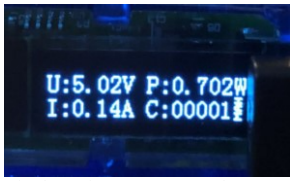

Fig. 10. LED Display of Measurement for DSP Voltage, Current , Power and Capacity Demand: During Bootup Operation of DSP µC

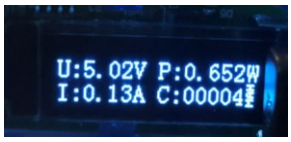

Fig. 11. LED Display of Measurement for DSP Voltage, Current , Power and Capacity Demand: During Normal Operation of DSP µC at ISR Frequency of 10kHz

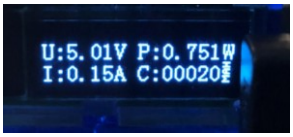

Fig. 12. LED Display of Measurement for DSP Voltage, Current , Power and Capacity Demand: During Normal Operation of DSP µC at ISR Frequency of 20kHz

Figs. 10-12 show the experimental setup LED display of the voltage, current and power demand of the DSP µC. It may be seen that the current and power demand at startup surges, but then settles to a lower value during normal operation. During normal operation, the current and power demand increases only when ISR frequency increases.

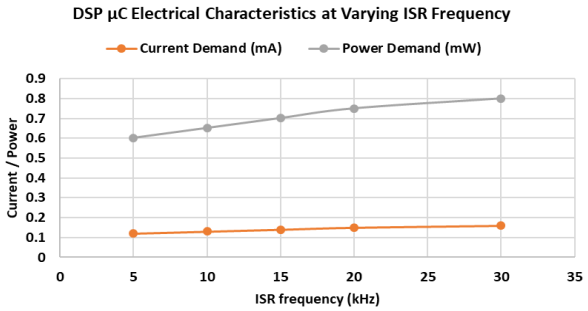

Fig. 13. Current and Power Demanded by DSP µC at varying ISR frequency (DSP control code is same as ISR ferquency varies)

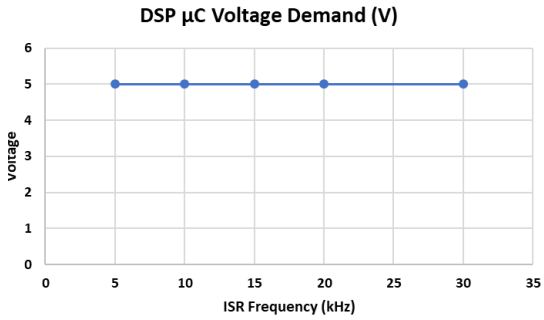

Fig. 14. Voltage Demanded by DSP µC at varying ISR frequency (DSP control code is same asISR frequency varies)

A plot of the current and power required for the same DER ELC controls code at different ISR frequencies are shown in Fig. 13 The voltage characteristics of the DSP µC is shown in Fig.14. It may be seen that the voltage demand is constant at 5.01~5.02 V as it is tightly regulated by linear voltage regulators. But as expected, the current and power demand increases with increasing ISR frequency. This variation in power demand may be characterized to accurately determine the ISR frequency of control code. In a scenario, where there is cyber intrusion by unauthorized access and manipulation of system clock frequency, the DSP power demand surge may be identified, and DER asset would be declared potentially compromised and taken offline and forced to be shutdown.

IV. Conclusions & Future Work

The current and power demand characteristics of a DSP µC, which is the brain of a DER ELC, has been utilized to detect cyber intrusion and manipulation of system operating conditions. The experimental demonstration of the detection technique has been shown in this paper. This technique makes the DER asset more reliable, secure and resilient from cyber intrusions. As a future work, the power consumed by each individual module inside a DSP µC may be characterized and utilized to detect cyber intrusions.

V. Acknowledgements

The authors would like to gratefully acknowledge support from Oak Ridge National Laboratory for allowing this research and also for supporting post-doctoral associates with funds for self-developmental, and self-initiative research works.

VI. References

[1] Mission Support Center Analysis DOE Report on “Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector” [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf. [Accessed: 23-July-2020]

[2] National Cybersecurity And Communications Integration Center Report on, “ Incident response / Vulnerability Coordination in 2014”, compiled by Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [Online]. Available: file:///C:/Users/p06/Oak%20Ridge%20National%20Laboratory/Communications,%20Controls,%20and%20Optimization%20Software%20Team%20-%20Documents/Papers/IEEE%20Cyber%20PELS%202020/Reference%20Papers/ICS-CERT_Monitor_Sep2014-Feb2015.pdf. [Accessed: 23 July 2020]

[3] A. Castillo, B. Arguello, G. Cruz and L. Swiler, "Cyber-Physical Emulation and Optimization of Worst-Case Cyber Attacks on the Power Grid," 2019 Resilience Week (RWS), San Antonio, TX, USA, 2019, pp. 14-18

[4] J. Foster, S. Lawson, and S. Cox, “Cybersecurity and Distributed Energy Resources”, NREL, Golden, Co, tech., 2020.

[5] P. Hutchins, “U.S. Energy Information Administration - EIA - Independent Statistics and Analysis,” 10-Jul-2019. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=40072. [Accessed: 24-Jul-2020].

[6] M. Mercure, “SEIA, Wood Mackenzie: Solar Accounts for 40 Percent of New U.S. Generating Capacity in 2019,” 20-Mar-2020. [Online]. Available: https://solarindustrymag.com/seia-wood-mackenzie-solar-accounts-for-40-of-u-s-electric-generating-capacity-in-2019. [Accessed: 23-Jul-2020].

[7] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal and M. J. Reno, "Power system effects and mitigation recommendations for DER cyberattacks," in IET Cyber-Physical Systems: Theory & Applications, vol. 4, no. 3, pp. 240-249, 9 2019

[8] H. Lei, B. Chen, K. L. Butler-Purry and C. Singh, "Security and Reliability Perspectives in Cyber-Physical Smart Grids," 2018 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), Singapore, 2018, pp. 42-47

[9] 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, 12 2016

[10] R. S. de Carvalho and D. Saleem, "Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources," 2019 Resilience Week (RWS), San Antonio, TX, USA, 2019, pp. 226-231

[11] H. Albunashee et al., "A Testbed for Detecting False Data Injection Attacks in Systems with Distributed Energy Resources," in IEEE Journal of Emerging and Selected Topics in Power Electronics