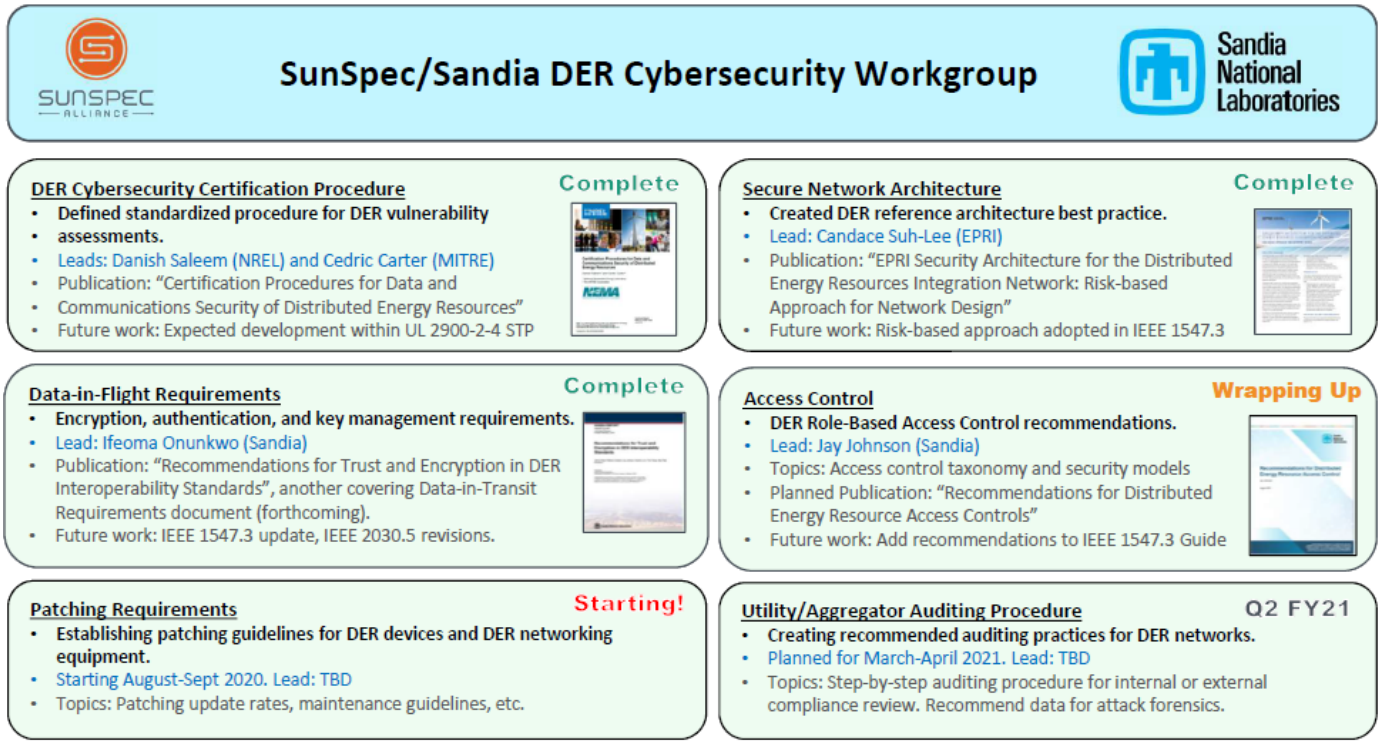
Summary of Sandia DER Cybersecurity Research

Contact Jay Johnson (jjohns2@sandia.gov) for more information.

Last update: September 14, 2020. Sandia Reference: SAND2020-9837 M.

For more than five years, Sandia National Laboratories' Distributed Energy Resource (DER) Cybersecurity Team has analyzed DER cybersecurity risks and addressed technical challenges associated with implementing novel security solutions. Here's a brief summary of this team's work.

DER Cybersecurity Workgroup. Sandia and the SunSpec Alliance formed the DER Cybersecurity Workgroup in Aug. 2017 after realizing the only way to develop realistic solutions in a non-federated environment was to bring all the stakeholders to the table and work through the technical, administerial, and regulatory challenges.[1] The public-private partnership has acted as a meeting place to discuss DER cybersecurity issues and establish recommendations for national and international DER cybersecurity standards. The workgroup participation is now over 500 experts, representing DER vendors, utilities, regulators, national laboratories, and third parties. Early in the workgroup activities, Sandia published a primer on DER cybersecurity to establish a common nomenclature and summarize DER cybersecurity concepts and standards.[2] The status of the workgroup is shown below, with subgroup titles, statuses, leaders, objectives, and outcomes.



[1] SunSpec/Sandia DER Cybersecurity Workgroup. URL: https://sunspec.org/cybersecurity-work-group/

[2] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia Technical Report, SAND2017-13113, Dec 2017.

Solar Roadmap. In 2017, the Department of Energy (DOE) Solar Energy Technologies Office (SETO) funded Sandia to develop a five-year roadmap for solar cybersecurity. The final report recommended activities and specific milestones in areas of stakeholder engagement, cybersecurity research and development, standards development, and industry best practices.[3] The solar roadmap has been a key reference for other DOE offices and used as a cybersecurity template for other renewable energy technologies, including wind.[4]

DER Cybersecurity Assessments. To better understand the type and extent of DER vulnerabilities, Sandia conducted a cybersecurity penetration test of a DER device and DER gateway. Like other security researchers,[5,6] the Sandia team found several security weaknesses in the DER products. The companies were contacted with the findings and the anonymized results were published.[7] The team has also assessed a prototype bump-in-the-wire (BITW) OT-network encryption technology called Module-OT[8,9] as part of a project led by the National Renewable Energy Laboratory, multi-party trust models using named data networking, and several other DER devices.

Threat Models and Consequence Analysis. In 2015, as part of an EPRI-led California Solar Initiative project, the team performed a simplified threat analysis for different DER grid-support functions and provided recommendations based on impact level scores.[10] Later, distribution and transmission power system simulations were conducted to better predict the impact of malicious control of DER resources on the power system[11] including a detailed distribution system analysis for malicious control of volt-var functionality.[12]

Network Architecture. The Sandia team used a power system and networking co-simulation environment to investigate cybersecurity improvements when deploying a suite of different cybersecurity defenses. By red teaming these simulated DER networks, defensive topologies were objectively evaluated using confidentiality, integrity, and availability scoring metrics. It was found that segmentation, encryption, and moving target defense (MTD)—which dynamically changes endpoint IP and port numbers using software-defined networks—all provided quantifiable improvements to the utility-to-DER control network.[13] In the DER Cybersecurity Workgroup, EPRI led a group to establish more comprehensive network architecture requirements based on impact/risk levels (e.g., DER nameplate ratings).[14] Sandia has also researched approaches for quantifying the

---

[3] J. Johnson, "Roadmap for Photovoltaic Cyber Security," Sandia Technical Report, SAND2017-13262, Dec 2017.
[4] A. Sanghvi, et al., "Roadmap for Wind Cybersecurity," US DOE EERE Report, July 2020.
[5] F. Bret-Mounet, "All your Solar Panels are Belong to Me," DEF CON 24.
[6] W. Westerhof, "How an Intern Hacked the Powergrid: The Horus Scenario," SHA2017.
[7] C. Carter, I. Onunkwo, P. Cordeiro, J. Johnson, "Cyber Security Assessments of Distributed Energy Resources," IEEE PVSC, Washington, DC, 25-30 Jun 2017.
[8] W. Hupp, et al., "ModuleOT: A Hardware Security Module for Operational Technology," IEEE Texas Power and Energy Conference (TPEC), College Station, TX, February 6–7, 2020.
[9] C. Lai, P. Cordeiro, A. Hasandka, N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, M. Martin, "Cryptography Considerations for Distributed Energy Resources," IEEE Power and Energy Conference at Illinois (PECI), Champaign, IL, 2019.
[10] J. Henry, et al., Cyber Security Requirements and Recommendations for CSI RD&D Solicitation #4 Distributed Energy Resource Communications, Oct. 2015.
[11] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches Bernal, M. Reno, "Power System Effects and Mitigation Recommendations for DER Cyber Attacks," IET Cyber-Physical Systems: Theory & Applications, Jan 2019.
[12] C. B. Jones, et al., Volt-Var Curve Reactive Power Control Requirements and Risks for Feeders with Distributed Roof-Top Photovoltaic Systems, Energies, Vol. 13, No. 17, pp. 4303, Aug 2020.
[13] J. Johnson, I. Onunkwo, P. Cordeiro, B. Wright, N. Jacobs, C. Lai, "Assessing DER Network Cybersecurity Defences in a Power-Communication Co-Simulation Environment," IET Cyber-Physical Systems: Theory & Applications, March 2020.
[14] "EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-Based Approach for Network Design," EPRI Report 3002016781, Oct 2019.

trust between network nodes in order to provide secure routing for DER traffic[15] and device-level verification of grid-support setpoints.[11]

DER Protocols. Sandia has studied the security features in IEC 61850 and IEEE 1547-mandated protocols extensively. Encryption, authentication, and key management recommendations for each of the data-in-flight protocols were created in a DER Cybersecurity Workgroup.[16] In another paper, a more comprehensive discussion of the IEEE 2030.5 Common Smart Inverter Profile (CSIP) trust and encryption requirements was presented along with an exploration of advanced or alternative approaches to security in the DER ecosystem.[17]

Access Control. Sandia led the Access Control subgroup within the DER Cybersecurity Workgroup to define a strict control environment where users are authorized to access DER monitoring and control features through three steps: (a) user is identified using a proof-of-identity, (b) the user is authenticated by a managed database, (c) and the user is authorized for a specific level of access. The subgroup identified options for the DER access control policy, model, and mechanisms and provided draft standards language that could be adopted for DER access control.[18]

Standards and Guides. With interoperability requirements being added to IEEE 1547 and California Electric Rule 21, there was increasing pressure on the DER industry and utilities to establish cybersecurity guidance. To address this gap, a committee was formed to create IEEE 1547.3 *Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*. Sandia volunteered to lead a subgroup to write the justification for the guide and background material sections; and contributed substantially to the access control section and data-in-flight requirements in the latest draft. In parallel with that effort, Sandia is contributing to cybersecurity discussions within the California Rule 21 Smart Inverter Working Group (SIWG) and is acting as an advisor for the NASEO and NARUC Cybersecurity Advisory Team for State Solar (CATSS) project.

Intrusion Detection Systems. Sandia leads a large R&D program to create a distributed proactive intrusion detection and mitigation system (PIDMS) sensors. In the project, communications to and between PV inverters or other DER is analyzed using behavior-based and signature-based intrusion detection system (IDS) tools to detect and prevent malicious commands to DER using machine learning-based classifiers that analyze the cyber-physical data using deep packet analysis. To date, the team has demonstrated the benefit of using cyber and physical data for classification[19], compared different machine learning algorithms and the performance differences between behavior- and signature-based IDSs,[20] and defined cyber-physical observability for power systems.[21]

---

[15] J. Obert, A. Chavez, J. Johnson, "Distributed Renewable Energy Resource Trust Metrics and Secure Routing," Computers & Security, vol. 88, pp. 101620, Jan. 2020.
[16] I. Onunkwo, "Recommendations for Data-in-Transit Requirements for Securing DER Communications," SAND report, (forthcoming).
[17] J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, R. Ih, "Recommendations for Trust and Encryption in DER Interoperability Standards," Sandia Technical Report, SAND2019-1490, Feb 2019.
[18] J. Johnson, "Recommendations for Distributed Energy Resource Access Control," SAND report (forthcoming).
[19] A. Chavez, C. Lai, N. Jacobs, S. Hossain-McKenzie, C. B. Jones, J. Johnson, A. Summers, "Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems," IEEE CyberPELS Workshop 2019, Knoxville, TN, April 29–May 1, 2019.
[20] C.B. Jones, A. Chavez, R. Darbali-Zamora, S. Hossain-McKenzie, "Implementation of Intrusion Detection Methods for Distributed Photovoltaic Inverters at the Grid-Edge," 11th Innovative Smart Grid Technologies, 2020.
[21] N. Jacobs, S. Hossain-McKenzie, A. Summers, C.B. Jones, B. Wright, A. Chavez, "Cyber-Physical Observability for the Electric Grid," 2020 Texas Power and Energy Conference, 2020.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY NNSA

Sandia National Laboratories