SAND2022-9431C

Sandia National Laboratories

Exceptional service in the national interest

Cybersecurity of Distributed Energy Resources

Abraham Ellis, Senior Manager, Renewable Energy Technologies
Jay Johnson, Distinguished Member of Technical Staff

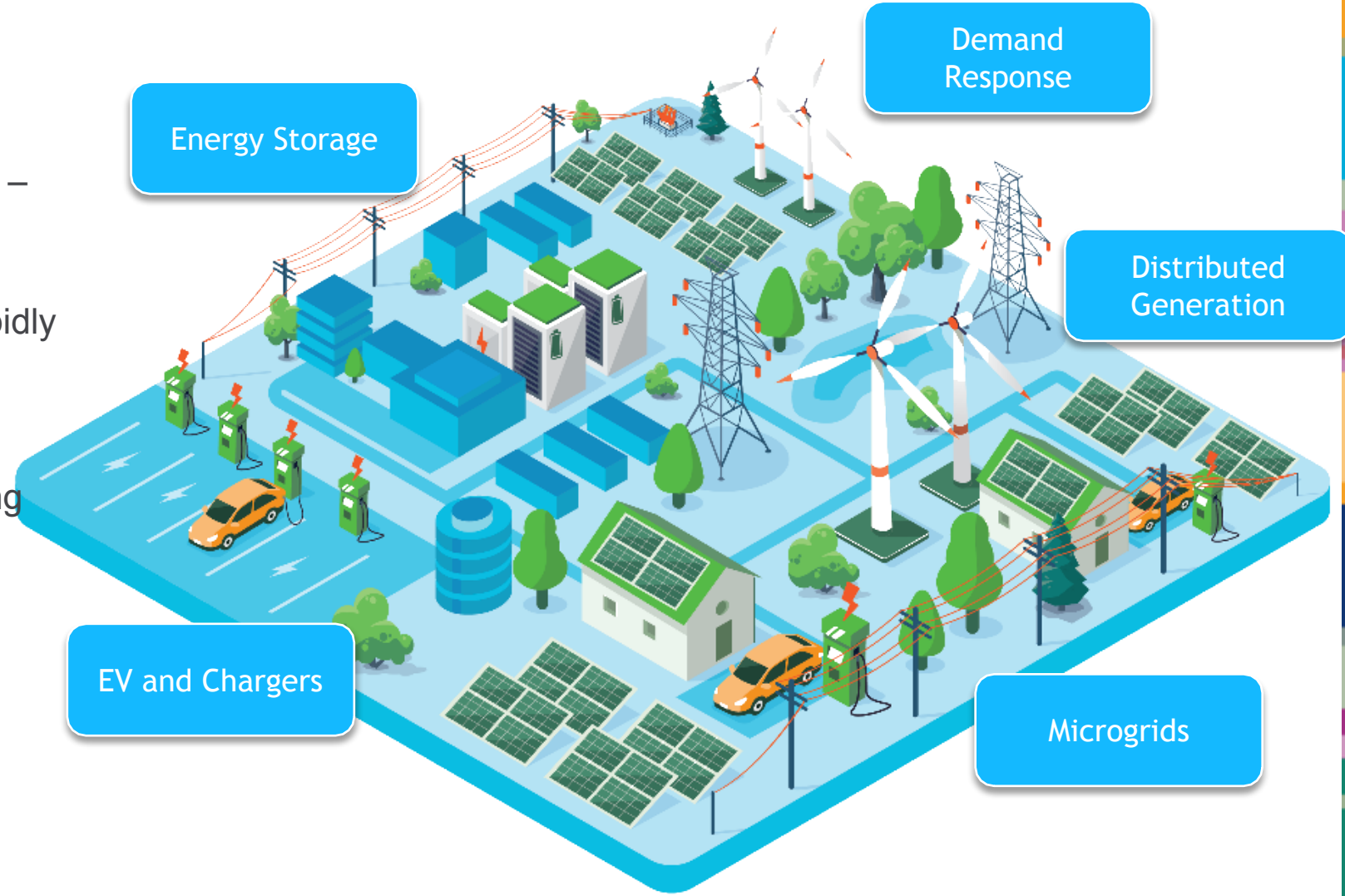
June 29, 2022

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

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.

Distributed Energy Resources and Cybersecurity

- Rapid DER deployment
  - 2017 – 2021: **78 GW** installed; 2022 – 2026: **175 GW** projected [U.S. DER Outlook, Wood Mackenzie]
  - Connected to the public internet, rapidly evolving environment
- Meanwhile…
  - Cybersecurity requirements still being formulated
  - Roles/responsibilities not defined
- We are all Stakeholders
  - Utilities, DER vendors, Standards Development Organizations, government/regulators, academia, cybersecurity researchers



The grid of the Future is increasingly distributed

A Key Focus of Activity: SunSpec/Sandia DER Cybersecurity Working Group

- In August 2017, Sandia National Laboratories and SunSpec Alliance launched the WG, sponsored by the DOE Solar Energy Technologies Office (SETO)
- Two programmatic tracks:
  - Educational: monthly webinar series
  - Technical: document best practices; inform cyber standards
- Impact:
  - 1,700 DER & cybersecurity experts, high engagement
  - IEEE P1547.3 *"Guide for Cybersecurity of DERs Interconnected With Electric Power Systems"* included recommendations directly from the WG reports
  - Recommendations leveraged by state regulators (e.g., NASEO/NARUC Cybersecurity Advisory Team).

U.S. DEPARTMENT OF ENERGY

SUNSPEC ALLIANCE

Sandia National Laboratories

https://sunspec.org/sunspec-der-cybersecurity-initiative

DER Cybersecurity WG – Webinar Program

2021 Webinar Series

- 1/21/21 – **Cybersecurity Advisory Group for State Solar (CATSS) Brief** – *NASEO*
- 2/25/21 – **Overview of IEEE 1547.3: A Guide for Cybersecurity of DER Interconnected with Electric Power Systems** – NPR Associates and Xanthus Consulting International
- 3/25/21 – **Conceptualizing Systems Cybersecurity Challenges for Rooftop Solar** – *DOE SETO*
- 4/22/21 – **Securing the Industrial Internet of Things: Cybersecurity for DER** – *NIST NCCoE*
- 5/27/21 – **An Industrial Cybersecurity Perspective** – *Dragos*
- 6/24/21 – **Centralized vs Decentralized DER Role-Based Access Control Implementation** – *UNM*
- 7/22/21 – **Software Vulnerabilities (Software Bill of Materials – Transparency in the Software Supply Chain; Longclaw – Firmware Analysis Framework; Next Generation Firmware Analysis for Energy Systems)** – *USDC NTIA, LLNL, SNL*
- 8/26/21 – **Cyber-Physical Intrusion Detection/Mitigation System** – *SNL*
- 9/14/21 – **Zero Trust Security for Distributed Energy Resources** – *Xage*
- 9/23/21 – **DER Incident Response** – *FireEye/Madiant*
- 10/28/21 – **Historical Public Key Infrastructure Failures** – *Tufts University*
- 11/18/21 – **CyTRICS: Cyber Testing for Resilient Industrial Control Systems** – *INL & DOE-CESER*
- 12/8/21 – **Cybersecurity Manufacturing Innovation Institute (CyManII)** – *UTSA*

2022 Webinar Series

- 1/27/22 – **Cybersecurity Risk Management for DERs** – NREL
- 2/25/22 – **Solar Inverter Risks and Defenses from Power Electronics Hardware Attacks** – University of Arkansas
- 3/24/22 – **Cryptographic, Protected Processors for DER Authentication, Control, Measurement, and Attestation** - Trusted Computing Group (TCG)
- 4/28/22 – **SunSpec Cybersecurity Certification for IEEE® 2030.5™ Client Gateways** – SunSpec Alliance
- 5/26/22 – **Defending America's Rural Electrical Grids: How to work with the National Rural Electric Cooperative Threat Analysis Center** – NRECA
- 6/23/22 – **Network Traffic Analysis with Malcolm** – INL
- 7/28/22 – TBD
- …

See the videos: https://sunspec.org/sunspec-cybersecurity-videos/

DER Cybersecurity Workgroup Activities

SunSpec/Sandia DER Cybersecurity Workgroup

DER Cybersecurity Certification Procedure

- **Defined standardized procedure for DER vulnerability assessments.**
- **Leads: Danish Saleem (NREL) and Cedric Carter (MITRE)**
- Publication: *"Certification Procedures for Data and Communications Security of Distributed Energy Resources"*
- Future work: Expected development within UL 2900-2-4 STP

Secure Network Architecture

- **Created DER reference architecture best practice.**
- **Lead: Candace Suh-Lee (EPRI)**
- Publication: *"EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-based Approach for Network Design"*
- Future work: Risk-based approach adopted in IEEE 1547.3

Data-in-Flight Requirements

- **Encryption, authentication, and key management requirements.**
- **Lead: Ifeoma Onunkwo (Sandia)**
- Publication: *"Recommendations for Trust and Encryption in DER Interoperability Standards"*, another covering Data-in-Transit Requirements document (forthcoming).
- Future work: IEEE 1547.3 update, IEEE 2030.5 revisions.

Access Control

- **DER Role-Based Access Control recommendations.**
- **Lead: Jay Johnson (Sandia)**
- Topics: Access control taxonomy and security models
- Planned: *"Recommendations for Distributed Energy Resource Access Controls"*
- Future work: Add recommendations to IEEE 1547.3 Guide

Patching Requirements

- **Establishing patching guidelines for DER devices and DER networking equipment.**
- **Lead: Ingo Hanke (SMA), Jay Johnson (Sandia)**
- Publication: *"Certification Procedures for Data and Communications Security of Distributed Energy Resources"*
- Future work: inclusion in IEEE 1547.3

DER System Security Evaluations

Convening!

- **Creating recommended auditing/assessment practices for DER systems and adding these recommendations to the DHS CISA Cyber Security Evaluation Tool (CSET).**
- **Started Jan 2022. Leads: Steve Bukowski (INL), Jay Johnson (Sandia)**
- Topics: Step-by-step auditing procedure for internal or external compliance review.

Related Activity: Blockchain Workgroup

- **Defined requirements and specifications for using blockchain to ensure the security of private keys in DER manufacturing environments.**
- **Leads: Jörg Brakensiek (Wivity) and Alfred Tom (Wivity)**

Workgroup information: https://sunspec.org/cybersecurity-work-group/
Email: support@sunspec.org to participate!

DER Network Architectures

- Reference architecture with requirements for DER sites based on criticality (nameplate rating)
- Requirements were broken into seven categories:
  - R1: Resource Criticality Levels
  - R2: Network Segmentation
  - R3: Boundary Protection
  - R4: Communication Partitioning
  - R5: Network Service Protection
  - R6: Communication Integrity
  - R7: Communication Confidentiality

EPRI ELECTRIC POWER RESEARCH INSTITUTE

EPRI SECURITY ARCHITECTURE FOR THE DISTRIBUTED ENERGY RESOURCES INTEGRATION NETWORK

RISK-BASED APPROACH FOR NETWORK DESIGN

EXECUTIVE SUMMARY

As distributed energy resources (DERs) expand rapidly as a major source of electricity generation and interconnect with the grid, the ability to securely monitor and control the operations of the resources in a large geographical area becomes increasingly important to maintain safety, reliability, and resiliency of the nation's grid. Remote monitoring and control of distributed generation require local devices and sensors to communicate operational status and receive commands from the remote systems, via public or private communication networks. In the meantime, the cyber-threats against the nation's grid is increasing as more and more devices become intelligent and connected. Without adequate cybersecurity protection, energy generation and interconnected systems are innately exposed to cyber threats.

This paper provides a practical set of cybersecurity requirements pertaining to the network components supporting distributed energy resources (DER) communications. The requirements specified herein aim to reduce the cybersecurity risk to the distribution grid to which various DER are connected. The requirements discussed herein do not make any assumption to the communication protocols, particular functional standards, or certain ownership/business models in terms of their effectiveness in cybersecurity. Rather, it aims to provide a holistic view of the interconnected systems, including DER, and it suggests how they can be protected from cyberattacks.

The scope of this report is limited to network security concerns. The goal is to provide guidelines for designing and implementing network infrastructure in a way that will minimize the likelihood, duration, or impact of a successful cyberattack.

It is important to note that network security architecture addresses only a portion of the cybersecurity risks associated with DER integration. To protect DER and the connected grid adequately, a more comprehensive cybersecurity standard must be developed and implemented.

The standard must consider various facets of cyber security including:

- Communications and protocol security
- Cryptographic key management
- End-point security for DER devices
- Personnel, physical, and environmental security
- Ongoing security operations—vulnerability and patch management, security monitoring, and incident response

TERMINOLOGY

In this report, *DER, distributed energy resource,* and *resource* are used interchangeably. The following terms that appear in the report might be used to convey slightly different meanings from their general usage:

- ***DER supporting system, supporting system, or system.*** A system, application, or device used to support the operation of DER or grid services in relation to DER.
- ***DER managing system or managing system.*** A supporting system specifically used to manage DER. The essential functions of a DER managing system include data acquisition and control.
- ***External network.*** A telecommunication network that extends external to the local area network (LAN)—that is, a wide area network (WAN), Internet area network (IAN or cloud), or the Internet.
- ***Security zone.*** One or more subnets or broadcast domains where a device in a zone can communicate with other devices within the zone freely, but access to and from devices outside the zone is controlled.

NETWORK SECURITY REQUIREMENTS

The general network security requirements described in this section are drawn from various cybersecurity standards available to the industry [1–6].

Access: https://www.epri.com/research/products/000000003002016781

Architecture Requirements 1-2

R1. Resource Criticality Level

R-1.1 – R-1.2:

Resource criticality classification for all participating resources

- High-Impact
- Medium-Impact
- Low-Impact

R-1.3 If a group of resources can be operated si through a same managing system, each resourc must be assigned the criticality level correspond aggregate risk posed by the simultaneous (mis)c resources in the group.

R-1.4 A managing system that can issue a write command to one or more resources must be as criticality level which corresponds to the aggreg simultaneous (mis)operation of all resources wh controlled by the managing system..

R-1.5 If a *resource* can be categorized into two different criticality levels, it must be categorized highest possible level.

A: non-segmented central management

For simplicity, consider only nameplate rating. Assume,

L: < 10 KW

M: 10-99 KW

R2. Network Segmentation

R-2.1 - Resources with different criticality levels must be located in different security zones.

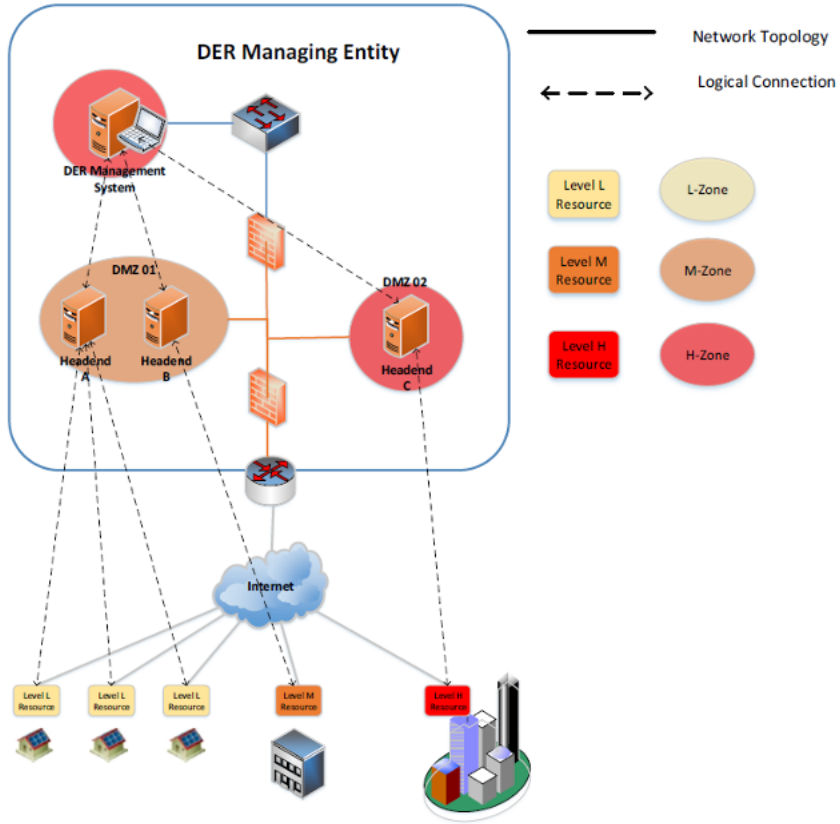
- High-impact-zone
- Medium-impact-zone
- Low-impact-zone

R-2.2 – Each security zone must have one or more security gateways with access control lists

R-2.3 - Communications between two different security zones must be routed through the security gateways with access control

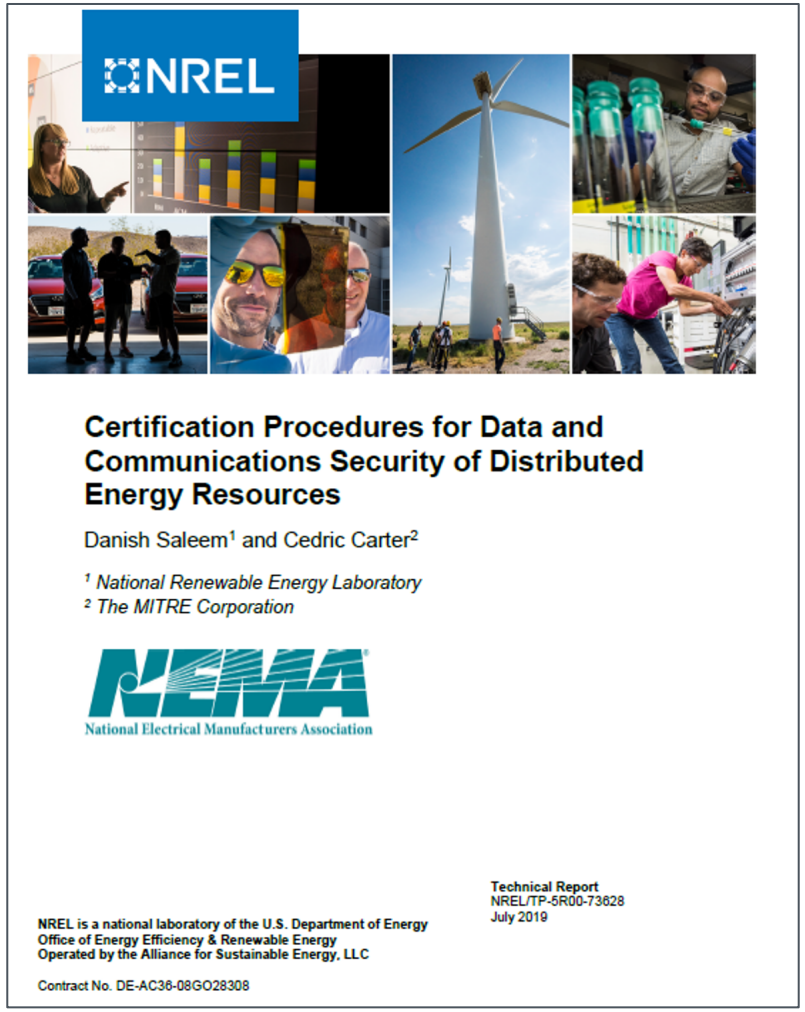
R-3.4 - Communications between systems or resources in the high-impact-zone and a system/resources in the low-impact-zone must be routed through a DMZ

R-3.5 - Communications to/from an external network must be routed through a DMZ



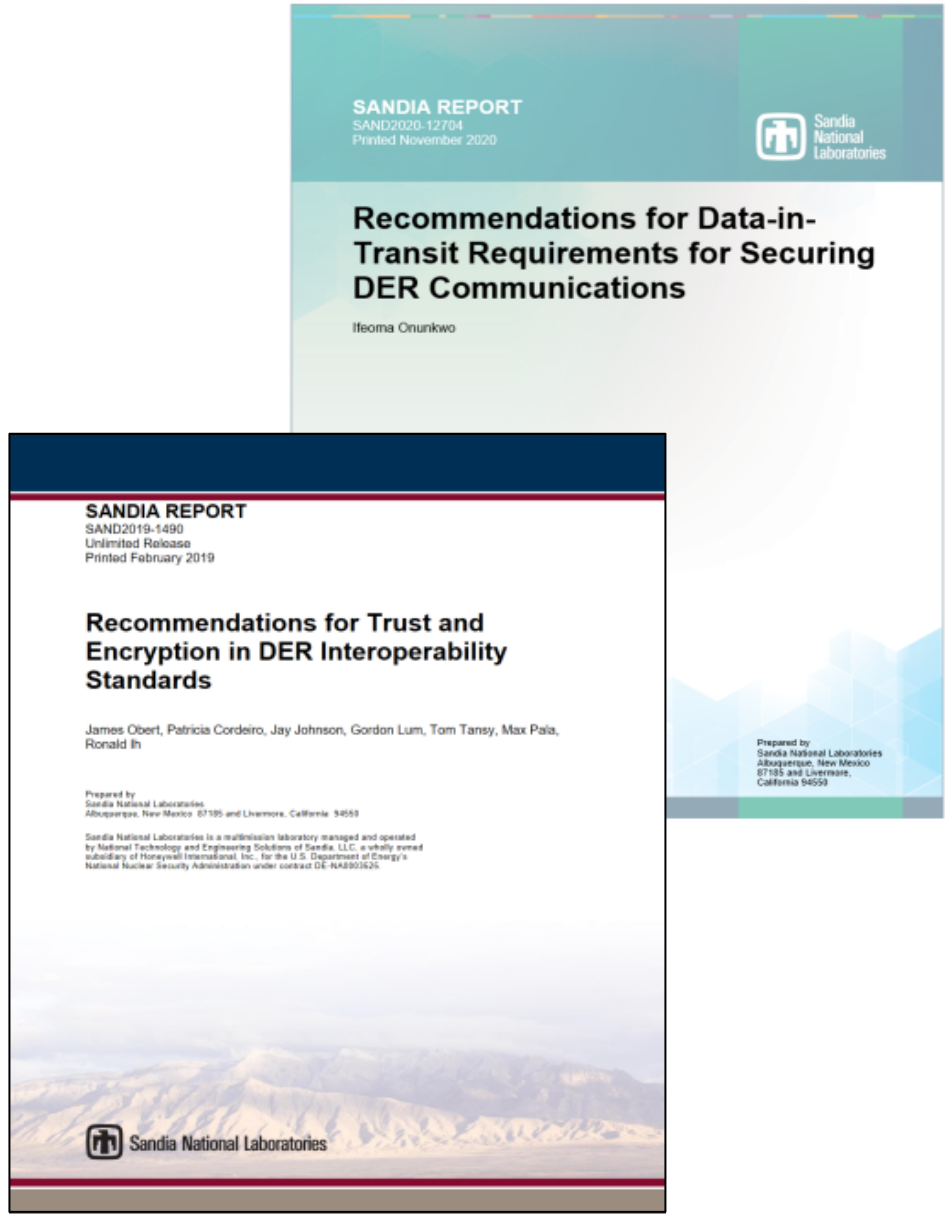
DER Cybersecurity Certification

- Focuses on verification security for DER communications
- Created several test cases
  - Two-Party Application Association (T1)
  - Transport Layer Security (T2)
  - Session Resumption/Renegotiation (T3)
  - Master Secret Key Update (T4)
  - Message Authentication Code (T5)
  - Multiple Certification Authorities (T6)—Optional
  - Certificate Revocation List (CRL) (T7)
  - Expired Certificate (T8)
  - Operating System and Service Version (T9)
  - Authentication and Password Management (T10)
  - Physical Security (T11)
- NREL-led WG now working with UL to develop a UL certification program
- Concepts included in IEEE 1547.3



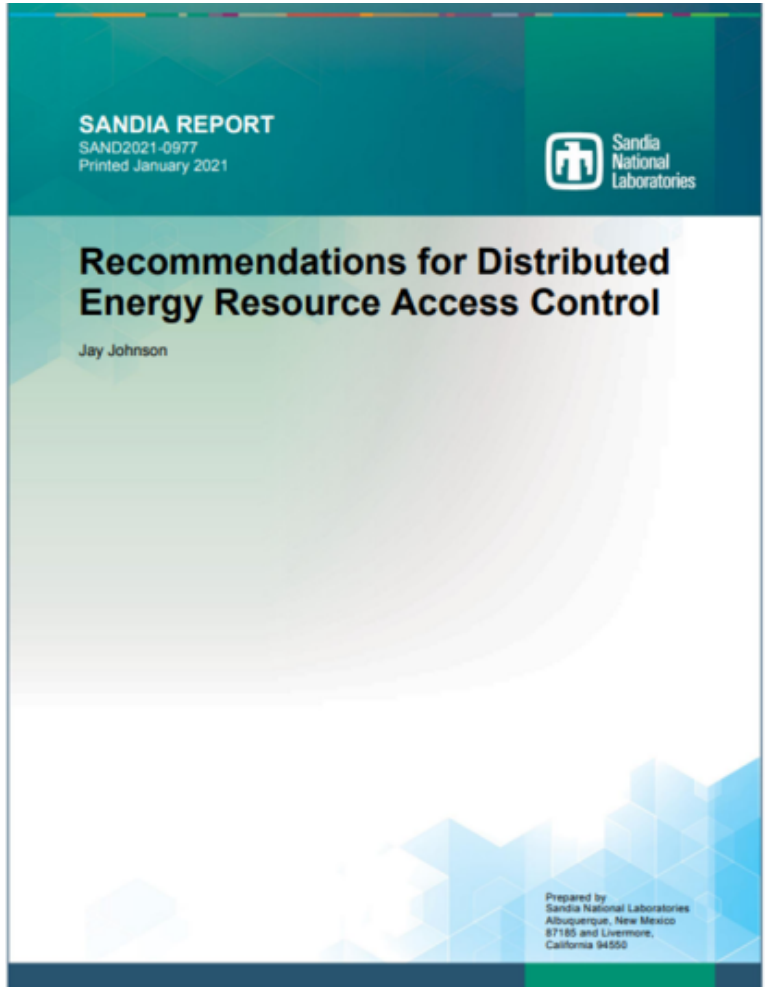
Data-in-Flight Security

- State-of-the-art encryption, key management, and authentication approaches for DER communications
- Modbus
  - **Strengths**: MODBUS/TCP Security an option
  - **Weaknesses**: Trust and cryptography features often unused for this protocol.
- IEEE 1815 – DNP3, IEEE 2030.5 – SEP2.0, IEC 61850/62351
  - **Strengths**: TLS v1.2+ encryption; Mutual client/server authentication via X.509v3 Digital Certificates
  - **Weaknesses**: TLS protocols support cipher suites with varying degrees of security; Uses different PKI models and supports self-signed certificates; Key exchange algorithms with noted vulnerabilities

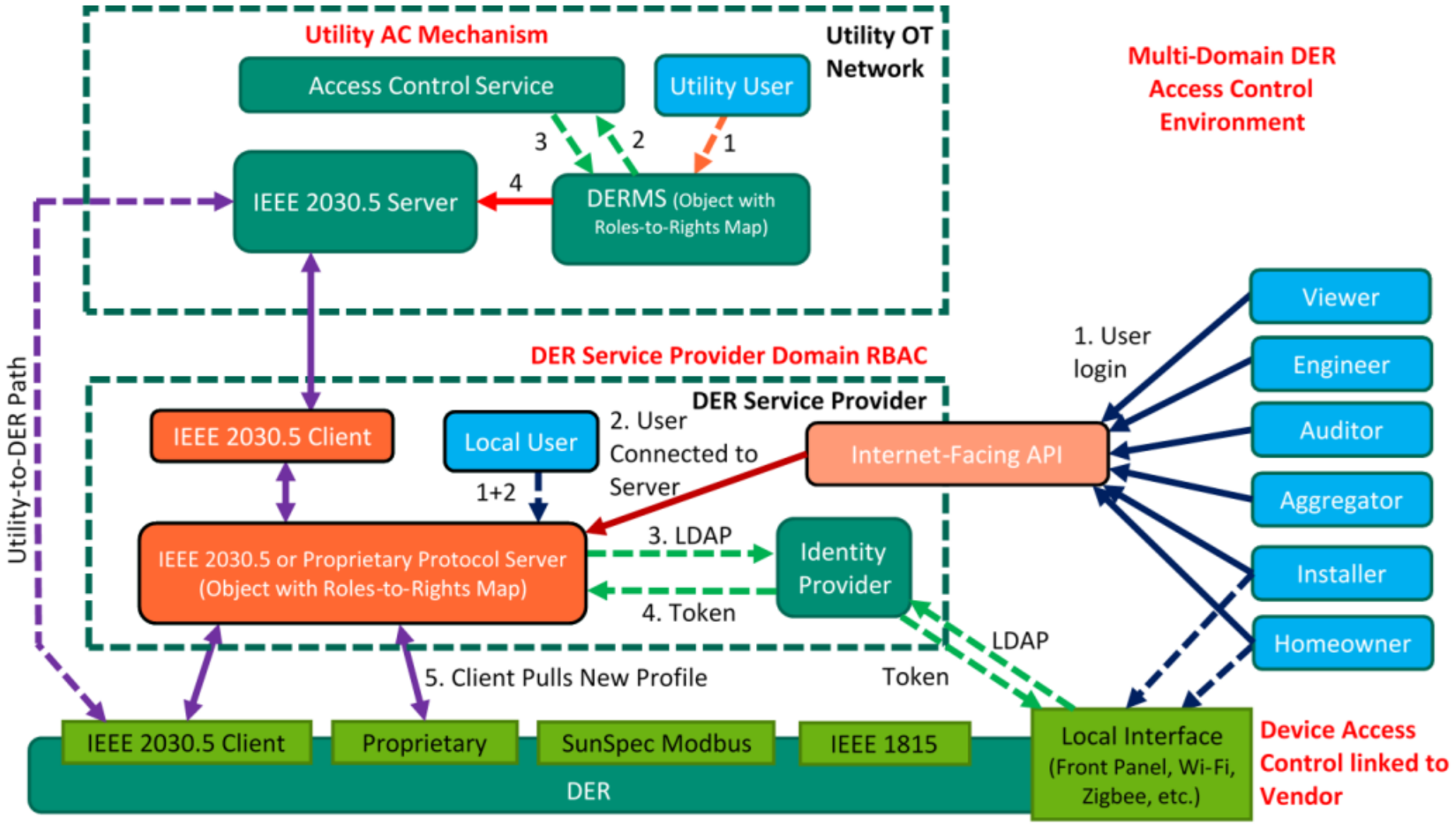


Access Controls

- Options to minimize unauthorized access to DER systems and functions
- Access to DER monitoring and control features via three steps:
  1. User is identified using a proof-of-identity
  2. User is authenticated by a managed database
  3. User is authorized for a level of access
- Recommendations for role-based access control (RBAC) implementation for DER
  - Defined roles (e.g., installer, owner, DER vendor, etc.)
  - Defined point-by-point role-to-rights for IEEE 1547 functionality represented in IEEE 2030.5 – SEP 2.0, IEEE 1815 – DNP3, and SunSpec Modbus



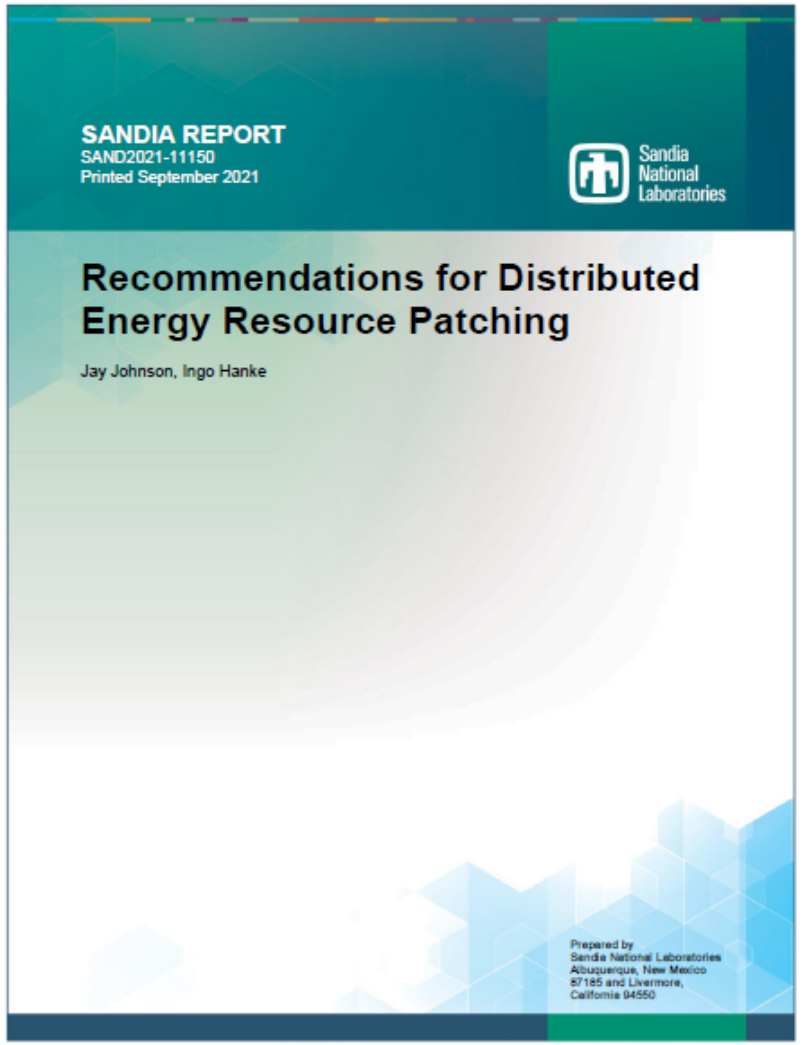
Implementation RBAC for DER in IEEE 2030.5



J. Johnson, "Recommendations for Distributed Energy Resource Access Control," Sandia Technical Report SAND2021-0977, January 2021.

Patching

- Patching recommendations based on IEC 62443-2-3 "*Patch management in the Industrial Automation and Control Systems (IACS) environment*"
- Scope:
  - Patch lifecycle: vulnerability disclosed → patch available → patch in test → patch authorized → patch installed
  - Patching requirements for DER vendors, aggregators, grid operators, etc.
  - Recommendations for patch integrity: checksums and digital signatures/code signing
  - Scheduling patches and prioritization (e.g., critical security patch)
  - Vendor requirements: policy for release after vulnerability disclosures, quality assurance, compatibility warnings, end-of-life notifications, etc.
  - Patch schema/file name conventions
- Recommendations included in IEEE 1547.3



Contact

Abraham Ellis
aellis@sandia.gov

Jay Johnson
jjohns2@sandia.gov