SAND2022-14633C

Sandia National Laboratories

Exceptional service in the national interest

A Pathway to DER Cybersecurity

9th International Conference on the Integration of Renewable & Distributed Energy Resources

Jay Johnson
Renewable and Distributed Systems Integration
Sandia National Laboratories, Albuquerque, NM, USA

Tuesday, October 25, 2022

Adelaide, Australia

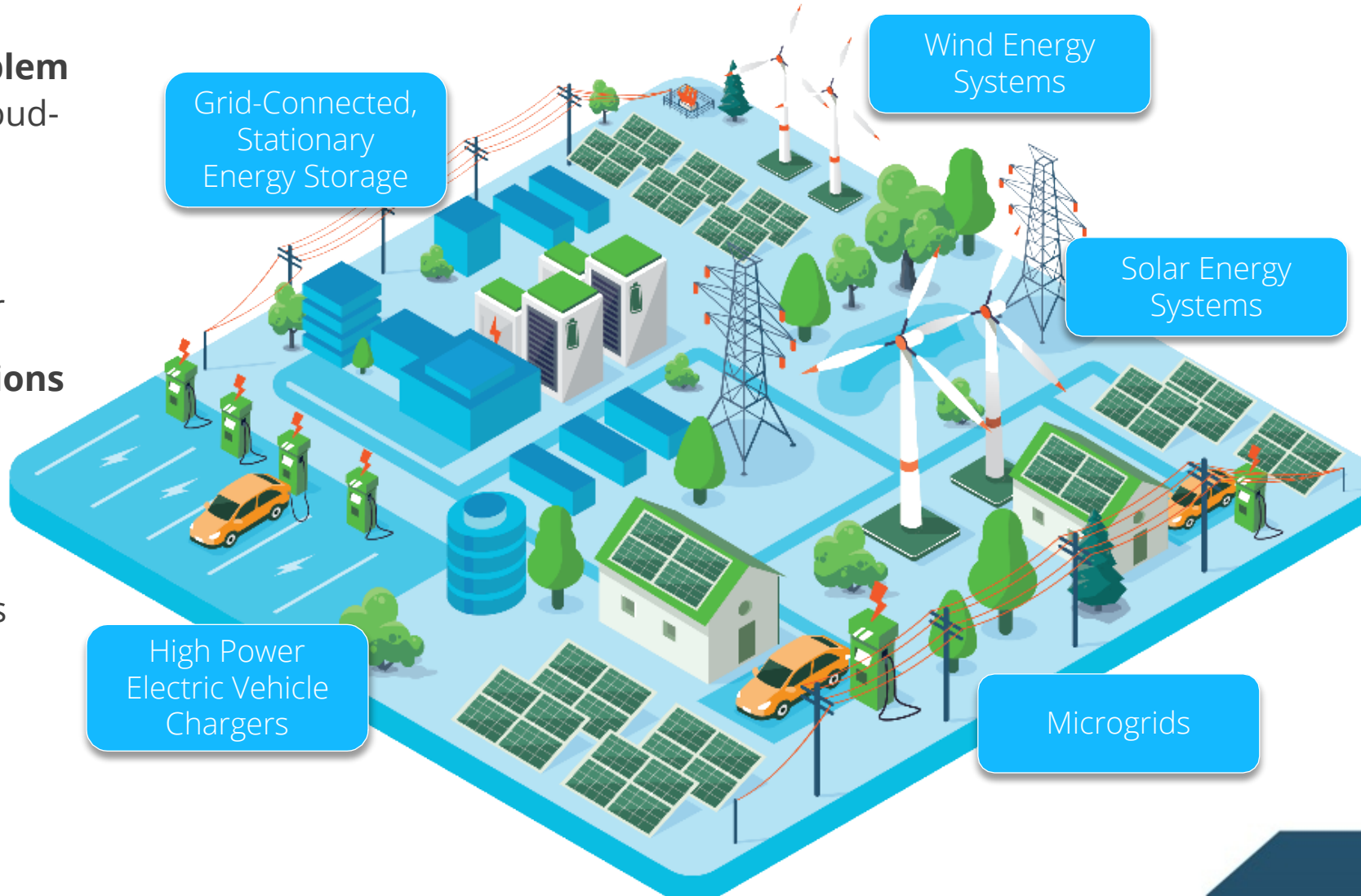
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

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 Cybersecurity

- Cybersecurity is paramount for ***energy*** and ***transportation*** infrastructures
- DER cybersecurity is a **complex problem**
  - Rapidly evolving with internet/cloud-connectivity
  - Risk ownership is a major issue: who pays for cyber upgrades?
  - Roles/responsibilities are unclear
- **Limited DER cybersecurity regulations exist**, yet the power system relies on reliable DER operations
- **Industry engagement** and **cutting-edge R&D** are critical to defending these devices and systems

Grid of the Future Elements



What could go wrong?

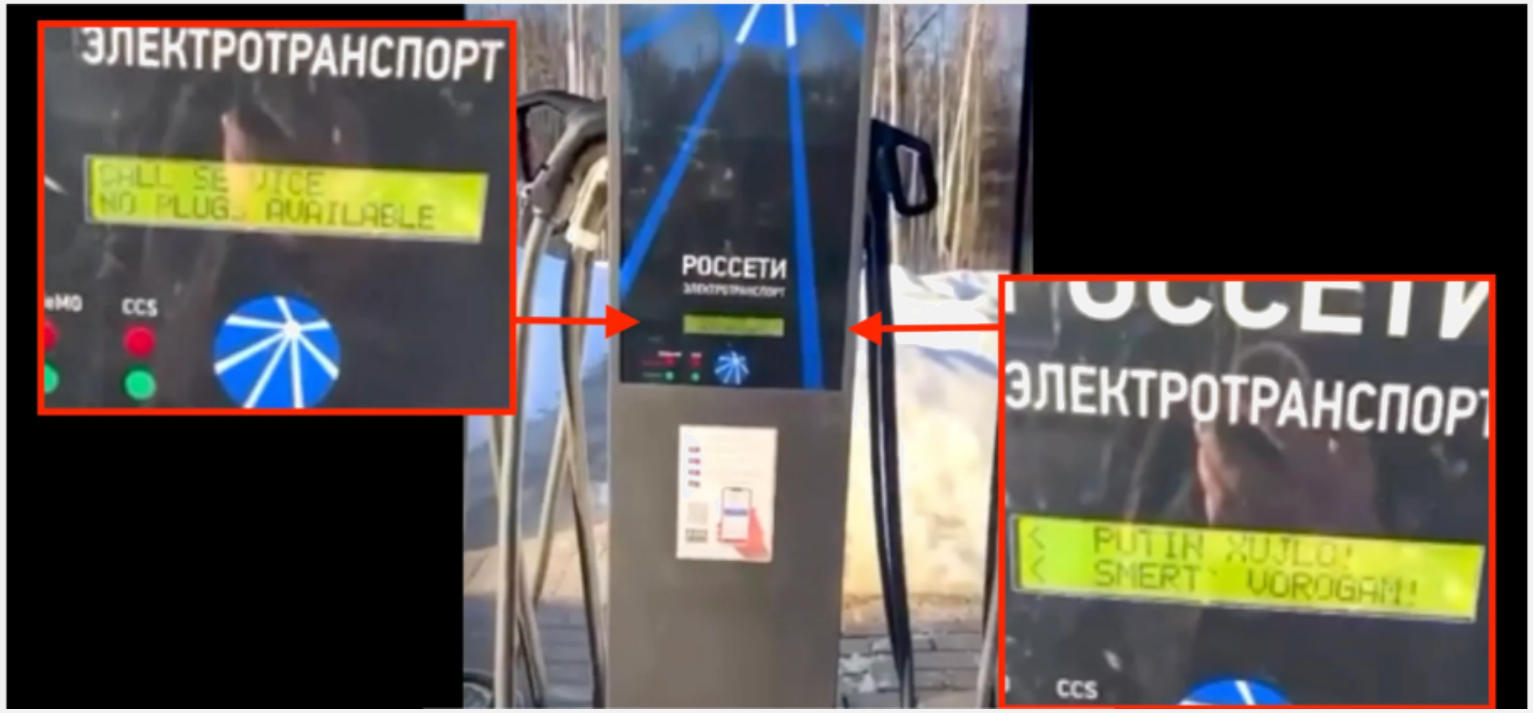
Malicious Firmware Updates and Supply Chain Vulnerabilities

Russian company, *Gzhelprom*, outsourced components in EV chargers to a Ukrainian Company, *Autoenterprise*

- Charging stations installed in 2020 on the M-11 route with backdoor access
- In early 2022, the chargers were disabled and displayed anti-Putin/pro-Ukraine messages

Hacked electric car charging stations in Russia display 'Putin is a d*ckhead' and 'glory to Ukraine'

Fred Lambert - Feb. 28th 2022 10:13 am PT @FredericLambert



https://electrek.co/2022/02/28/hacked-electric-car-charging-stations-russia-displays-putin-dckhead-glory-to-ukraine/
https://www.dailymail.co.uk/news/article-10565697/Russian-electric-vehicle-chargers-hacked-display-message-supporting-Ukraine.html
https://jalopnik.com/russian-company-outsourced-the-main-components-in-ev-ch-1848603252

Maintenance and Internal Interfaces

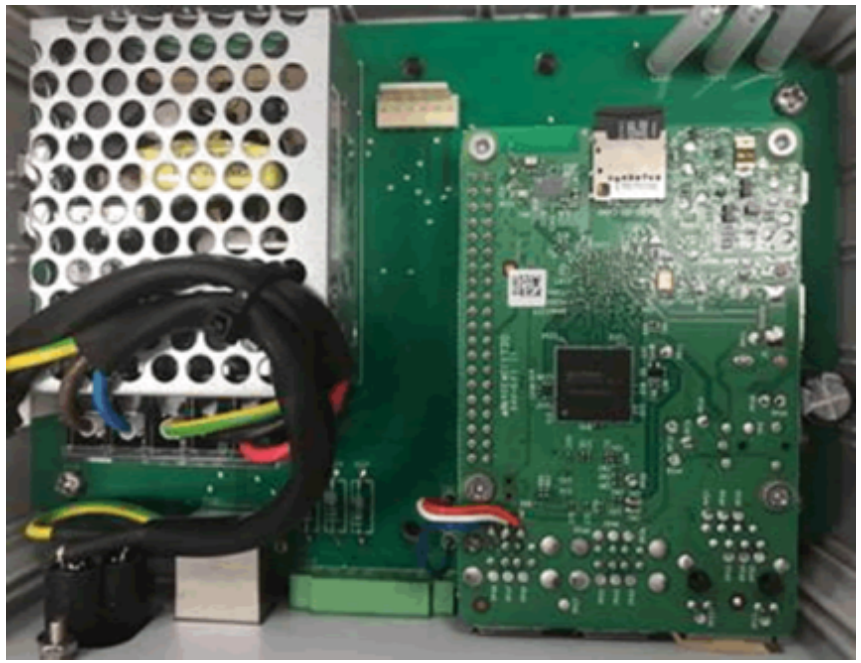
Maintenance interfaces are common on DER and EV Chargers, including:

- Serial (e.g., RS485, RS232, serial over USB, etc.)
- Wi-Fi or Ethernet (e.g., SSH, Telnet, HTTP, etc.)
- Bluetooth
- Front panel/screen codes

Fraunhofer found USB ports that would copy logs and configuration data including the OCPP server login and password, and authentication tokens from previous users.

Pen Test Partners noted issues with **secure storage** and **secure boot**.
Example exploit of eoHUB:

- Step 1: Remove the SD card
- Step 2: Inject root account
- Step 3: Boot device and SSH into system
- Step 4: Exfiltrate/modify anything of value
  - Full source code of device
  - FTP Credentials
  - SMTP Credentials
  - Cloud communication encryption/decryption keys



PEN TEST PARTNERS

- https://media.ccc.de/v/34c3-9092-ladeinfrastruktur_fur_elektroautos_ausbau_statt_sicherheit
- https://usa.kaspersky.com/blog/electric-cars-charging-problems/14357/
- https://www.pentestpartners.com/security-blog/pwning-a-smart-car-charger-building-a-botnet/
- https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/

DER Cybersecurity Standardization

DER Cybersecurity Industry outreach and standardization

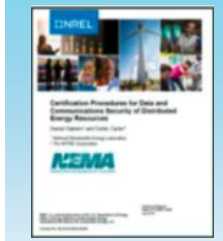
SunSpec/Sandia DER Cybersecurity Workgroup was founded in Aug 2017

- **2,000+ DER and cybersecurity experts** with high engagement
- Two programmatic tracks:
  - Educational: monthly webinar series
    Technical: generate best practices for national/international cyber standards
- **Impact**: DER cyber guide, IEEE 1547.3, was balloted with verbatim recommendations from several of the technical subgroup reports.
- Recommendations leverage by Public Utility Commissions and other state regulators (NASEO/ NARUC Cybersecurity Advisory Team).

Webinars by:

NASEO, NARUC National Association of Regulatory Utility Commissioners, CYMANII the cybersecurity manufacturing innovation institute, DRAGOS, INL Idaho National Laboratory, NREL, Solar Energy Technologies Office U.S. Department Of Energy, NM, NIST, IEEE, xage SECURITY, Tufts UNIVERSITY, Sandia National Laboratories, Trusted Computing Group, NTIA, MANDIANT, FIREEYE, SUNSPEC ALLIANCE, U.S. DEPARTMENT OF ENERGY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Technical Workgroups



DER Cybersecurity Certified Procedure
Lead: Danish Saleem (NREL) and Cedric Carter (MITRE)

Secure Network Architecture
Lead: Candace Suh-Lee (EPRI)

Patching Requirements
Lead: Jay Johnson (Sandia), Ingo Hanke (SMA)

Data-in-Flight Requirements
Lead: Ifeoma Onunkwo (Sandia)

Access Control
Lead: Jay Johnson (Sandia)

DER System Security Evaluation Tool Development
Lead: Steve Bukowski (INL), Jay Johnson (Sandia)

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

Upcoming Guides, DER Certification Programs, and Regulations

Cybersecurity Guidance

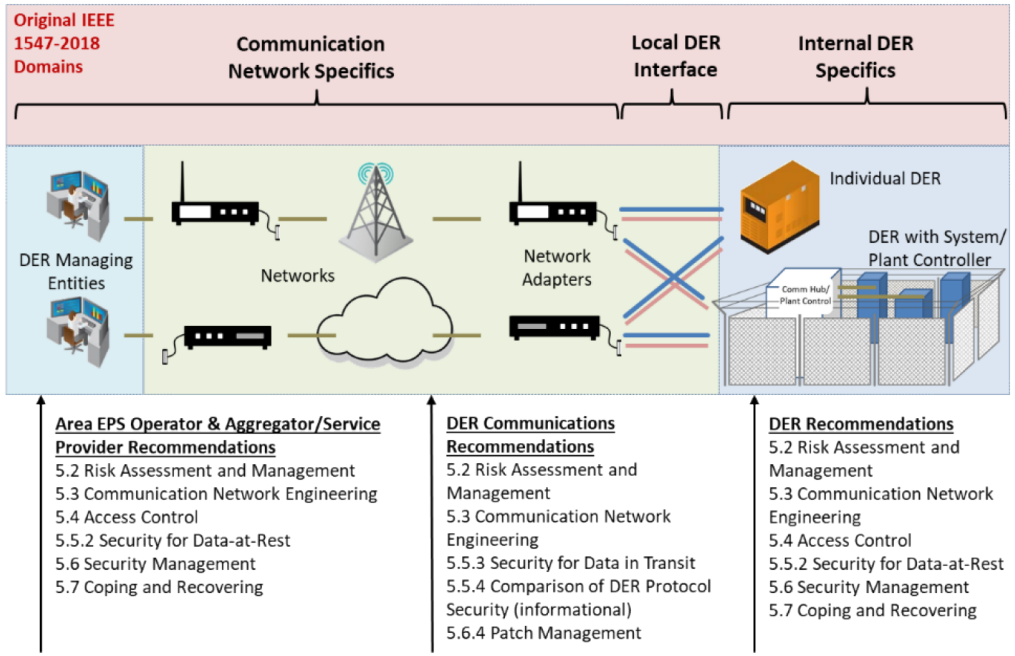
- IEEE 1547.3 “Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems”

DER Certification Programs

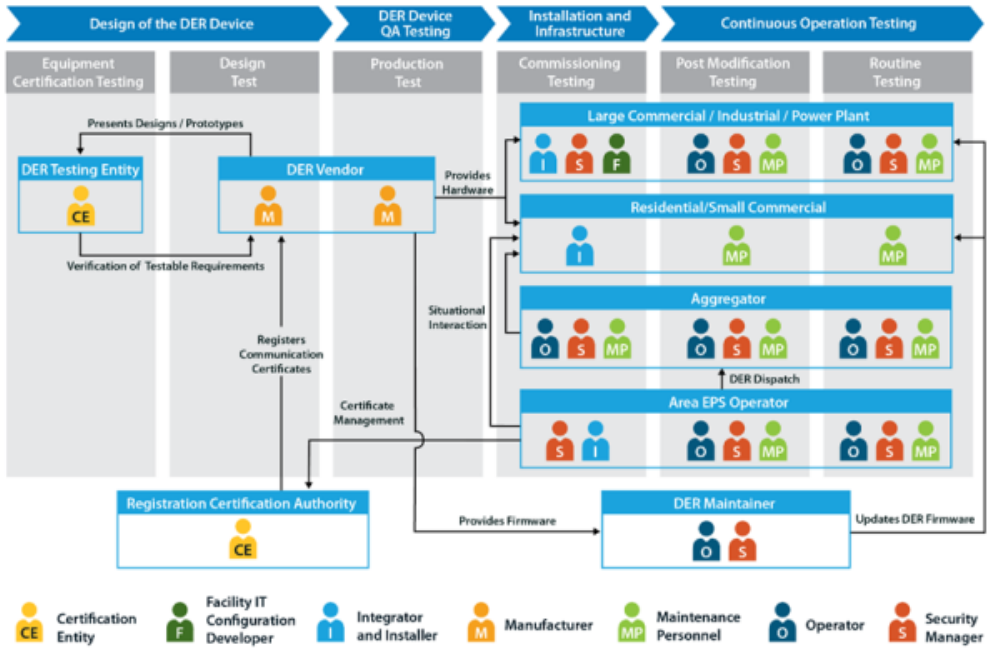
- UL 2941 “Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources”
- SunSpec DER Cybersecurity Certification Program, announced April 28, 2022 (https://sunspec.org/sunspec-cybersecurity-certification-work-group/)

State Regulations

- California Public Utilities Commission: Smart Inverter Operationalization Working Group (SIOWG) Cybersecurity Subgroup



IEEE 1547.3 Scope



Cybersecurity Tests in IEEE 1547.3

Sandia's DER Cybersecurity Research

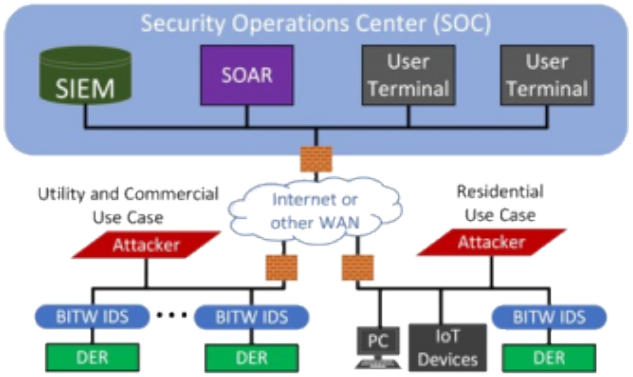
Intrusion Detection and Mitigation for Photovoltaics

2022 R&D 100 WINNER

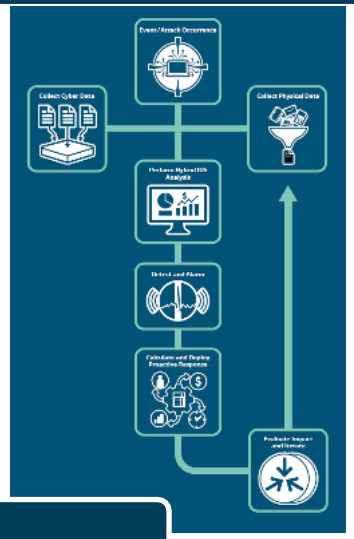
Sandia is developing **solar-specific Security Operations Centers (SOCs)** with **intrusion detection and automated mitigation**

- **Cyber-physical** approach uses network and power system data to detect attacks
- Adaptive Resonance Theory establishes detection thresholds for physical attacks with online learning

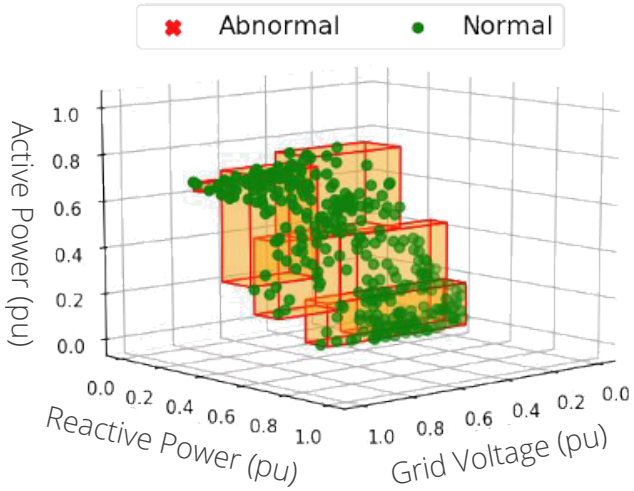
Security Operations Center



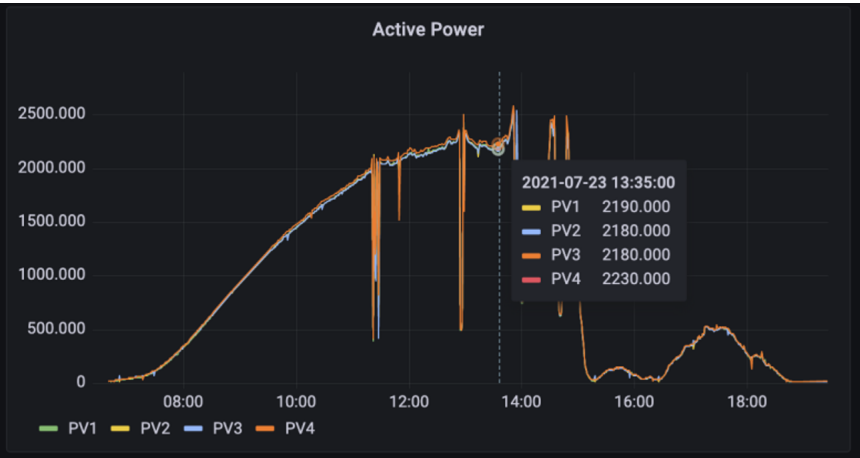
Hybrid analysis and mitigation process

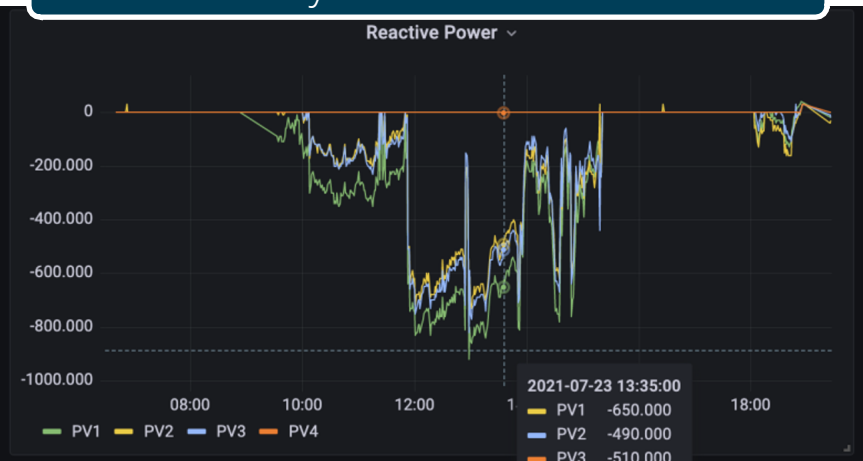


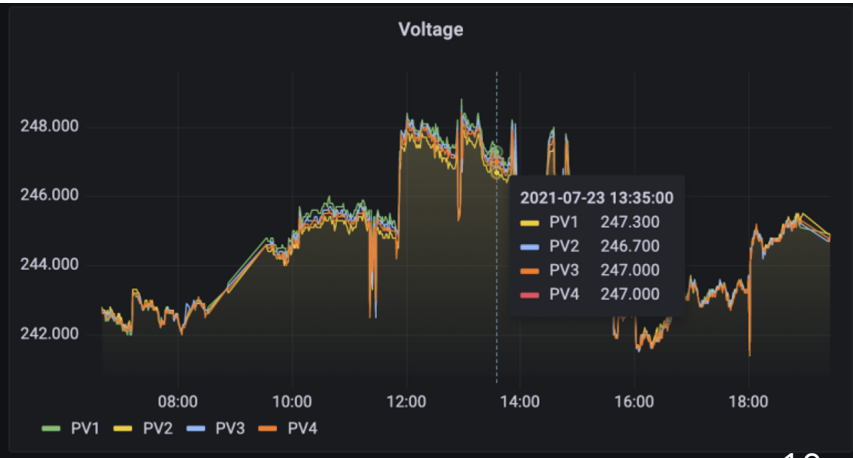
Machine learning data classification



Physical DER data

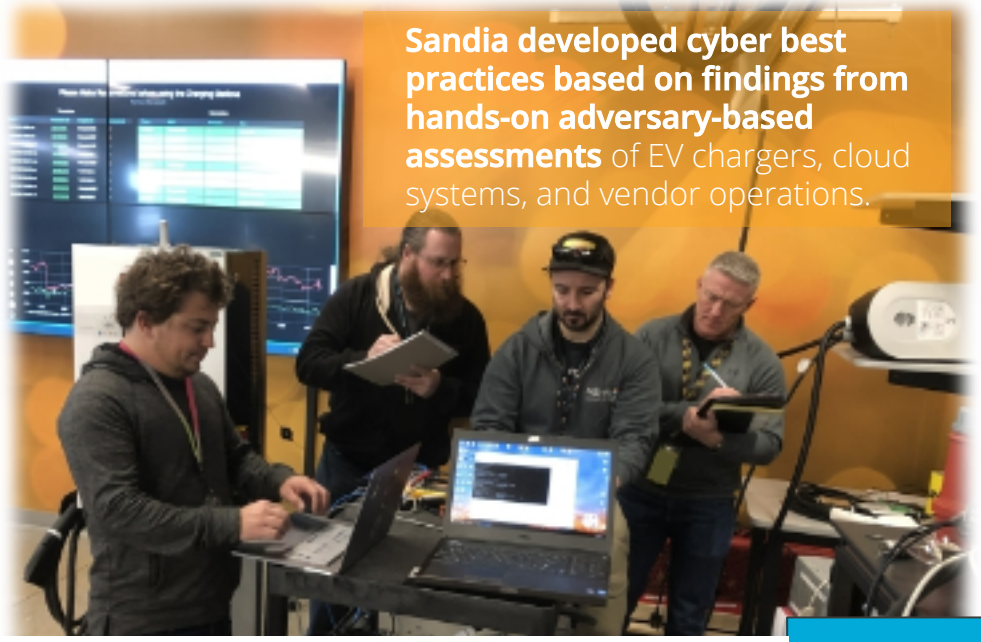




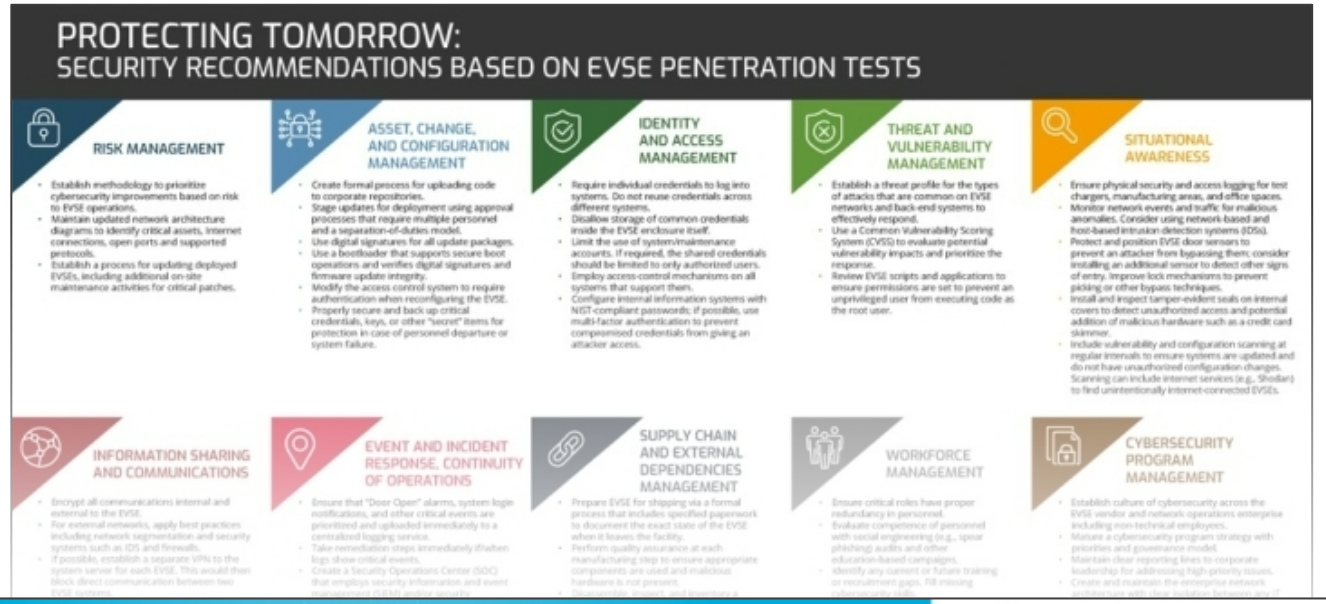


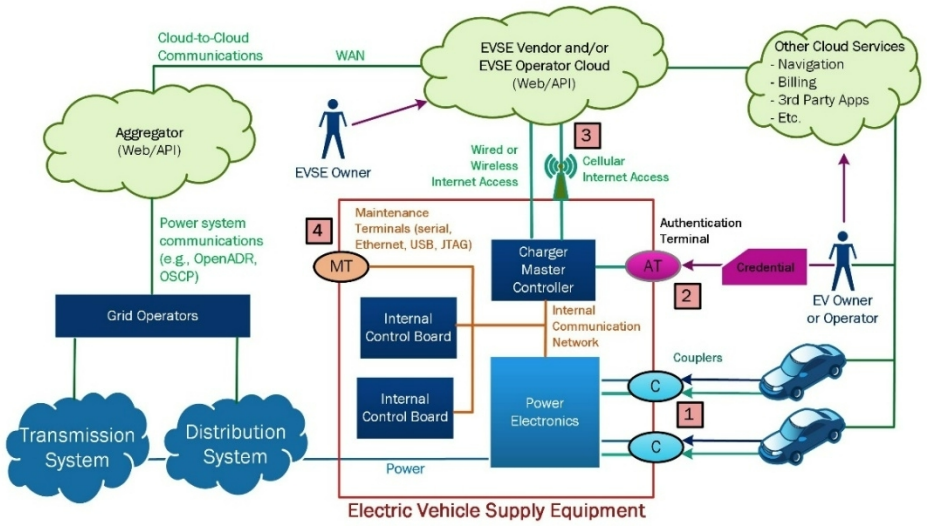
Cyber

Guidance for EV Supply Equipment (EVSE) Cybersecurity



Sandia developed cyber best practices based on findings from hands-on adversary-based assessments of EV chargers, cloud systems, and vendor operations.





- Johnson, et al. "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses," Energies, vol. 15, no. 11, p. 3931, May 2022. https://www.mdpi.com/1996-1073/15/11/3931
- https://www.researchgate.net/publication/344888849_Recommended_Cybersecurity_Practices_for_EV_Charging_Systems

Wind Energy Cybersecurity Projects

- Cybersecurity Roadmap for Wind Systems
  - Defined a **DOE 5-year strategy for wind cybersecurity**
- Hardening Wind Systems to Cyber Threats
  - Leveraged Sandia's **Emulytics co-simulation tools** to enable live, **interactive attacker/defender scenarios**
- WindWeasel: Host-based Intrusion Detection Systems for Site and Turbine Controllers
  - Cyber-Physical analysis detects malicious actions, which are reported to Security Operations Centers

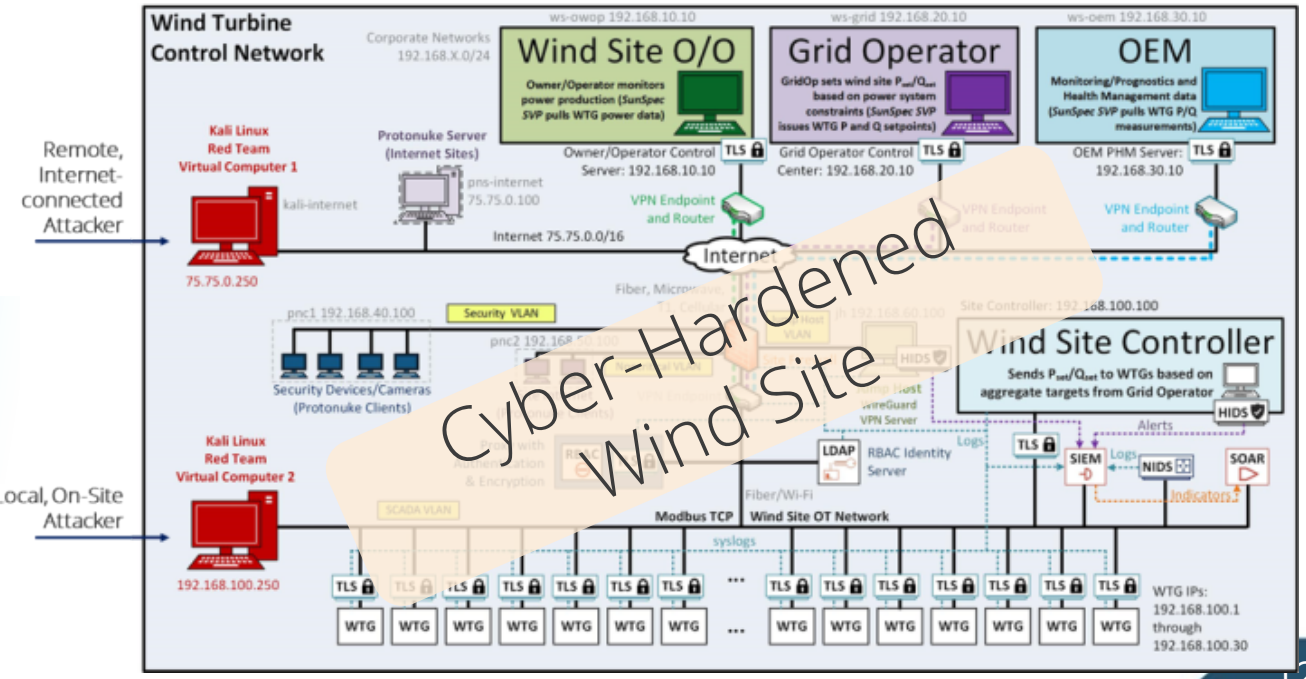
Attack scenarios include wind turbine fires which account for more than 10% of catastrophic failures

Security Operations Center defending wind site attacks

Wind Roadmap Partners

Idaho National Laboratory

NREL

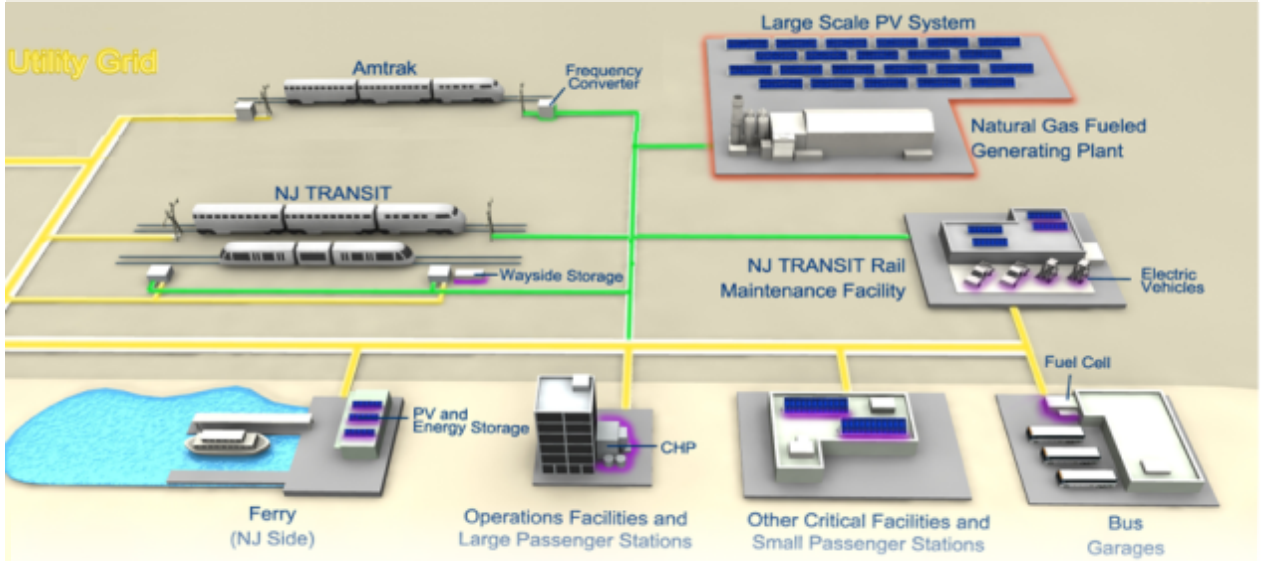


Microgrid cybersecurity research

The $570B **NJ TRANSITGRID** project will provide **civilian egress and first responder ingress** to Manhattan

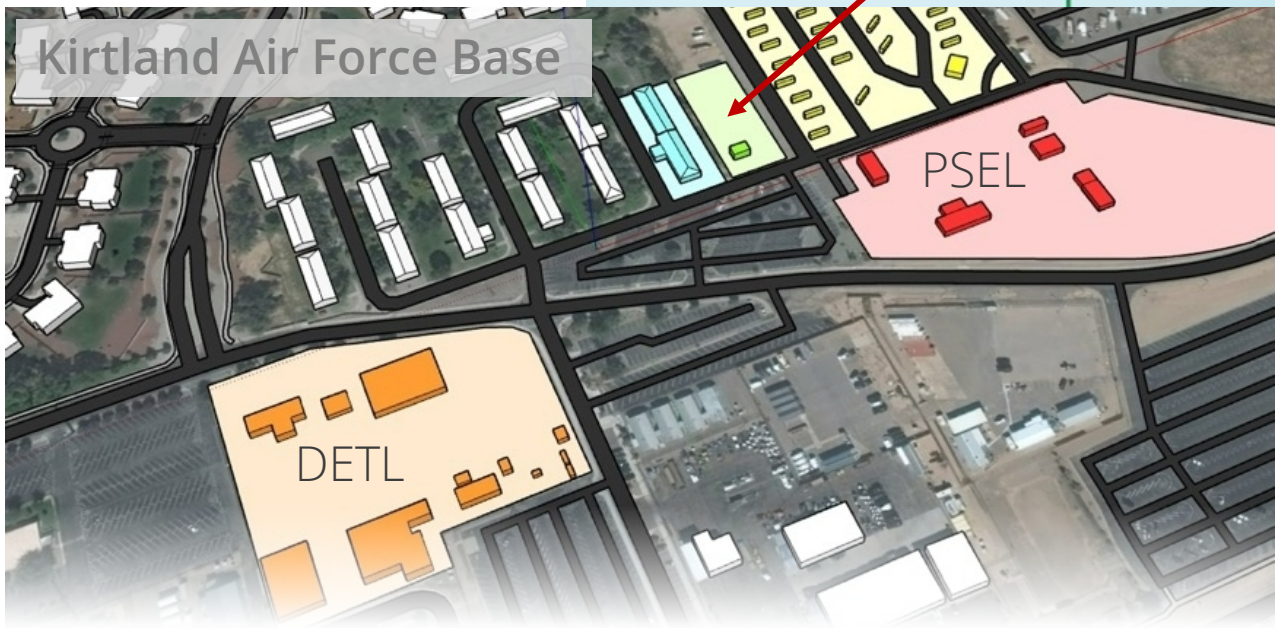
- Phase 1: Sandia **identified security improvements** for the 20% design
- Phase 2: Provide procurement guidance:
  - **reference network architecture**
  - **intrusion detection** designs
  - **remedial action schemes**
  - **moving target defense** capabilities

NJTRANSIT The Way To Go. NJ TRANSITGRID



Security assessment of the **Emera 250 kW DC Microgrid** found several security issues.

Emera is **addressing vulnerabilities before commercial deployments** and Kirtland expansion.



Future Research Recommendations

Local DER Interfaces
- Hardened and sanitized local web services.
- Additional device-level security features including secure bootloaders, host-based intrusion detection systems, and tamper-resistant technologies.

DER Equipment
- Firmware update mechanisms that address key/certificate provisioning and storage.
- Improved credential, sensitive data (e.g., Wi-Fi password), and Personally Identifiable Information (PII) storage.

Upstream Communications
- Communication solutions with end-to-end confidentiality, integrity, authentication, authorization, non-repudiation, and auditing.
- Improved authentication and authorization mechanisms for DER equipment, including those established with PKIs.
- Network-based intrusion detection and mitigation systems.
- Alerts sent to dedicated DER Security Operations Centers (SOCs).

Cloud Environments
- Cloud, website, and API security solutions that prevent manipulation or information disclosure with authentication on all endpoints.

Conclusion

Cybersecurity researchers must continue to identify DER vulnerabilities

- It's part of a **continuous process of hardening charging infrastructure** against cyberattacks
- DER vendors should have **bug bounty programs** and support **responsible disclosure processes**
- DER vendors and 3rd parties should consider adopting **zero-trust principles** in addition to traditional perimeter defenses

Federal and state governments should **seek policies to improve the security of DER systems**

- Expect to see U.S. states and other jurisdictions adding cybersecurity requirements soon
- There is also a lot of work in securing EV Supply Equipment (EVSE)
  - See UK's "The Electric Vehicles (Smart Charge Points) Regulations 2021", 2021 No. 1467.

Comprehensive national cybersecurity approach must include:

- **Information sharing programs** in conjunction with EVSE/cloud **anomaly/intrusion detection systems**
- **Incident response strategies**, especially for coordinated/widespread attacks on grid infrastructure
- Strong cybersecurity stakeholder education and **workforce development** programs

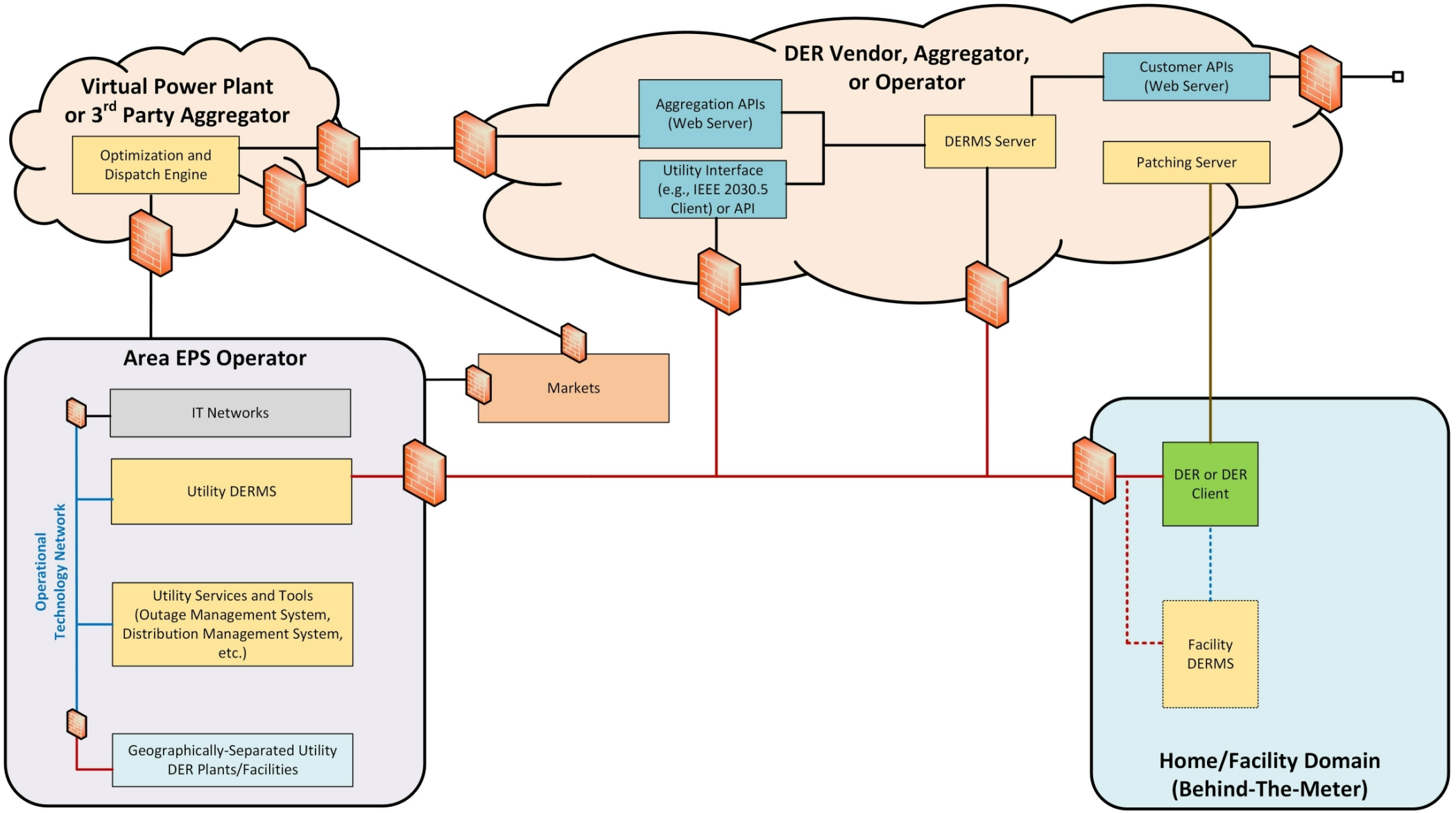
Thank You!

Jay Johnson

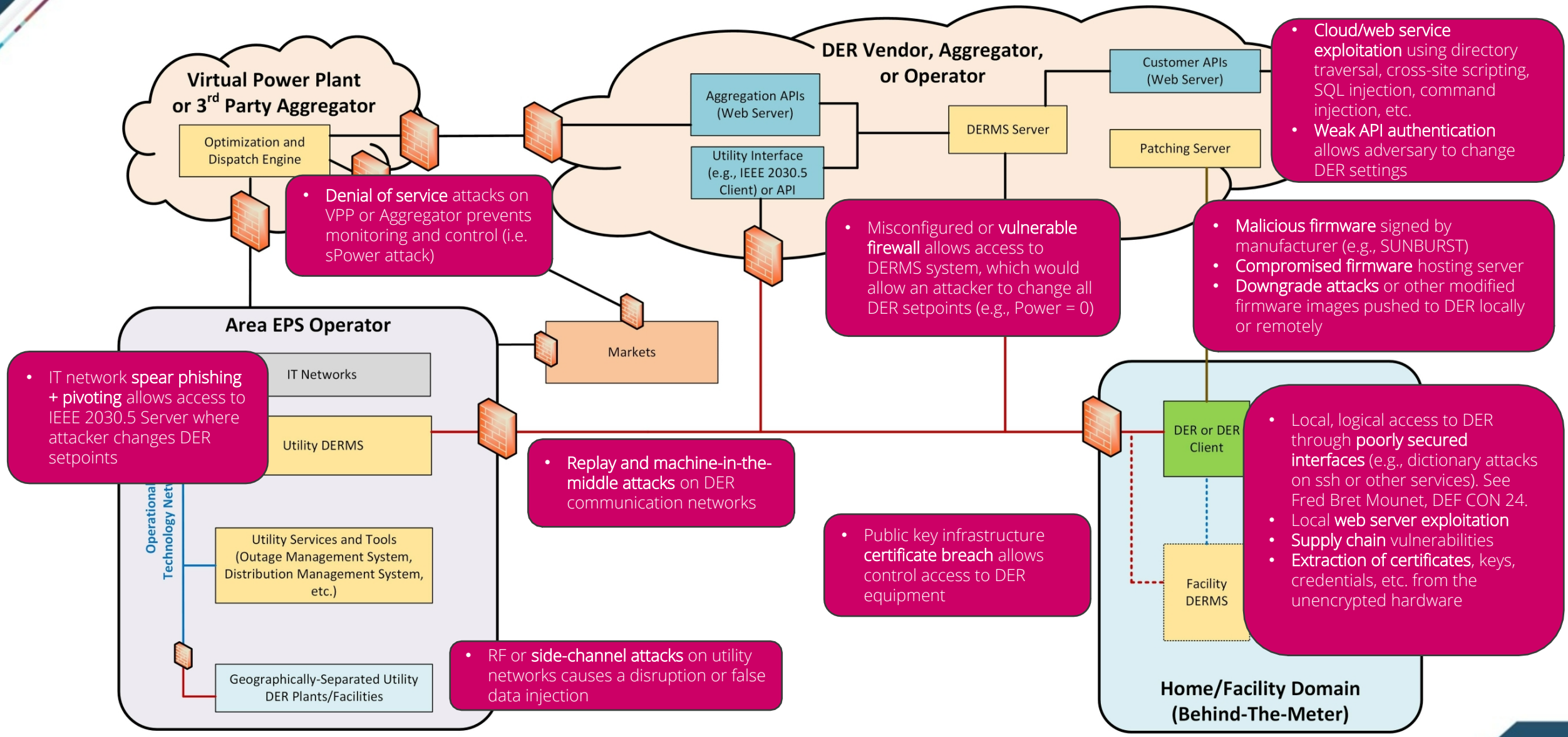
jjohns2@sandia.gov

DER Cyber Threats and Defenses

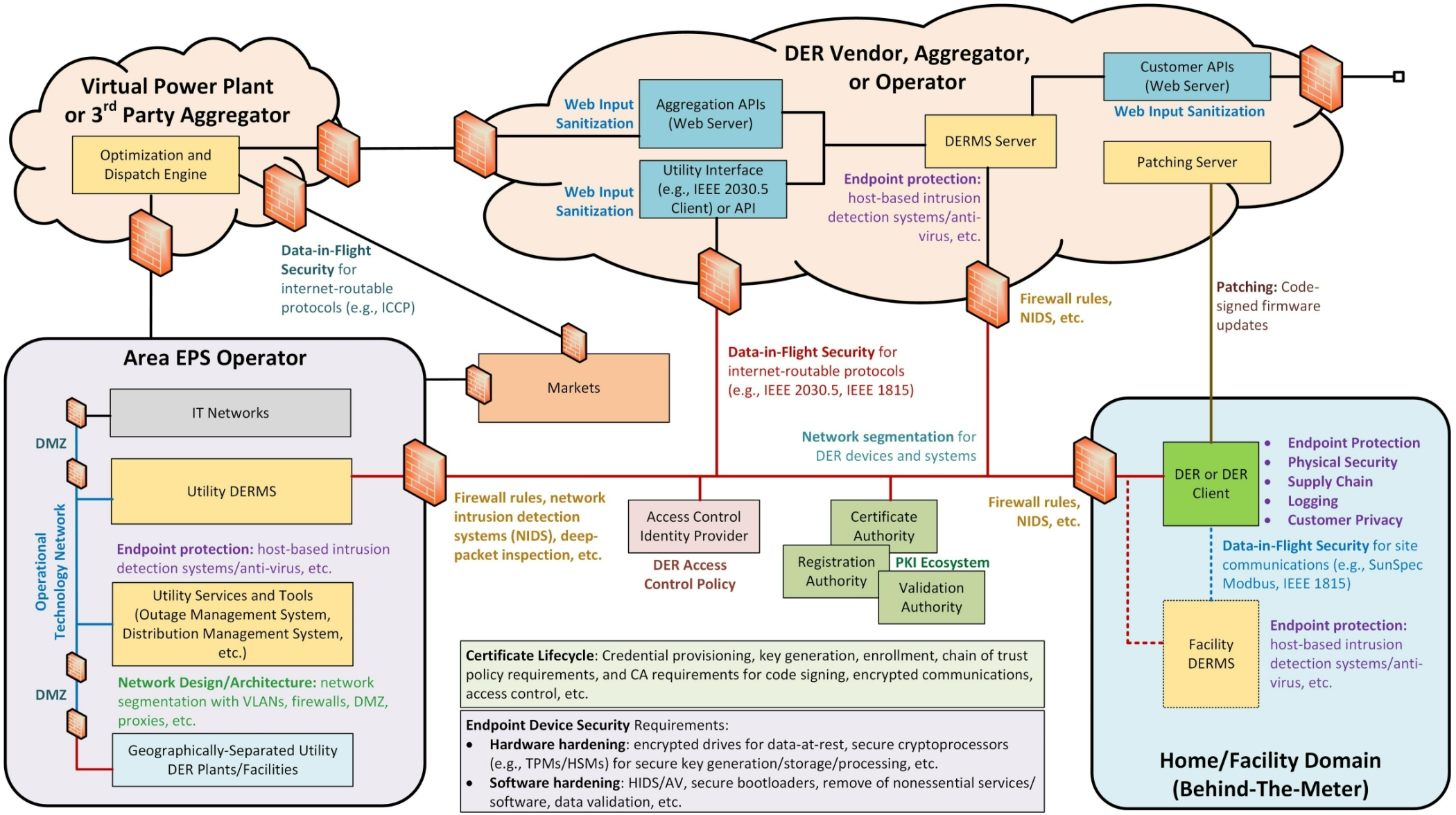
DER Communications



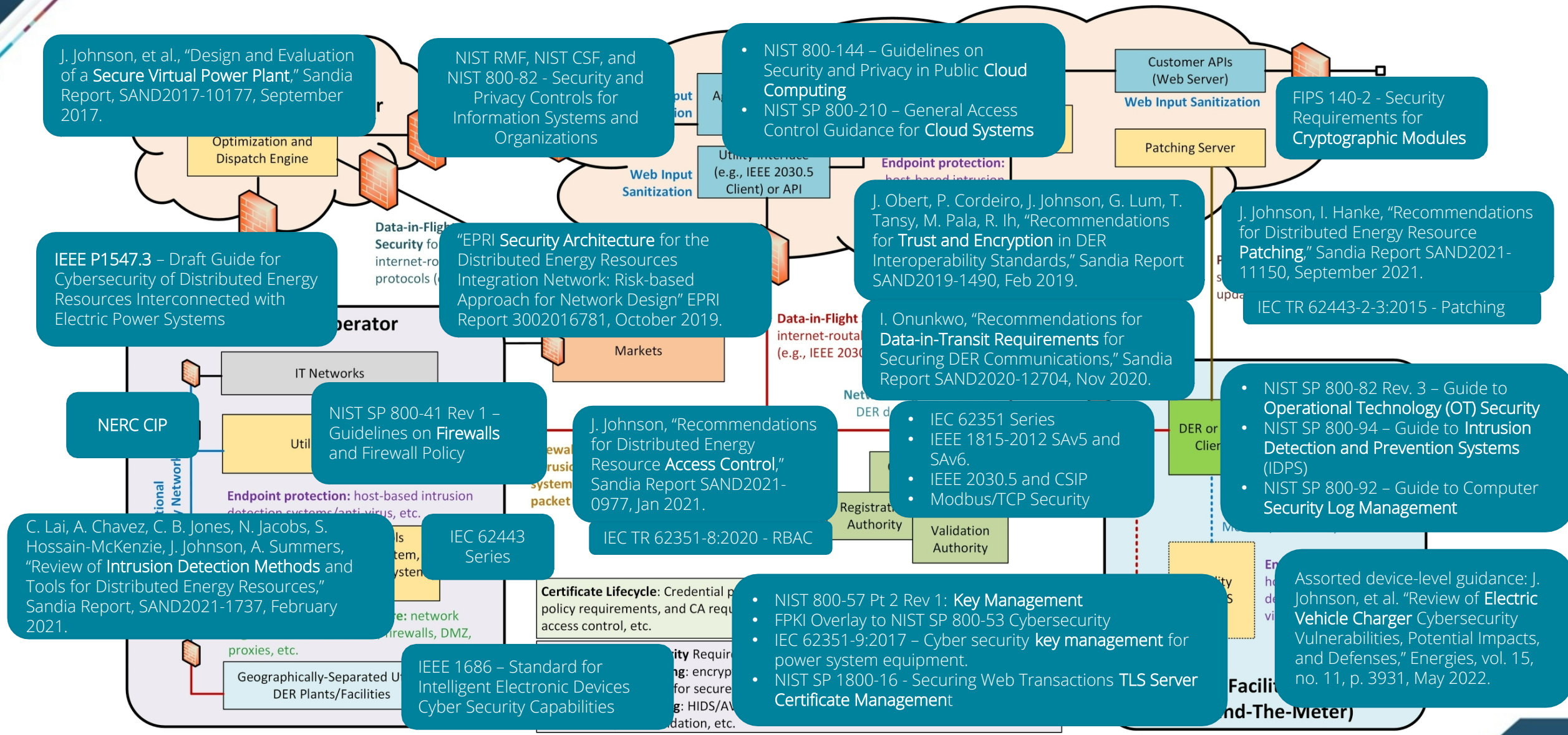
Potential Threats



Hardening Recommendations



Hardening Guidance



J. Johnson, et al., "Design and Evaluation of a **Secure Virtual Power Plant**," Sandia Report, SAND2017-10177, September 2017.

NIST RMF, NIST CSF, and NIST 800-82 - Security and Privacy Controls for Information Systems and Organizations

- NIST 800-144 – Guidelines on Security and Privacy in Public **Cloud Computing**
- NIST SP 800-210 – General Access Control Guidance for **Cloud Systems**

FIPS 140-2 - Security Requirements for **Cryptographic Modules**

IEEE P1547.3 – Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

"EPRI **Security Architecture** for the Distributed Energy Resources Integration Network: Risk-based Approach for Network Design" EPRI Report 3002016781, October 2019.

J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, R. Ih, "Recommendations for **Trust and Encryption** in DER Interoperability Standards," Sandia Report SAND2019-1490, Feb 2019.

J. Johnson, I. Hanke, "Recommendations for Distributed Energy Resource **Patching**," Sandia Report SAND2021-11150, September 2021.

IEC TR 62443-2-3:2015 - Patching

I. Onunkwo, "Recommendations for **Data-in-Transit Requirements** for Securing DER Communications," Sandia Report SAND2020-12704, Nov 2020.

NERC CIP

NIST SP 800-41 Rev 1 – Guidelines on **Firewalls** and Firewall Policy

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

IEC TR 62351-8:2020 - RBAC

- IEC 62351 Series
- IEEE 1815-2012 SAv5 and SAv6.
- IEEE 2030.5 and CSIP
- Modbus/TCP Security

- NIST SP 800-82 Rev. 3 – Guide to **Operational Technology (OT) Security**
- NIST SP 800-94 – Guide to **Intrusion Detection and Prevention Systems** (IDPS)
- NIST SP 800-92 – Guide to Computer **Security Log Management**

C. Lai, A. Chavez, C. B. Jones, N. Jacobs, S. Hossain-McKenzie, J. Johnson, A. Summers, "Review of **Intrusion Detection Methods** and Tools for Distributed Energy Resources," Sandia Report, SAND2021-1737, February 2021.

IEC 62443 Series

- NIST 800-57 Pt 2 Rev 1: **Key Management**
- FPKI Overlay to NIST SP 800-53 Cybersecurity
- IEC 62351-9:2017 – Cyber security **key management** for power system equipment.
- NIST SP 1800-16 - Securing Web Transactions **TLS Server Certificate Management**

Assorted device-level guidance: J. Johnson, et al. "Review of **Electric Vehicle Charger** Cybersecurity Vulnerabilities, Potential Impacts, and Defenses," Energies, vol. 15, no. 11, p. 3931, May 2022.

IEEE 1686 – Standard for Intelligent Electronic Devices Cyber Security Capabilities

Possible DER Cybersecurity Requirements for California

Requirements - Logging

- Devices SHALL log security events with the user ID and timestamp. Security events include, at a minimum: (a) successful and unsuccessful login attempts, (b) detected failure of event logging, (c) changes to device settings, (d) software updates and changes, (e) changes to access controls or accounts.
- Devices SHALL store logs locally or remotely.
- Device network traffic SHALL be logged with a time-stamp and retained regardless of power loss.
- Devices SHALL have a log timestamp resolution of at least 1 millisecond.
- Devices SHALL store power system logs, which include at minimum: (a) when a function is enabled or disabled (b) when there is a change to adjustable settings of the device.
- Devices SHALL store security event logs for 90 days, power system logs for 90 days, and network traffic for 14 days.
- Devices SHALL maintain time accuracy within +/- 1 min of Coordinated Universal Time (UTC) for all logging timestamps.
- Devices SHALL log any service or firewall changes.
- Devices SHALL include the ability to send syslog (RFC 5424) messages to an owner-defined server with an update period of at least once per 24 hours.

Requirements – Access Control and Authentication

- Device vendors SHALL report all open ports and their business use.
- Device local or remote electronic access SHALL be protected with an authentication mechanism that identifies a user with a unique user identification (UID).
- Devices SHALL assign users permissions to access data, services, resources, or other operations including:
  - Reading DER nameplate or configuration information, measurement data (voltage, current, power, energy, status, alarms, etc.), and control mode settings.
  - Writing control mode settings that alter the operational characteristics of the DER.
- Devices SHALL require passwords with eight or more characters that contain at a minimum the following: (a) at least one uppercase and one lower case letter, (b) at least one number, (c) at least one non-alphanumeric character (e.g., @, %, &, *).
- Devices SHALL require user passwords to be changed upon commissioning.
- Devices SHALL log out a user after five minutes of inactivity.
- Devices SHALL support adjustable account lockout thresholds and durations for access failures.
- All authenticated sessions to/from devices SHALL have a timeout period.

Requirements – Encryption and Privacy

- Devices SHALL encrypt all cryptographic keys stored on the device.
- Devices SHALL encrypt all internet-routed traffic.
- Devices SHALL include a factory reset function where the software restores the electronic device to its original system state by erasing all of the information stored on the device.
- Devices SHALL delete all user data following a factory reset.

Requirements – Patching

- Devices SHALL support updating all security and operational software functions.
- Devices SHALL support remote updates.
- Devices SHALL support automated updates.
- Devices SHALL include the ability to disable automated updates.
- Devices SHALL check for updates every 7 days, at minimum.
- Devices SHALL verify the authenticity and integrity of software updates.
- Devices SHALL validate the product supplier's identity for all firmware updates.
- Devices SHALL confirm receipt and installation of all firmware updates.
- Devices SHALL use mechanisms that prevent firmware downgrade attacks.
- Devices SHALL incorporate secure boot mechanisms to validate its software has not been altered other than in accordance with a secure software update.