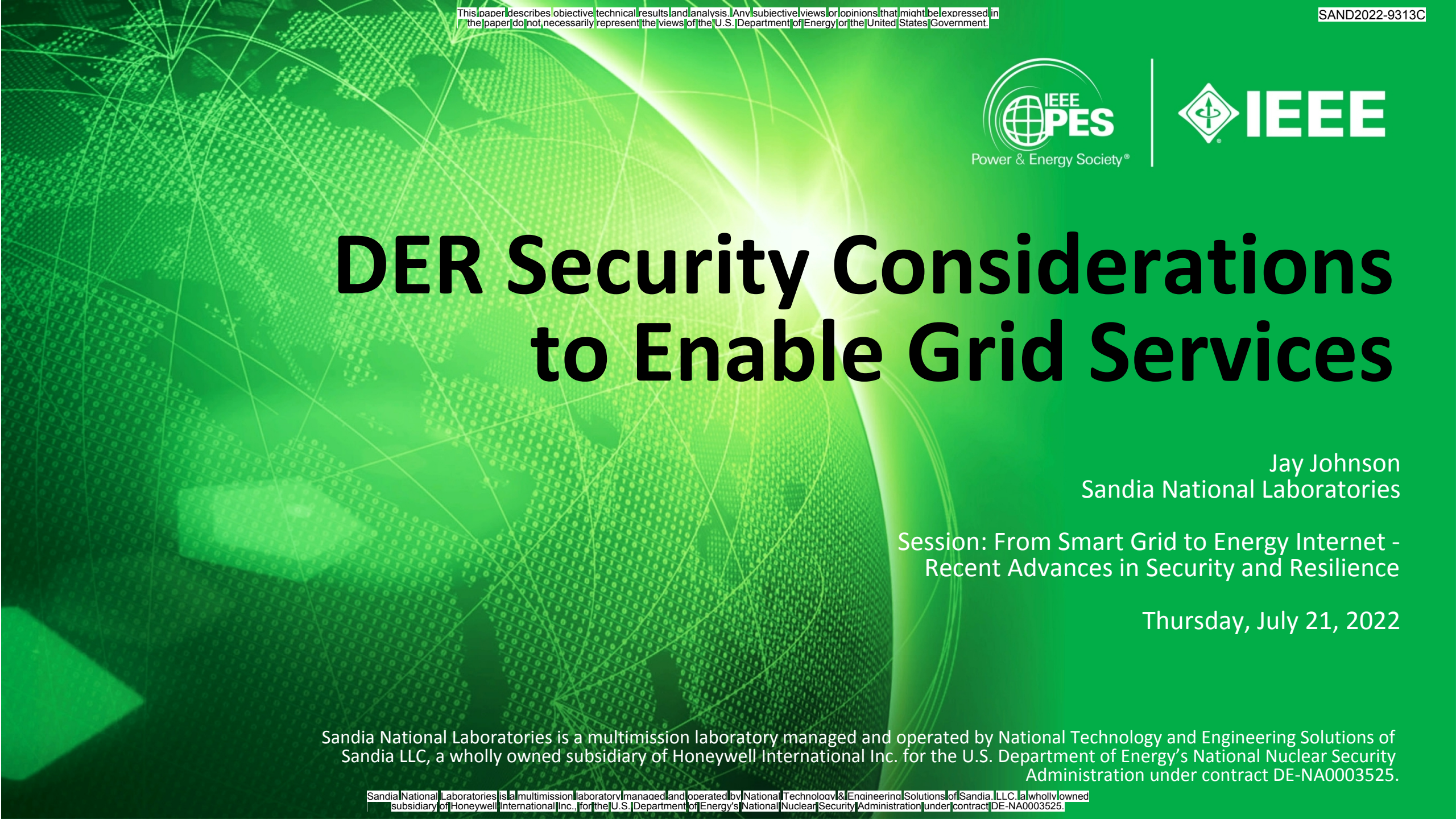
SAND2022-9313C



DER Security Considerations to Enable Grid Services

Jay Johnson
Sandia National Laboratories

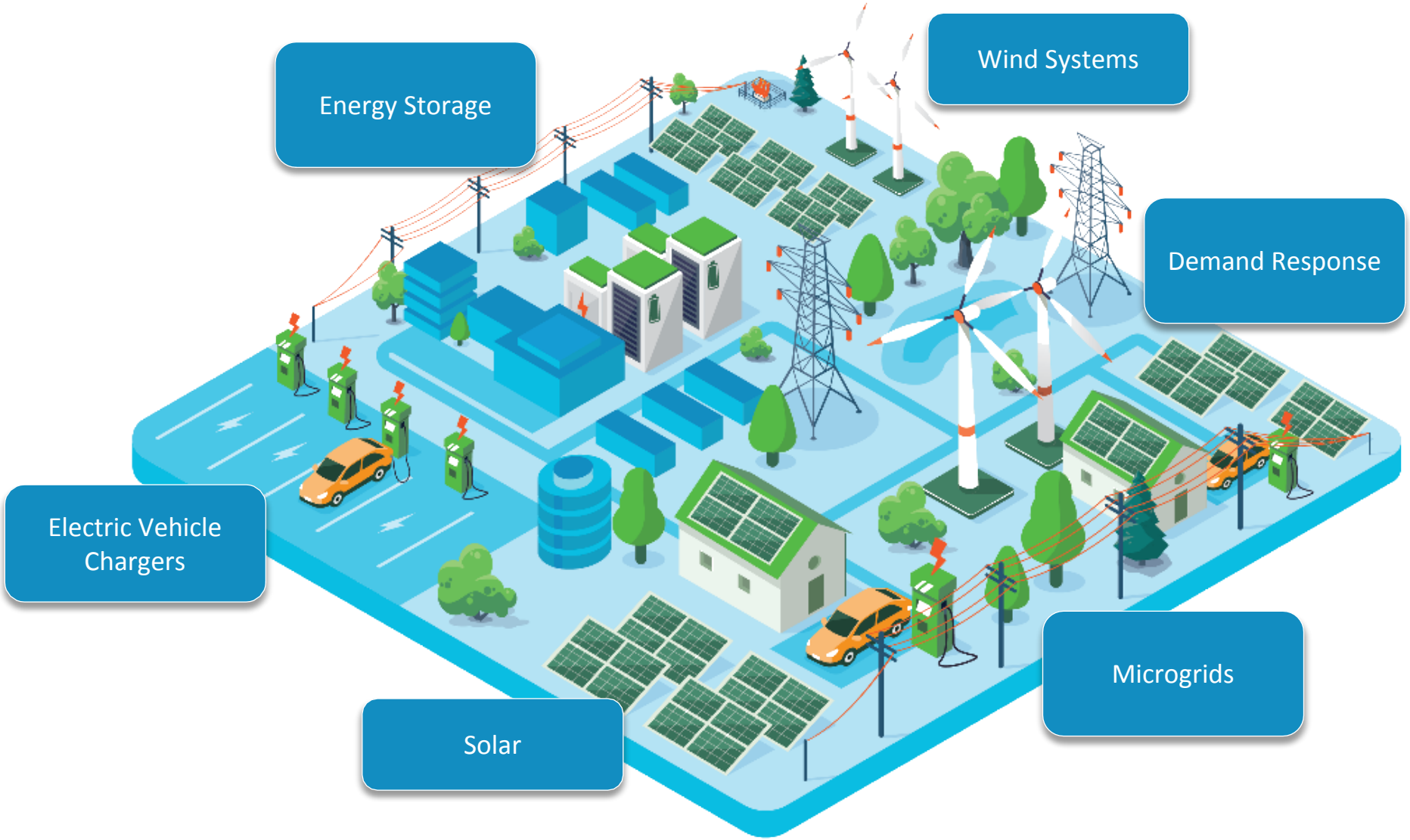
Session: From Smart Grid to Energy Internet - Recent Advances in Security and Resilience

Thursday, July 21, 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.

Grid-Service Participants in the Future Grid



Utility-Interactive Converters are Smart Grid Building Blocks

Advanced, **interoperable, grid-support functions** for solar, energy storage, wind, and other DER assets **are the building blocks** for an efficient, **optimized power system** which supports high penetrations of renewable energy.

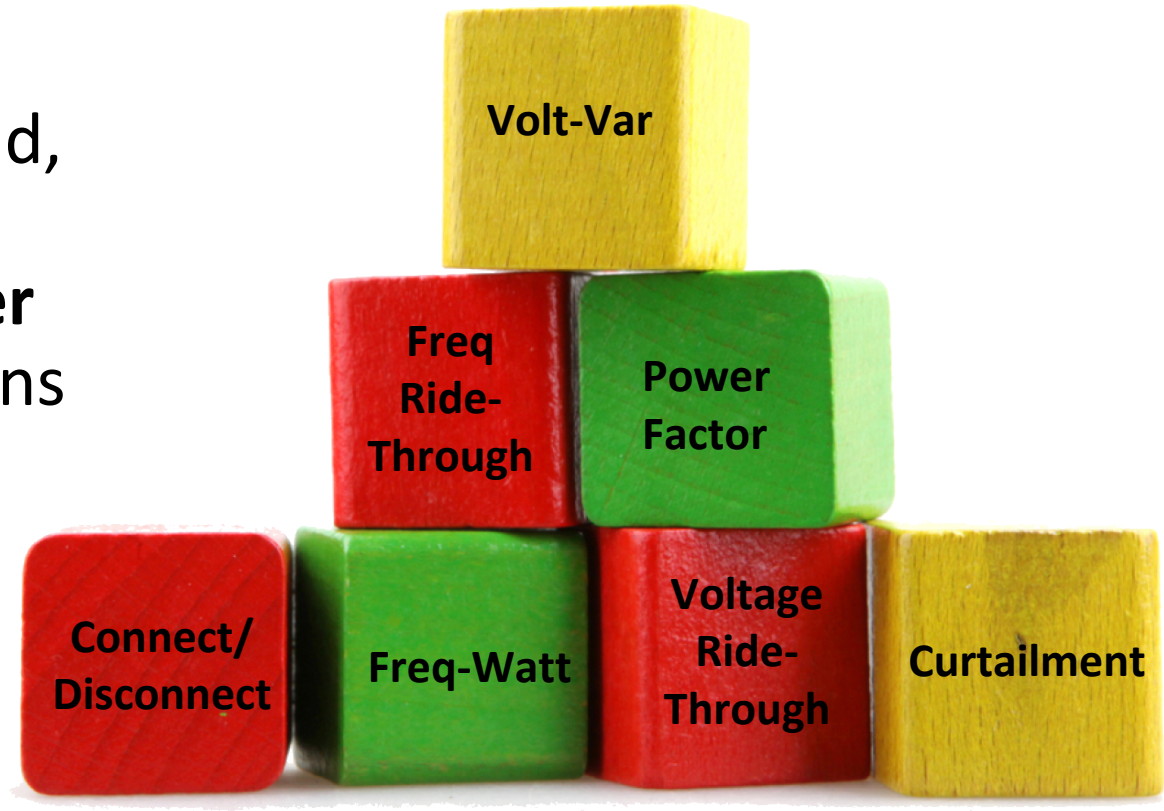
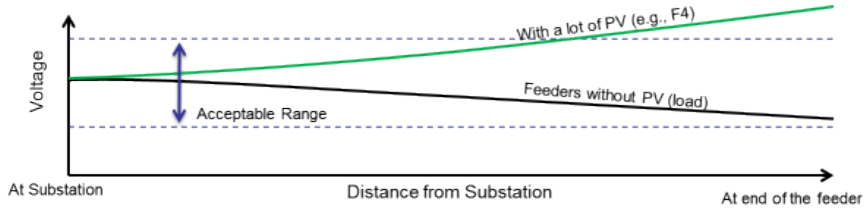


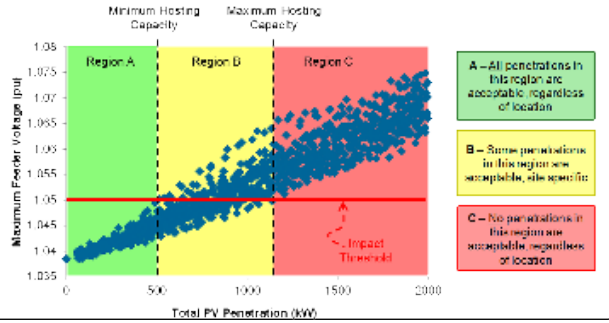
Image: BetaNews

Grid-support functions = visibility and control

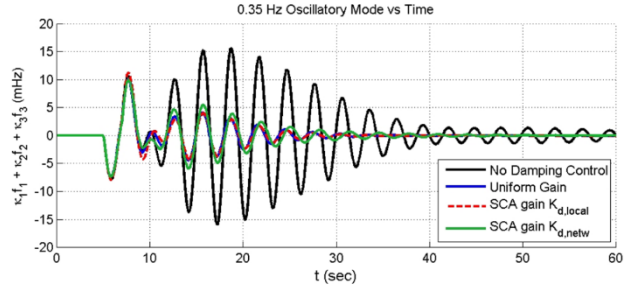
Distribution Voltage Regulation[1]



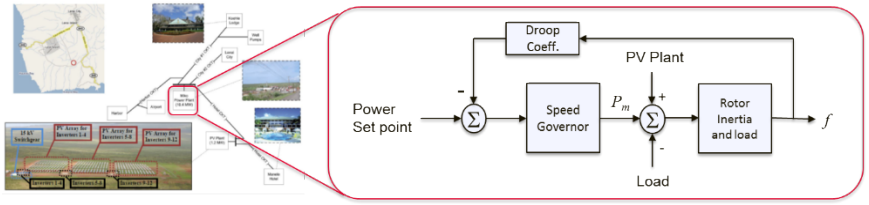
Feeder Hosting Capacity[2]



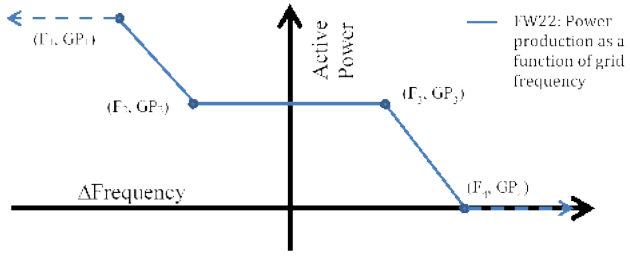
Wide-Area Damping[3]



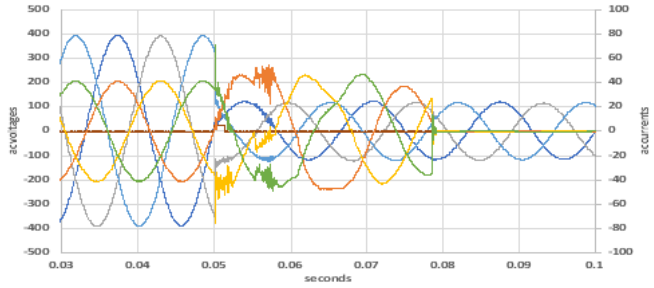
Frequency Control[4]



Ancillary Reserves[5]



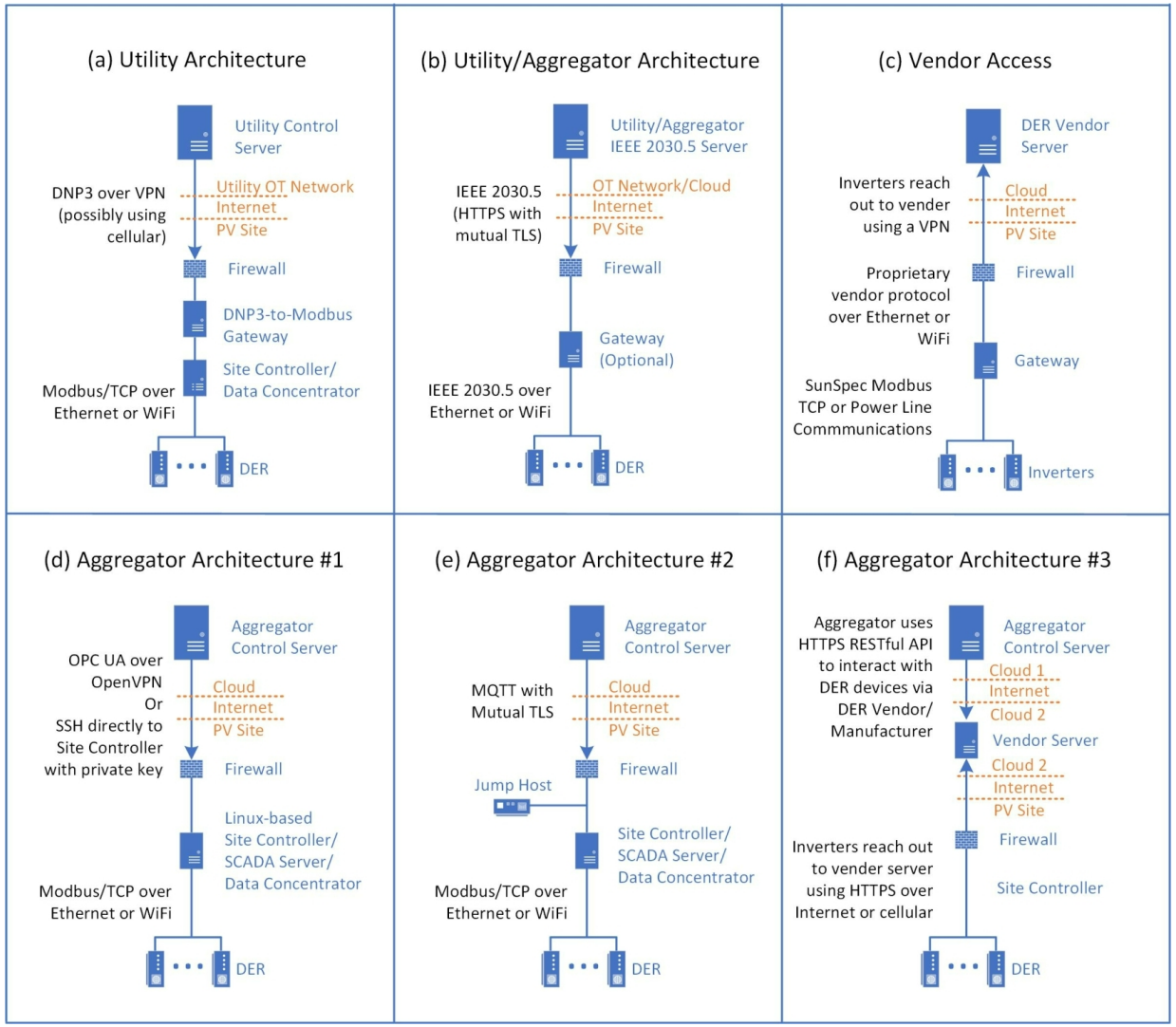
Protection Support[6]



1. J. Seuss, M.J. Reno, R.J. Broderick, R.G. Harley, "Evaluation of reactive power control capabilities of residential PV in an unbalanced distribution feeder," 2014 PVSC, pp. 2094-2099, 8-13 June 2014.
2. M. Rylander J. Smith, "Stochastic Analysis to Determine Feeder Hosting Capacity for Distributed Solar PV," Report 1026640, 31 Dec 2012.
3. J. Neely, J. Johnson, R. Bryne, R. T. Elliott, Structured optimization for parameter selection of frequency-watt grid support functions for wide-area damping, DER Journal, vol. 11, no. 1, pp. 69-94, 2015.
4. J. Neely, S. Gonzalez, J. Delhotal, J. Johnson, M. Lave, Evaluation of PV Frequency-Watt Function for Fast Frequency Reserves, IEEE Applied Power Electronics Conference (APEC), Long Beach, CA, March 20-24, 2016.
5. J. Johnson, J. Neely, J. Delhotal, M. Lave, "Photovoltaic Frequency-Watt Curve Design for Frequency Regulation and Fast Contingency Reserves," IEEE Journal of Photovoltaics, vol. 6, no. 6, pp. 1611-1618, Nov. 2016.
6. S. Gonzalez, N. Gurule, M. J. Reno, J. Johnson, Fault Current Experimental Results of Photovoltaic Inverters Operating with Grid-Support Functionality, 7th World Conference on Photovoltaic Energy Conversion (WCPEC-7), Waikoloa, HI, 10-15 Jun 2018 (submitted).

Distributed Energy Cybersecurity

- **Challenge**: The power system is rapidly evolving with cloud and internet-connected distributed energy resources (DER)
  - Cybersecurity is paramount for national energy infrastructure.
- Unique risks and hurdles:
  - Customer-owned and 3rd-party operated assets in a **non-federated environment**
  - **Rapidly evolving environment** with **unclear responsibilities**
- DER cybersecurity is inherently different than 'business -as-usual' because:
  - DER often connected to grid operators via **public internet or cellular networks**
  - DER typically have **limited processing capabilities**, so they often do not support many cipher suites or host-based intrusion detection systems (HIDS)



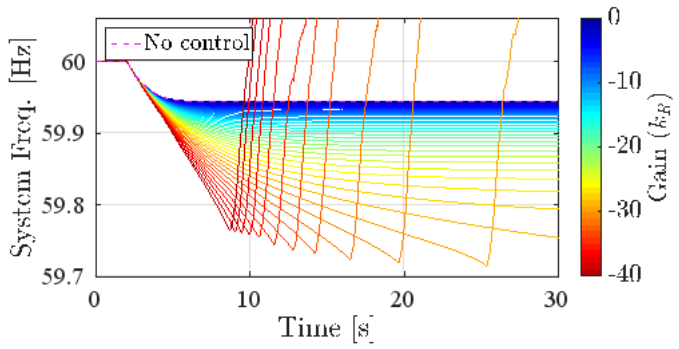
DER Communication Options

What could possibly go wrong?

Frequency Droop

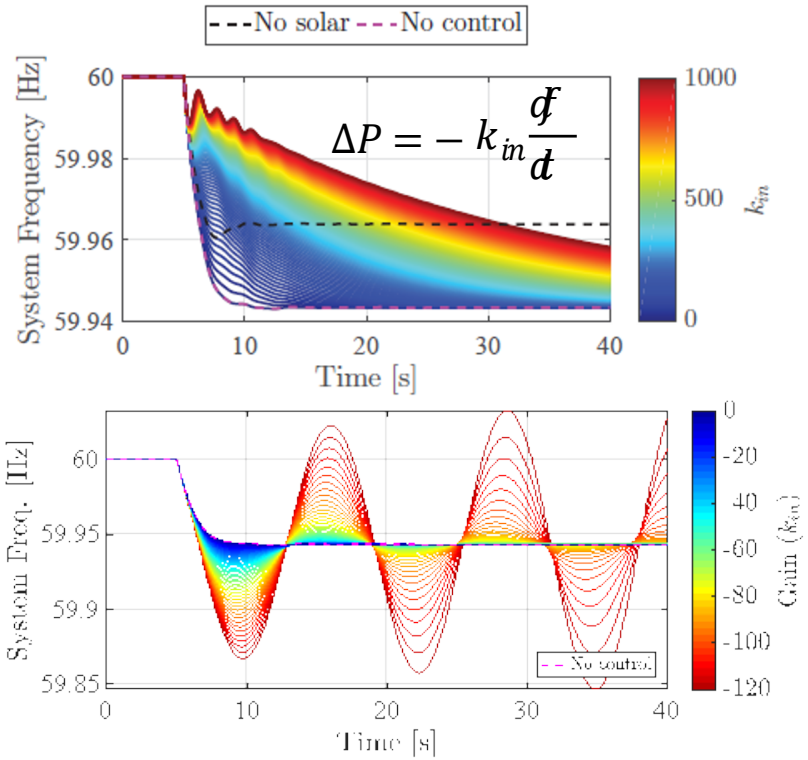
$$\Delta P_j = \frac{f_{ref} - f_{eq}}{R} = k_R(f_{ref} - f_{eq})$$

$$\Delta P_j^{attack} = -\frac{f_{ref} - f_{eq}}{R} = -k_R(f_{ref} - f_{eq})$$



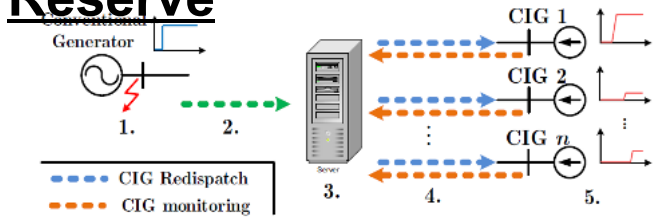
Attack: frequency-watt function is inverted to inject power at high frequency and absorb power at low frequency.
Result: Lower frequency nadirs, possibly leading to load shedding.
k_R<-25 causes loss of synchronism.

Synthetic Inertia



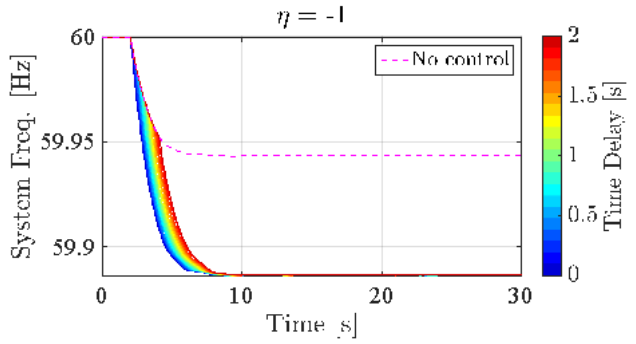
Attack: reverse sign on inertial gain to create positive feedback.
Result: Nadir is reduced and oscillatory behavior in the power system is created, leading to instability and possible blackouts.

Fast Acting Imbalance Reserve



CIG = Converter-Interfaced Generator

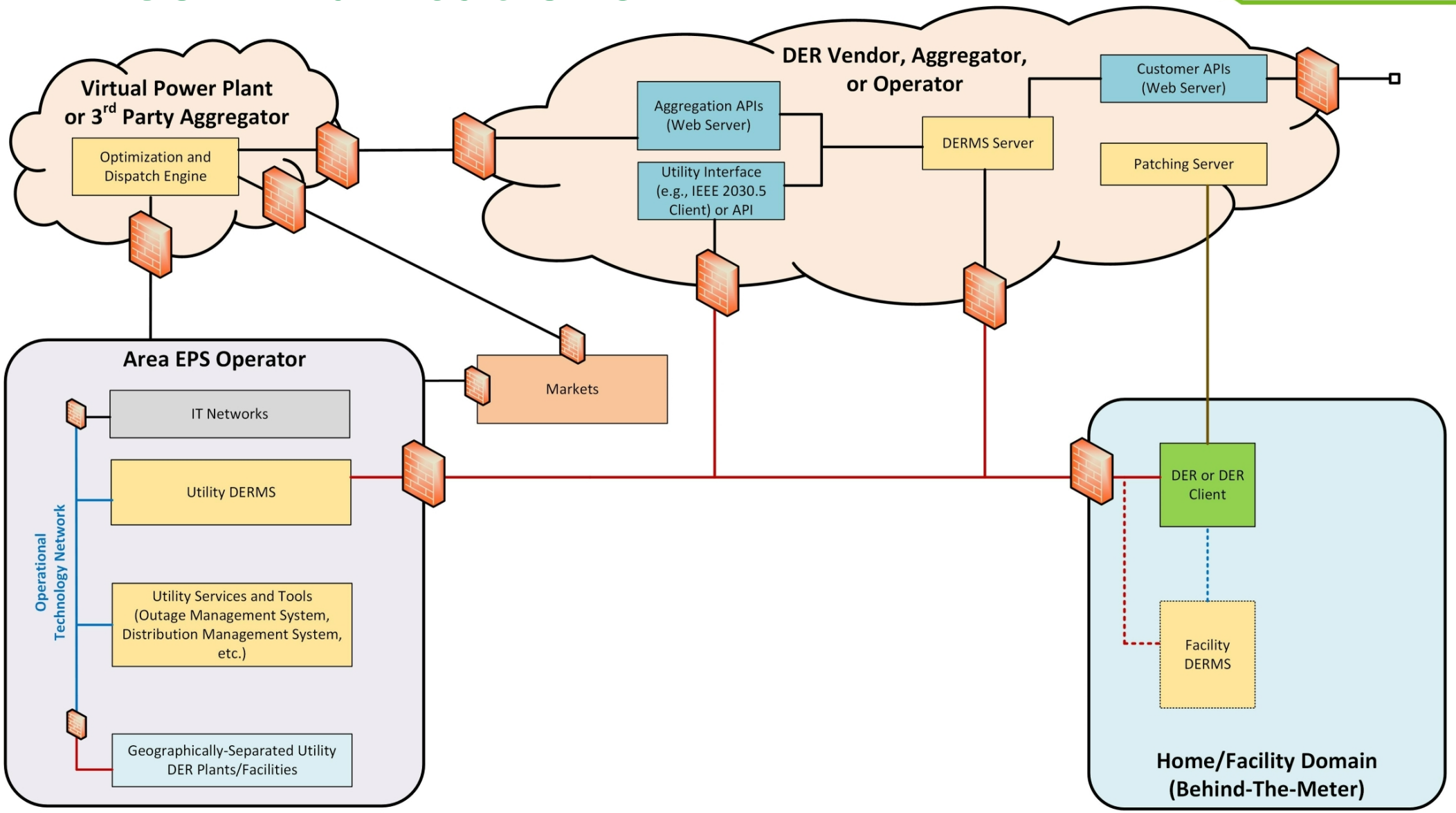
$$\Delta P_i = K_{FF}^i P_{imbal} \qquad K_{FF}^i = \eta \frac{P_i}{P_{avail}}$$



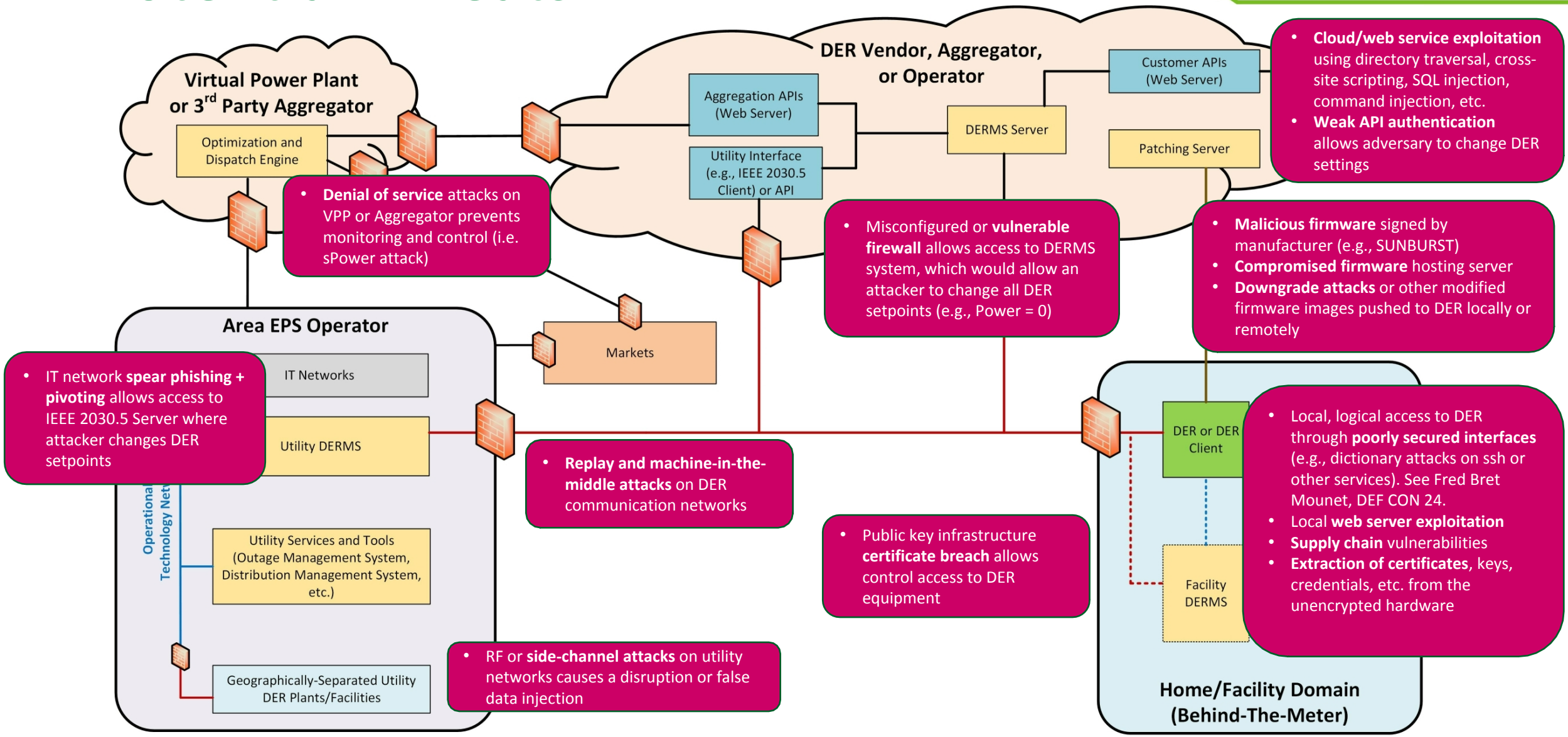
Attack: imbalance power compensation level, η, is set to reduce the power by the magnitude of the imbalance. In an attack: η=-1.
Result: Imbalance is worsened, possibly leading to a blackout.

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.

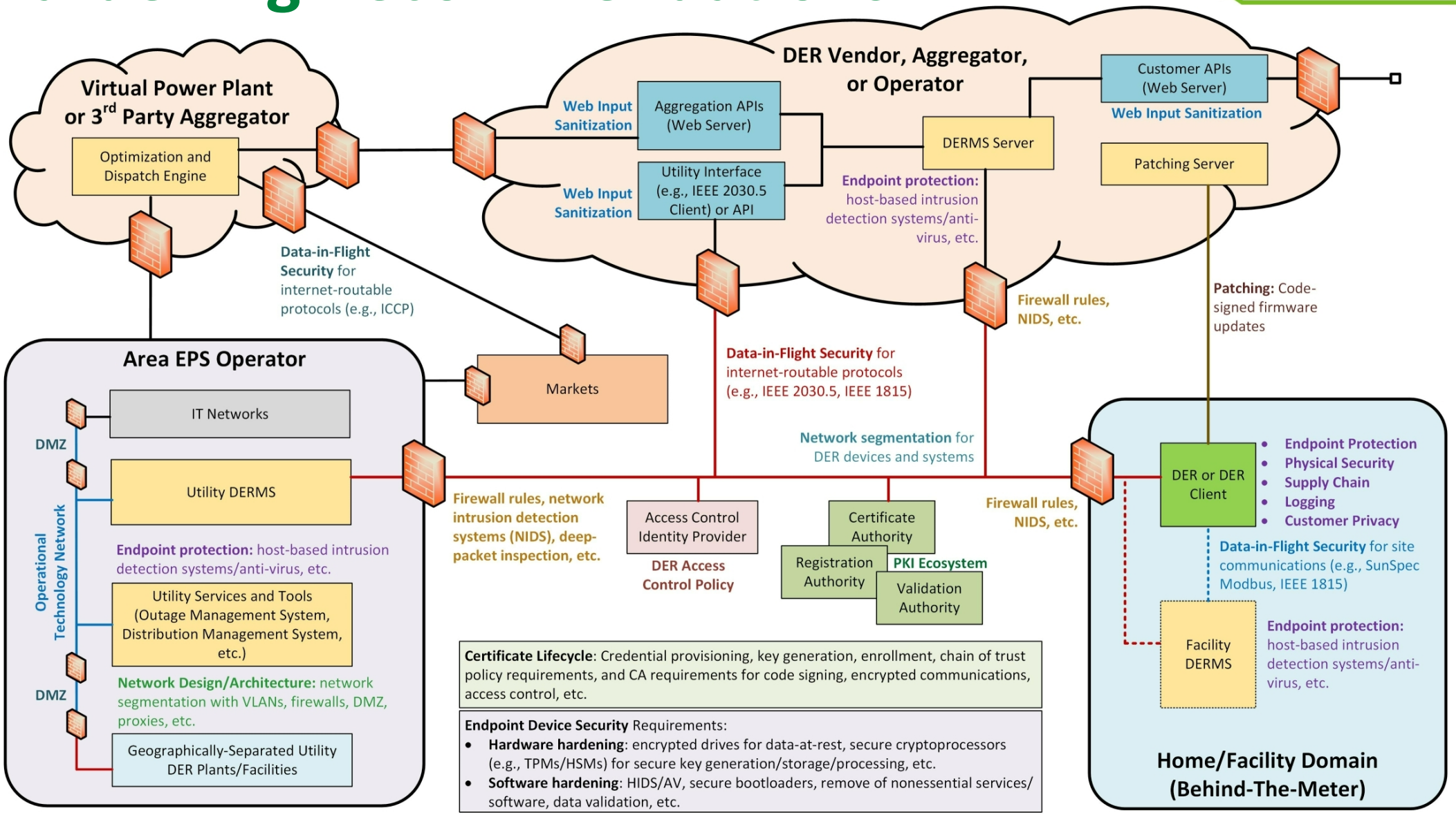
DER Communications



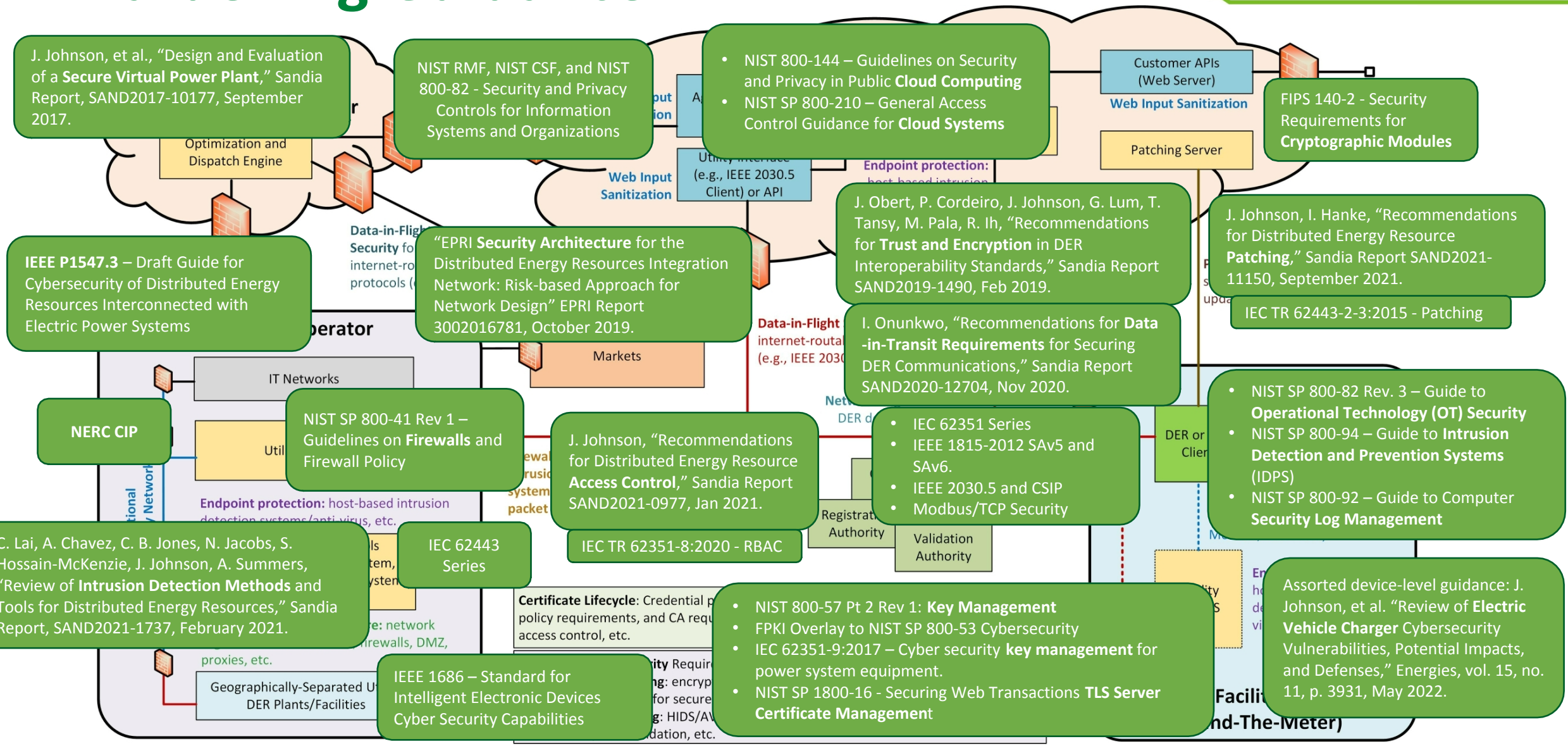
Potential Threats



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 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**

IEC TR 62351-8:2020 - RBAC

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**

IEEE 1686 – Standard for Intelligent Electronic Devices Cyber Security Capabilities

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.

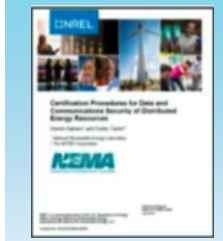
Join the conversation!

SunSpec/Sandia DER Cybersecurity Workgroup was founded in Aug 2017

- **1,700+ DER and cybersecurity experts**
- 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 state regulators (NASEO/NARUC Cybersecurity Advisory Team).
- Funded through 3 DOE SETO cybersecurity projects

Webinars by

Technical Publications



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
Lead: Steve Bukowski (INL), Jay Johnson (Sandia)

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

Learn More - Educational 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 – **Integrated Cyber Risk Management for DER and EV Charger Supply Chains** – *Fortress Information Security*
- …

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

Contact

Jay Johnson
jjohns2@sandia.gov

Market Trends Driving DER Cybersecurity

EPRI Smart Inverter functions paper published

"50.2 Hz Problem" discovered in Germany

Smart Inverter Working Group starts at PUC

HI remotely upgrades 800K inverters

CA selects IEEE 2030.5 as default protocol

IEEE 1547-2018 published with communication required

SunSpec test procedures & PKI established

CSIP defined

CA Rule 21 Phase 1

IEEE 1547.1 published

CA Rule 21 Phase 2

U.S. roll out of interoperable DER commences

2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

Hawaii
Rule 14H

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"*
- Included in IEEE P1547.3 Draft. Future work unknown.

Data-in-Flight

- **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.
- Included in IEEE P1547.3 Draft. Future work unknown.

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"*
- Included in IEEE P1547.3 Draft. Future work unknown.

Patching

- **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"*
- Included in IEEE P1547.3 Draft. Future work unknown.

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 SunSpec Activity: SunSpec Cybersecurity Certification Workgroup

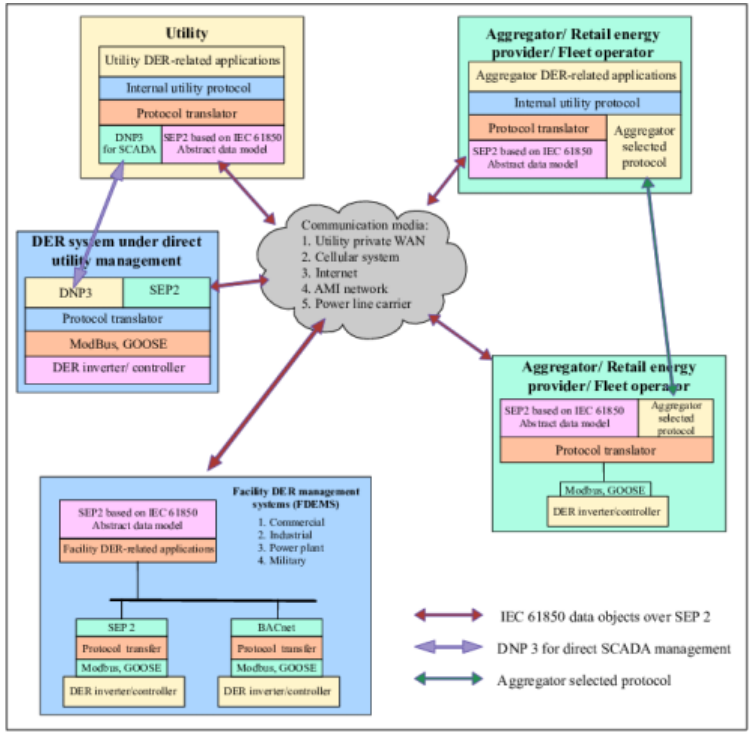
- **Establishing voluntary DER/client cybersecurity certification test protocol.**
- **Lead: Jörg Brakensiek (Wivity)**

Related SunSpec Activity: Blockchain Workgroup

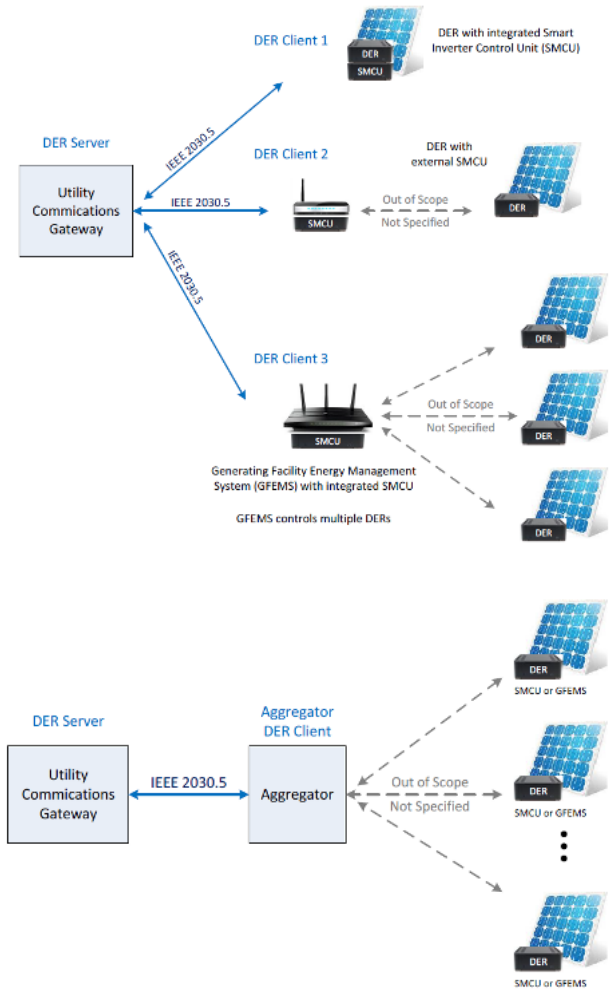
- **Defined requirements and specifications for using blockchain to ensure the security of private keys in DER manufacturing environments.**
- **Lead: Jörg Brakensiek (Wivity) and Alfred Tom (Wivity)**

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

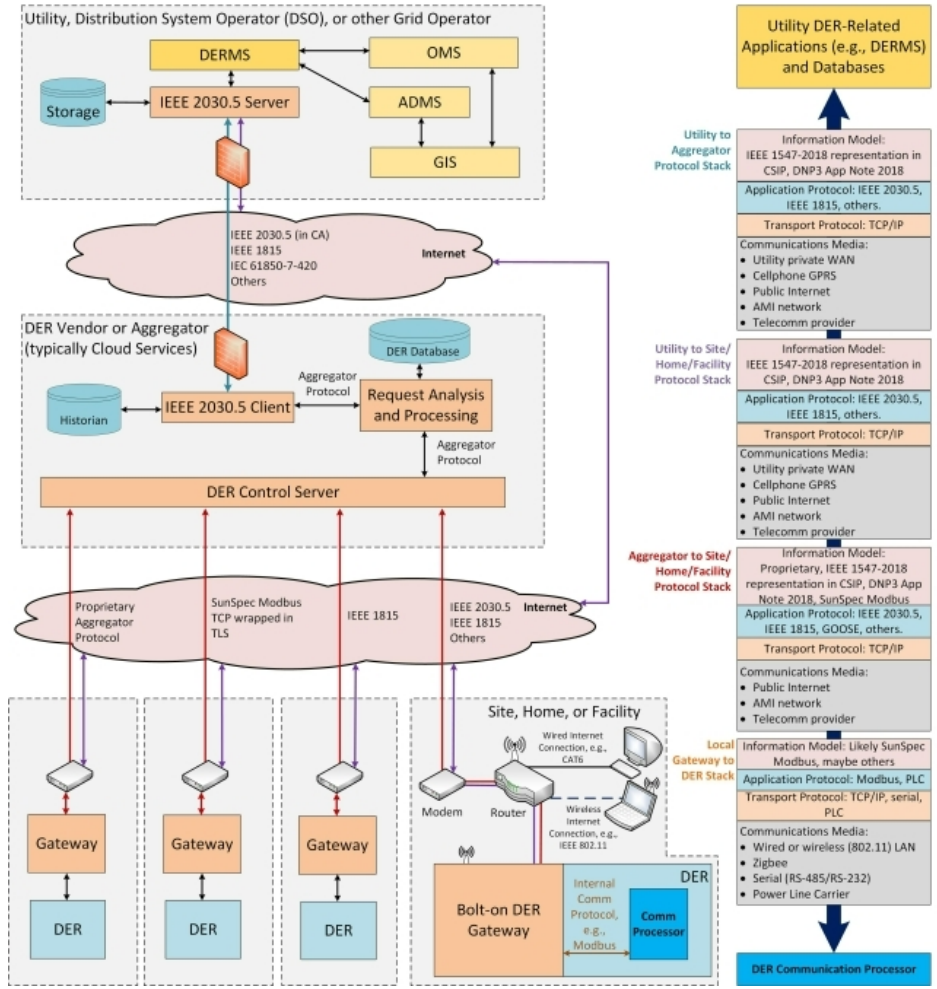
DER Comms: A new power system attack vector



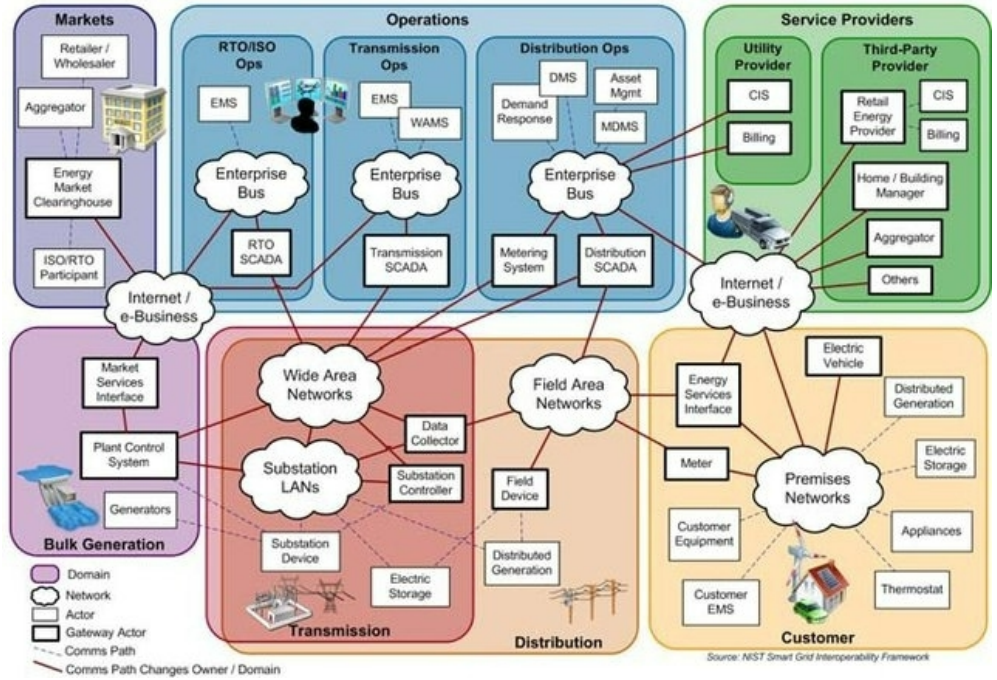
A. Nagarajan, B. Palmintier, M. Baggu, Advanced inverter functions and communication protocols for distribution management, 2016.



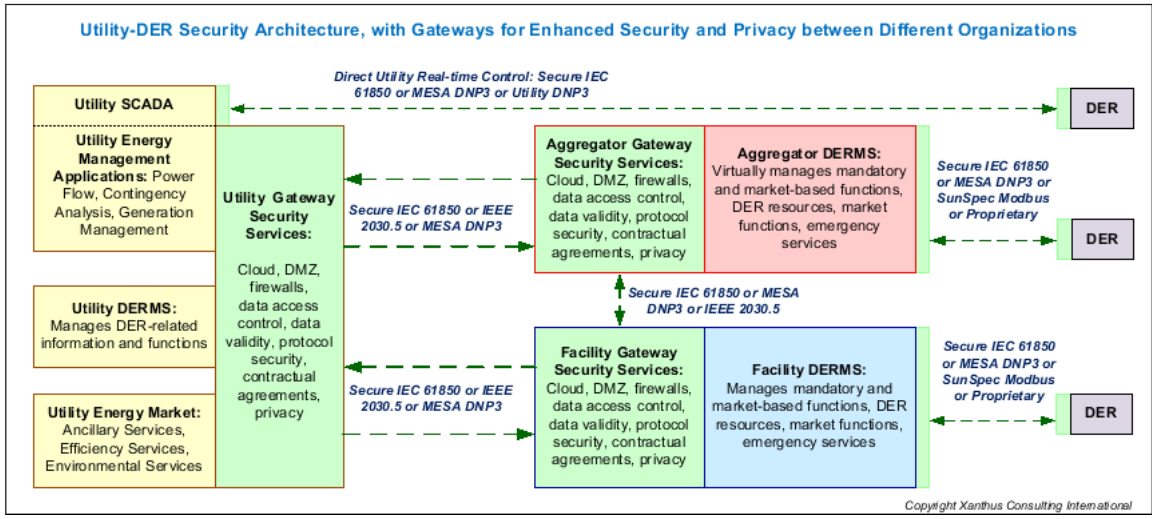
Common Smart Inverter Profile Implementation Guide v2.1, March 2018.



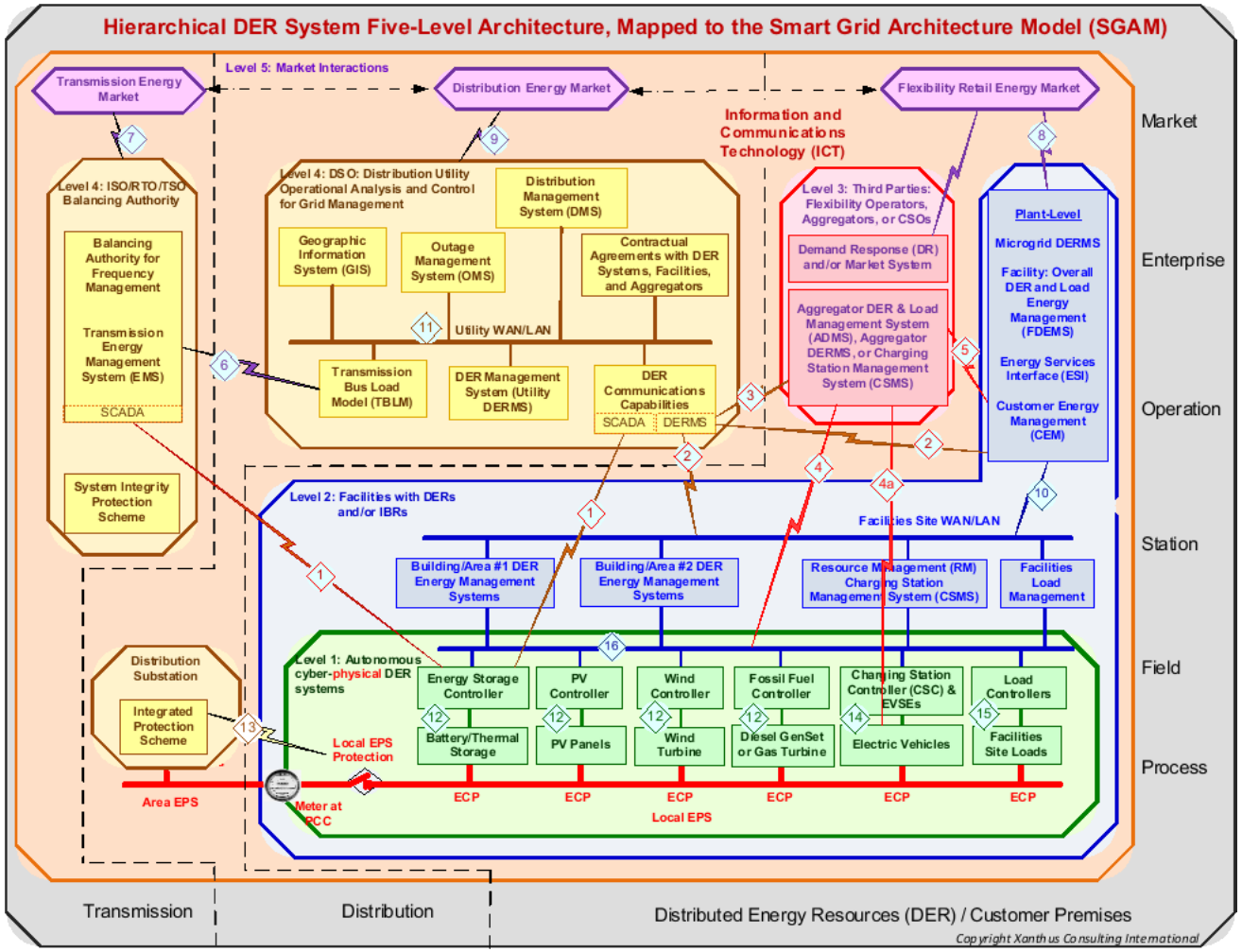
I. Onunkwo, SAND2020-12704



NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.



From the IEEE 1547.3 Draft



From the IEEE 1547.3 Draft