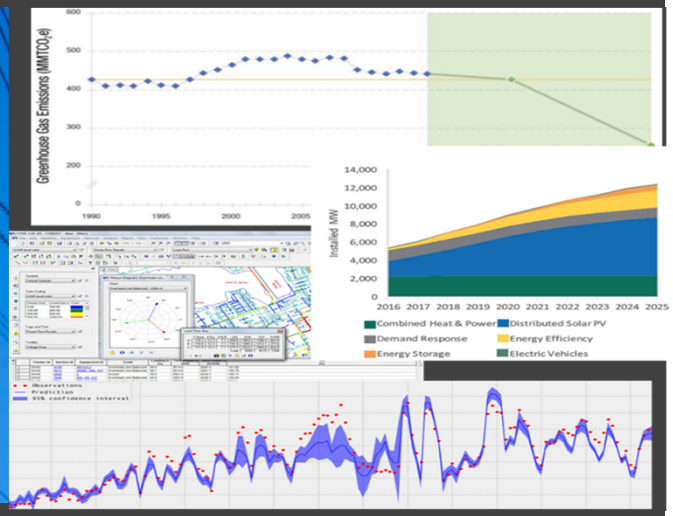
Practical Considerations in the Standardization of Cyber Security for Inverter-Based Resources

VT-MPR Seminar on Cybersecurity of the Electric Power Grid
March 16, 2023, 2:45 pm



Paul Duncan, MPR Associates, Inc., pduncan@mpr.com, (703) 519-0478

MPR is a world leading specialty engineering and management services organization.

We provide highly diversified engineering, project management, risk management and other innovative solutions to domestic & international clients in:

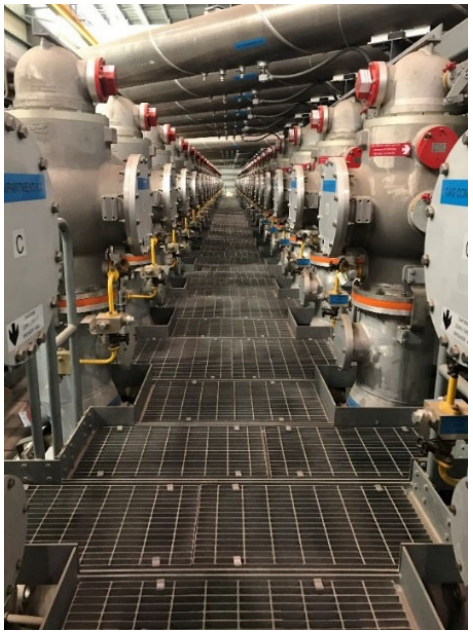
- Energy
- Defense & National Security
- Health & Life Sciences

Objectivity and independence combined with seasoned risk-focused engineering leadership creates an exceptional level of experience and impact unique to MPR

MPR's Transmission & Distribution Practice

MPR's team works to deliver high value solutions that mitigate risk for our T&D clients in the areas of:

- Equipment Engineering: Design, Procurement, Test, Analysis
  - Transformers, Power Electronics
  - Energy Storage Technology Development
  - Reliability and Safety
- Energy Storage Projects and Implementation
  - Project Design, Delivery, Commissioning
  - Utility Partner Working Groups: Smart Inverters, M&C, ITWG
  - Grid Modernization Design and Implementation
- Power Systems Analysis
  - Arc Flash, EMTP-RV HEMP, Benchmarking Studies
- Risk Management
  - Aerial Inspection Programs, 500 kV Underground Transmission
  - Resiliency and Black Start
- Transmission Projects
  - Bulk Power System Project Contracting, Management and Controls
  - Project Execution and Delivery
- Standards Leadership
  - IEEE 1547, IEEE P2800, IEEE 2030.7, others



3

Today's Goals

Today's presentation is designed so that you have a better sense of the system-wide challenges facing standardization of cybersecurity for inverter-based resources (IBRs).

Topic items:

- **The Problem: Sample Use Cases Facing the Industry**
- **What Needs to be Secure?**
- **Cyber-Security Challenges: Architecture & Stakeholder Considerations**
- **Landscape of Cybersecurity Standards & Guidelines for IBRs**
- **Current State of Cybersecurity for IBRs**
- **Standardized Approach to Cybersecurity Implementation**
- **Standards Impacting Cybersecurity**
- **Takeaways**

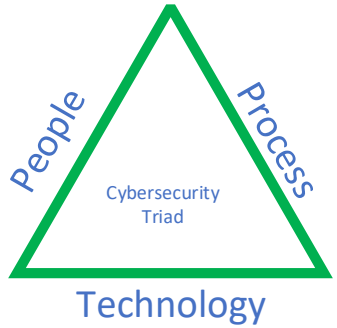
Sample Use Cases that Face the Industry & Challenge Security

1) **School district purchases 60 electric buses, each with a maximum demand of 200 KW. The utility circuit can only supply 10MW total for all loads, so wants to control charging schedule a day in advance. The system uses a mixture of a private, secure utility network as well as public networks to communicate.**

2) **The Independent System Operator (ISO) sends a public message to market participants to curtail solar generator production by 10% between 2 pm and 5 pm. An Aggregator of solar assets accepts the bid and communicates to their assets to reduce forward power. Communication is across public networks. The Aggregator is concerned about spoofing, because if the command signal is incorrect, the financial impact to the Aggregator could be severe.**

3) **Energy storage system (ESS) maintenance personnel are on site servicing an inverter that is part of a large ESS site and have connected their field laptops to the ESS local network, effectively giving them access to the utility SCADA network. Physical connections to the ESS network exists as well as providing updates to production software. This brings non-utility computers and hardware directly in contact with devices that are part of the utility SCADA network.**

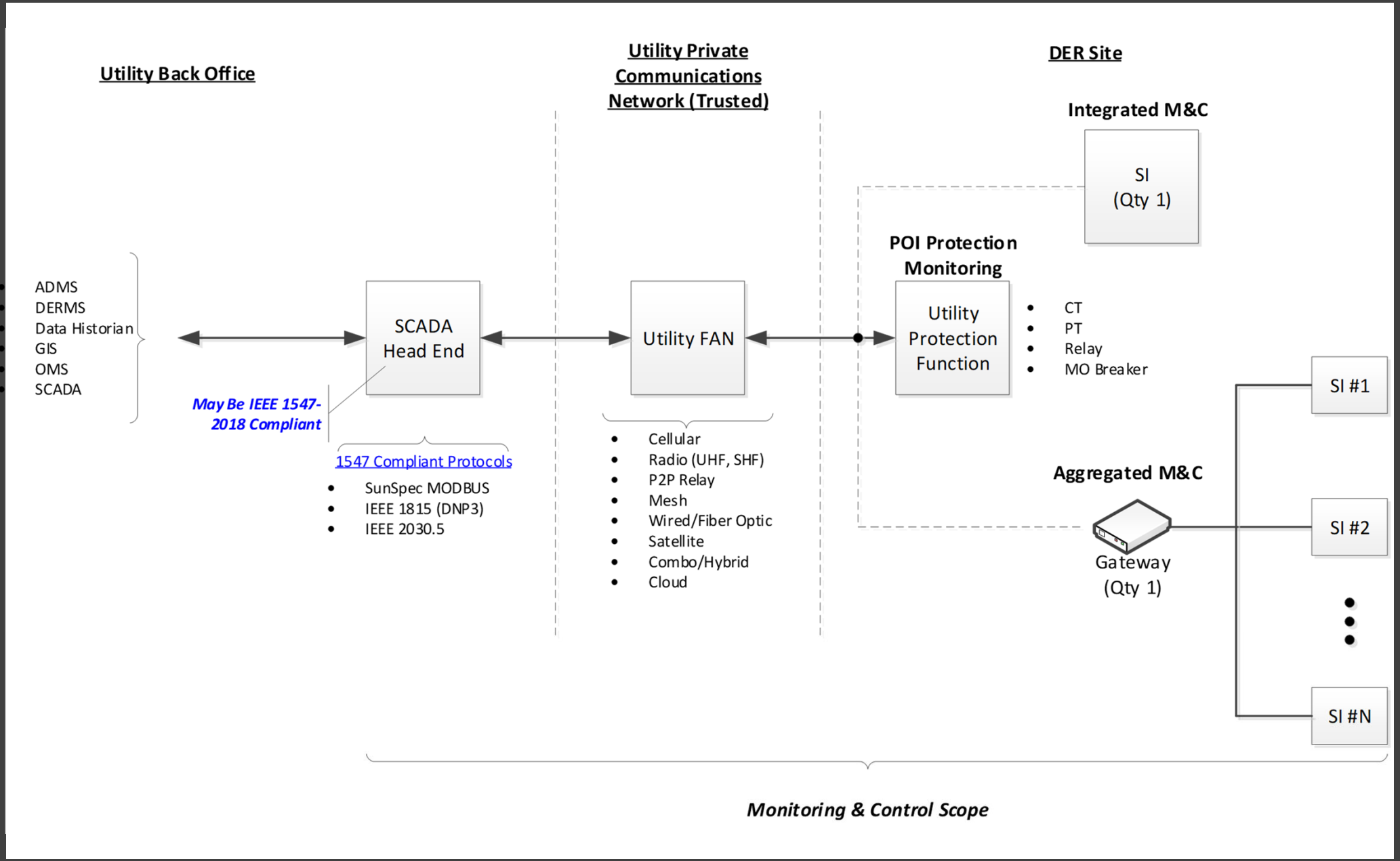
What Needs to be Secure?



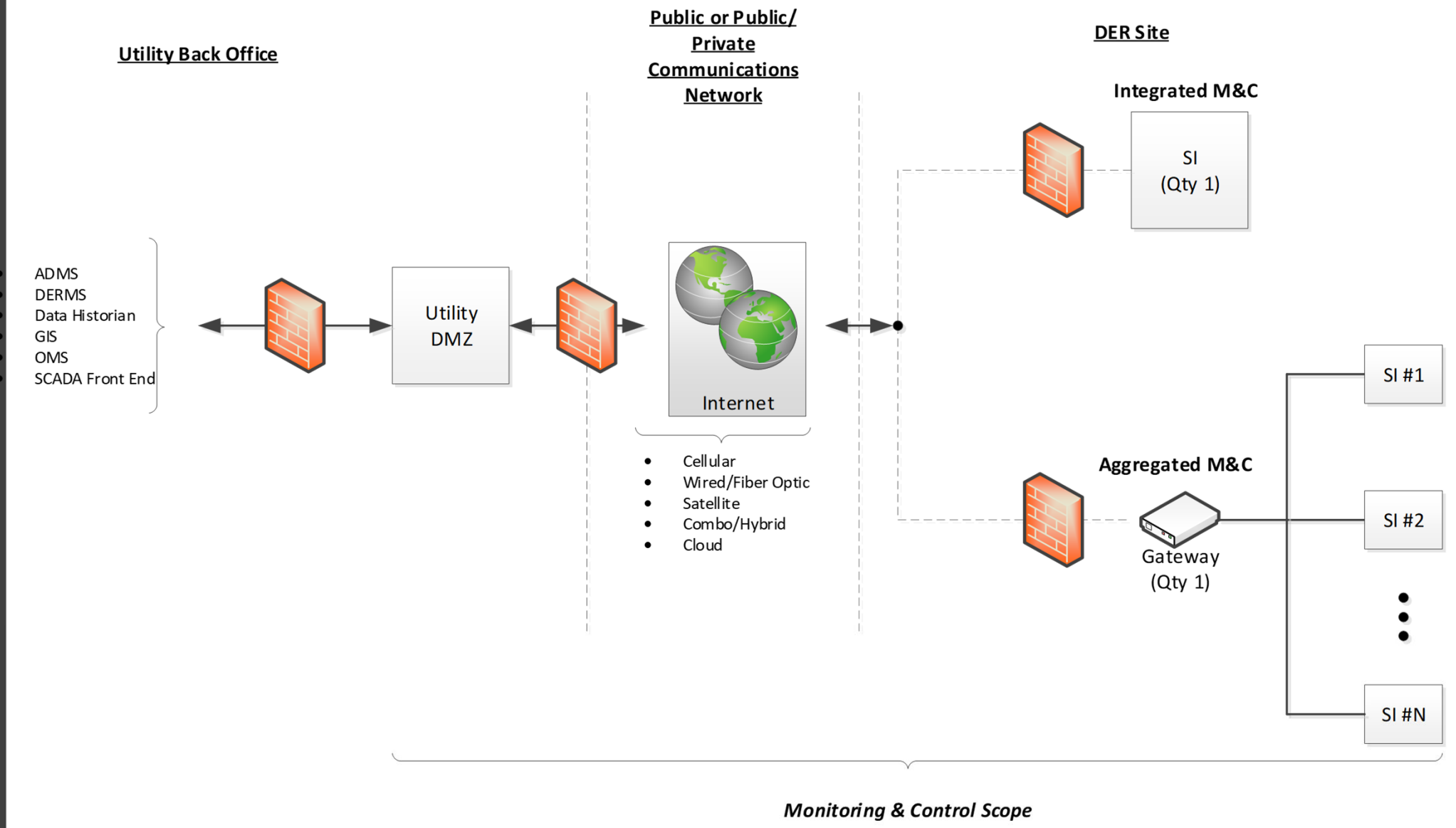
- **Hardware at the Site: Modems, Gateways, Switches, RTACs, Inverters**
- **Public networks carrying monitoring and control information used to stabilize power delivery**
- **Cloud infrastructures: AWS, Google, Azure, Comcast, Private (e.g., Fortinet, Cloudflare, Palo Alto, Nokia, etc.)**
- **Site Control / Dispatch Authority: These entities directly control power to/from sites**
- **Access by other stakeholders**

The attack surface is enormous and as more inverter-based resources are added, the surface and corresponding risk increases.

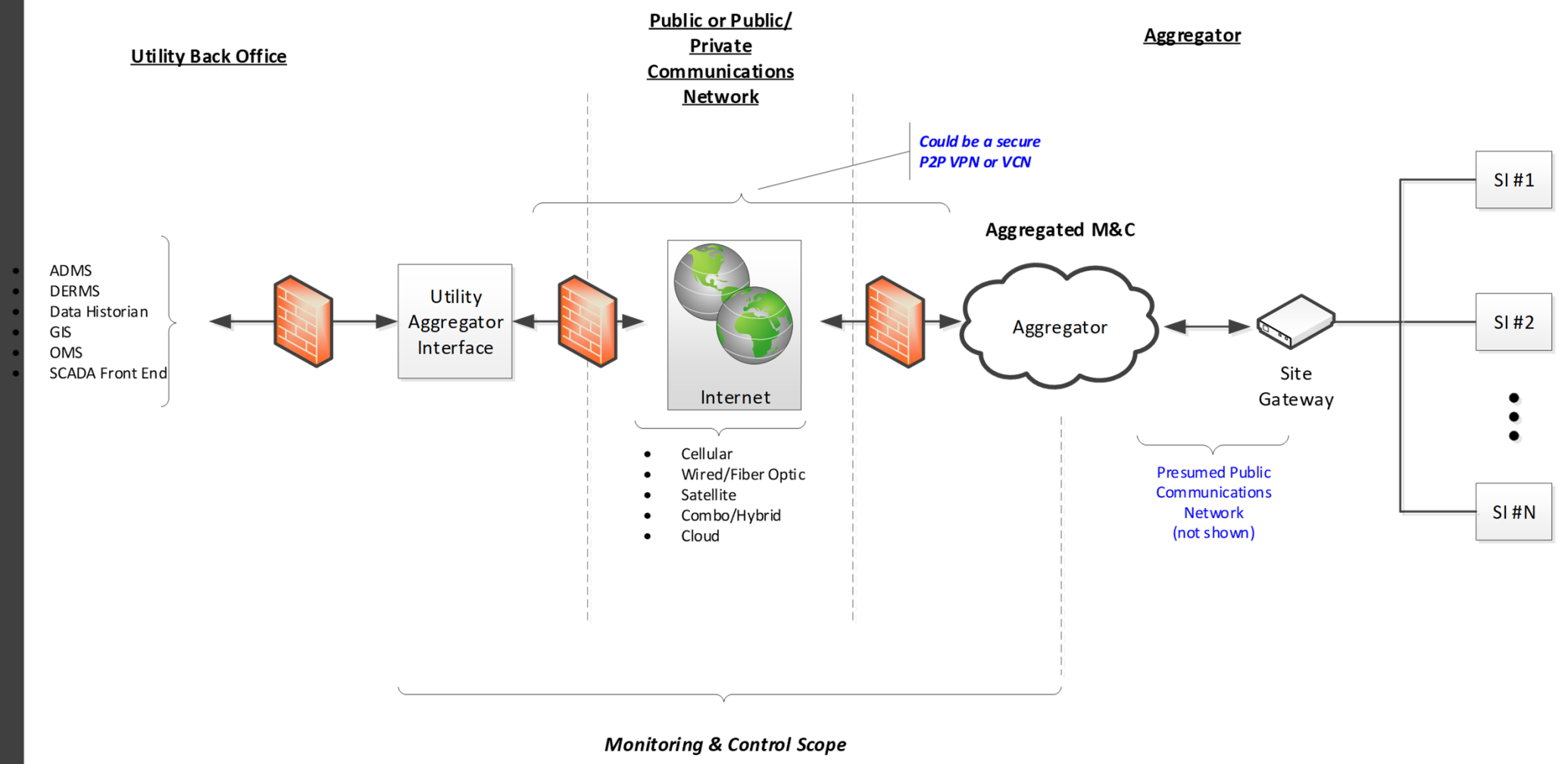
Cybersecurity Challenges: Utility-Centric Private Network



Cybersecurity Challenges: Joining Public/Private Networks

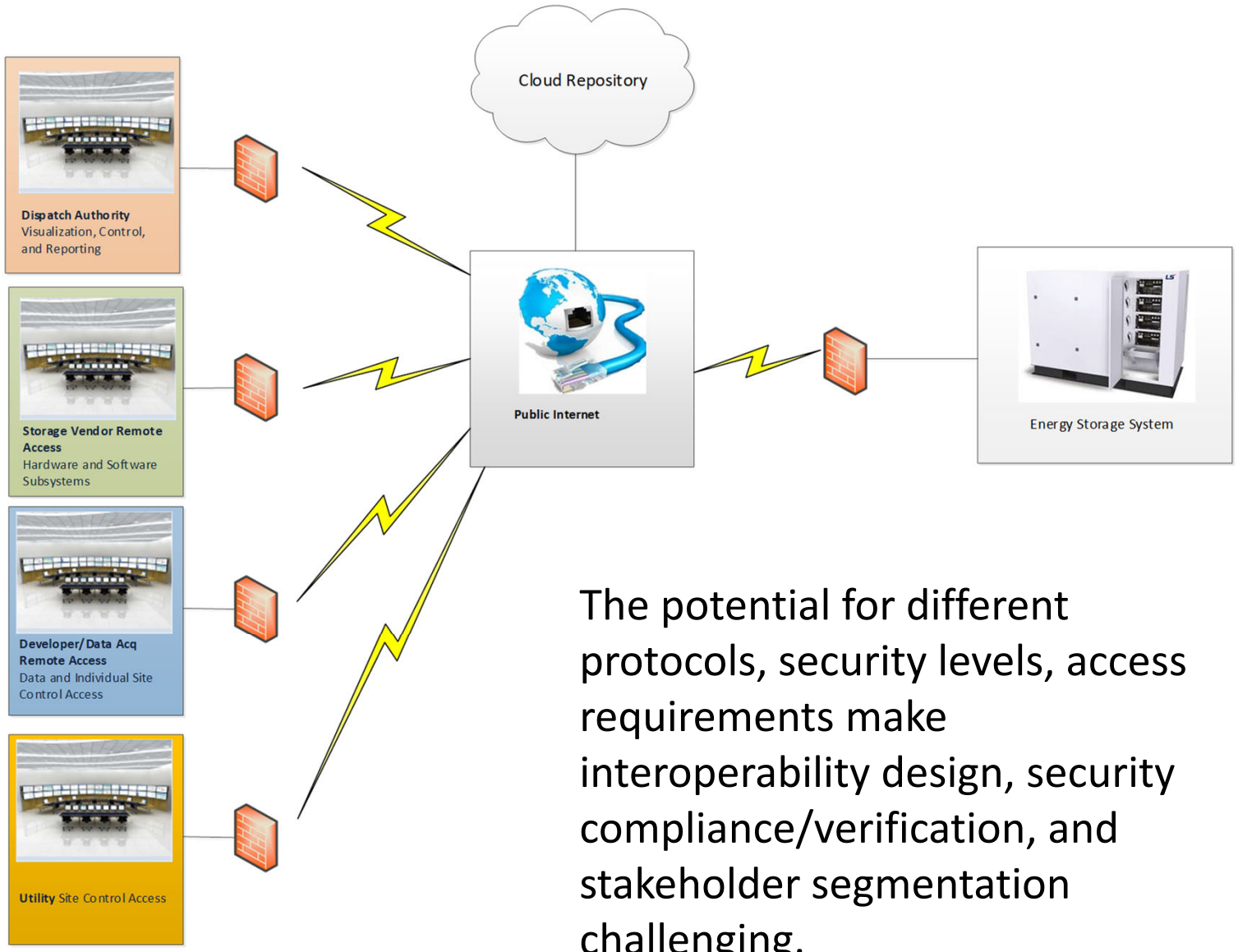


Cybersecurity Challenges: Aggregator-Centric Model



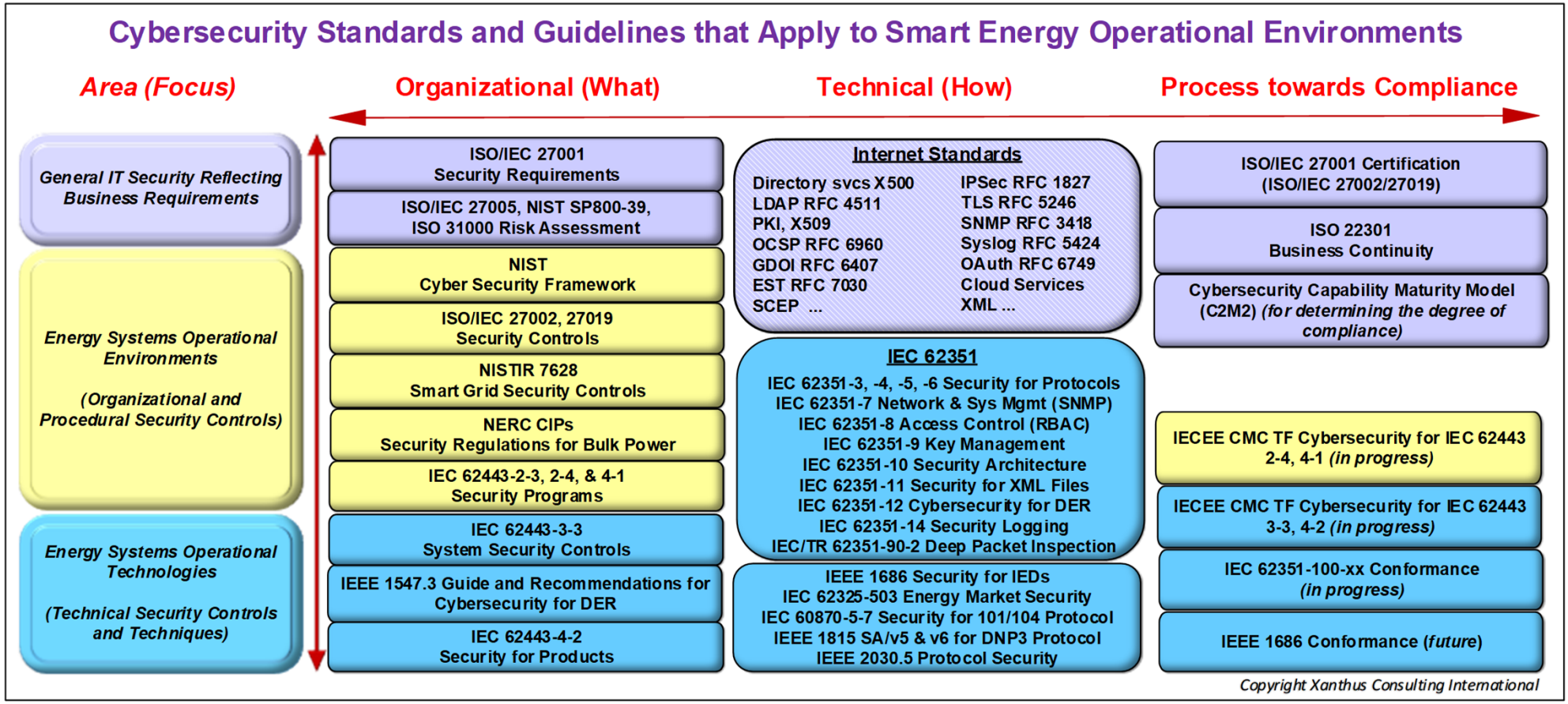
Cybersecurity Challenges: Disparate Stakeholders and Access

- Dispatch Authority (Control)
- Maintenance Vendor / Alarms
- Owner, Warrantee Compliance
- Utility SCADA Monitoring



The potential for different protocols, security levels, access requirements make interoperability design, security compliance/verification, and stakeholder segmentation challenging.

Landscape of Cybersecurity Standards & Guidelines for IBRs



Standards and guidelines exist but are complex to harmonize and implement within an organization, or across multiple organizations/stakeholders.

Current State of Cybersecurity for IBRs

Significant Thought Leadership on Best Practices

Implementation Standards & Guidance Underway

Complex Landscape of Standards & Guidance

Business / Financial Risk

Inability to Perform Consistent Risk Assessments

Poor Interoperability and Security at All Levels

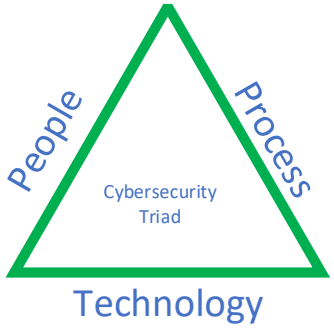
No "Approved" NRTL* Certification Path

**Nationally Recognized Testing Laboratory*

Standardized Approach to Cybersecurity Implementation

The NIST cybersecurity framework provides a structured approach to address cyber security requirements for independent stakeholder groups, and is finding wide adoption.

- ***Identify (cyber components)***
- ***Protect (limit, contain attack surface)***
- ***Detect (incident)***
- ***Respond (to cyber incident)***
- ***Recover (normal operations)***



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Standards Impacting Cybersecurity: IEEE 1547-2018

- **In 2018 there was an update to IEEE 1547, "Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces"**

- **This standard (IEEE 1547-2018) is being accepted as a mandatory requirement for interconnecting IBRs to the electric power system by distribution utilities, as it specifies both power-electronics performance as well as communication requirements:**
  - New York IOUs (January 2023)
  - Hawai'i Electric Company (February 2023)
  - California IOUs (expected mid-2023, final revisions ongoing)
  - Others (Maryland, Minnesota)

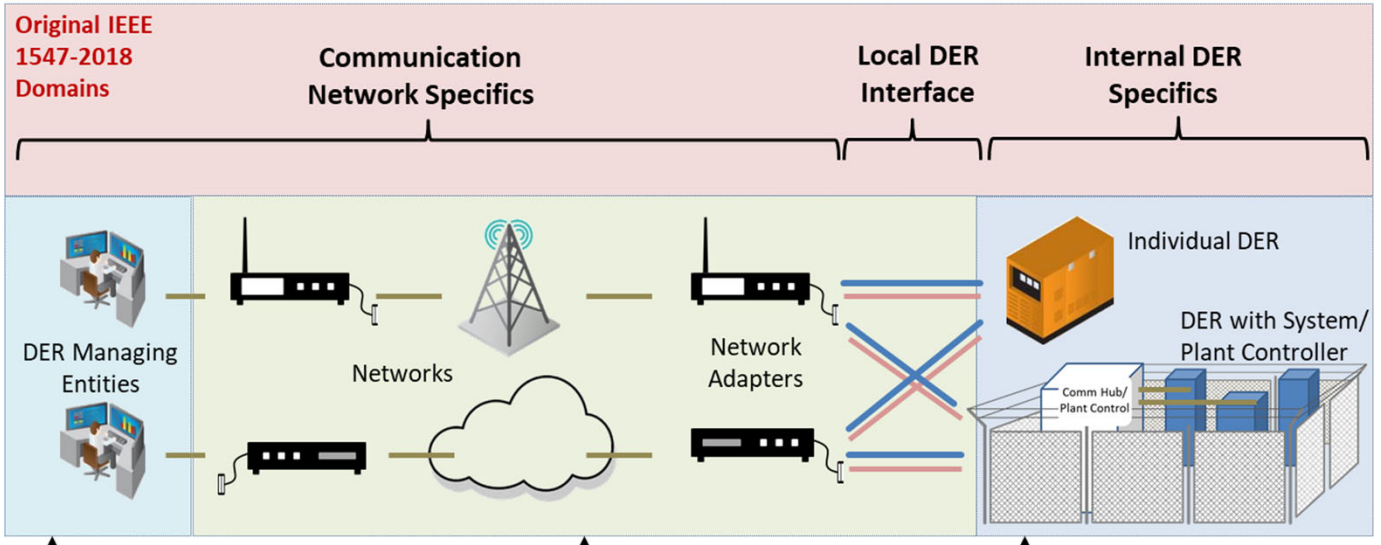
- **This standard mandates one of 3 protocols to be used with IBRs:**
  - IEEE 1815 (DNP 3)
  - IEEE 2030.5
  - Sunspec Modbus

- **Research, development, and implementation should focus on end-to-end protection of communication pathways connecting IBRs to user systems using these protocols.**

Standards Impacting Cybersecurity : IEEE P1547.3

- **This year (2023) will see the approval of IEEE P1547.3, "Guide for Cybersecurity of Distributed Energy Resources (DER) Interconnected with Electric Power Systems"**

- **Clause 5 of this standard specifies technical cybersecurity recommendations for DER operations, and changes depending on the location within the path:**



Area EPS Operator & Aggregator/Service Provider Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.4 Access Control
5.5.2 Security for Data-at-Rest
5.6 Security Management
5.7 Coping and Recovering

DER Communications Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.5.3 Security for Data in Transit
5.5.4 Comparison of DER Protocol Security (informational)
5.6.4 Patch Management

DER Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.4 Access Control
5.5.2 Security for Data-at-Rest
5.6 Security Management
5.7 Coping and Recovering

Takeaways

- IEEE 1547-2018 and IEEE P1547.3 (2023) are impactful and are targeted at interconnecting / communicating with IBRs that are connected to the area electric power system.

- As we add IBRs to our generating mix, the attack surface is growing, not shrinking. Tools (technologies), processes, and education are required to “keep the genie in the bottle”.

- There is no NRTL cybersecurity certification path for connected IBRs at the present time. The industry needs to focus on moving in this direction to reduce the attack surface across disparate devices as well as developing interoperable cybersecurity standardization that can be verified by 3rd parties.

Thank You!

Spencer Paul
MPR Associates, Inc.
(703) 519-0520
spaul@mpr.com

Paul Grems Duncan
MPR Associates, Inc.
(703) 519-0458
pduncan@mpr.com