SAND2021-2788PE

# Cybersecurity of Battery Energy Storage Systems

**Rodrigo D. Trevizan, PhD**

**Senior Member of Technical Staff**

**Sandia National Laboratories**

IEEE SMARTGRID

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.
SAND2021-XXXXX C

IEEE Advancing Technology for Humanity

# Outline

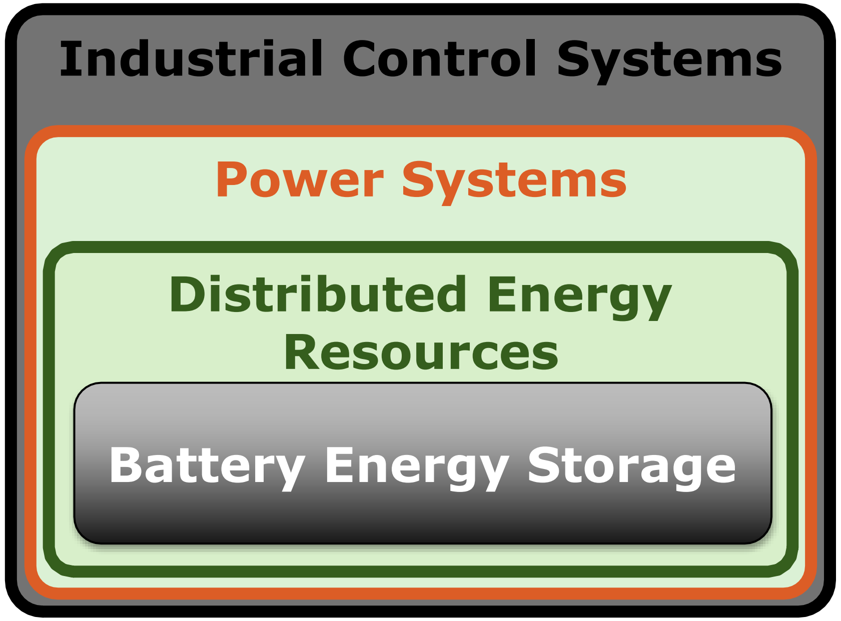
- Introduction
- Overview of BESS
- Risks Associated with BESS
- Standards and Best Practices
- Conclusion

# Introduction

- Increase in Battery Energy Storage Systems (BESSs)
- Seven U.S. states have mandates for storage capacity
- FERC Order 2222
- Lithium-ion batteries
  - Electric vehicles

# Introduction

- BESSs and other DERs
  - Similar scale
  - Power Conversion Systems (PCS)
  - Controllable
  - Distributed
- Other energy storage systems (ESS) share the similar characteristics



# Introduction

- Inherent risks of stored energy
- Need for specific equipment to perform those functions
  - Battery Management Systems
  - Fire Suppression
  - Networks
  - Permanent damage
- Communication with inverter and energy management

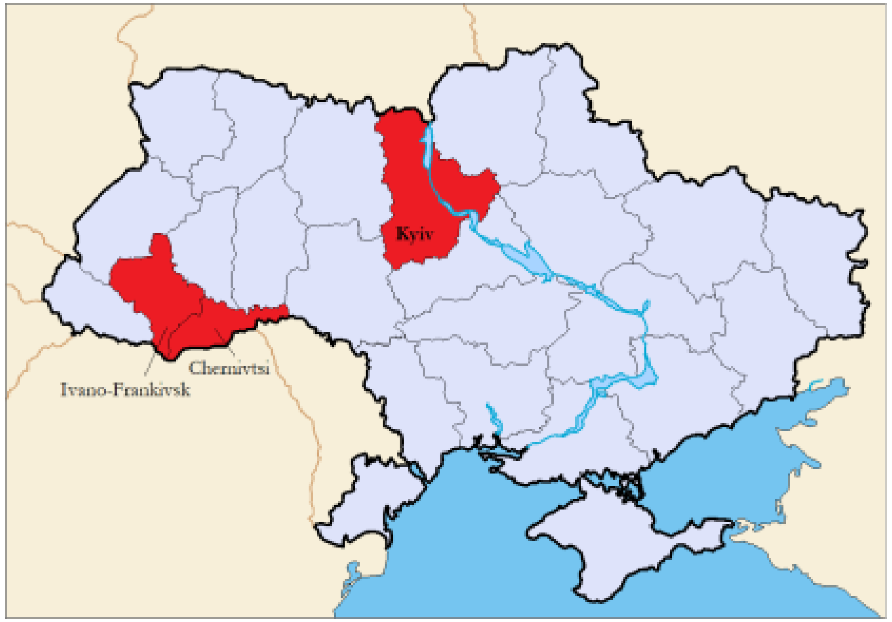
# Notable Cyberattacks

2010 – Natanz Uranium Enrichment Plant, Iran

- Stuxnet
  - Targeted Programmable Logic Controllers (PLCs)
- Attacked centrifuges used for Uranium enrichment

2015 – Ukraine

- Access through spear-phishing emails and malware in MS Office files
- Remotely disconnected 7 110kV and 23 35kV substations
- 1 to 6-hour outages affecting 225,000 customers
- Denial-of-service



Ukrainian *oblasts* affected during the 2015 cyberattack.

# Notable Cyberattacks

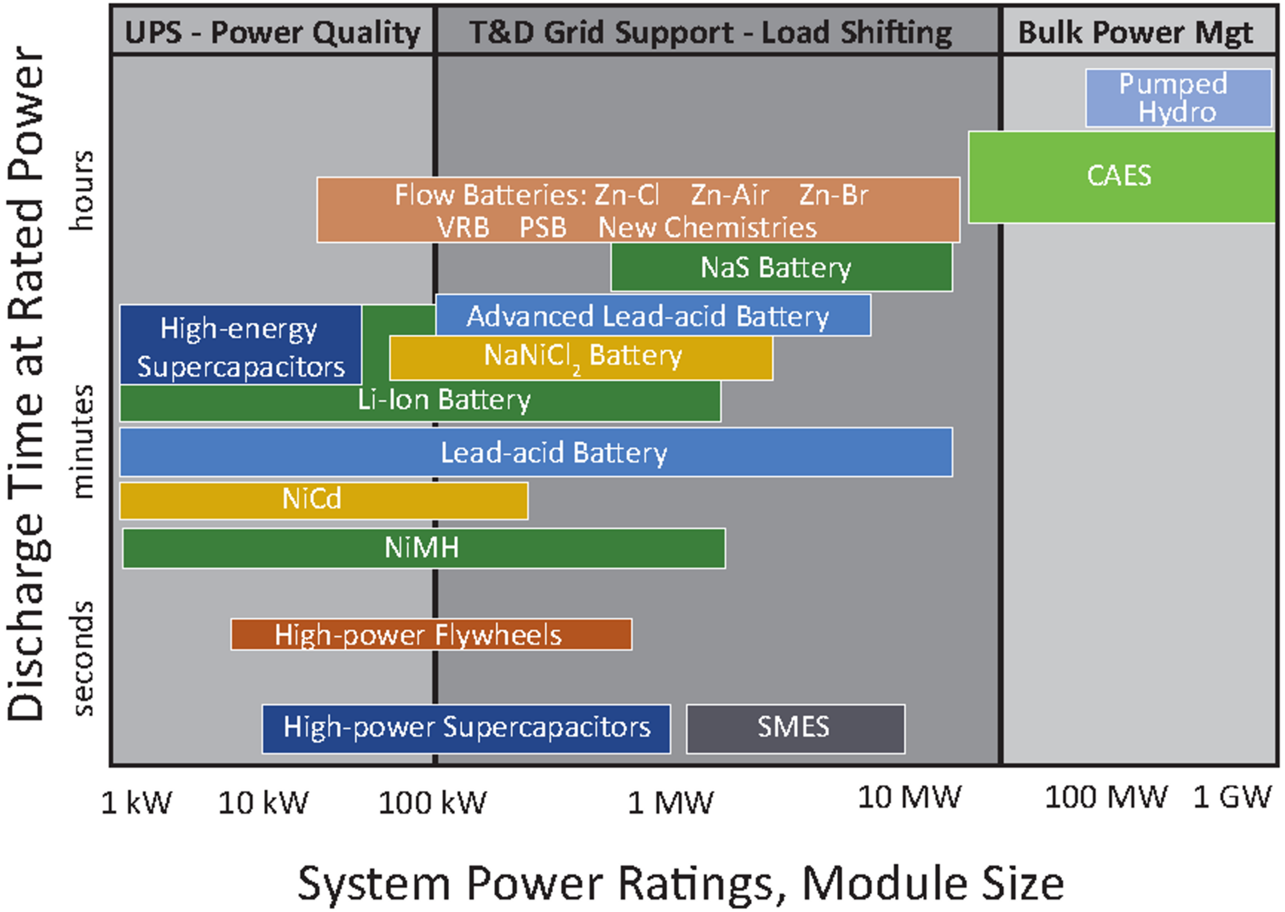
2016 – Ukraine
- Industroyer/Crashoverride malware framework
  - More sophisticated than 2015 attack but less successful
- Attack on transmission station led ro 1-hour outage in Kiev region
- Goal was to permanently damage grid equipment following switch to manual

2018 – Intrusion in control rooms of US power utilities
- Believed to be part of a reconnaissance operation

2019 – First Cyberattack on Wind and Solar in the US
- Denial-of-service
- Unpatched firewall vulnerability

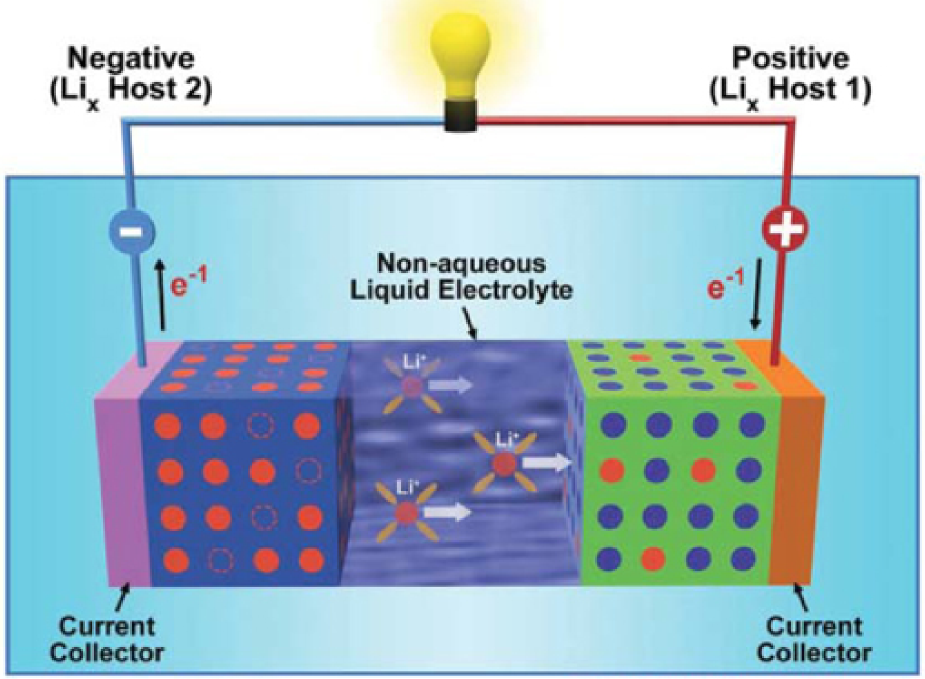
2019 – Ransomware attack on Natural Gas Pipeline in US
- Halted operations of a natural gas compression facility for 2 days
- Spear-phishing attack
- Attacker accessed Operational Technology network following Information Technology intrusion

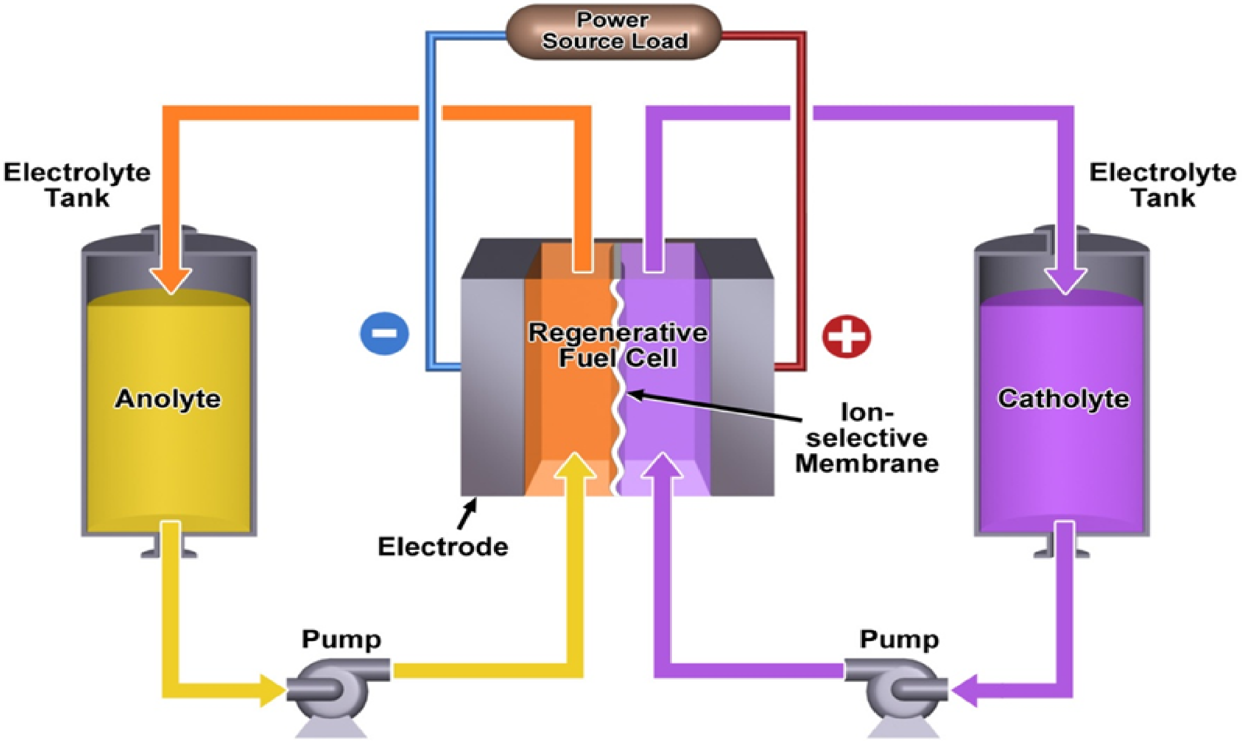
# Overview of BESS



Source: DOE/EPRI Electricity Storage Handbook in Collaboration with NRECA, 2013

# Overview of BESS



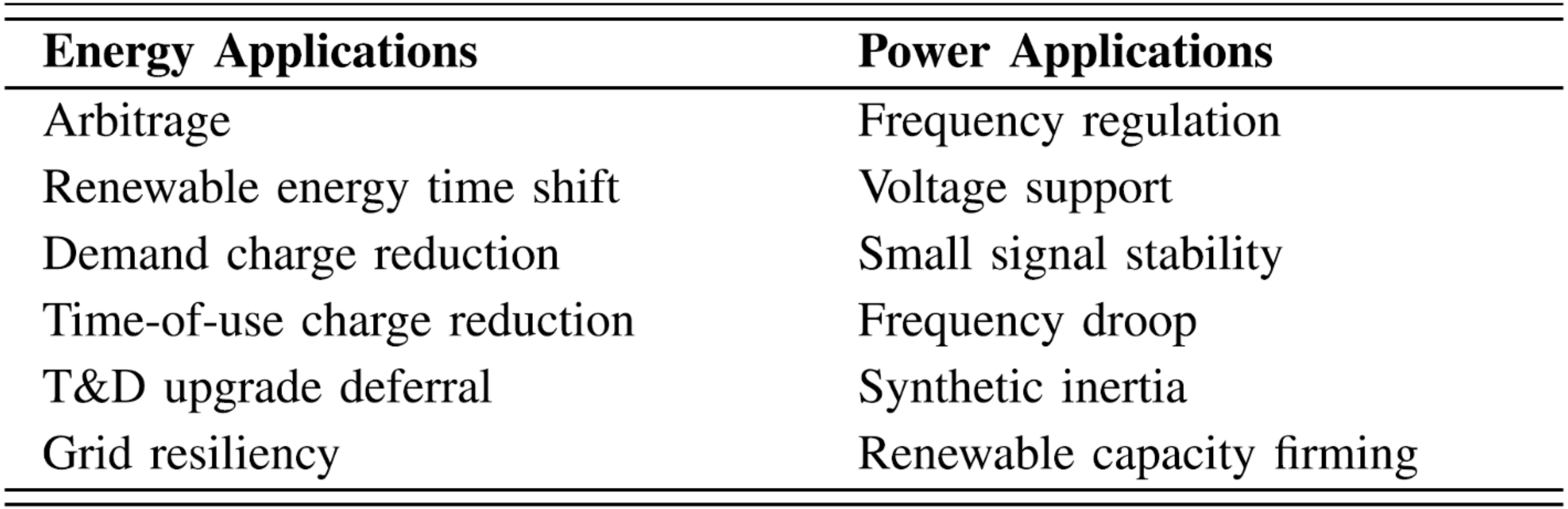


Anode: $Li_xC_6 \xrightarrow{discharge} xLi^+ + xe^- + C_6$

Cathode: $Li_{1-x}CoO_2 + xLi^+ + xe^- \xrightarrow{discharge} LiCoO_2$

*Source: Z. Yang JOM September 2010, Volume 62, Issue 9, pp 14-23*

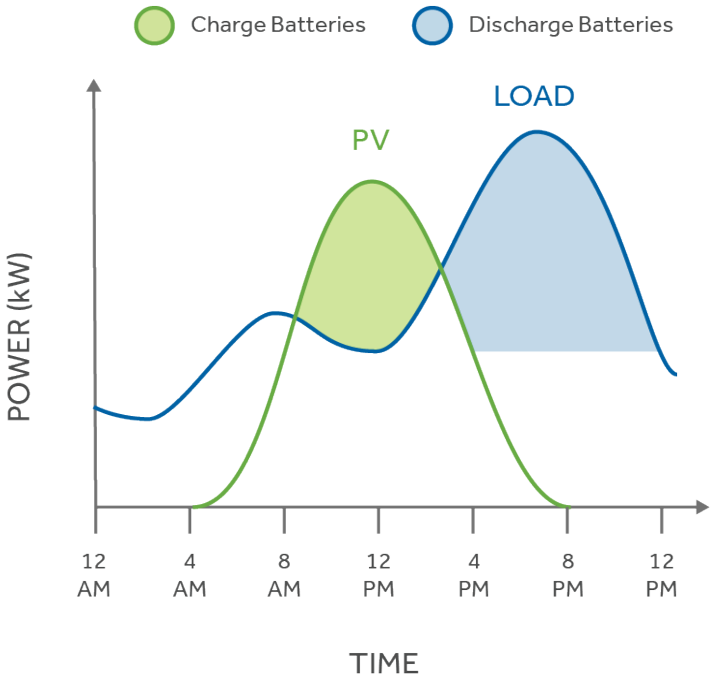
# Overview of BESS



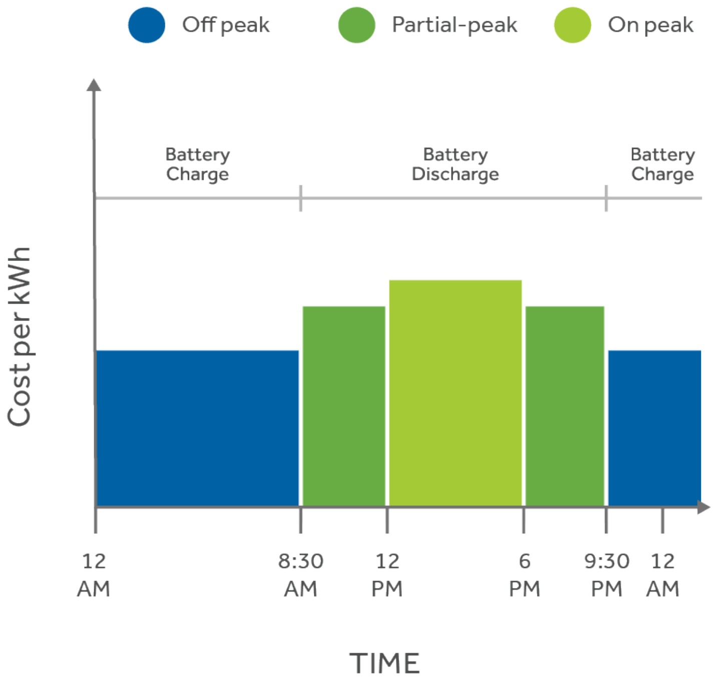
| Energy Applications | Power Applications |
|---|---|
| Arbitrage | Frequency regulation |
| Renewable energy time shift | Voltage support |
| Demand charge reduction | Small signal stability |
| Time-of-use charge reduction | Frequency droop |
| T&D upgrade deferral | Synthetic inertia |
| Grid resiliency | Renewable capacity firming |

Source: R. H. Byrne, T. A. Nguyen, D. A. Copp, B. R. Chalamala, and I. Gyuk, “Energy management and optimization methods for grid energy storage systems,” IEEE Access, vol. 6, pp. 13 231–13 260, 2018.

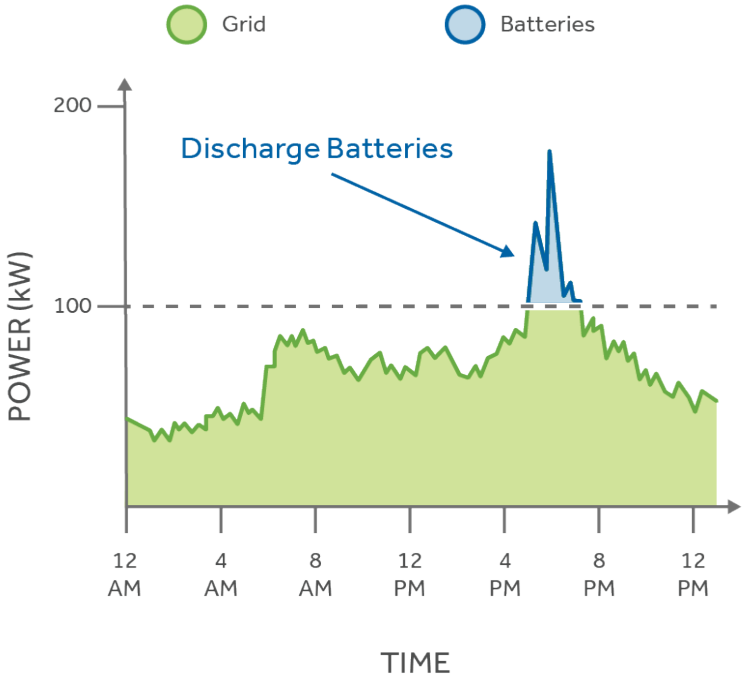
# Overview of BESS



**Renewable Time Shift**



**Time-of-use Management**



**Demand Charge Reduction**

Source: T. Nguyen, R. Byrne, “QuESt: An Energy Storage Application Suite,” SAND2019-13567 PE

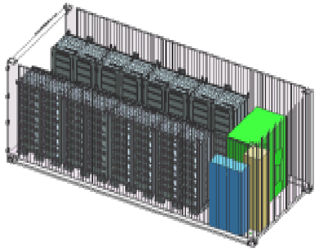
# BESS Overview

Storage

••Cell

••Battery Management & Protection

••Racking



Integration

••Container / Housing

••Wiring

••Climate control

PCS

••Bi-directional Inverter

••Switchgear

••Transformer

••Skid

EMS

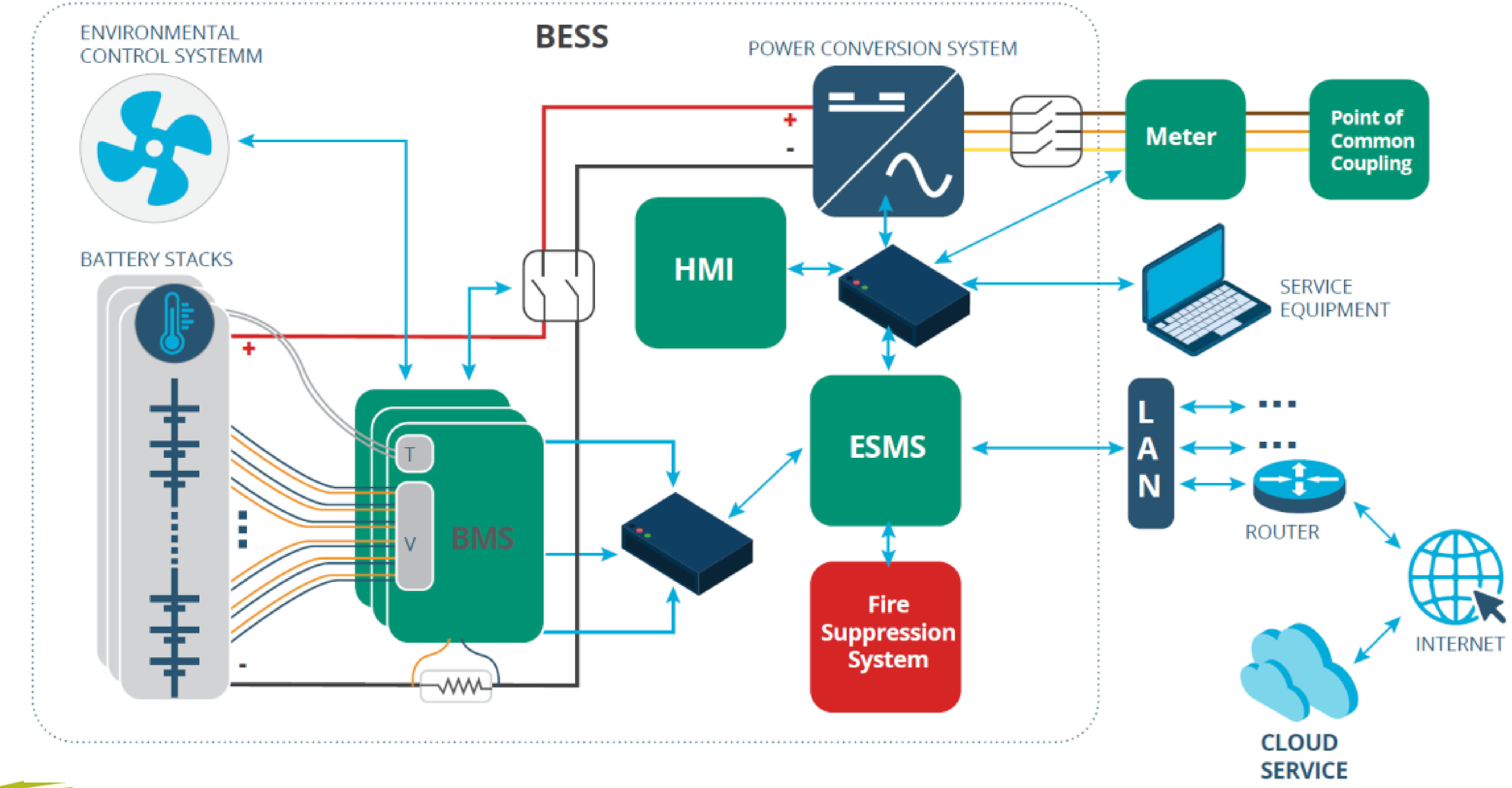
••Charge / Discharge

••Load Management

••Ramp rate control

••Grid Stability

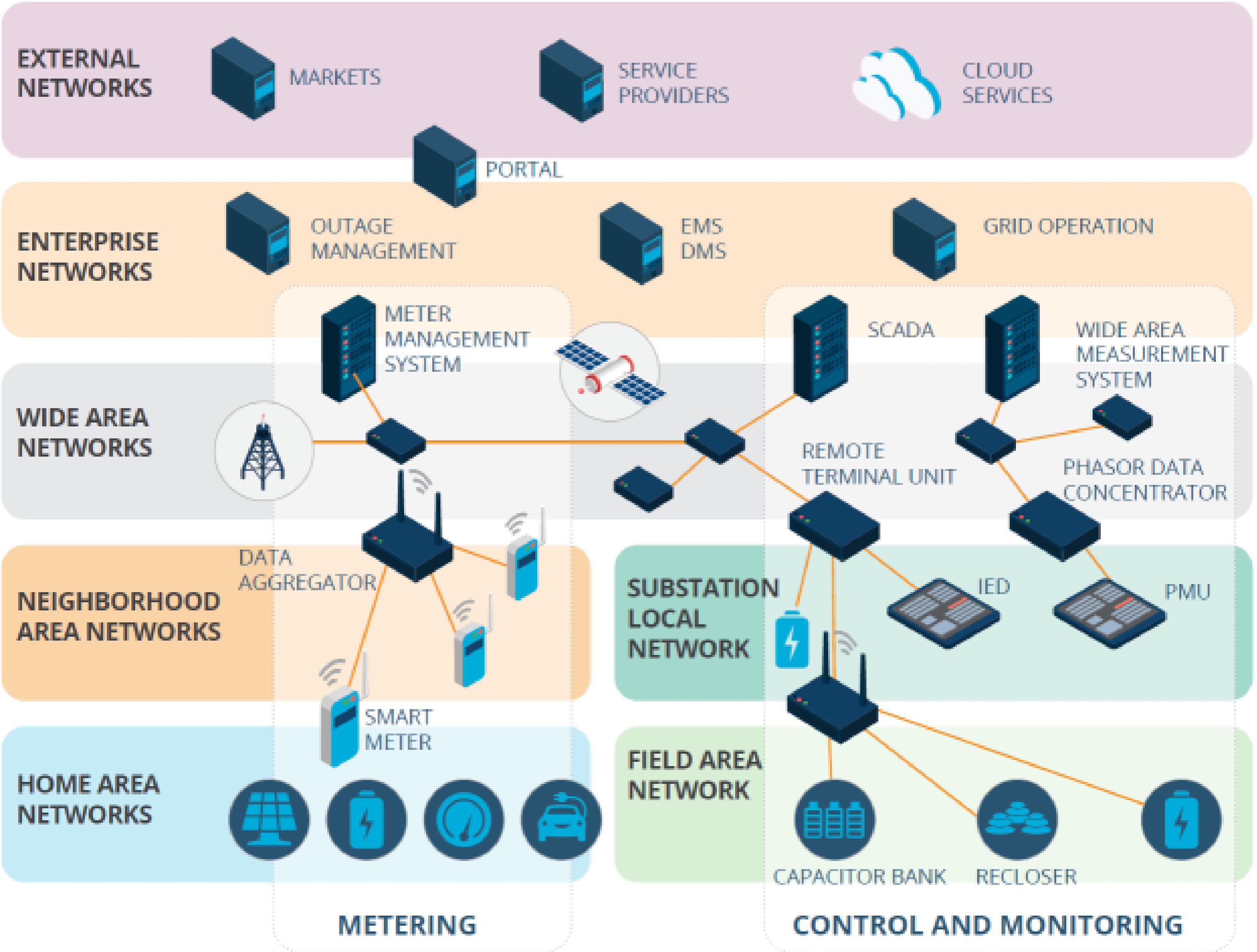
# Overview of BESS



IEEE SMARTGRID

IEEE Advancing Technology for Humanity

# Overview of BESS



Adapted from.: E. Hossain, Z. Han, H. V. Poor, Smart Grid Communications and Networking, Cambridge University Press, 2012.

# Overview of BESS

Rely on external communications for control and monitoring

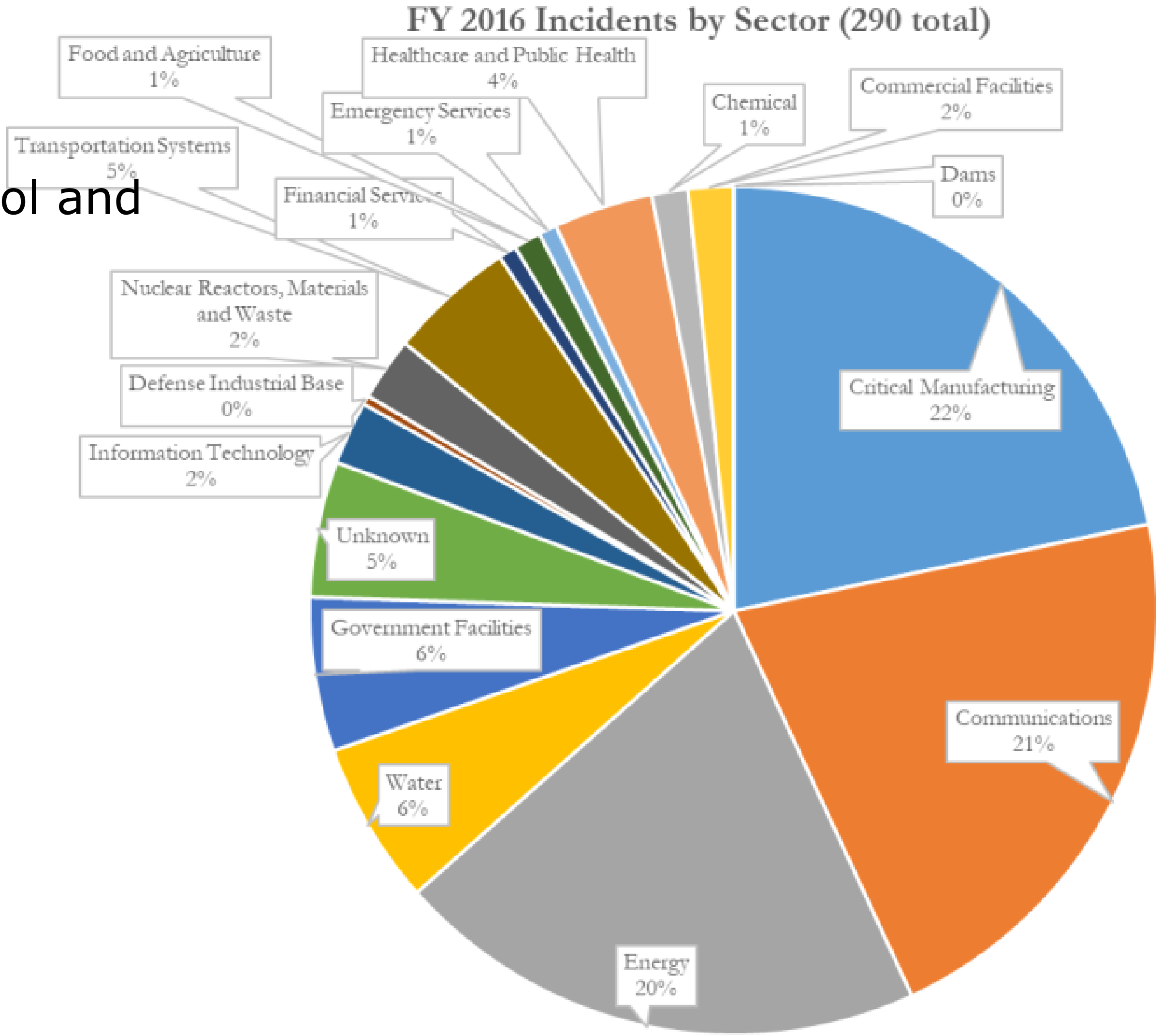
Many outward facing systems

- Portals
- Cloud services
- Human Machine Interfaces (HMIs)

Critical infrastructure

Cybersecurity-related standards?

- NIST
- NERC
- IEEE
- ISA
- IEC
- …



Source: ICS-CERT Year in Review 2016 Incident Response Pie Charts

# Risks: Gas and Fire

- Probabilities of failure of one cell is very low
  - Utility-scale BESS – hundreds/thousands of cells
- Defects

Consumer Cells (0.5-5 Ah)

Large Format Cells (10-200 Ah)

Transportation Batteries (1-50 kWh)

Utility Batteries (MWh)

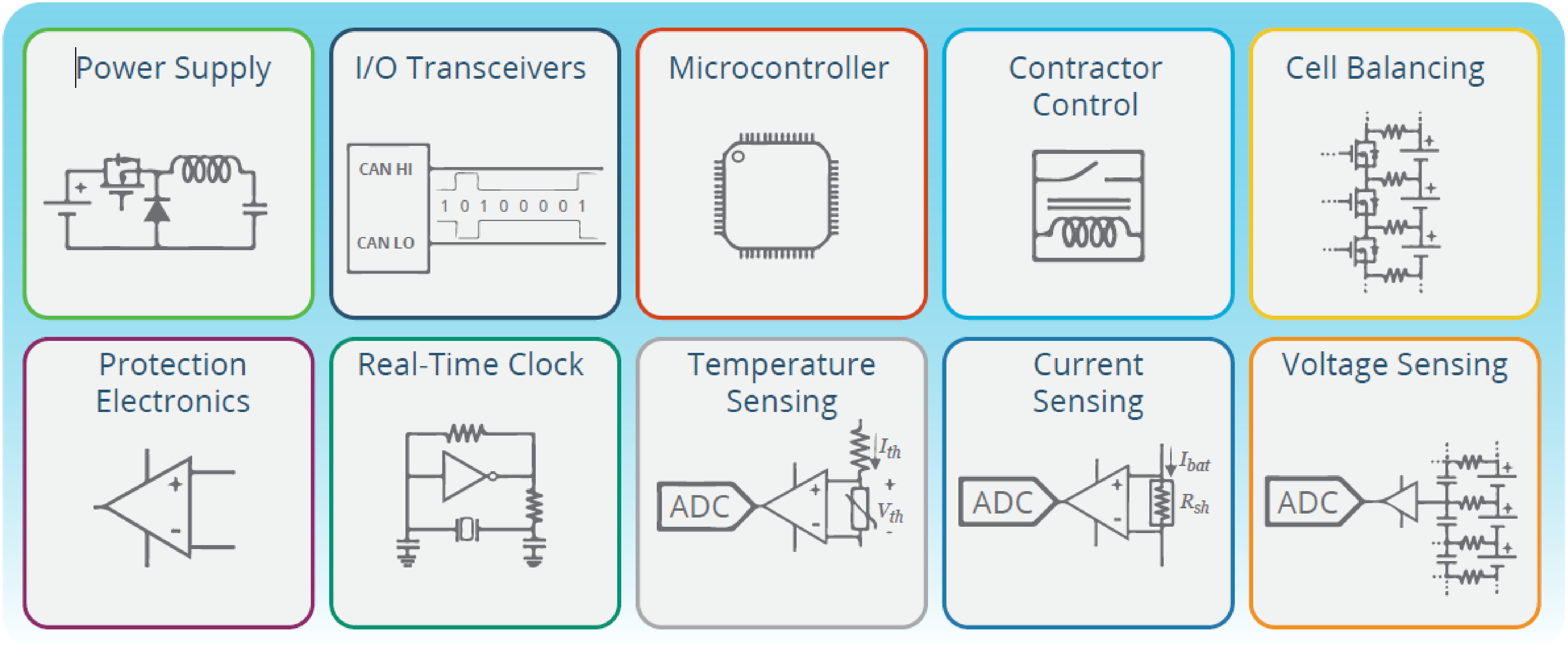
www.ford.com www.samsung.com www.saftbatteries.com

# Risks: Gas and Fire

- Off-gassing
  - Toxic, flammable
- Fire
  - Smoke
- Thermal runaway
- Smoke/gas detectors
- Fire suppressants

Source: M. B. McKinnon, S. DeCrane, and S. Kerber, “Four Firefighters Injured In Lithium-Ion Battery Energy Storage System Explosion - Arizona,” UL Firefighter Safety Research Institute, 2020.

# Battery Management Systems



Power Supply

I/O Transceivers

Microcontroller

Contractor Control

Cell Balancing

Protection Electronics

Real-Time Clock

Temperature Sensing

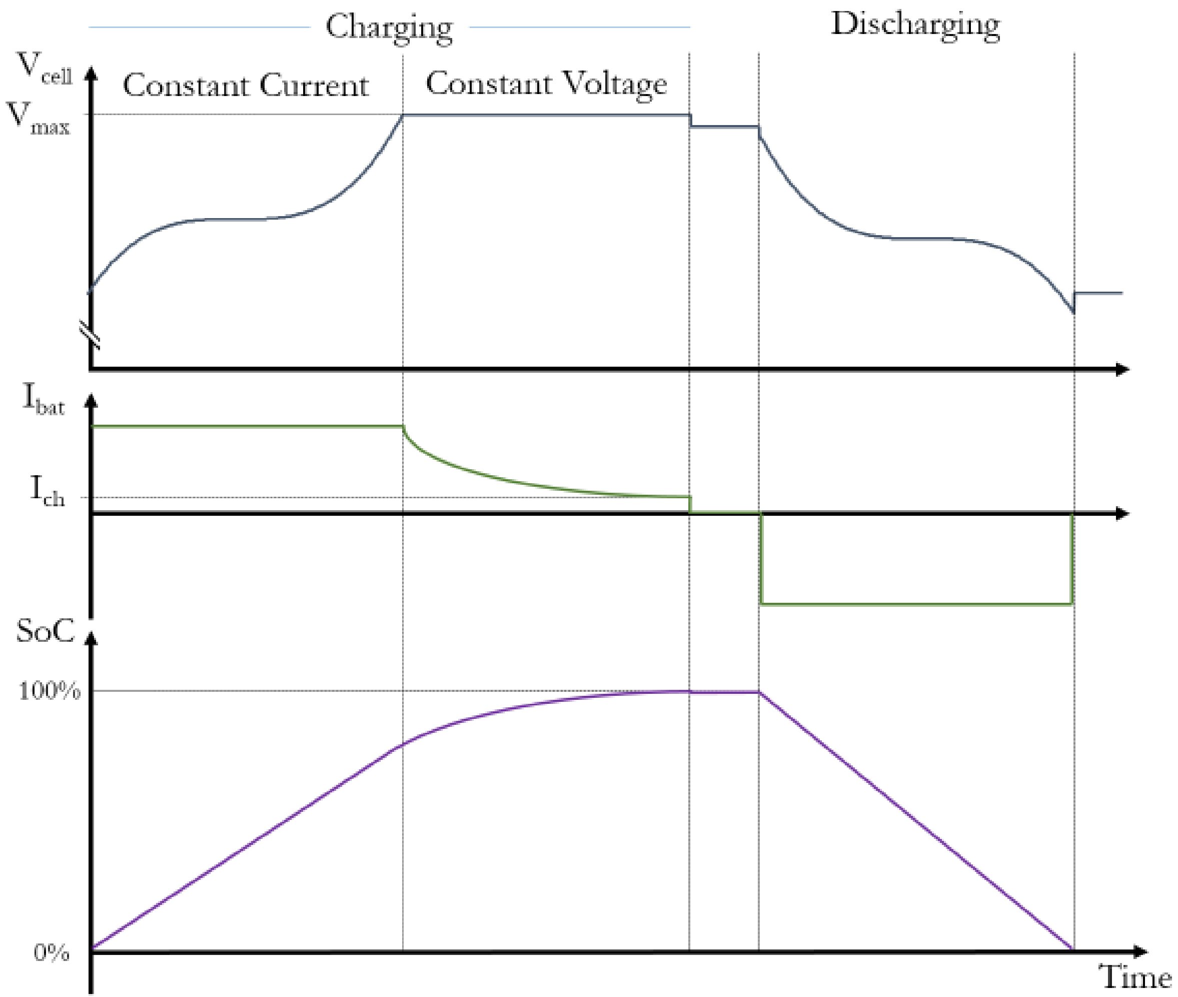
Current Sensing

Voltage Sensing

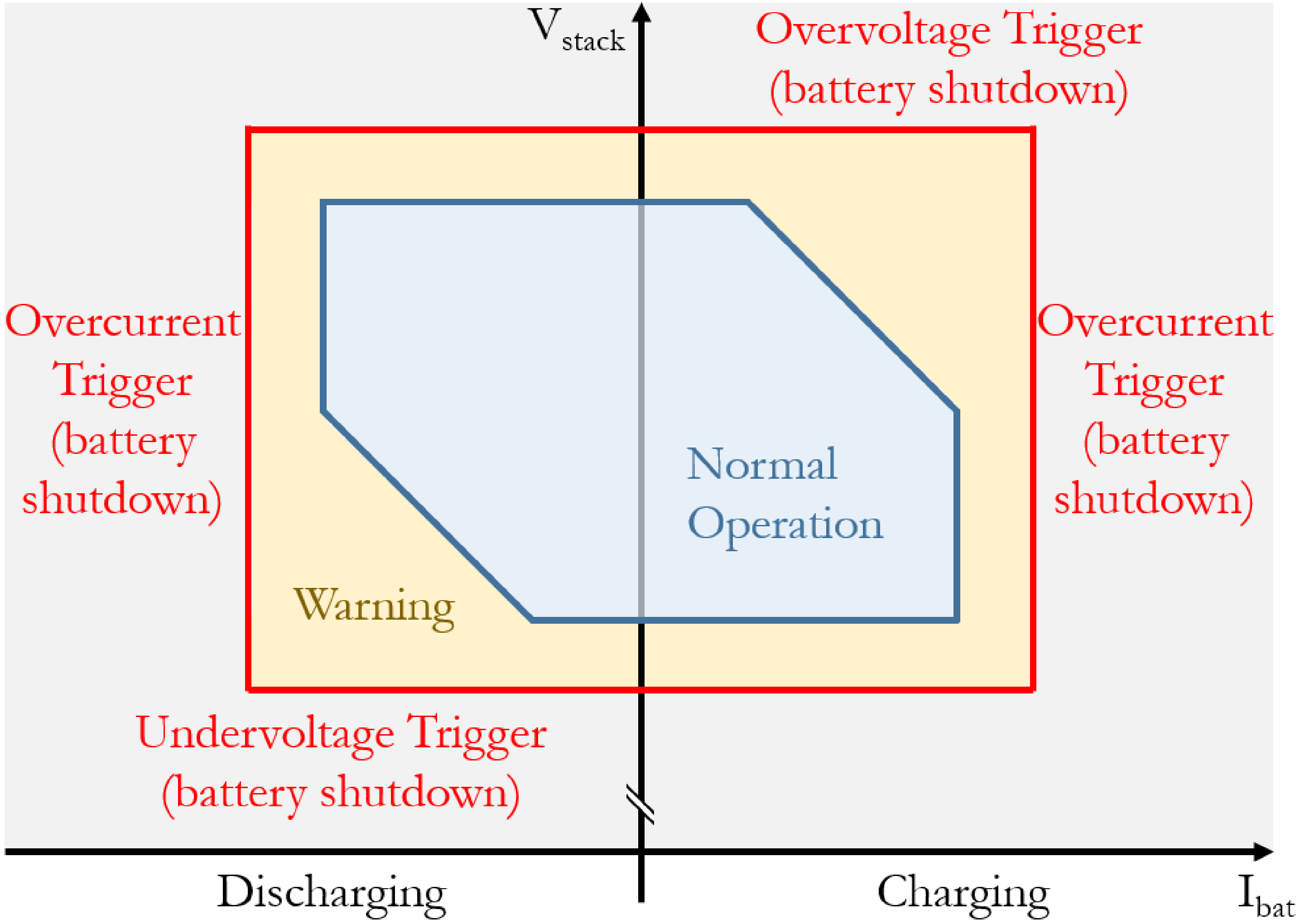
Adapted from.: A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. Al Faruque, "A security perspective on battery systems of the internet of things," Journal of Hardware and Systems Security, vol. 1, no. 2, pp. 188–199, Jun 2017. [Online]. Available: https://doi.org/10.1007/s41635-017-0007-0

# Battery Management Systems

- Charge/discharge
- State-of-charge
- State-of-health
  - Degradation
  - Capacity fade
  - Power fade



# Battery Management Systems



# Cybersecurity Risks

- Complexity and maintenance
  - Vendor might have to bypass network security
  - Credentials
- Connectivity to the internet
  - Advanced analytics/preventative maintenance
- Poor observability into ICS network
- Consumer owned

# Effects of Compromised BMS

- Violations of operational constraints
  - Overcharge
  - Overdischarge
  - Temperature derating
  - Accelerated degradation
  - Failure/damage

# Effects of Compromised BMS

- Battery Depletion (Denial-of-Service)
  - In mobile devices: "sleep deprivation torture‟ attack
  - Many BMS are powered by an auxiliary power source
  - Potentially undetected: placement of current sensors
  - Passive cell balancing circuits

# BESS vs other DER

Physical security:

- Facilities are often unmanned
- Minimal physical security
- Outsider threat actors will have time to carry out their action

Safety:

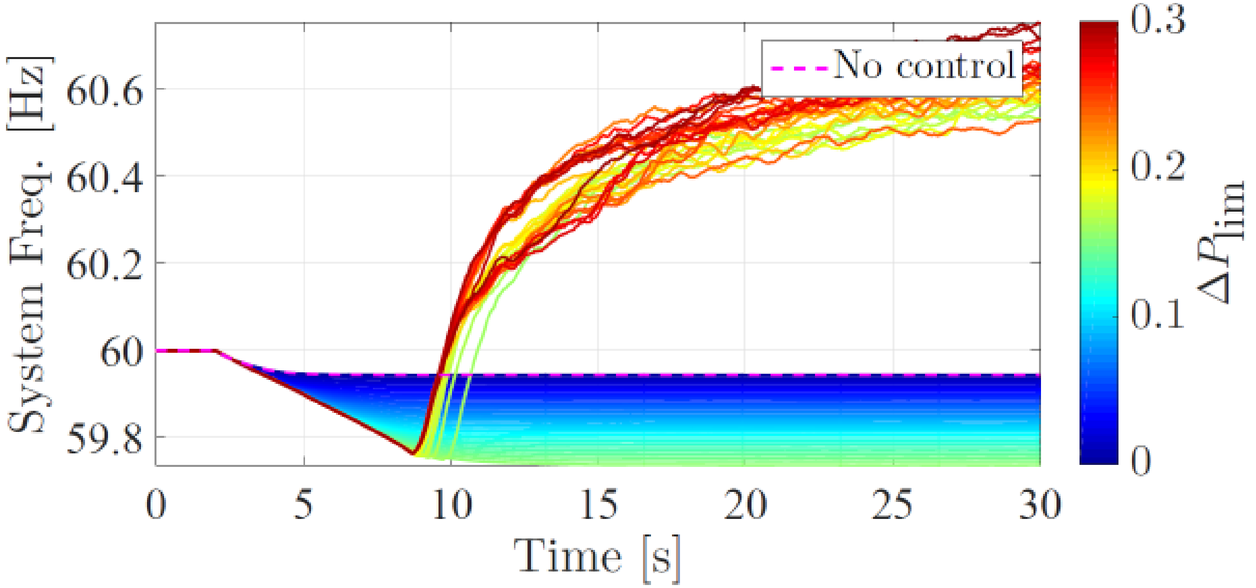
- Stored energy has inherent risks
- Batteries – gassing, fire, toxic chemicals
- Dams, compressed air, flywheels…
- Safety risks are mitigated with electronics

Cybersecurity:

- Disable protection mechanisms
- Cause damage or malfunction of BESS
- Induce power grid instability – (Centralized or DER)
- Modify readings to harm awareness

# Effects of Compromised BESS Controls

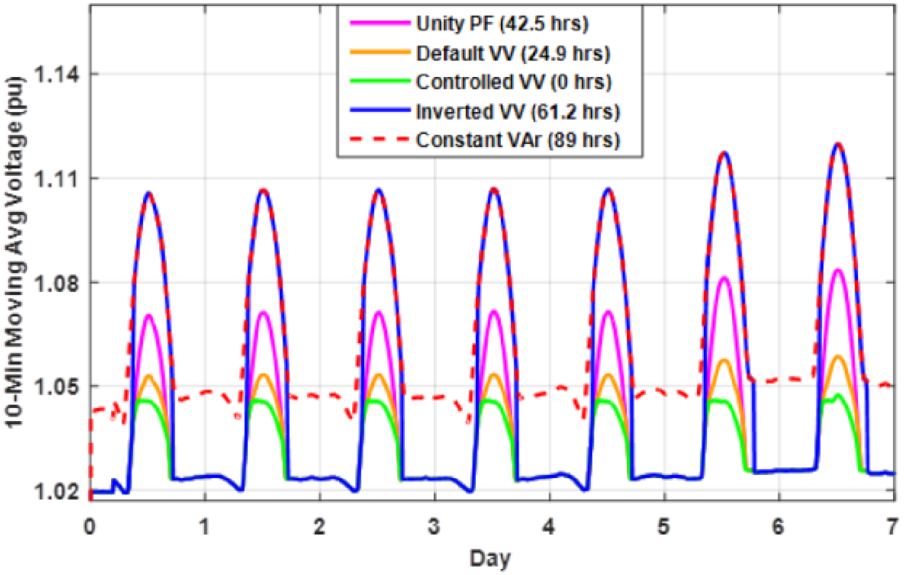
- Ineffective/harmful control operation
  - Frequency response

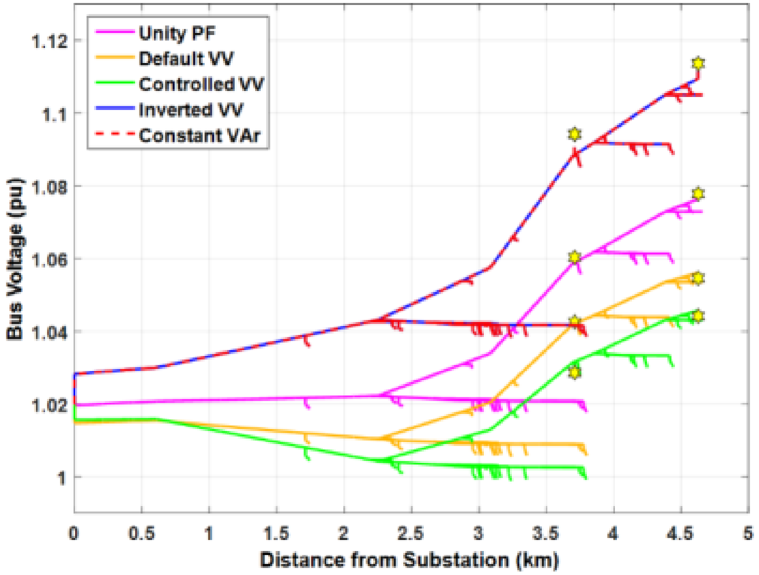


F. Wilches-Bernal, R. Concepcion, J. Johnson and R. H. Byrne, "Potential Impacts of Misconfiguration of Inverter-Based Frequency Control," 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, 2018, pp. 1-5, doi: 10.1109/PESGM.2018.8586272.

# Effects of Compromised BESS Controls

- Ineffective/harmful control operation
  - Voltage control in distribution systems

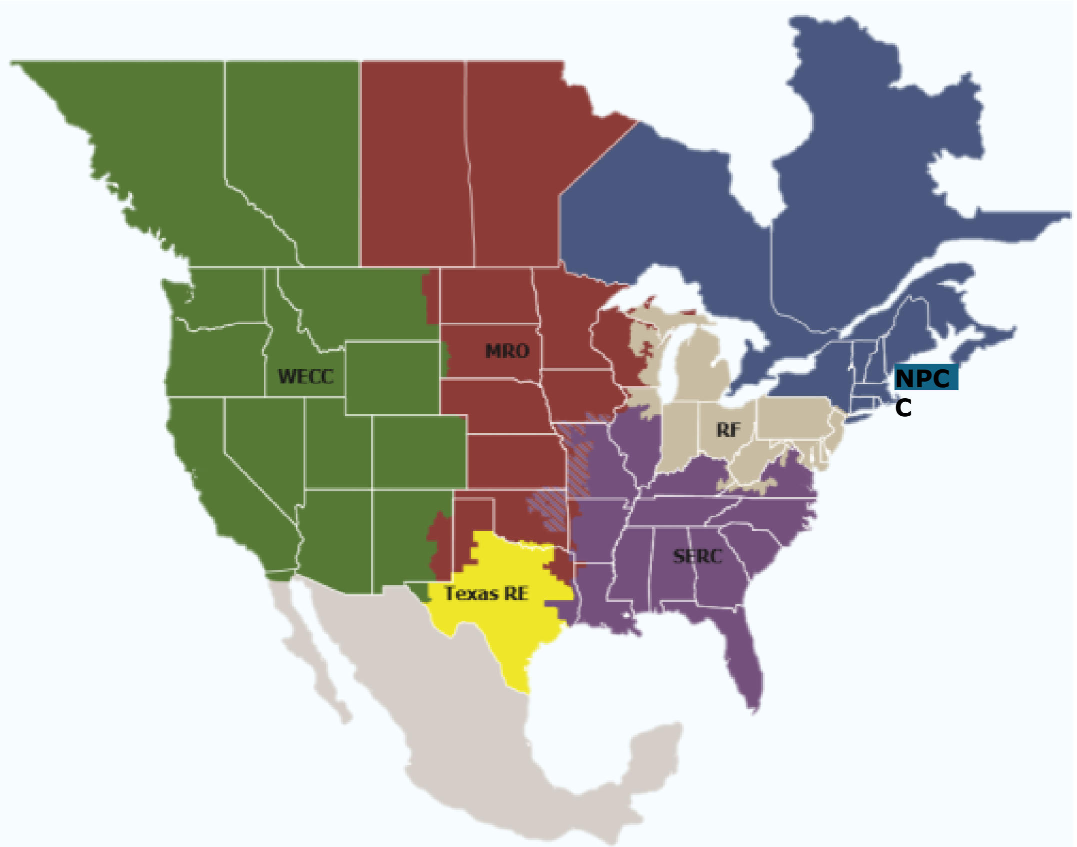




Johnson, Jay; Quiroz, Jimmy; Concepcion, Ricky; Wilches-Bernal, Felipe; Reno, Matthew J.: 'Power system effects and mitigation recommendations for DER cyberattacks', IET Cyber-Physical Systems: Theory &amp; Applications, 2019, 4, (3), p. 240-249.

# NERC CIP

- **N**orth American **E**nergy **R**eliability **C**orporation **C**ritical **I**nfrastructure **P**rotection
- NERC works with the industry to develop standards
- FERC approves the standards
  - Penalty Structure
  - Audit Cycles



# NERC CIP

- Energy Storage is an inverter-based resource
- Identify and protect cyber assets used to operate the Bulk Electric System (BES) critical infrastructure
  - Might apply to ESS, since it applies to:
  - "[…] Transmission Elements operated at 100 kV or higher […]"

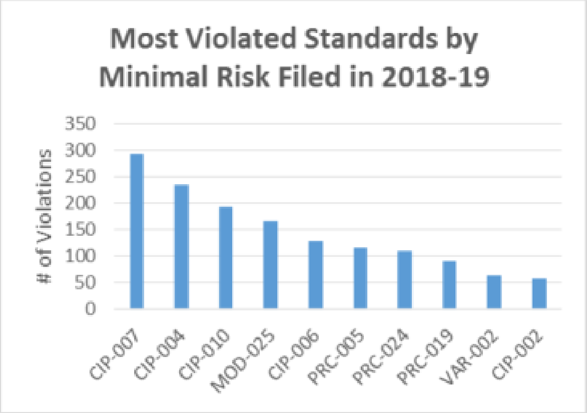
# NERC CIP

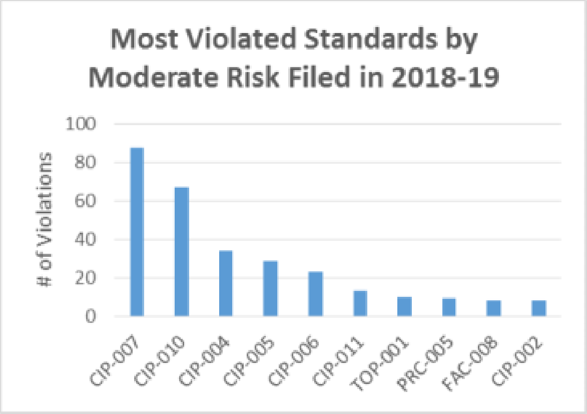
- Generating resources
  - gross individual nameplate greater than 20 MVA OR gross aggregate nameplate greater than 75 MVA
- Dispersed power producing resources
  - Aggregate capacity greater than 75 MVA

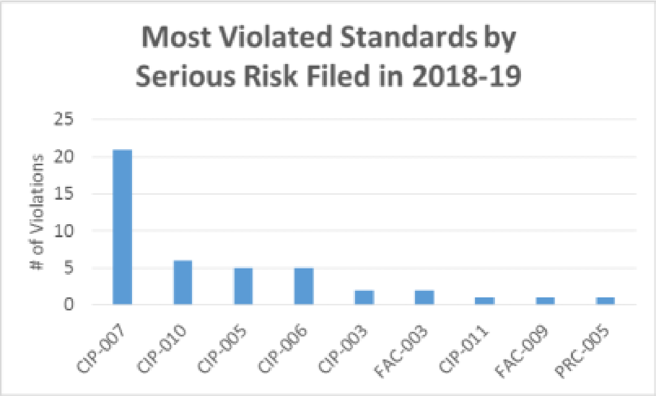
# NERC CIP

- **Standards Subject to Enforcement**

| | |
|---|---|
| CIP-002-5.1a | Cyber Security — BES Cyber System Categorization |
| CIP-003-8 | Cyber Security — Security Management Controls |
| CIP-004-6 | Cyber Security - Personnel & Training |
| CIP-005-5 | Cyber Security - Electronic Security Perimeter(s) |
| CIP-006-6 | Cyber Security - Physical Security of BES Cyber Systems |
| **CIP-007-6** | **Cyber Security - System Security Management** |
| CIP-008-5 | Cyber Security - Incident Reporting and Response Planning |
| CIP-009-6 | Cyber Security - Recovery Plans for BES Cyber Systems |
| CIP-010-2 | Cyber Security - Configuration Change Management and Vulnerability Assessments |
| CIP-011-2 | Cyber Security - Information Protection |
| CIP-014-2 | Physical Security |

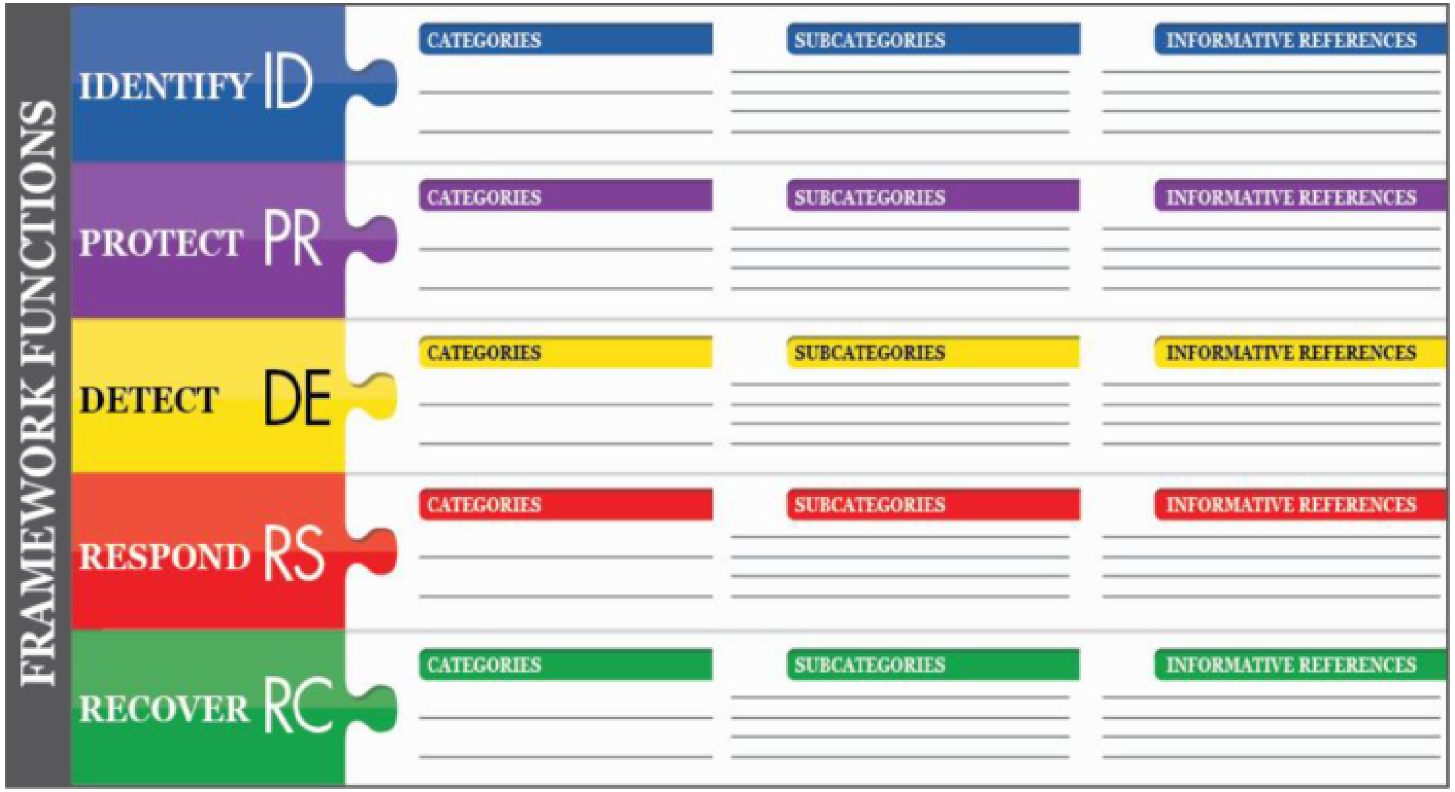






# NIST Cybersecurity Framework

- Cybersecurity Enhancement Act of 2014
- Starting point for organizations
- Voluntary
- An organized approach
  - Functions
  - Categories
  - Subcategories
  - Informative references
- Implementation tiers
- Framework profile
- Other relevant frameworks
  - ISO 27001
  - ISA-95
  - ISA/IEC 63443 (ISA-99)



FRAMEWORK FUNCTIONS

| | | | |
|---|---|---|---|
| IDENTIFY ID | CATEGORIES | SUBCATEGORIES | INFORMATIVE REFERENCES |
| PROTECT PR | CATEGORIES | SUBCATEGORIES | INFORMATIVE REFERENCES |
| DETECT DE | CATEGORIES | SUBCATEGORIES | INFORMATIVE REFERENCES |
| RESPOND RS | CATEGORIES | SUBCATEGORIES | INFORMATIVE REFERENCES |
| RECOVER RC | CATEGORIES | SUBCATEGORIES | INFORMATIVE REFERENCES |

# IEEE 2030-2011

- IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads
- Smart grid interoperability reference model (SGIRM)
  - Power Systems
  - Communications
  - Information technology
- Interoperability Architectural Perspective (AIP)
- Entities and Descriptions
- Data flows

Subclause 4.5 on Security and Privacy overview

  - Mention to ISO/IEC 27000 series
  - NISTIR 7628, “Guidelines for Smart Grid Cyber Security”

# IEEE 2030.2-2015

- 2030.2-2015 - IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure
  - Discusses how discrete and hybrid energy storage systems can be integrated with electric power infrastructure
- Clause 8 on Security and Privacy
  - More specific than 2030-2011
  - Still high level
- Compilation of security issues, standards, security requirements, risk management, security design…
- Examples of storage applications
  - SGIRM interfaces
  - SGIRM dataflows

# IEEE 1547-2018

- IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces
  - Not a cybersecurity standard, but contains some elements of cybersecurity
  - Mandates at least one of the following protocols
    - IEEE 2030.5 (SEP2)
    - IEEE 1815 (DNP3)
    - Sunspec Modbus
- Annex D.4 of IEEE 1547-2018 presents list of cybersecurity requirements
  - Focus on Local DER communication interface security
  - Some guidelines on system architecture and interfaces

# IEEE 1547.3-2007

- IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems
  - Clause 9 Security Guidelines for DR implementations
  - Discuss security issues
  - Lists options for securing communications
- New version of 1547.3 Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems
  - More detailed requirements for cybersecurity
  - Broadened scope
    - Cybersecurity is an organization-wide effort

# Best Practices

- There are several resources that provide good guidance
  - NIST 800-82, Guide to Industrial Control Systems (ICS) Security
  - NIST 800-53, Security and Privacy Controls for Information Systems and Organizations
  - DHS NCCIC and ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
  - CIS Critical Security Controls
- Cybersecurity Self-Evaluations and Audits
  - DHS US-CERT Cyber Security Evaluation Tool (CSET)
  - Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
  - Information Design Assurance Red Team (IDART™)
  - Risk management frameworks
    - NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

# Conclusion

- BESS are a new technology, but can be framed as another Industrial Control System
- Cybersecurity codes and standards provide a roadmap
- Organize and understand interoperability
- Cybersecurity must be effort of the entire organization
- New standards have become more specific
- "Hard shell, soft and chewy center"
  - Defense-in-depth

# Conclusion

- BESS have significant similarities with other DER
  - Solutions have to take into account risks specific to BESS
  - Risks are managed using electronic components
  - BMS, Gas and Fire Detection add to complexity
  - Applications
  - Complexity
- Risk has to be properly understood before applying security measures
  - Ownership/maintenance? Application? Size?
- BESS safety is an evolving field

# Acknowledgment

This research was funded by the energy storage program at the U.S. Department of Energy under the guidance of **Dr. Imre Gyuk**. Sandia National Laboratories is a multi-mission 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 National Nuclear Security Administration under contract DE-NA-0003525. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.
Special thanks to Dr. Babu Chalamala, Dr. Tu A. Nguyen, Dr. Valerio de Angelis, James Obert and Dr. Vittal Rao

# CEU Q1:

- What is the name of the organization that develops and enforces Bulk Power Grid Reliability Standards in North America, including Critical Infrastructure Protection?

- a. North American Electric Reliability Corporation (NERC)
- b. Institute of Electrical and Electronics Engineers (IEEE)
- c. International Electrotechnical Commission (IEC)
- d. Cybersecurity and Infrastructure Security Agency (CISA)

# CEU Q2:

- Which device collects voltage, current and temperature data from battery cells , balances battery charge, and estimates the state of charge locally?

- a. Battery management systems
- b. Fire suppression systems
- c. Environmental control systems
- d. Power conversion systems

# CEU Q3:

- What are the five functions of the NIST Cybersecurity Framework?

- a. Identify, protect, detect, respond, and recover
- b. Intrusion detection, firewall, physical security, network segmentation, and virtual private network
- c. Information protection, electronic security perimeter, personnel & training, system security management, and incident reporting and response planning
- d. NEMA, NIST, FERC, NERC, and CISA

IEEE SMARTGRID

IEEE Advancing Technology for Humanity

# CEU Q4:

- Which country has suffered major power grid cyberattacks in 2015 and 2016?

- a. Ukraine
- b. Angola
- c. Colombia
- d. Vietnam

# CEU Q5:

- Cyber Security Evaluation Tool (CSET), Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and Information Design Assurance Red Team (IDART) are examples of:

- a. Cybersecurity Self-Evaluations and Audits
- b. Intrusion detection systems
- c. IEEE Standards
- d. Supply Chain Risk Management