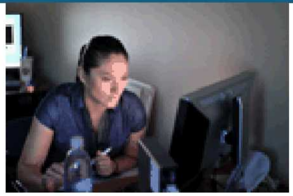
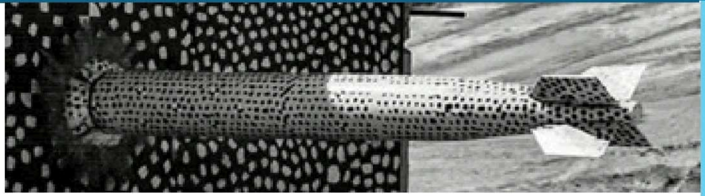
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2020-10728C

Security of Energy Storage Systems





2020 Biennial Center for Power Systems Studies South Dakota Regional Power (SoDaRP) Conference, October 5th, 2020

PRESENTED BY

Rodrigo D. Trevizan, Ph.D.

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.

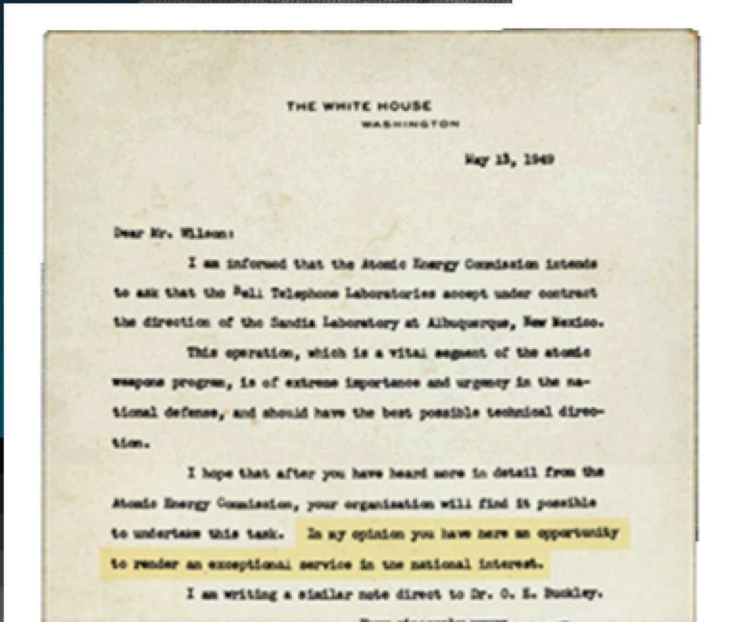
Outline

1. Sandia National Laboratories
2. Energy Storage Systems Program
3. Introduction
4. Notable Cyberattacks
5. Risks
6. Standards
7. Best Practices
8. Conclusion

SANDIA'S HISTORY IS TRACED TO THE MANHATTAN PROJECT

> *…In my opinion you have here an opportunity to render an exceptional service in the national interest.*

- July 1945
  Los Alamos creates Z Division
- Nonnuclear component engineering
- November 1, 1949
  Sandia Laboratory established
- AT&T: 1949–1993
- Martin Marietta: 1993–1995
- Lockheed Martin: 1995–2017
- Honeywell: 2017–present



THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

I am writing a similar note direct to Dr. O. E. Buckley.

Very sincerely

Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.

SANDIA HAS FACILITIES ACROSS THE NATION

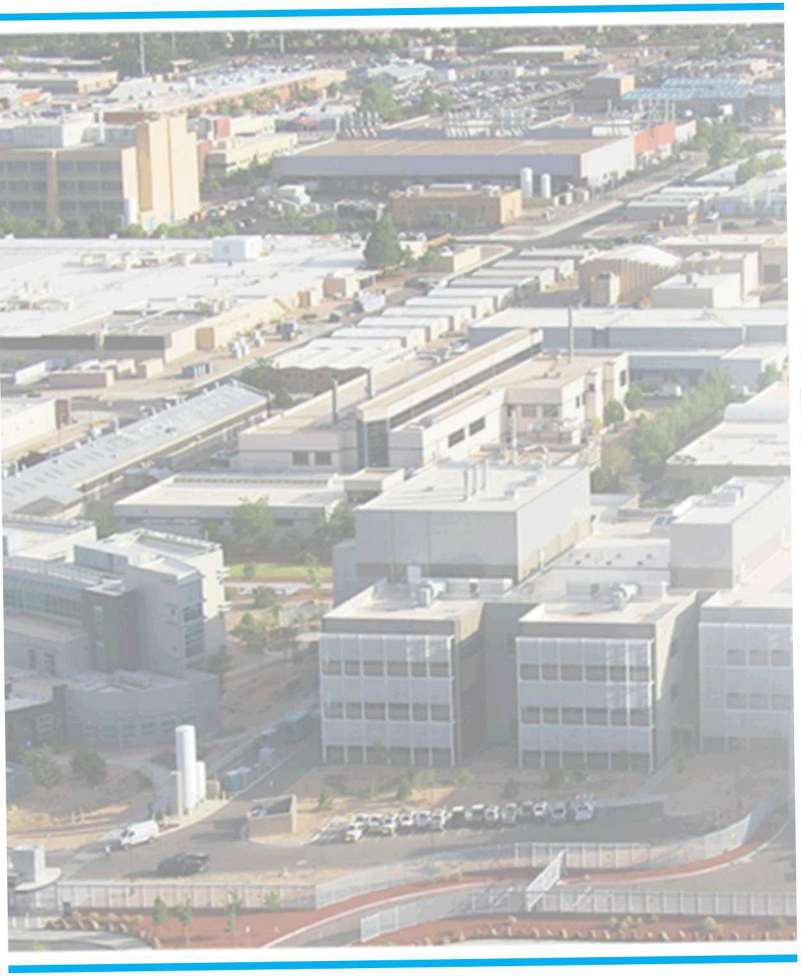
Activity locations

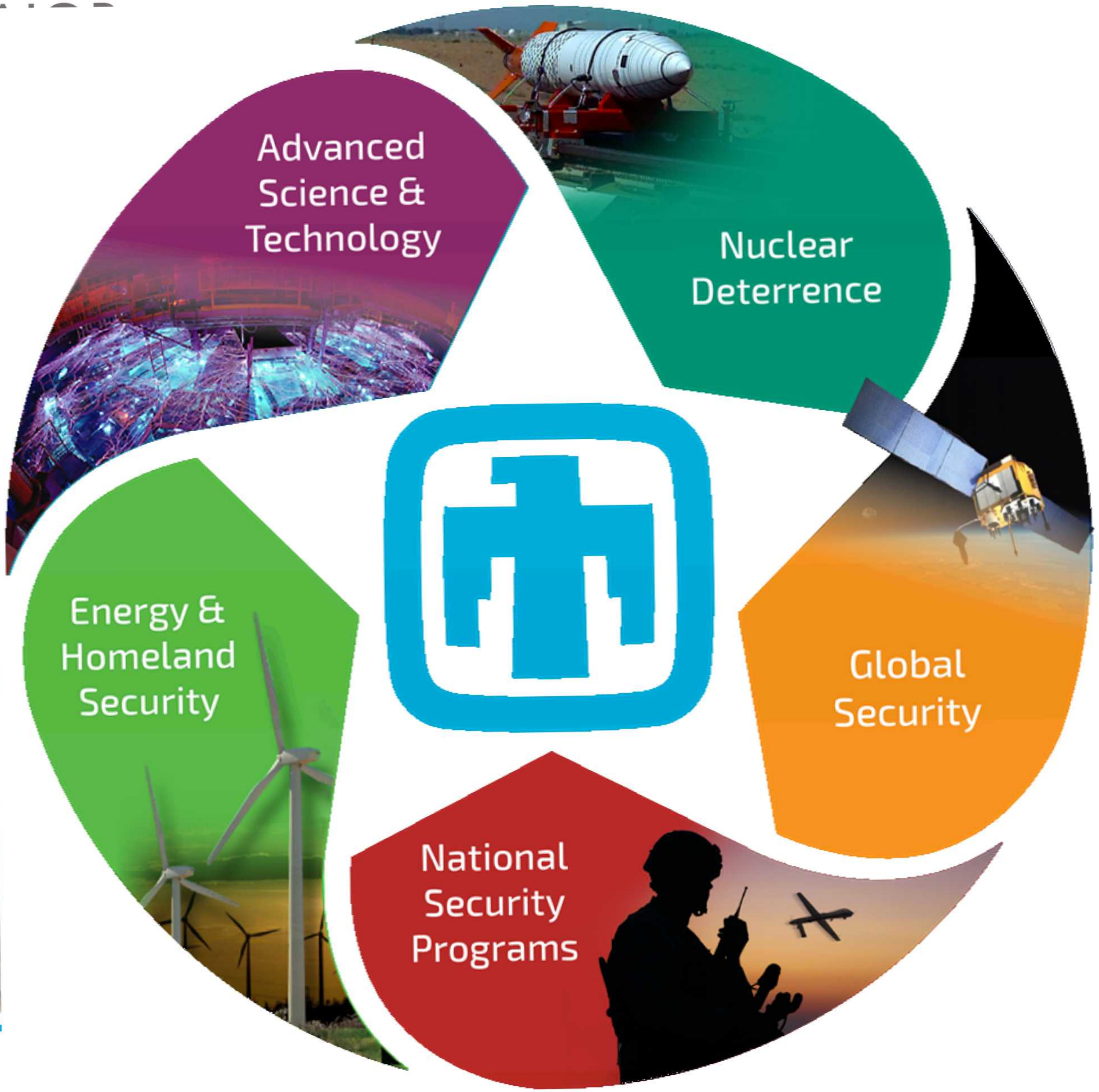
- Kauai, Hawaii
- Waste Isolation Pilot Plant, Carlsbad, New Mexico
- Pantex Plant, Amarillo, Texas
- Tonopah, Nevada

Main sites

- Albuquerque, New Mexico
- Livermore, California

SANDIA HAS FIVE MA
PROGRAM PORTFOL





Advanced Science & Technology

Nuclear Deterrence

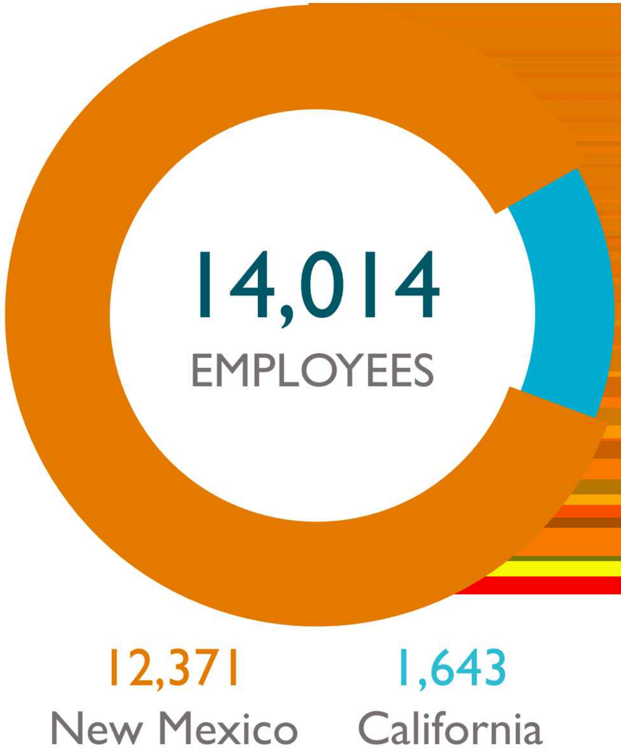
Global Security

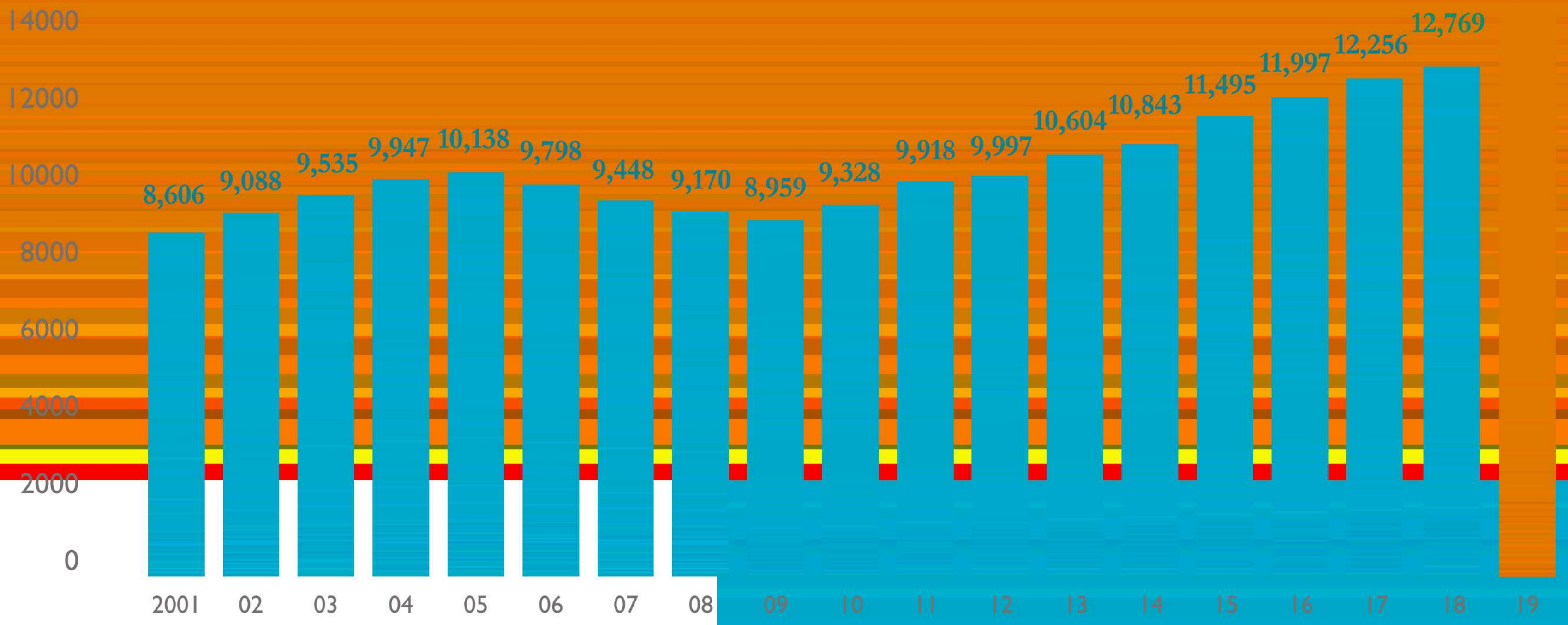
National Security Programs

Energy & Homeland Security

SANDIA'S WORKFORCE IS GROWING

Staff has grown by over 5,000 since 2009 to meet all mission needs





Energy Storage Systems Program

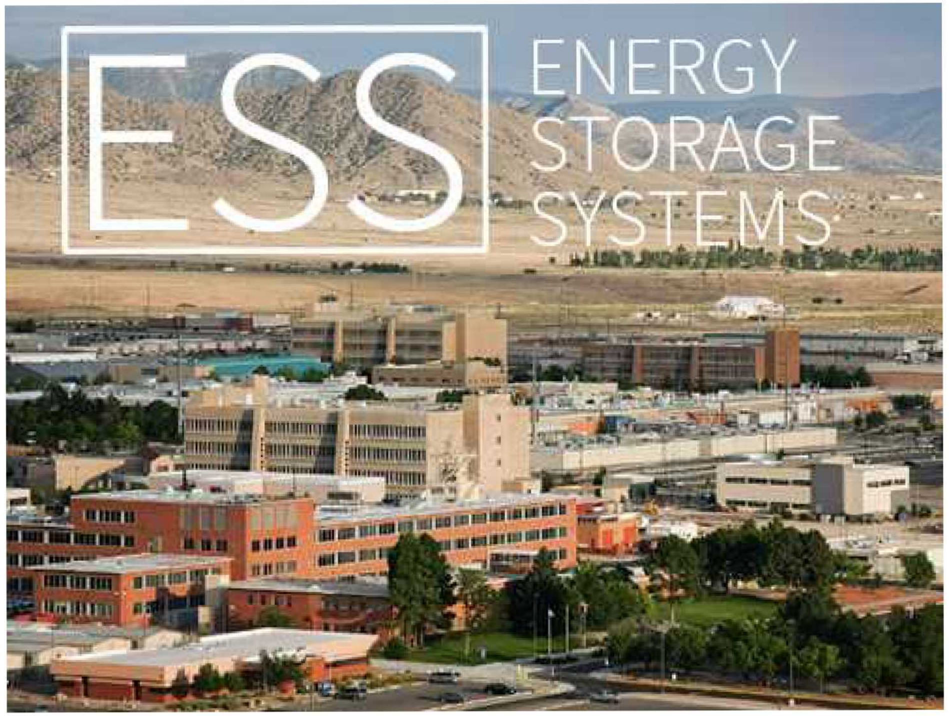
Started in 1950's

- Develop power sources for Nation's nuclear stockpile

From 1970s on, focus moved to electric power

- Develop advanced energy storage technologies and systems
- Increase the reliability, performance, and competitiveness of electricity generation and transmission
- Electric grid
- Standalone systems

For more information: https://www.sandia.gov/ess-ssl/



DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

Sandia National Laboratories

Pacific Northwest NATIONAL LABORATORY

OAK RIDGE National Laboratory

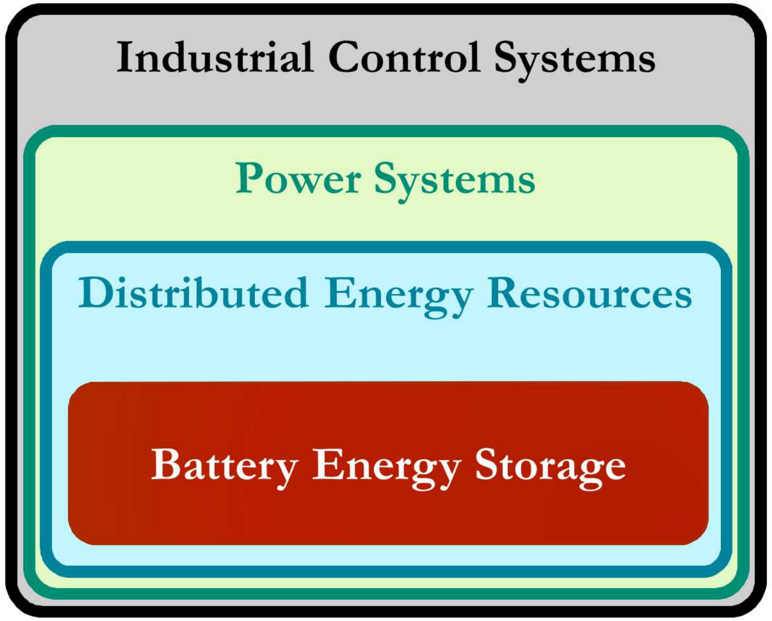
Introduction

Battery Energy Storage Systems (BESSs) have many similarities with other DERs
- Similar scale
- Power Conversion Systems (PCS)
- Controllable

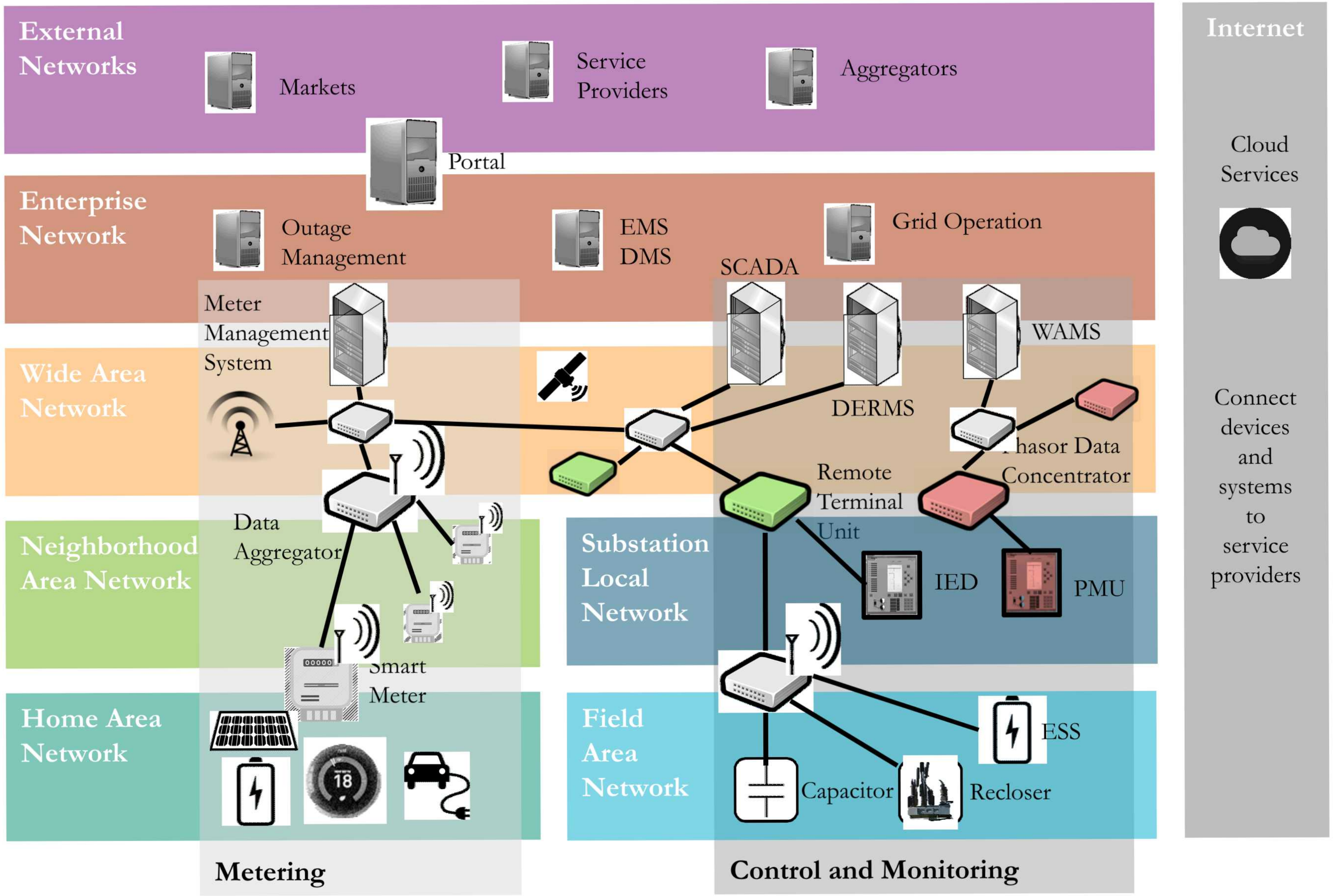
Other Energy storage systems (ESS) share the similar characteristics

But some particularities
- Inherent risks of stored energy
- Dedicated management of energy for each technology
- Need for specific equipment to perform those functions
  - Battery Management Systems
  - Fire Suppression
  - Networks
  - Permanent damage
- Need to communicate with PCS and energy management systems

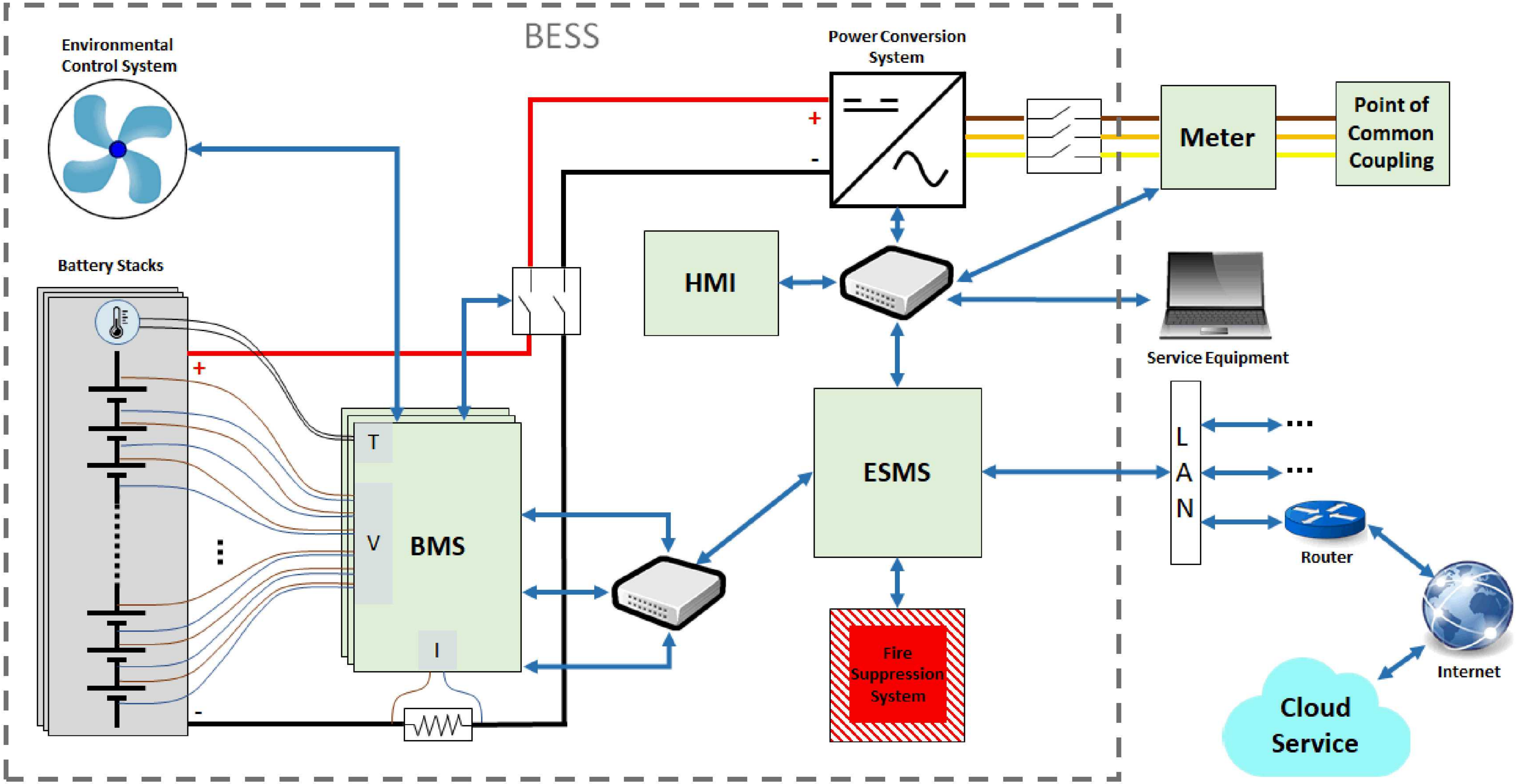
BESS and DER are new technologies
- Context of power systems and Industrial Control Systems



Introduction



Introduction



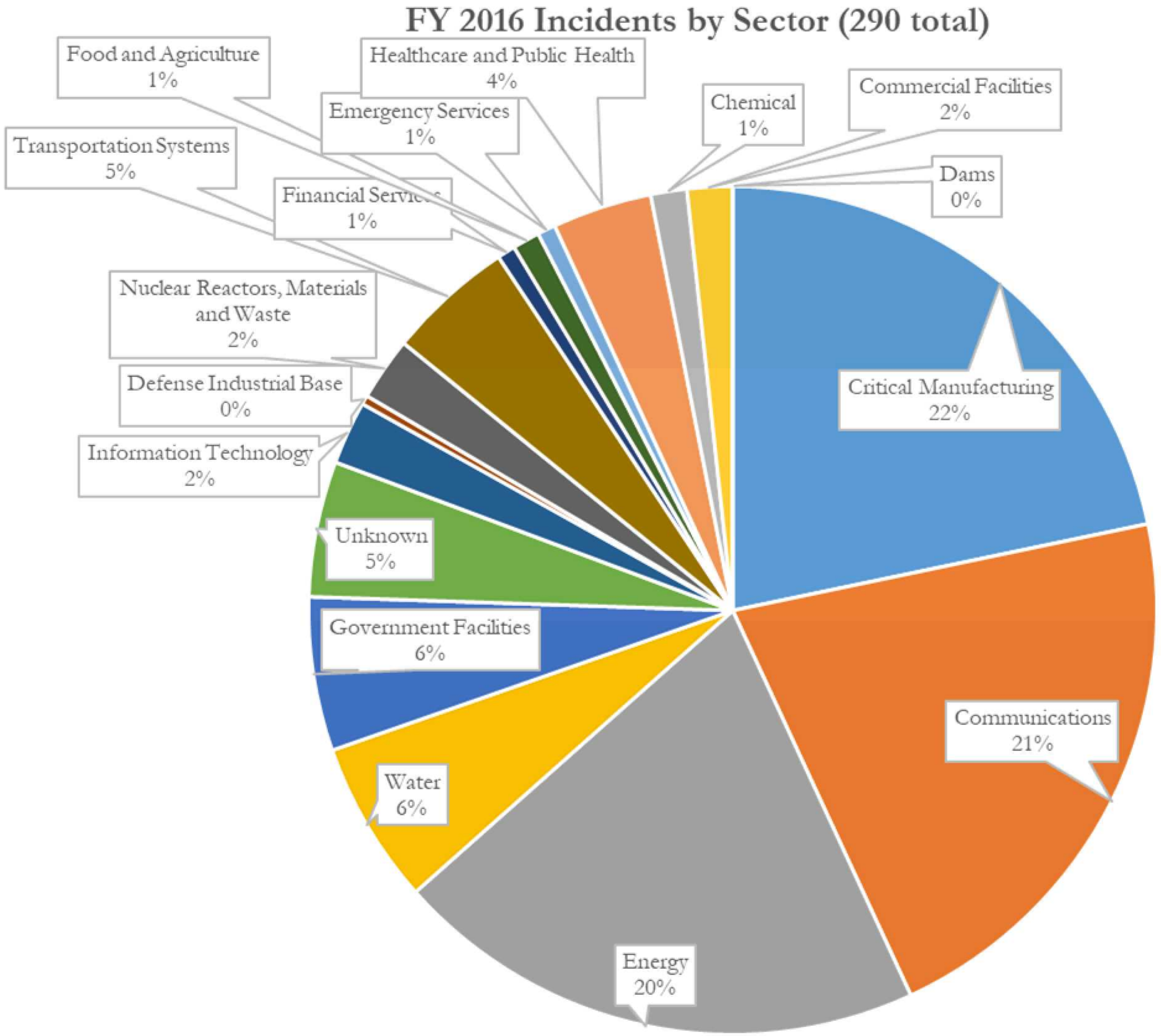
Introduction

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

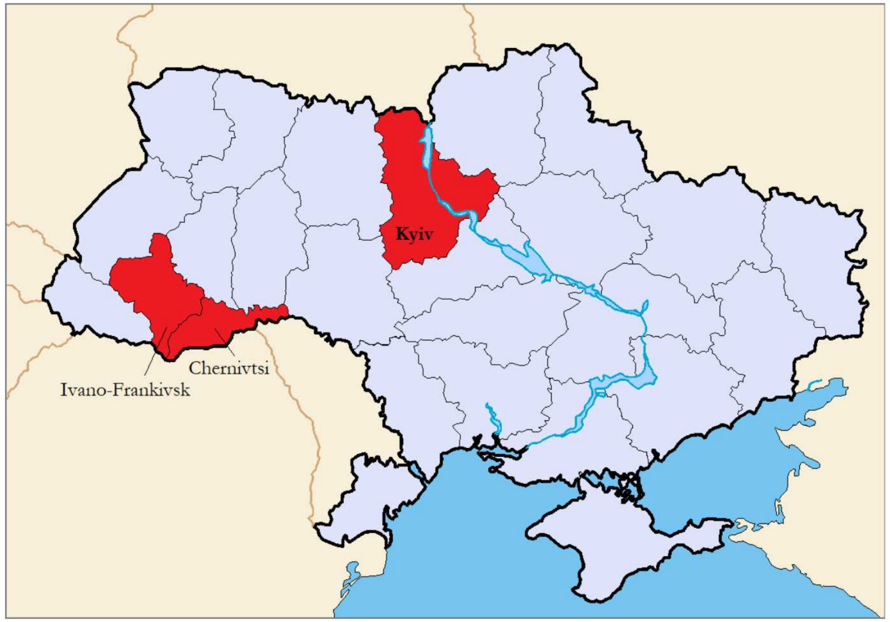
Notable Cyberattacks

2010 – Natanz Uranium Enrichment Plant, Iran

- Stuxnet
  - Infection through USB drives and Windows vulnerabilities
  - Targeted Programmable Logic Controllers (PLCs)
- Attacked centrifuges used for Uranium enrichment

2015 – Ukraine

- Access through spear-phishing emails and malware in MS Office files
- Use of Black Energy 3 Malware
- Threat actors performed reconnaissance over several months
- 3 regional power distribution utilities
- 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

Risks

Physical security:

- Facilities are often unmanned with 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…

Cybersecurity

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

Diesel generator set damage during 2007 Aurora Generator Test.

NIST Cybersecurity Framework

Cybersecurity Enhancement Act of 2014

Starting point for organizations

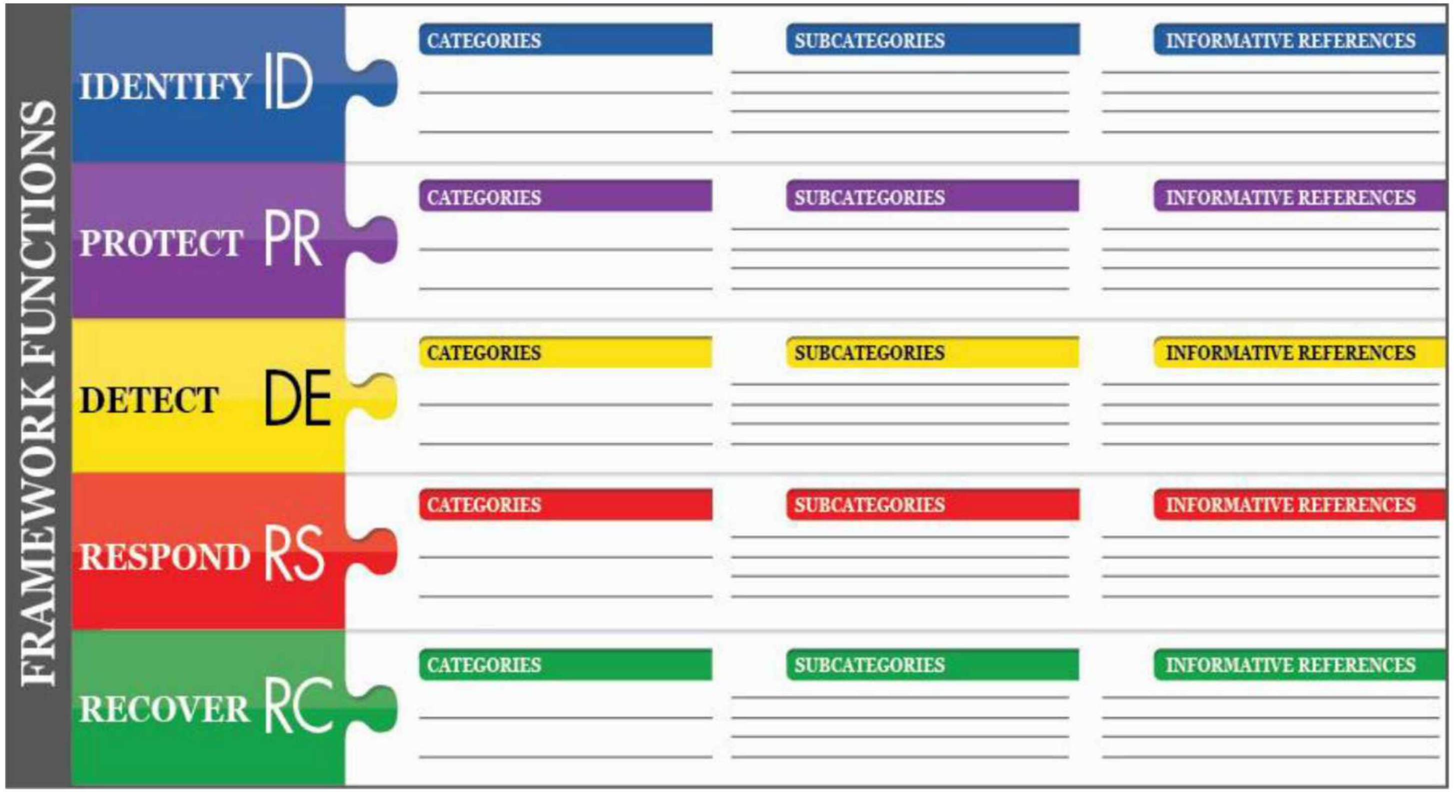
Voluntary

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

NERC CIP

North American **E**nergy **R**eliability **C**orporation **C**ritical **I**nfrastructure **P**rotection

NERC works with the industry to develop standards

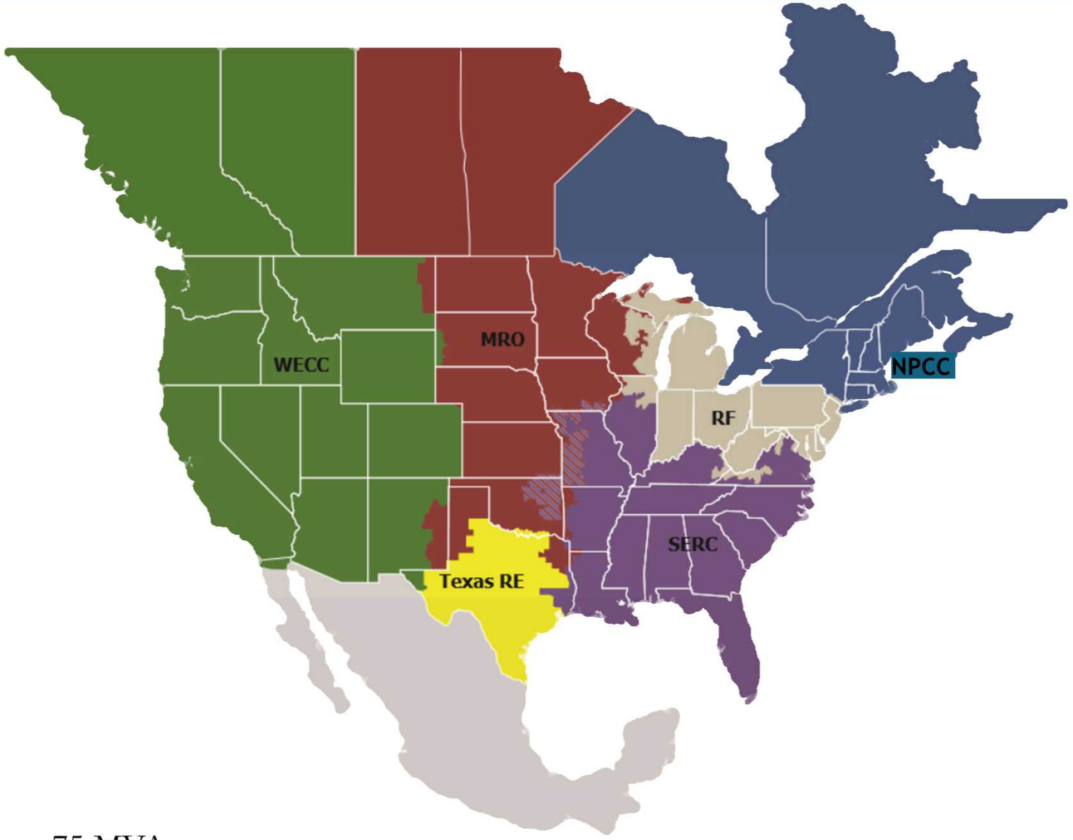
FERC approves the standards

- Penalty Structure
- Audit Cycles

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 […]"
- 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



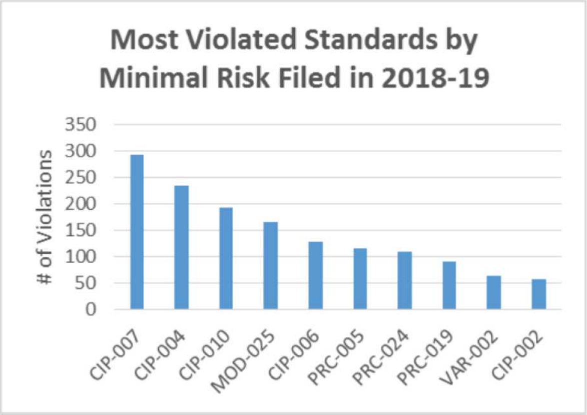
NERC CIP

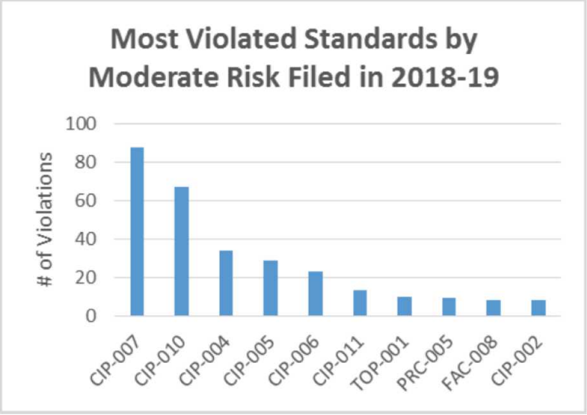
Standards Subject to Enforcement

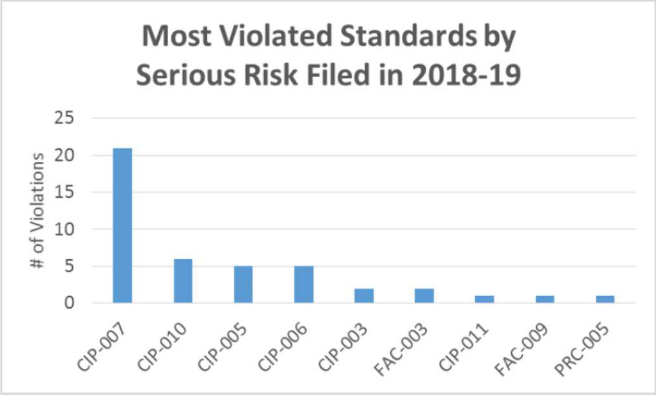
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization
CIP-003-8	Cyber Security — Security Management Controls
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-6	**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

Standards Subject to Future Enforcement

CIP-005-6	Cyber Security — Electronic Security Perimeter(s)
CIP-008-6	Cyber Security — Incident Reporting and Response Planning
CIP-010-3	Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP-012-1	Cyber Security – Communications between Control Centers
CIP-013-1	Cyber Security - Supply Chain Risk Management







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^{TM})
- Risk management frameworks
  - NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

Best Practices

Patching

- Common for IT network
- For OT devices, it is more tricky

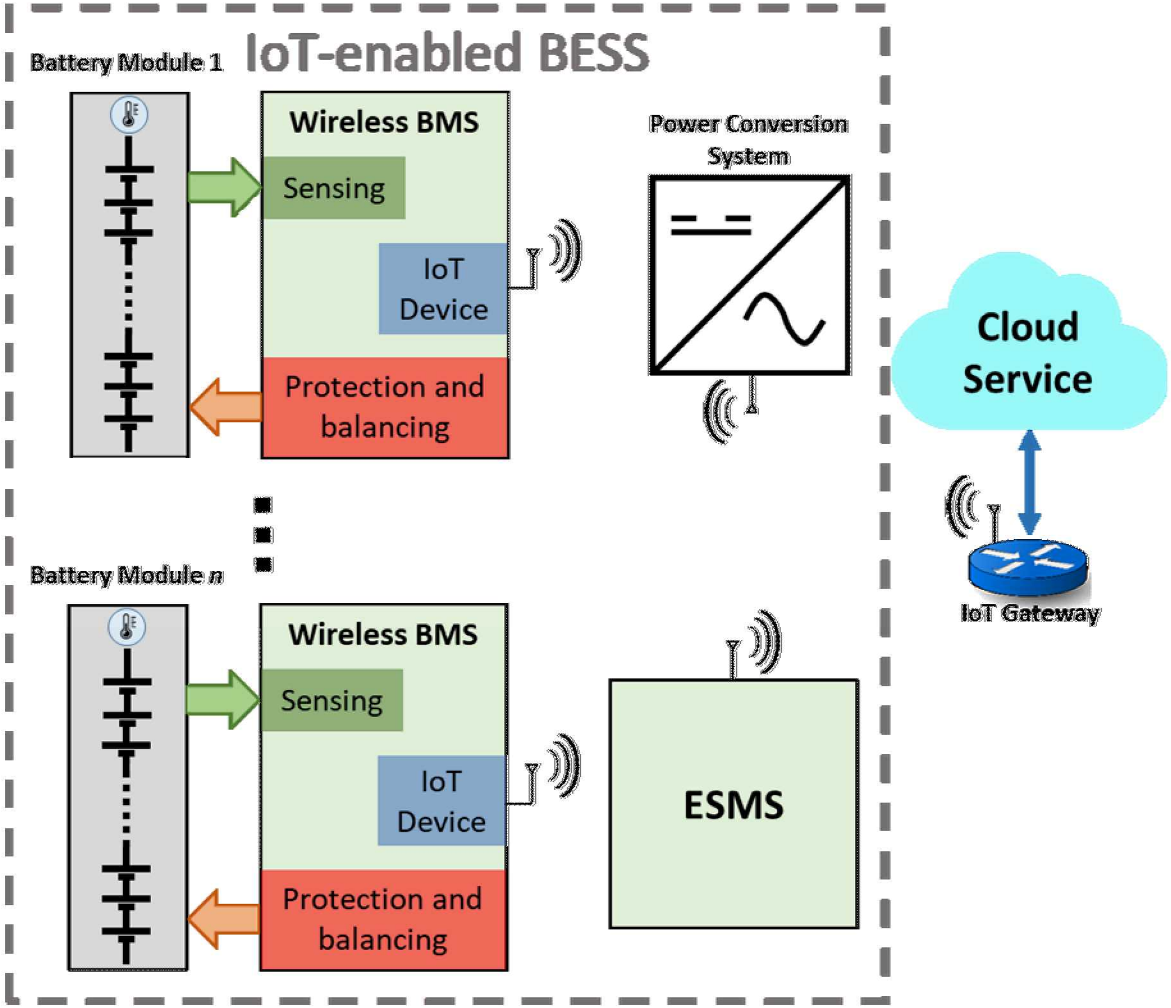
Supply Chain Risk Management

- D. Shackleford, Combatting Cyber Risks in the Supply Chain, SANS Institute Report, Sept 2015
- SAE International, Standard ARP9134A, "Supply Chain Risk Management Guideline"
- NEMA, CPSP 1-2015, Supply Chain Best Practices, Document ID: 100742
- SAE International, Standard AS5553A, "Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria"
- SAE International, Standard AS5553B, "Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition"

Research

Internet-of-Things

- Devices controllable/readable over the internet
- Already exists for many consumer electronics
  - Thermostats
- Embedded systems can benefit from computational power of cloud servers
- Scalability
- Security concerns

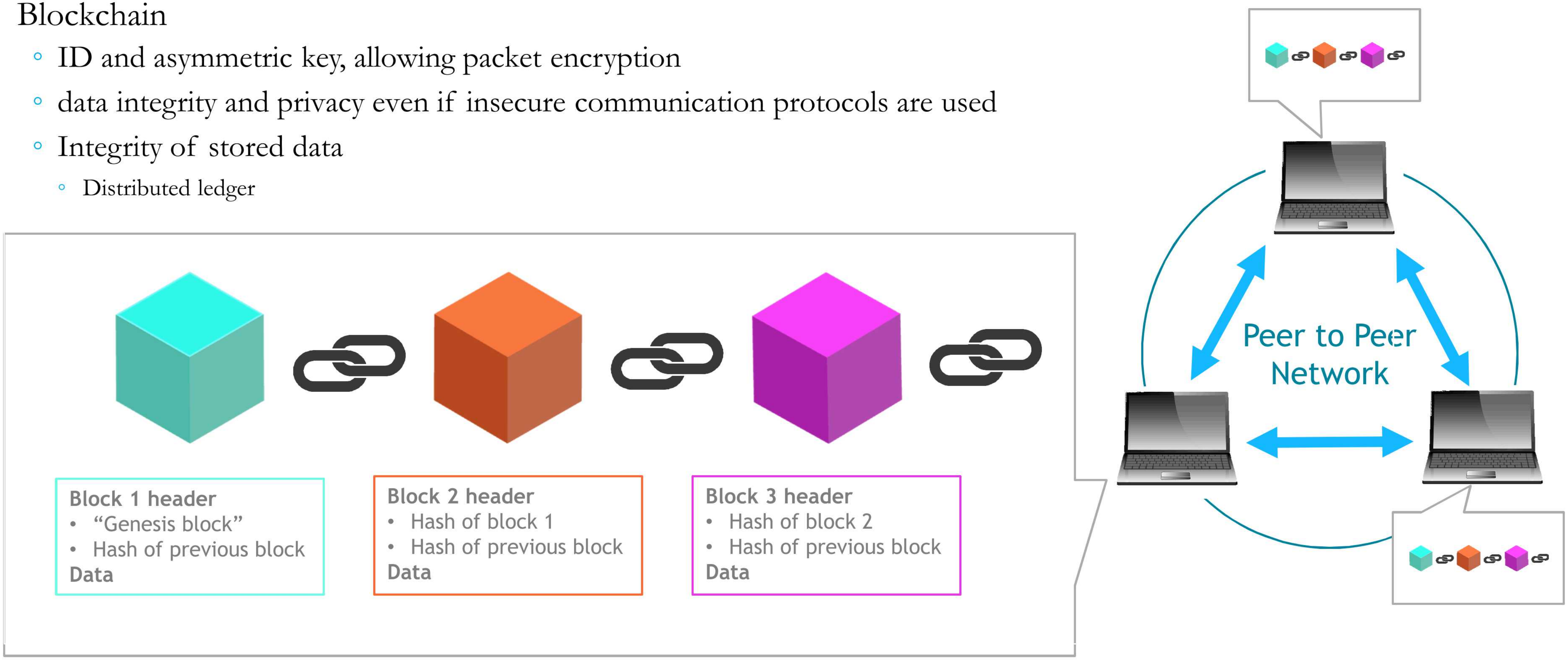


Source: T. Faika, T. Kim, J. Ochoa, M. Khan, S. Park and C. S. Leung, "A Blockchain-Based Internet of Things (IoT) Network for Security-Enhanced Wireless Battery Management Systems," *2019 IEEE Industry Applications Society Annual Meeting*, Baltimore, MD, USA, 2019, pp. 1-6, doi: 10.1109/IAS.2019.8912024.

Research

Blockchain

- ID and asymmetric key, allowing packet encryption
- data integrity and privacy even if insecure communication protocols are used
- Integrity of stored data
  - Distributed ledger



Block 1 header
- “Genesis block”
- Hash of previous block

Data

Block 2 header
- Hash of block 1
- Hash of previous block

Data

Block 3 header
- Hash of block 2
- Hash of previous block

Data

Peer to Peer Network

Research

Smart contract

- access control can be leveraged to guarantee data privacy
- contracts can also be used to assess the integrity of firmware

Blockchain technology for supply chain management

- Identify and trace system components
  - electronics,
  - batteries and
  - E.g. TrustChain and POMS

Blockchain protocols are usually computationally intensive

Conclusion

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

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.

Thank you!

Q&A?