Sandia National Laboratories

Exceptional service in the national interest

CYBERSECURITY CONSIDERATIONS

For Battery Energy Storage Systems

Victoria O'Brien, Ph.D.

Sandia National Laboratories

Energy Storage Webinar Series

Session 5: Cybersecurity

July 8, 2026

U.S. DEPARTMENT of ENERGY | NNSA National Nuclear Security Administration

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.

SAND2026-23120PE

BATTERY ENERGY STORAGE SYSTEM (BESS) OVERVIEW

COMPONENTS IN A BESS

- BESSs are complex cyber-physical systems with integrated systems and subsystems
- Combine components and software from multiple vendors across the globe

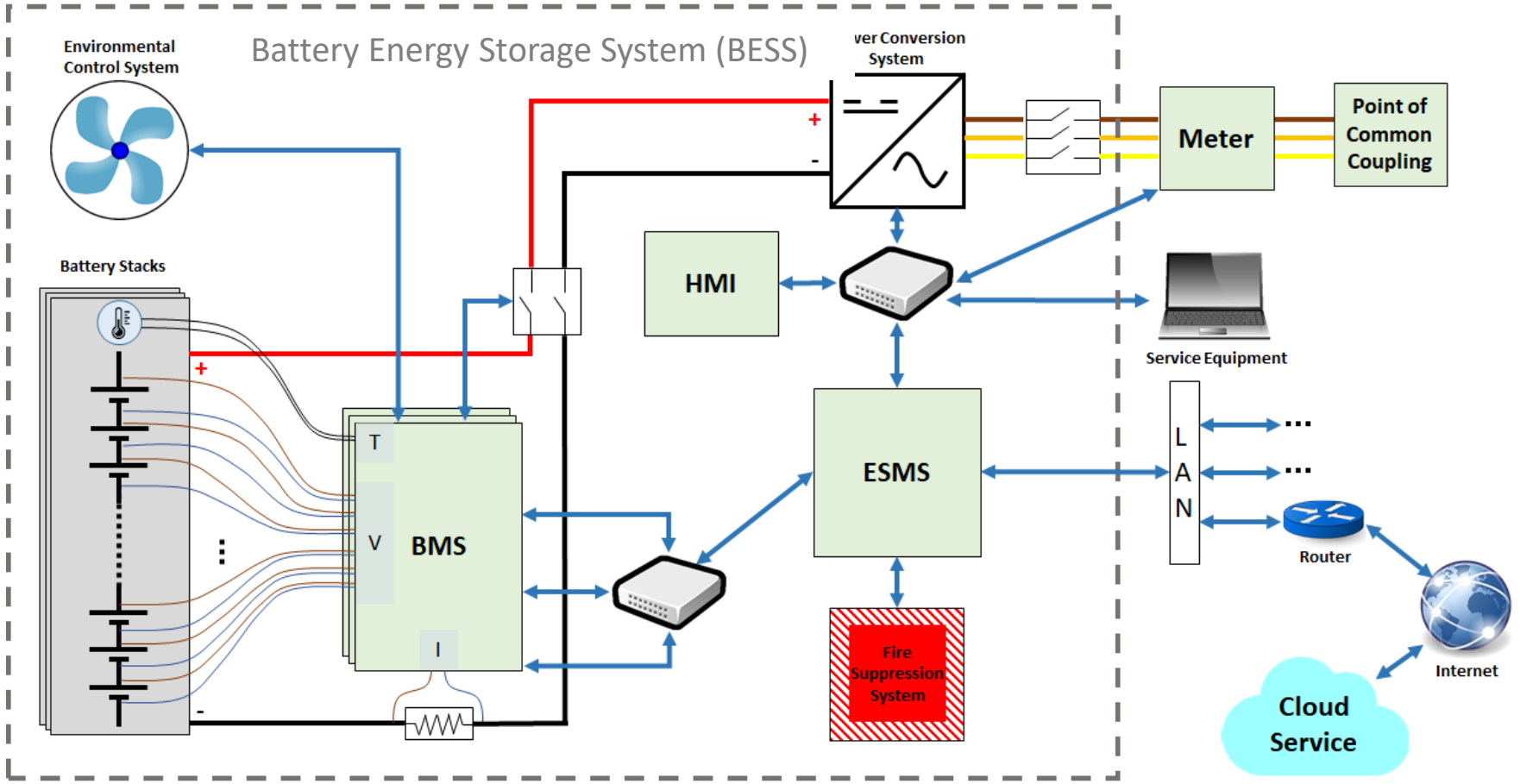
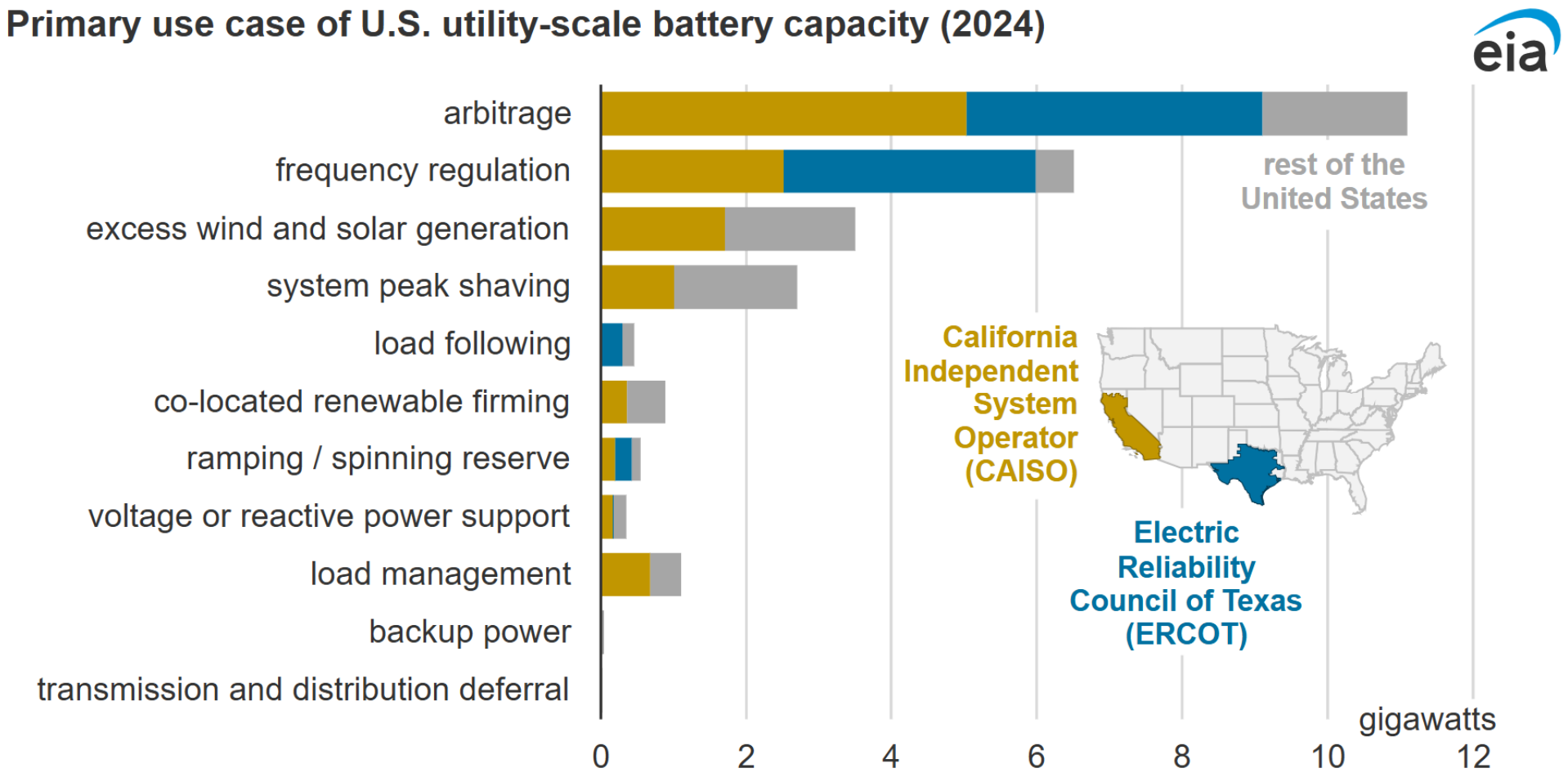


Diagram of a BESS from [1]

USES OF UTILITY-SCALE BESS



Primary uses of BESS [2]

*I believe going forward we will see BESSs used to support data centers and load growth

MOSS LANDING BATTERY FIRES

- The September 2022 incident:
  - Water ingress caused overheating which led to fire [3]
  - Battery system was disconnected from the grid and remained offline for three months [3]
- The January 2025 incident:
  - Cause unknown [4]
  - Burning and destruction of many battery cells and release of smoke plume, fire lasted days

2025 Moss Landing fire
Photo from [4]

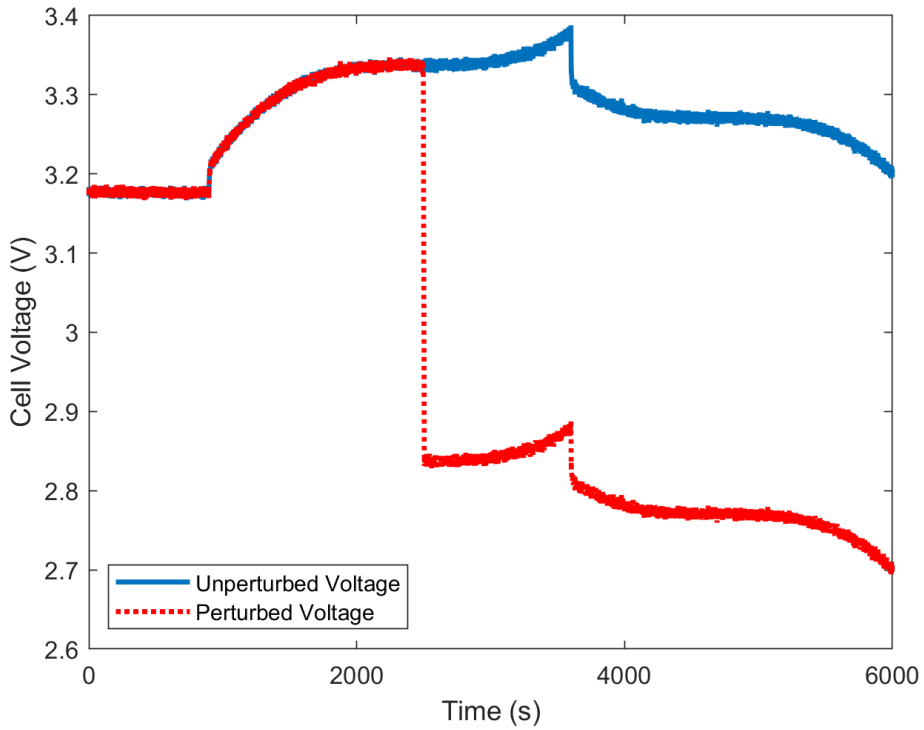
Foul play is not suspected in either of the Moss Landing incidents
Imagine the increased damage if these events had been caused by a bad actor

BESS THREAT EXEMPLARS

HYPOTHETICAL SCENARIOS

SCENARIO 1: FALSE DATA INJECTION ATTACK

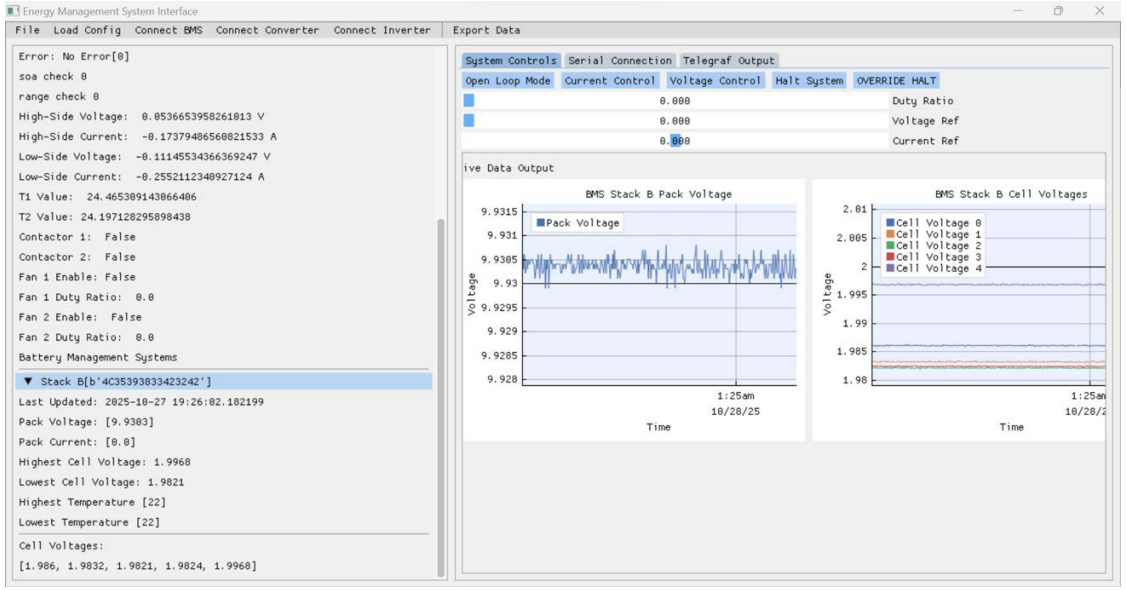
- Exemplar: False data injection attack (FDIA)
  - An adversarial nation hacks into the battery management system (BMS) of a BESS and corrupts the incoming voltage measurements
- Consequences: Corrupted control system
  - Battery degradation or damage
  - Overcharge/overdischarge
  - Overheating, thermal runaway, fire
- Similar incident: Stuxnet (2010)
  - Stuxnet worm sent false centrifuge readings to control system, causing the devices to spin out of control



Voltage following -500 mV FDIA

SCENARIO 2: MALICIOUS UPDATE

- Exemplar: Malicious software update
  - An energy management system company offers an update to their software via the cloud. Unfortunately, a bad actor has tampered with the code and removed the management systems' safety limits
- Consequences:
  - Corrupted safety subsystems
  - Overcharge/overdischarge
  - Overheating, thermal runaway, fire
- Similar incident: SolarWinds attack (2020)
  - Hackers inserted a malicious backdoor into SolarWinds' Orion network which was pushed to thousands of users, causing data theft and spying



Emulated energy management system dashboard containing safety checks
Photo courtesy of Armando Montoya

SCENARIO 3: RANSOMWARE / INSIDER THREAT

- Exemplar: BESS system held for ransom
  - While checking their email, a utility employee clicked on a malicious attachment. Ransomware was downloaded and the employee was locked out of their machine.
- Consequences:
  - Potential data leakage
  - Inability to access system
- Similar incident: Colonial Pipeline (2021)
  - DarkSide hackers obtained access to Colonial Pipeline's IT infrastructure, stole data, and locked access, demanding millions in payouts

Example of ransomware attack 'WannaCrypt'
Photo from [5]

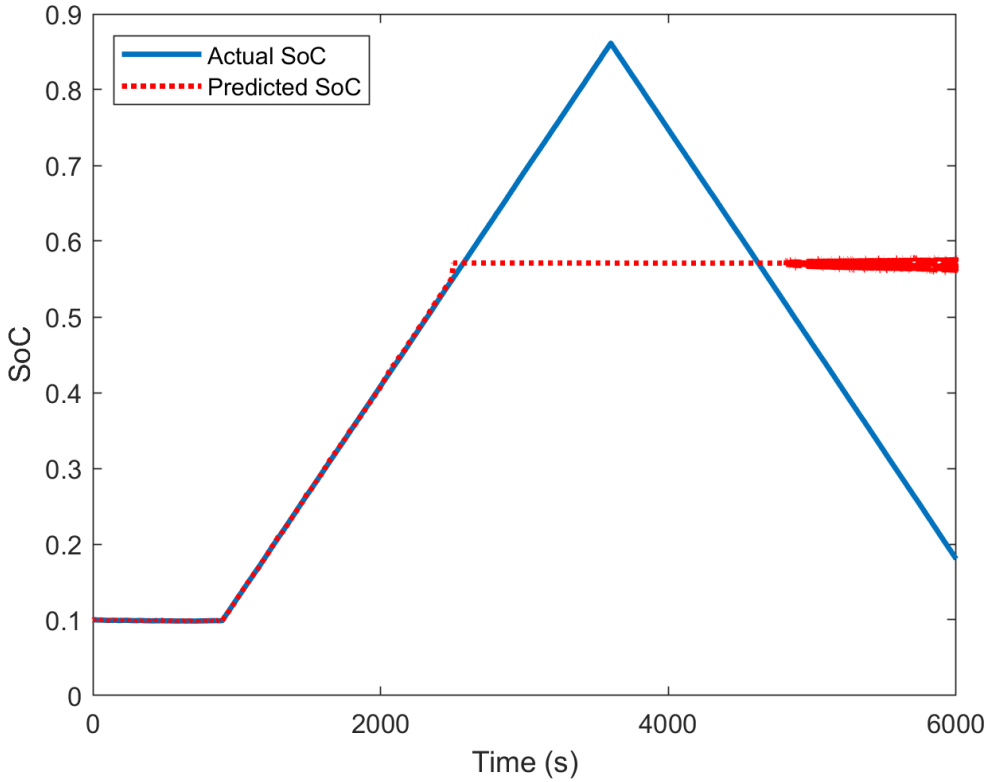
SCENARIO 4: DENIAL OF SERVICE (DOS) ATTACK

- Exemplar: Denial of service (DoS)
  - Hackers flood the communication channels of a BESS, causing data loss and communication delays
- Consequences:
  - Missing readings
  - Time offline
  - Corrupted controls
- Similar incident: Solar farm DoS attack (2019)
  - A vulnerability in the firewall of a solar farm was exploited, causing the system to repeatedly reboot for 12 hours, communication outages, and reduced visibility

Missing temperature data due to communications failure
Photos courtesy of Armando Montoya

SCENARIO 5: SUPPLY CHAIN

- Exemplar: Supply chain
  - A BESS is controlled by proprietary software. Bad actors hide a bug in the control software that corrupts Coulomb counting after one year of deployment
- Consequences: Corrupted control system
  - Battery degradation or damage
  - Overcharge/overdischarge
  - Overheating, thermal runaway, fire
- Similar incident: Pager explosions (2024)
  - Pagers were intercepted and tampered with by adding explosive devices near the Lithium-ion battery, explosives were then remotely detonated



Corrupted state of charge

SCENARIO 6: PHYSICAL DAMAGE

- Exemplar: BESS shooting
  - A bad actor uses firearms and explosive devices to destroy a BESS deployment
- Consequences:
  - BESS damage and destruction
  - Time offline
  - Degraded public trust
- Similar incident: Grid substation shootings (2013, 2020s)
  - Multiple substations shot up by bad actors across the U.S. throughout the 2020s. In addition, the infamous Metcalf Substation shooting of 2013

Footage from Metcalf shooting
Photo from [6]

THE BESS THREAT SURFACE

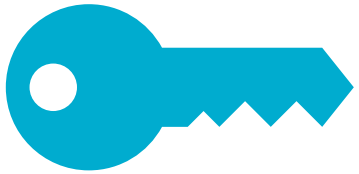
THREAT ACTOR GOALS

Advanced Persistent Threats	Insider Threats	Hacktivists	Hackers	Vigilantes
• Damaging systems • Stealing intellectual property	• Revenge / sabotage • Leaking data • Espionage • Financial gain	• Demonstrations • Propaganda • Fame • Social change	• Enhance skills • Revenge • Exploit vulnerabilities • Financial gain • Completing jobs	• Protect from unethical hackers

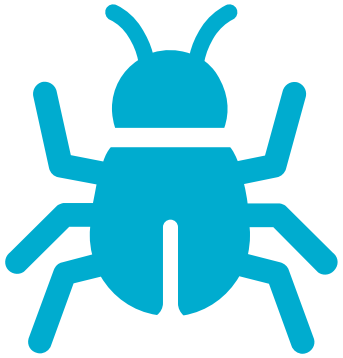
Threat actors and their goals [7]

ENERGY SECTOR THREAT MODEL

Advanced Persistent Threat

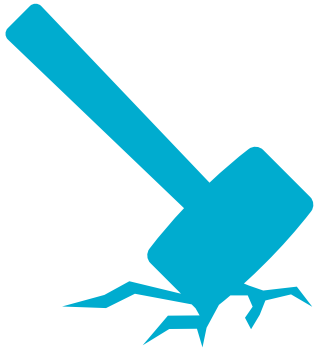


Insider Threat



Hackers

Extreme Weather

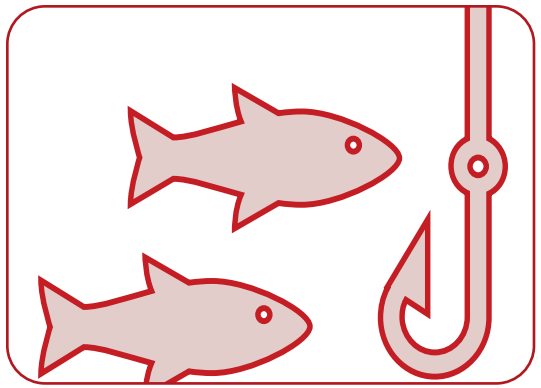


Physical Threat

Hardware / Software Supply Chain Threats

Energy critical infrastructure threat matrix [8]

CONCERNS FROM ELECTRIC UTILITIES – CYBERATTACKS

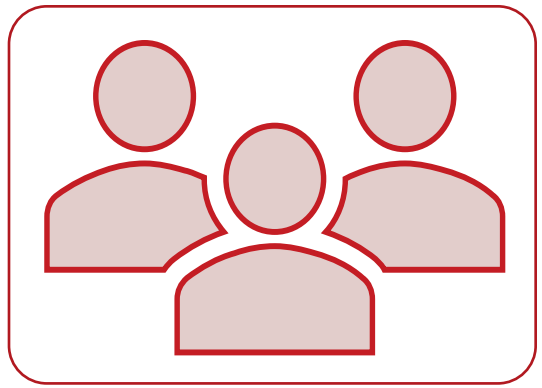


Phishing: using communications to obtain data or deploy malware

- compromised email
- spear phishing
- whaling
- vishing
- smishing

Malware: software intended to harm systems, obtain information, or obtain money

- viruses
- worms
- ransomware
- spyware



Social Engineering: manipulation technique to exploit human error

- social media phishing
- watering hole attack
- USB baiting
- physical social engineering

CONCERNS FROM ELECTRIC UTILITIES – ARTIFICIAL INTELLIGENCE

Using artificial intelligence to lower the barrier to entry for hackers

Using artificial intelligence to create more complex attacks

Using artificial intelligence to reverse engineer grid models and launch stealthy attacks

Using large language models to create more convincing phishing emails and social engineering attacks

CONCERNS FROM ELECTRIC UTILITIES – SUPPLY CHAIN

- 2014: Powerline Inc. counterfeit batteries sold to U.S. Government
- White labeling BESS components or control systems

PRESS RELEASE

Former CEO Of Simi Valley Company Guilty Of Bilking Navy By Selling $2.6 Million In Knock-Off Batteries Used On Aircraft Carriers And Subs

Headline for sale of counterfeit batteries to U.S. government
Photo from [9]

- Monopoly on BESS component supply chains, removal of CATL batteries

Ribbon cutting for CATL BESS deployment
Photo from [10]

BESS THREAT SPACE

- Neglecting “Secure by Design” Principles
- Deception attacks on sensors (voltage, current, temperature) – FDIAs, man in the middle attacks, replay attacks
- Denial of service attacks
- Software and hardware supply chain attacks
- Insider threats – tampering with proprietary modeling / estimation capabilities
- Lack of regulations / policy / guidelines for BESS cybersecurity
- Physical attacks
- Combination attacks

The biggest threat to the cybersecurity of BESSs is allowing cybersecurity to be an afterthought – we need to be designing cybersecure systems PROACTIVELY

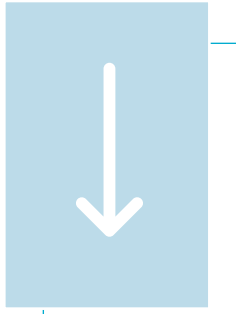
CONSEQUENCES FOR CRITICAL CONTROL ELECTRONICS [11]

- Critical Control Electronics (CCE) including all associated electronics (hardware, firmware, software, communications gateways, and remote access devices) related to the BESS
  - Safety CCE: if compromised, could result in loss of life, injury, equipment damage, or infrastructure damage
    - Level 1 & 2 Battery Management System (BMS): the control system used to monitor, protect, balance, and manage battery cells, modules, racks, or packs, including measurement of voltage, current, temperature, state of charge, and battery health
    - Fire Safety System: Prevents thermal runaway and fire propagation. Provides information to first responders
  - Operational CCE: if compromised, does not represent a safety risk, but could result in the ESS going offline
    - L3 BMS / BESS Controller: the controller used to manage and coordinate the operation of one or more battery strings, racks, stacks, or arrays
    - Site Controller: the control system used to coordinate the BESS with other generation sources, loads, and facility-level operating requirements

*** The information included in this slide is from [11]**

MITIGATING AND CONTAINING BESS THREATS

PRIMARY CYBERSECURITY GOALS



Minimize risks

Quickly and properly respond to incidents

Proactively guard against incidents

Investigate incidents

Detect and monitor for incidents

Remain in compliance with regulations

CYBERSECURITY FUNDAMENTALS

Unknown Probability of an Attack

- Hard to predict what vulnerabilities may be exploited
- New vulnerabilities can be discovered
- Different studies have differing results regarding the likelihood of cyberattacks

Zero-Trust Approach

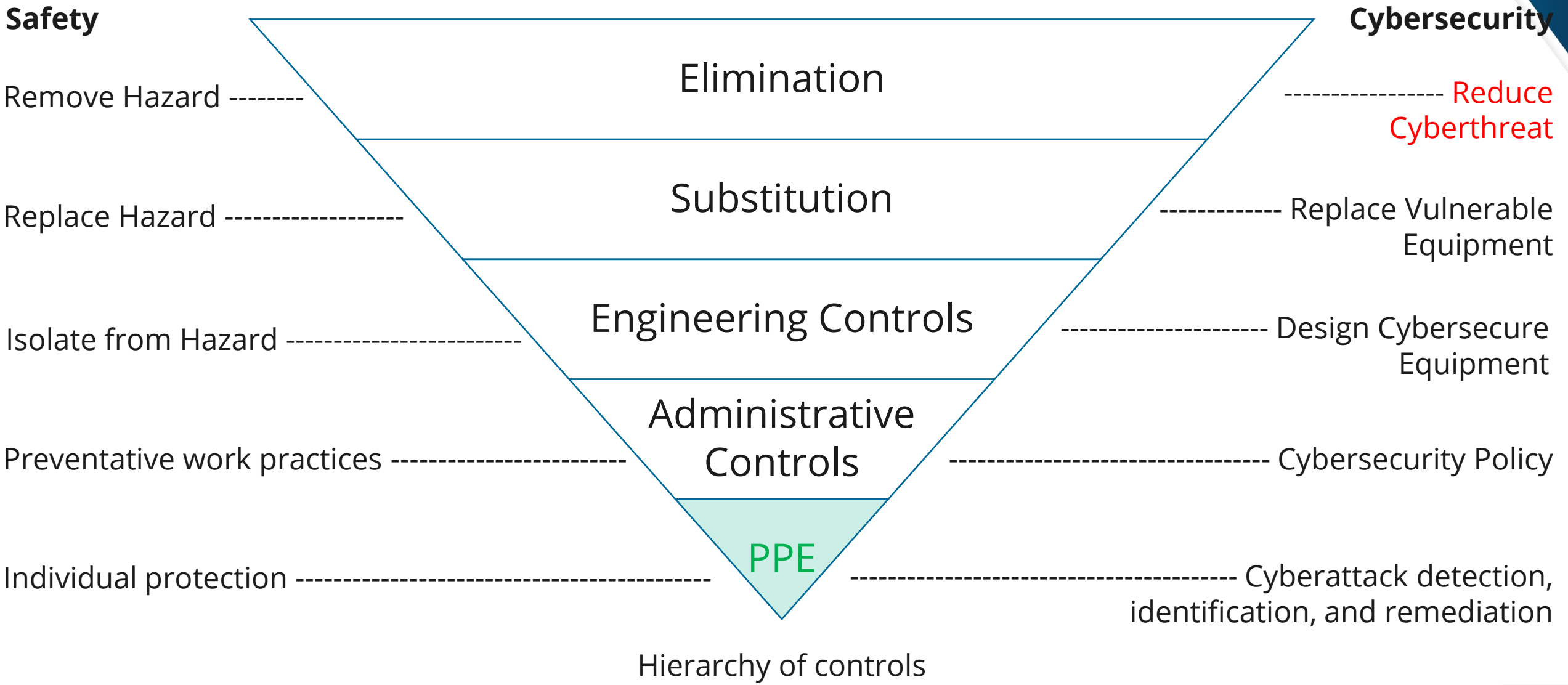
- Do not assume a system or device is attack free
- Do not assume it is impossible to compromise a system
- Authentication, Authorization, and Validation can help with this

Defense-in-Depth Approach

- Add as many layers of protection to the system as reasonable / possible
- If one layer is compromised, backup layers exist stop threats
- Some layers may include: policy, physical, network, application, device

Fundamentals for battery energy storage system cybersecurity

CYBERSECURITY AND THE HIERARCHY OF CONTROLS



Hierarchy of controls

REDUCE CYBER THREATS: PHYSICAL SECURITY

Barriers: Fences, Walls, Gates	Locks	Guards, Visitor Management Processes
Closed-Circuit Television (CCTV), Cameras, Video Surveillance	Alarms, Motion Detectors	Culture of Security, Well-Trained Staff, “See Something, Say Something”
Fire Suppression Systems	Access Cards / Badges (Monitoring, Audits, Tracking)	Proper Lighting, Signage

Physical security controls from [8]

REDUCE CYBER THREATS: PRINCIPLE OF LEAST PRIVILEGE

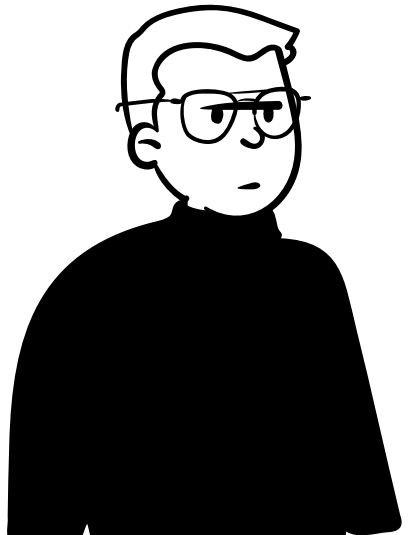
- Users should have the least amount of access required to do their jobs

System Admin
Assigns users minimum permissions required

IT Technician
Granted access only to servers they are in charge of maintaining

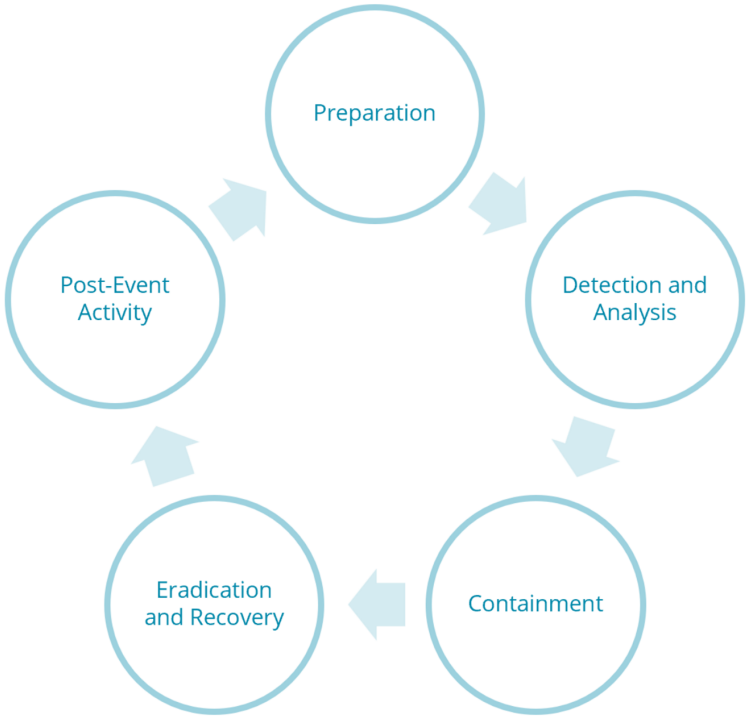
Student Intern
Granted access only to project documents they are working on

Principal Investigator
Granted access to view financial information for projects they lead



REPLACE VULNERABLE EQUIPMENT

- Supply chain considerations: use trusted vendors for hardware, software, firmware
  - Critical control electronics should be scrutinized the most
- Update systems that are out-of-date or have known vulnerabilities
- Perform rigorous software testing before deploying new software
  - Understand software and software dependencies
- Learn from past incidents and fortify systems using lessons learned
  - Have plans in place for responding to incidents (i.e. playbooks)



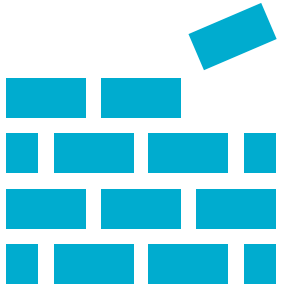
Incident response lifecycle [12]

DESIGNING CYBERSECURE EQUIPMENT: SECURITY BY DESIGN

- Think about security throughout the lifecycle of the project

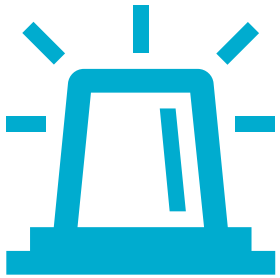
Design

Adopting Policy



Building Product

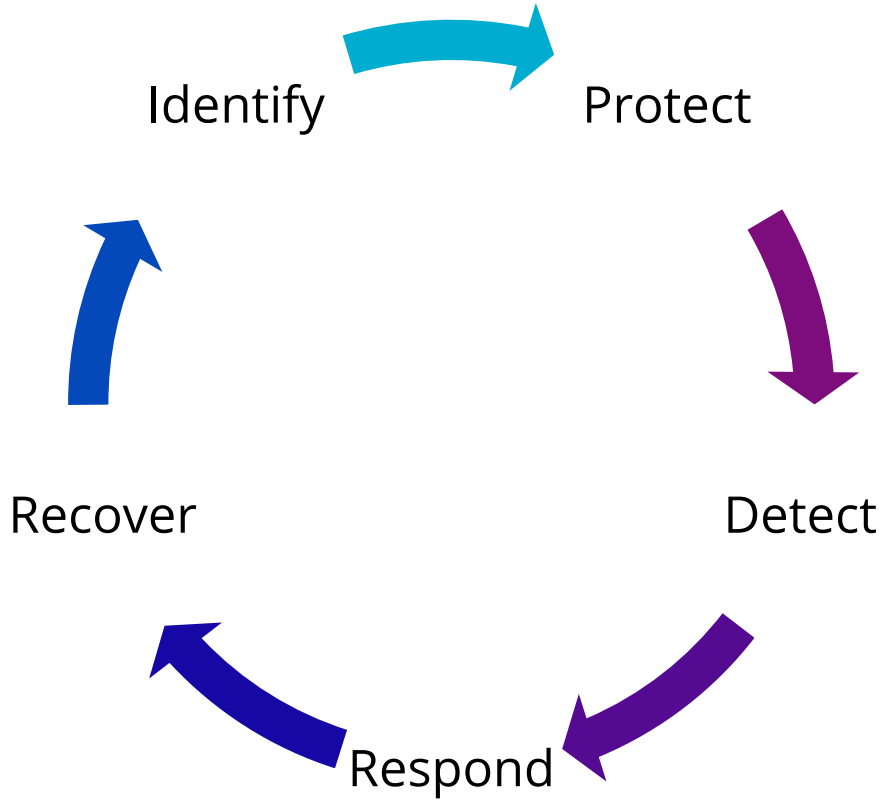
Maintenance



Emergency

Disposal

ADMINISTRATIVE: NIST CYBERSECURITY FRAMEWORK (NIST CSF)



Steps for a strong cybersecurity posture

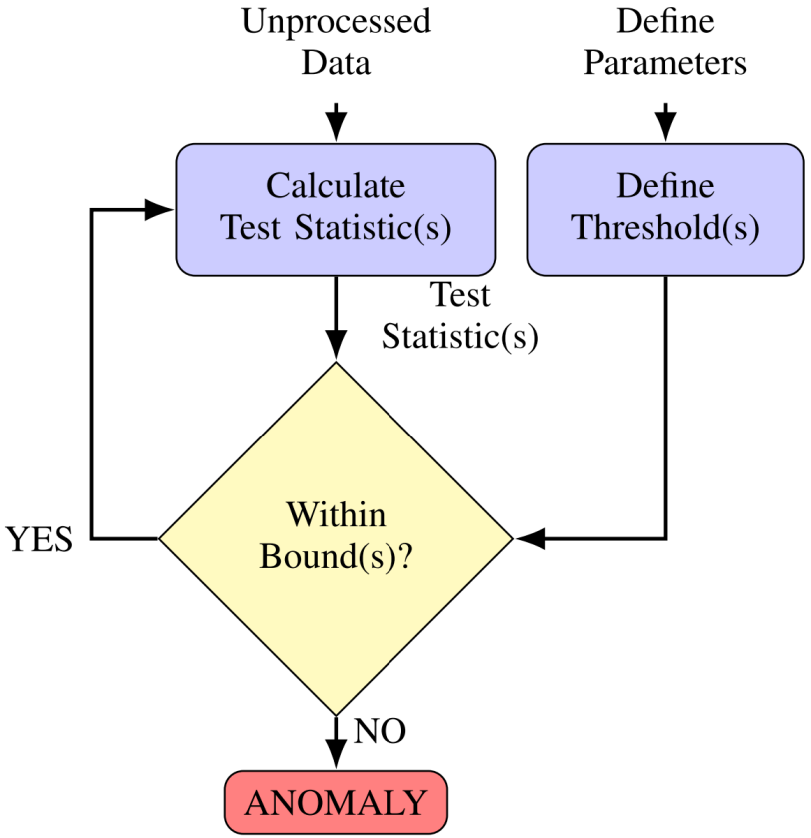
NIST CSF

- NIST: National Institute of Standards and Technology
- Voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risks
- Versatile, commonly implemented
- https://www.nist.gov/cyberframework

INTRUSION DETECTION: THE "PPE" OF BESS

Goal: to repurpose anomaly detection methods and detect FDIAs targeting the sensors of battery stacks, to **increase** the **availability** and **reliability** of grid-connected battery systems [13].

- **Step 1:** Accurate battery model to represent system
- **Step 2:** Estimator to estimate states and measurements
- **Step 3:** Compare estimated measurements to sensor readings, generate residual
- **Step 4:** Residual used by anomaly detector to flag anomalies



General model-based anomaly detector

A STRONG CYBERSECURITY POSTURE – WHAT DO WE NEED?

- **Cybersecurity standards / policy / recommendations specifically for BESS**
- Threat analysis and prioritization for BESS
- **Adding a cybersecurity layer to BMSs and EMSs (working with industry)**
- Learning from cyber events targeting other cyber-physical systems and applying mitigation strategies to BESS
- **Workforce training and development**
- **Intrusion detection systems integrated in BESS**
- Guidelines for securing hardware and software supply chain – China is the largest battery manufacturer and controls most battery raw materials
- Improved battery modeling capabilities
- Secure by design practices
- Constant updating of BESS cybersecurity practices

We need more researchers in this field!

A STRONG CYBERSECURITY POSTURE – IT TAKES ALL OF US!

- Collaborating with cybersecurity experts of different backgrounds
- Staying knowledgeable about known threats inside and outside of your field of study
- Workforce training and encouraging a culture of cybersecurity
- “See something, say something”
- Red teaming, blue teaming, and purple teaming
- **Proactively** implementing cybersecurity best practices

THANK YOU!

For more recommendations on securing critical infrastructure refer to [8] and [14]

ACKNOWLEDGEMENTS

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.

This material is based upon work supported by the U.S. Department of Energy, Office of Electricity (OE), Energy Storage Division.

Special thanks to Rodrigo Trevizan, Yuliya Preger, Jake Mueller, Valerio De Angelis, Irving Derin, Oindrilla Dutta, Armando Montoya, Robert Wauneka, and Mo Kamaludeen.

Victoria A. O'Brien
vaobrie@sandia.gov

REFERENCES AND PHOTO CREDIT

[1] R. D. Trevizan, J. Obert, V. De Angelis, T. A. Nguyen, V. S. Rao and B. R. Chalamala, "Cyberphysical Security of Grid Battery Energy Storage Systems," in *IEEE Access*, vol. 10, pp. 59675-59722, 2022, doi: 10.1109/ACCESS.2022.3178987.

[2] A. Mey and O. Comstock. "Utility-scale batteries are more commonly used for price arbitrage." eia.gov. Accessed: June 18, 2026. [Online.] Available: https://www.eia.gov/todayinenergy/detail.php?id=66164

[3] P. Doherty. "PG&E Shares Findings of September 2022 Moss Landing Megapack Incident." pge.com. Accessed: June 20, 2026. [Online.] Available: https://www.pge.com/en/newsroom/currents/safety/pg-e-shares-findings-of-september-2022-moss-landing-megapack-inc.html

[4] C. Crownhart. "What a major battery fire means for the future of energy storage." technologyreview.com. Accessed: June 6, 2026. [Online.] Available: https://www.technologyreview.com/2025/02/13/1111843/battery-fire-moss-landing-power-plant/

[5] A. Wagner. "Everything you need to know about the 'WannaCrypt' ransomware attack." pbs.org. Accessed: June 21, 2026. [Online.] Available: https://www.pbs.org/newshour/science/everything-need-know-wannacrypt-ransomware-attack

[6] M. Martinez. "Sniper attack on Silicon Valley power grid spurs security crusade by ex-regulator." cnn.com. Accessed: June 21, 2026. [Online.] Available: https://www.cnn.com/2014/02/07/us/california-sniper-attack-power-substation

[7] "Types of Threat Actors." coursera.org. Accessed: June 22, 2026. [Online.] Available: https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/kBG3Z/types-of-threat-actors

[8] V. A. O'Brien, T. M. Kroeger, K. Ruehl, A. Holloway, S. Hossain-McKenzie, K. Davis, M. Bishop, "Containing Cyber Risks on Energy Critical Infrastructure: Effective Practices and Gaps," accepted to *IEEE Security & Privacy*.

[9] United States Attorney's Office. "Former CEO Of Simi Valley Company Guilty Of Bilking Navy By Selling $2.6 Million In Knock-Off Batteries Used On Aircraft Carriers And Subs." justice.gov. Accessed: May 1, 2026. [Online.] Available: https://www.justice.gov/usao-cdca/pr/former-ceo-simi-valley-company-guilty-bilking-navy-selling-26-million-knock-batteries

[10] M. Martina. "Duke Energy to remove Chinese battery giant CATL from marine corps base." reuters.com. Accessed: June 21, 2026. [Online.] Available: https://www.reuters.com/business/energy/duke-energy-remove-chinese-battery-giant-catl-marine-corps-base-2024-02-09/

[11] M. Worry, "NAATBatt Cybersecurity Committee Plan," presented to NAATBatt Cybersecurity Committee, Virtual, Mar. 19, 2026. [PowerPoint Slides.] Accessed: Mar. 19, 2026.

[12] P. Cichonski, T. Millar, T. Grance, K. Scarfone, "Computer Security Incident Handling Guide," National Institute of Standards and Technology, Special Publication 800-61 Revision 2, Aug. 2012. Accessed: Feb.11, 2025. [Online.] Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[13] V. A. O'Brien and R. D. Trevizan, "Scaling Up Online Model-Based Anomaly Detection Methods for Use in Large Battery Stacks: Addressing Challenges in Online Monitoring of Battery Systems," in IEEE Industry Applications Magazine, vol. 32, no. 3, pp. 42-55, May-June 2026

[14] V. A. O'Brien, T. M. Kroeger, K. Ruehl, A. Holloway, S. Hossain-McKenzie, K. Davis, and M. Bishop, "Containing Cyber Risks on Energy Critical Infrastructure: Effective Practices and Gaps," Sandia National Laboratories, Albuquerque, NM, USA.