WHAT DOES SAFETY AND GRID SECURITY MEAN FOR LDES

SAFETY AND GRID SECURITY TIGER TEAM

LEAD, DAN RICCI, IDAHO NATIONAL LABORATORY (INL)
CO-LEAD, HOPE CORSAIR, OAKRIDGE NATIONAL LABORATORY (ORNL)

LDES Safety and Grid Security Recommendations

- Overview of the LDES Challenges as Related to Safety and Grid Security
- Industry & Lab Representation for Safety and Grid Security
- Safety Recommendations
- Security Recommendations
- Next Steps
- Summary

LDES Challenges as Related to Safety and Grid Security

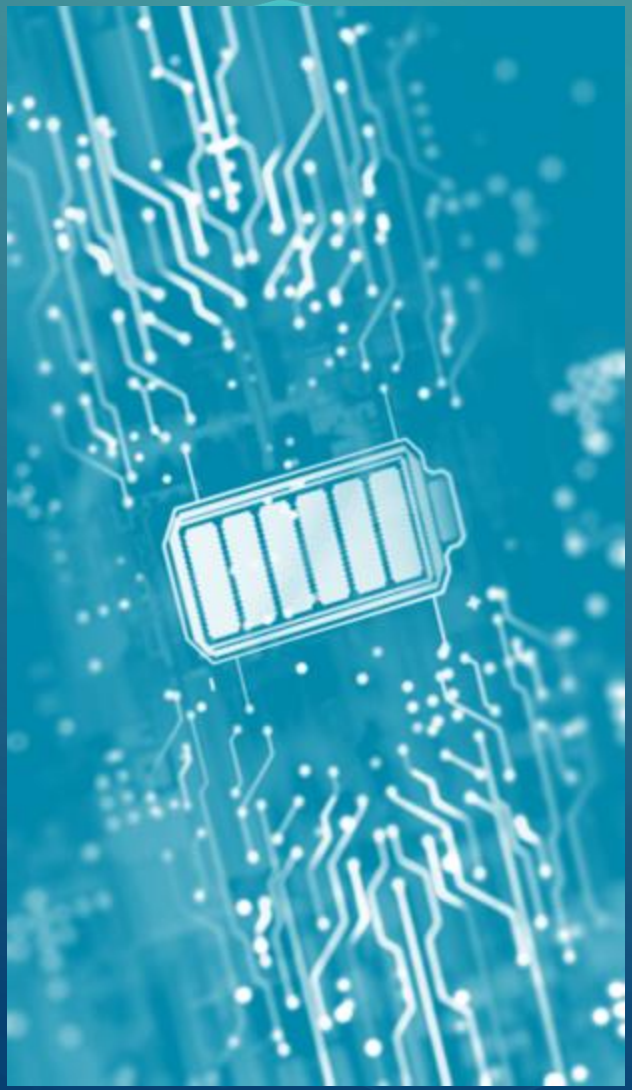
The following two LDES challenges applicable to safety and grid security were identified in DOE LDES Liftoff report: “Pathways to Commercial Liftoff: Long Duration Energy Storage” March 2023.

Identified Challenge #3: The specific needs related to LDES workforce training (i.e., skills and training) are presently not well defined.

Identified Challenge #6: There is presently a lack of resources regarding how to evaluate grid upgrades or expansions that will be necessary to accommodate both new variable renewable generation sites and LDES systems.

Tiger Team reviewed challenges and made recommendations on how to address

Late April/early May was the targeted timeframe for 1st set of draft recommendations



Industry & Lab Representation for Safety and Grid Security

Name	Organization	Role
Steve Willard	EPRI	Safety
Lakshmi Srinivasan	EPRI	Safety
Dr. Davoud Zamani	GridWrap, Inc.	Safety/Security
Eric Ruffel	City Light & Power Engineering, LLC	Security
Alex Dresser	City Light & Power Engineering, LLC	Safety
Karthi Chakaravarty	EarthEn	Safety/Security
Manas Pathak	EarthEn	Safety/Security
Jesse Hoffman	Energy Systems Group LLC	Safety
Daniel Dalpiaz	Infineon Technologies Americas Corp	Safety/Security
Kraig Bockhost	Infineon Technologies Americas Corp	Safety/Security
Steve Baxley	Southern Company	Safety
Kieran Claffey	Southern Company	Safety
Matthew Millard	CapyBara Energy	Industry Advisor/ Safety
Huiyi Jackson	Edison Electric Institute	Safety
Kaitlin Brennan	Edison Electric Institute	Security
Kristine Martz	Edison Electric Institute	Safety
William Pfister	Edison Electric Institute	Safety
Mitch Zafer	Coffman Engineers, Inc.	Safety/Security
Elias Greenbaum	GTA, Inc.	Safety
Pejman Kazempoor	University of Oklahoma	Security
Owais Amin	e-zinc	Safety/Security
Loraine Torres-Castro	Sandia National Laboratory (SNL)	Safety
Chris O'Reilley	Oakridge National Laboratory (ORNL)	Security
Jackie Huynh	Pacific Northwest National Laboratory (PNNL)	Safety

SAFETY CHALLENGES & RECOMMENDATIONS

Challenge 3: Safety Recommendations 1

3-1. Recommendation: Develop and implement safety and standards specifically for LDES technologies that can incorporate existing National Fire Protection Association (NFPA) 855, Standard for the Installation of Stationary Energy Storage Systems (2023) and International Fire Code (ICC) 2018. This will ensure that they are efficient and effective for training workforces for current and future LDES technologies.

3-1. Rationale: The NFPA 855, while providing mandatory requirements for safety strategies and features for safety strategies and features of energy storage systems, does not specifically address the unique safety considerations of LDES technologies. Similarly, the International Fire Code 2018 while encompassing a broad range of fire safety regulations, does not specifically address LDES. By developing and implementing safety regulations and standards specifically for LDES, we can ensure that the workforce is adequately trained and prepared to safely operate and maintain LDES systems.

3-1. Recommendation Recipients: This recommendation would be implemented by international standards organizations such as the International Code Council (ICC), which oversees the International Fire Code and National Fire Protection Association (NFPA), which oversees the NFPA 855. Additionally, safety standards organizations, regulatory bodies, and industry stakeholders involved in the development, implementation, and enforcement of safety regulations and standards for energy storage systems would also play a crucial role in implementing this recommendation.

Challenge 3: Safety Recommendations 2

3-2. Recommendation: Subsea LDES electrolytic hydrogen production and storage systems are the safest approach to gigawatt-scale clean hydrogen. All unit operations needed for subsea electrolytic hydrogen production and storage are already being performed by the workforce of the offshore gas and oil industry, albeit in different contexts. A testing and engineering company should be tasked with constructing a pilot scale system.

3-2. Rationale: Subsea hydrogen LDES systems are fire and explosion proof. Combustible oxygen is not accessible. The hazards of above-ground PEM electrolyzer hydrogen production and storage systems are documented. Brophy has provided guidance for a category of electrolyzers that are needed: "Electrolyzers need to live outside. Equipment that is designed with its own all-weather enclosure and that solves the hazardous area classification, ventilation and safety issues within its own footprint is enormously valuable."

3-2. Recommendation Recipients: State and federal funding agencies, investors, energy developers, EPC companies.

Challenge 3: Safety Recommendations 3

3-3. Recommendation: Develop a comprehensive LDES workforce training program that includes specific modules and certifications on the safe installation and maintenance of battery storage cabinets. These modules should emphasize the importance of adequate spacing between cabinets to reduce the risk of DC arch flash, ensure efficient cooling, and facilitate accessibility for maintenance.

3-3. Rationale: The safe operation of LDES systems requires a well-trained workforce that understands the specific risks associated with these systems and how to mitigate them. By including modules and certification on the safe installation and maintenance of battery storage cabinets in the training program, we can ensure that the a qualified workforce is equipped with the necessary skills to reduce risks and ensure the efficient operation of LDES systems.

3-3. Recommendation Recipients: The DOE should take the lead in coordinating development of specific modules on the safe installation and maintenance of battery storage cabinets used in LDES technologies. National Laboratories and private sector companies developing and manufacturing LDES technologies would develop the best practices for installations and maintenance of LDES systems. Their real-world experience would ensure the training modules are relevant and effective. Technical colleges and trade schools would be responsible for integrating these training modules into their curriculum. They would work closely with the National Laboratories and other stakeholders to ensure the training program is comprehensive and up to date. Industry associations such as American Clean Power (ACP) can help disseminate these training modules to their members. They can also provide industry insights and feedback to help refine the training program.

Challenge 6: Safety Recommendations 1

6-1. Recommendation: Invest in research and development for advanced, climate-controlled housing for integrated electrolyzer Hydrogen production and storage systems that prioritize safety.

6-1. Rationale: Hydrogen production and storage present explosion and fire hazards, necessitating advancements in technology and safety measures. Climate-controlled housing for integrated electrolyzer Hydrogen production and storage can mitigate these risks, ensuring safe and efficient operations.

6-1. Recommendation Recipients: This recommendation would be implemented by energy regulatory bodies, research institutions, and industry stakeholders involved in the development of and implementation of Hydrogen production and storage technologies. This includes the Department of Energy (DOE), and the National Laboratories, and other relevant international standards organizations.

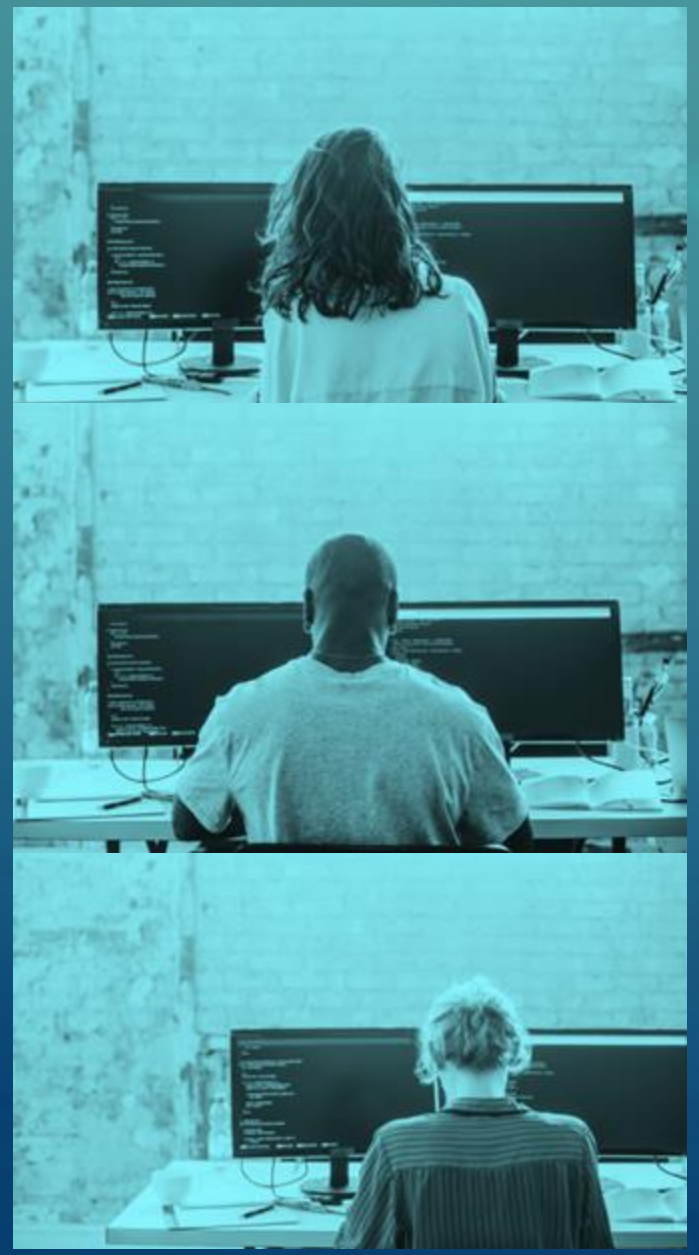
SECURITY CHALLENGES & RECOMMENDATIONS

Challenge 3: Security Recommendations 1

3-1. Recommendation: Establish a dedicated working group or task force to develop a comprehensive LDES workforce training program for both operators and security professionals, with strong emphasis on LDES security certification. This program should provide clear guidelines on the necessary skills and training for certifying the workforce to ensure the security of the storage systems and protect the connection to grid-connected power generation resources (e.g., Distributed Energy Resources)

3-1. Rationale: As the energy landscape evolves towards a multitude of grid-connected power generation and connected storage systems, grid security becomes increasingly critical. A dedicated work group or task force can develop a robust certification training program that equips the qualified workforce with the necessary skills to ensure LDES security when connecting to the grid, thereby addressing the current lack of definition in workforce LDES security training needs.

3-1. Recommendation Recipients: The Department of Homeland Security, Critical Infrastructure Security Agency (CISA) and National Institute of Standards and Technology (NIST) can provide oversight and ensure that the training program aligns with existing and future grid security guidelines for LDES integration with renewable energy generation as a distributed energy resource in the grid. National laboratories, and private sector companies together through trade associations such as American Clean Power (ACP) can provide research support and resources, ensuring that the security certification training program stays up to date with the latest industry trends and technologies.

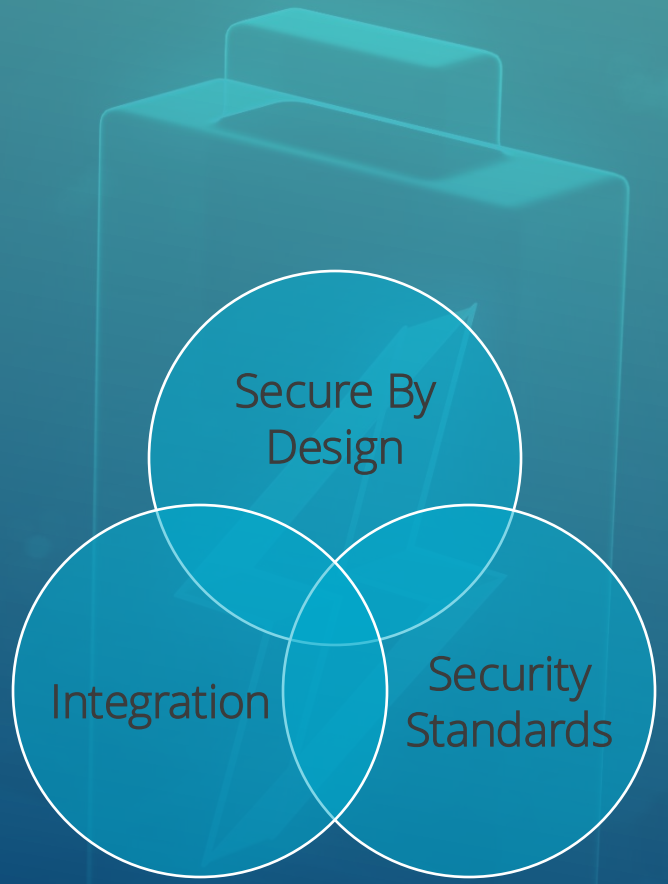


Challenge 6: Security Recommendations 1

6-1. Recommendation: Prioritize the development of comprehensive guidance through NIST standards that address grid security vulnerabilities such as standards applicable to the LDES system manufacturers/vendors or to those purchasing, implementing, using, maintaining that will be integrated with the grid as part of the LDES systems integration. This is particularly crucial as we transition from a few centralized power generation sites to a multitude of grid-connected renewable power generation and storage systems.

6-1. Rationale: The traditional utility model, with SCADA systems and controls, is currently designed to manage a limited number of generation sites and key nodes within power distribution systems. However, the shift towards advanced metering, distributed renewable energy resources, and LDES systems significantly increase the number of data sources required for successful operations. This increase in data needs and uses introduces new vulnerabilities. As such, it's crucial to develop recommended cyber and physical security technical guidelines for LDES security configurations across the ecosystem of distributed energy resource components connected to the grid, with emphasis on LDES systems. Furthermore, the interdependence between hardware, software, and firmware in these systems necessitates a holistic approach to developing interoperability requirements.

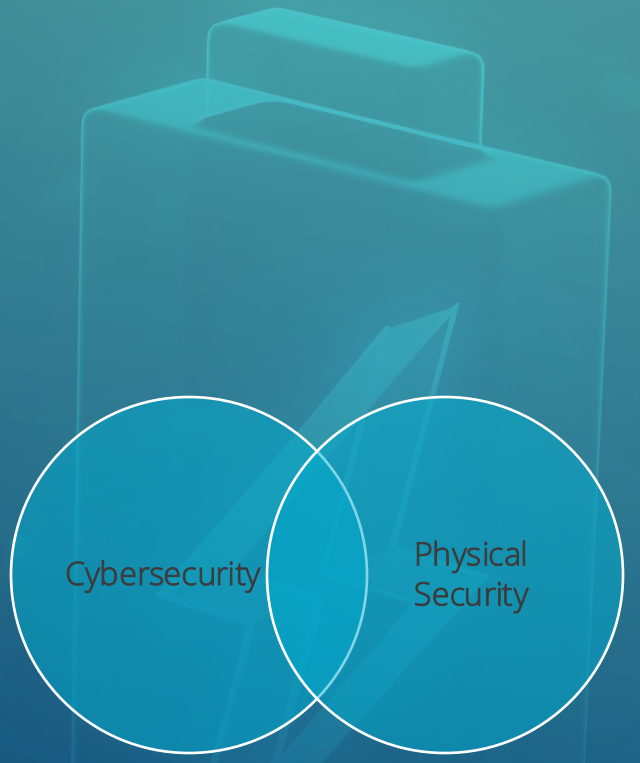
6-1. Recommendation Recipients: This recommendation should be implemented by a standards group, such as IEEE and NIST, that is responsible for developing technical requirements for both hardware, software, and firmware. These groups should work in tandem to ensure that hardware, software, and firmware are developed together for LDES and other storage systems. Key recipients would include LDES technology developers, , research institutions like the National Laboratories, and industry stakeholders involved in the development and implementation of grid upgrades, expansions, and cybersecurity measures.



Challenge 6: Security Recommendations 2

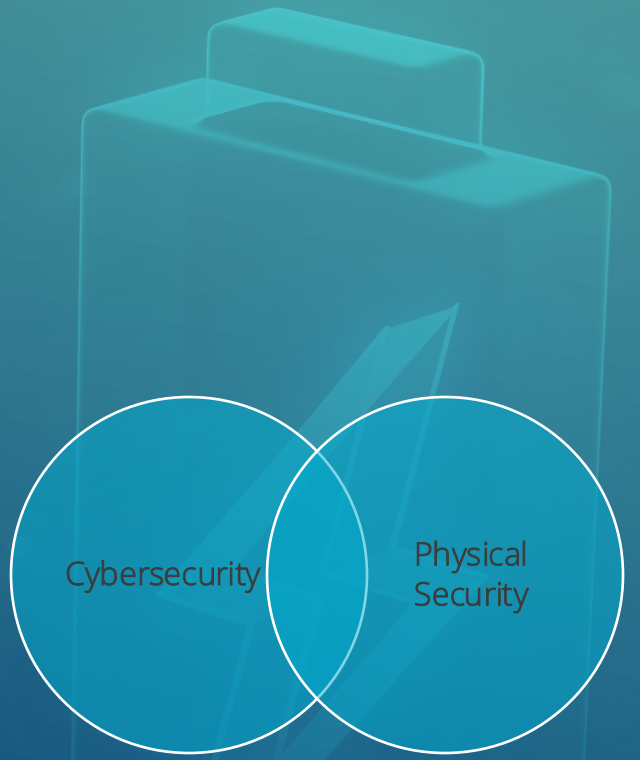
6-2. Recommendation: Develop cybersecurity and physical security guidance documentation for interconnecting LDES with the grid that encompasses a variety of use-case scenarios such as:

- Use case 1: Grid-scale energy storage for seasonal load balancing. In this scenario, a large-scale LDES is interconnected to the grid to provide seasonal load balancing services. The LDES charges during the time of low electricity demand and discharges during periods of high demand.
    - Cybersecurity guidelines: The control system of the LDES needs to be secured against unauthorized access and potential cyber-attacks. This includes securing local and remote access over different communication transmission paths, implementing strong authentication, secure protocols, and maintaining system updates to address vulnerabilities.
    - Physical security guidelines: The physical infrastructure of the LDES, including the energy storage unites and control system, needs to be secure against unauthorized access, theft, vandalism, and natural disasters. This could involve perimeter fencing, video surveillance systems, locks, tamper switches, and disaster-resistant construction methods.



Challenge 6: Security Recommendations 2

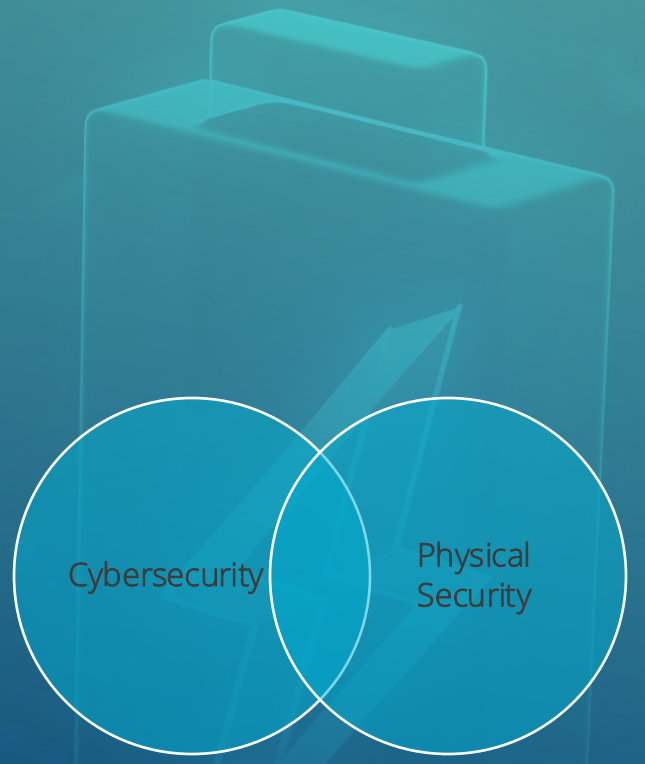
- Use case 2: Emergency backup power for critical infrastructure. In this scenario, a LDES is interconnected to grid and provides emergency backup power for critical infrastructure such a hospital connected to distributed energy resources. The LDES charges continuously from distributed energy resources and provides emergency backup power in the event of a grid outage.
    - Cybersecurity guidelines: The LDES control systems need to have robust cybersecurity measures in place in when directly connected to the critical infrastructure (e.g., public utilities, food, transportation, healthcare, emergency services). This includes intrusion detection systems, regular system audits, incident response plans, and disaster recovery plans for potential cyber-attacks.
    - Physical security guidelines: The LDES needs to be physically secured to ensure it can provide reliable backup power. This includes securing the energy storage units against tampering and ensuring the control systems are contained within secure locations.



Challenge 6: Security Recommendations 2

- Use case 3: Renewable energy integration in this scenario, LDES is used to supplement the intermittent power supply from a wind farm or solar power plant. The LDES charges when there is excess power production and discharges when the production is low.
  - Cybersecurity guidelines: The LDES control system security will be focused on securing against cyber-attacks that would disrupt the balance of power supply and demand. Security measure to be taken include restricting access through a multi-tiered firewall perimeter between the wind farm or solar power plant control systems and the LDES.
  - Physical security guidelines: The physical infrastructure of the wind farm or solar power plant and the LDES need to be protected against unauthorized access and ensure equipment cannot be tampered, damaged, or destroyed. Preventive measures include high fence perimeter and locked gate(s), vegetation management along fence lines, inspection of fence integrity, monitored video surveillance, locked enclosures for control system equipment, and access control system monitoring of LDES facility.

This documentation should consider such scenarios involving the grid, DERS, coupled with LDES technologies.



Challenge 6: Security Recommendations 2

6-2. Rationale: LDES systems are dependent on digital communication systems to be responsive to LDES technologies connected to the grid, and as such, should meet cybersecurity and physical security requirements while providing energy and supporting LDES availability. Different scenarios may require different approaches to transmission and distribution, and a understanding how digital communications is configured for each. Understanding these dynamics will help develop security guidelines that leveraging existing assets and supporting integration of new LDES technologies.

6-2. Recommendation Recipients: DOE and National Laboratories should take the lead in developing recommendation. The DOE has the authority and the National Laboratories have the expertise to develop security guidelines. Additionally, private sector companies and other research institutions involved in the development and operation of LDES systems can provide practical insights and feedback, ensuring the guidance documents are feasible and effective in real-world scenarios.

Challenge 6: Security Recommendations 3

6-3. Recommendation: Develop a Change Configuration Management plan for asset owners/operators specifically for LDES systems. This plan should include a structured process for documenting and tracking software updates and maintenance activities, particularly those related to inverter software changes and updates that impact battery performance.

6-3. Rationale: Software updates, particularly those related to inverter software, can significantly impact the performance of current battery energy storage systems (BESS), and may impact battery technology used in LDES systems. Without proper documentation and tracking, asset owners/operators may not be aware of these changes, which can lead to unexpected issues and make troubleshooting more difficult.

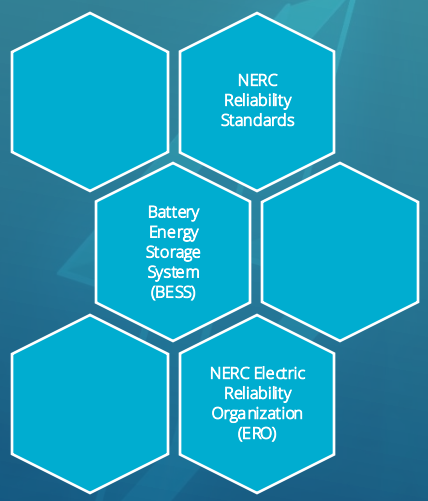
6-3. Recommendation Recipients: NIST could be key standards bodies that could provide oversight and support for the implementation of a change configuration management plan in the NIST SP 800-82 - Guide to Operational Technology (OT) Security. The National Laboratories could contribute their research expertise and resources to the development of the plan, which could include working with private sector companies to develop standard software bill of materials (SBOMS) for LDES technology. Private sector companies that manufacture, install, and maintain LDES systems would be crucial in assisting asset owners in implementing the change configuration management plan in their operations. They could further provide insight and feedback to help refine plans, ensure they are effective in real-world operations.

Challenge 6: Security Recommendations 4

6-4. Recommendation: Participate in existing or establish efforts to analyze existing NERC Reliability Standards against documented reliability risk to the Bulk Electric System from Battery Energy Storage System (BESS) to determine where regulatory enhancements such as NERC Standards projects, and BES Definition Review, are necessary to reduce security risks. Note that distribution side BESS are not within NERC's jurisdiction and would not be subject to compliance with the NERC CIP Standards.

6-4. Rationale: The NERC ERO has developed disturbance reports, alerts, guidelines, etc. that highlight that abnormal inverter-based resource (IBR) performance issues post a significant risk to bulk power system (BPS) reliability. In November 2022, FERC directed NERC to identify and register owners and operators of currently unregistered bulk power system connected IBRs. NERC established a work plan to address the order that includes consideration for determining which reliability standards (including those specific to security) should become applicable to the newly registered IBRs. Since the NERC CIP Standards are not applicable to BESS today, it would be relevant to perform an analysis of security risk against existing NERC CIP Standards. This may not need to be a standalone initiative for this group. It may be participation in ongoing work led by NERC and industry.

6-4. Recommendation Recipients: FERC, NERC, BESS Asset Owners.



Challenge 6: Security Recommendations 5

6-5. Recommendation: Analyze existing interconnection requirements and revise them to include minimum security requirements for BESS.

6-5. Rationale: Studies have shown that increases in inverter-based resources, in the absence of synchronous machine-based solutions, need grid forming (GFM) IBRs such as LDES. The cybersecurity risk to the power system increases significantly when extending communications to IBR and Distributed Energy Resources (DER) devices because of the increased number of devices connected to the utility supervisory control and data acquisition (SCADA) network. In addition, SCADA control signals may be issued over public internet channels instead of using traditional dedicated telecommunications lines. While there are existing cyber security guidelines and standards that could be used to enhance grid security such as Institute of Electrical and Electronics Engineers (IEEE) standards: IEEE 1686, IEEE 2030.5, IEEE P2800, and Underwriters Laboratories (UL) 1741, and others, they are often not included in interconnection agreements.

6-5. Recommendation Recipients: Standards groups developing cyber security certifications for IBRs and DERs, State Regulators, FERC, NERC, BESS Asset Owners.

Next Steps

- Safety and Grid Security Tiger Team developed four additional challenges with recommendations focused on:
  - Addressing the lack of comparative studies on the safety of each LDES type or category and the gaps in the safety testing, etc, in emerging LDES technologies and unique battery chemistries and thermal energy storage. We need a common framework and language to discuss and compare.
  - Safety standards and testing have not been developed yet for emerging technologies, e.g., UL testing.
  - Need to update the codes and standards (NFPA 855, NEC70, IFC, etc.) to consider different types of LDES technologies. Examples of LDES technologies that codes and standards do not consider currently are:
    - Flow Battery: vanadium flow, iron flow battery, zinc aqueous, hydrogen
    - Mechanical storage: Gravity (pump hydro), kinetic (spin)
    - Thermal storage: Molten salt, compressed air
  - Addressing the different safety needs to develop based on the type of LDES such as safety for hydrogen sensors, safety shut-off valve, and different egress, fire suppression systems, and PPE when compared to Li-Ion batteries for specific types of LDES technologies.

Summary

Safety and Grid Security Tiger Team has developed and submitted LDES recommendations for following challenges:

- **Challenge #3**: The specific needs related to LDES workforce training (i.e., skills and training) are presently not well defined.
- Safety: 3
- Security: 1

- **Challenge #6:** There is presently a lack of resources regarding how to evaluate grid upgrades or expansions that will be necessary to accommodate both new variable renewable generation sites and LDES systems.
- Safety: 1
- Security: 5

Submission of four additional challenges and recommendations are to be submitted to LDES Consortium and DOE in September.

THANK YOU!