CHAPTER 18
PHYSICAL SECURITY AN D CYBERSECURITY OF ENERGY STORAGE SYSTEMS

Jay Johnson, Jeffrey R. Hoaglund, Rodrigo D. Trevizan, Tu A. Nguyen, Sandia National Laboratories

Abstract

Energy storage systems (ESSs) are becoming an essential part of the power grid of the future, making them a potential target for physical and cyberattacks. Large-scale ESSs must include physical security technologies to protect them from adversarial actions that could damage or disable the equipment. Many grid-support applications require ESS equipment to coordinate with other grid operators, devices, or systems, which need reliable, cybersecure communications. These networks must be designed for high availability, confidentiality, and integrity to provide grid operators with effective ESS control and monitoring functionality. This chapter presents risks and consequences of physical and cyberattacks as well as current research, standards, and industry best practices.

Key Terms

Cybersecurity, cybersecurity codes and standards, distributed energy resources (DER), physical protection system (PPS), physical security, security risks, threats

1. Introduction

As the penetration of energy storage systems (ESSs) increase and grid operators place more reliance on ESS functionality, it becomes critical to protect those assets from physical or cyberattacks to maintain grid reliability and continuity of service. These threats may manifest themselves in different ways. A range of kinetic attacks may employ vehicles, handguns, rifles, pipe bombs, or other attack vectors. Cybersecurity attacks exploit vulnerabilities in communications or control systems to disrupt system operations or execute malicious actions. With the advent of distributed energy resources (DER), which include consumer-owned small ESSs often connected to public networks, the attack surface has greatly increased.

This chapter presents an overview of topics related to ESS physical security and cybersecurity. To highlight the importance of these areas, this first section presents background information on security aspects of ESSs. Section 1.2 describes recent incidents involving security of power grids. Section 2 summarizes the current state of the art of ESS physical security, including current practices, best practices and standards, and future trends. Section 3 presents an outline of ESS cybersecurity.

1.1. Basic Definitions

Availability is the capacity of an information system to ensure “timely and reliable access to and use of information.” [1]

Confidentiality, often used as a synonym of privacy, refers to the preservation of “authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.” [1]

Cybersecurity is defined as the “prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.” [2] Cybersecurity, also referred to as information security, has the objective of providing information confidentiality, integrity, and availability to information systems. [1]

Information integrity “means guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.” [1]

Physical security is defined as a “combination of physical protective measures and security procedural measures employed to safeguard personnel, property, operations, equipment, facilities, materiel, and information against loss, misuse, theft, damage, or destruction by disaffected persons (insiders), vandals, activists, extremist protesters, criminals (individuals and organized groups), terrorists (domestic, state-sponsored, and transnational), saboteurs and spies.” [3]

Risk is a “measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” [4]

Threat is “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.” [4]

Vulnerability is a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.” [4]

1.2. Notable Physical and Cyberattacks to Power Grid Infrastructure

Electric grid infrastructure is a fundamental asset to modern society. Disruptions to the power grid can affect multiple sectors, including industry, government, security forces, and others. Therefore, attacks to the power grid can serve as a proxy to indirectly disrupt targets that are vulnerable to power interruptions. With the growing importance of ESSs to the grid, it is necessary to protect these assets from physical and cyberattacks.

There have been multiple notable attacks to power grid infrastructure:

- In 2005, a rifle attack on a transformer caused oil tank leakage at a Progress Energy substation in Florida, leading to an explosion and a local power outage [5].
- In 2013, an individual in Arkansas carried out a series of attacks on unprotected grid infrastructure. In the first attack in the series, the person tried to bring down a transmission tower by removing bolts from the base of the tower and attempting to attach a cable to a moving train. Later that year, the same individual set fire to a switching station and used a tractor to bring down two electric poles [6]. In total, the acts of sabotage caused over $4.5 million in damage and interrupted power service to about 9,000 people [7].

- Also in 2013, snipers shot 17 power transformers and cut communication cables from the Metcalf Transmission Substation near San Jose, CA [8]. Pacific Gas and Electric operators quickly responded to this attack which caused little interruption of service to Silicon Valley. The perpetrators remain at large and the reason for the attack remains unknown, but the Metcalf incident has raised awareness for physical security of power grids, including new North American Electric Reliability Corporation (NERC) standards [9] and state legislation [10].

Cyberattacks to the power grid have also occurred:

- In December 2015, a coordinated attack on three Ukrainian regional power distribution utilities remotely disconnected seven substations, causing a power outage that affected approximately 225,000 customers [11]. The perpetrators also took actions to make operators unaware of the situation and to hinder system restoration.
- Another cyberattack outage happened in 2016 in Ukraine [12]. This time, the attack was launched in a much more automated manner using the sophisticated malware, *Crash Override*. The malware targeted multiple power transmission control systems in an to attempt to create a sequence of events leading to a catastrophic outcome:
    1. Remotely opening circuit breakers to cause power outages and then exploiting a vulnerability of protective relays to disable overload or fault protection capabilities.
    2. As a result, following manual service restoration, the system would be unprotected, which could result in permanent damage to transmission devices due to uncleared power line faults.
    3. This would lead to a sustained and large-scale power interruption.
    4. Due to lack of knowledge about the target systems by the threat actors, the sequence of events did not take place [13]. The attack was more ambitious than the previous year’s, but it failed to cause as much disruption.

In 2018, it was reported that control rooms of US power utilities have been targets of cyber intrusions [14]. Even though no attacks were performed, these intrusions are thought to be part of a reconnaissance operation. More recently, a Denial-of-Service (DoS) attack on an unpatched firewall led to loss of visibility of 500 MW of generation assets in the United States [15]. The affected power company experienced intermittent service due to frequent reboot of the firewall, which ended after a patch was applied. These incidents show the difficulty in adopting and maintaining cybersecurity defenses for grid operators, generator managers, and other power sector actors.

2. Current State of ESS Physical Security Technology

2.1. ESS Physical Layout

ESSs are composed of several devices that can pose a safety hazard or capital loss if damaged or operated incorrectly (refer to Chapter 20. Safety of Electrochemical Energy Storage Devices for hazards related to batteries). In addition to that, threat actors might be interested in stealing valuable objects or even damaging or disabling ESSs to cause damage to assets or disrupt the continuity of power service. Therefore, adopting best practices for the physical security of ESSs is important to ensuring these systems fulfill their role in improving power grid reliability.

Depending on application, size, technology and space constraints, ESSs might be installed inside buildings dedicated for the system, occupy one or more rooms of a larger building, or be housed in weather-proof enclosures. Grid-scale battery ESSs (BESSs) and flywheels are typically composed of several shipping container-sized modular units. The enclosure of a flow battery composed by two containers is shown in Figure 1 and Figure 2. Indoor ESSs commonly comprise components mounted in industrial racks housed in dedicated rooms.

The ESS housing provides protection from the elements, means for controlling physical access and thermal management for the battery racks, power conversion systems, and other ESS components. Batteries must be protected from the elements and they must operate under controlled conditions. For some technologies, such as lithium-ion, grid-scale ESSs represent a fire hazard, therefore, these systems are often equipped with fire suppression systems and appropriate fire-resistant enclosures. Flywheels typically do not pose chemical fire hazards, however, containment of rotor or bearing failures can be challenging. For more details, refer to Chapter 7: Flywheels.

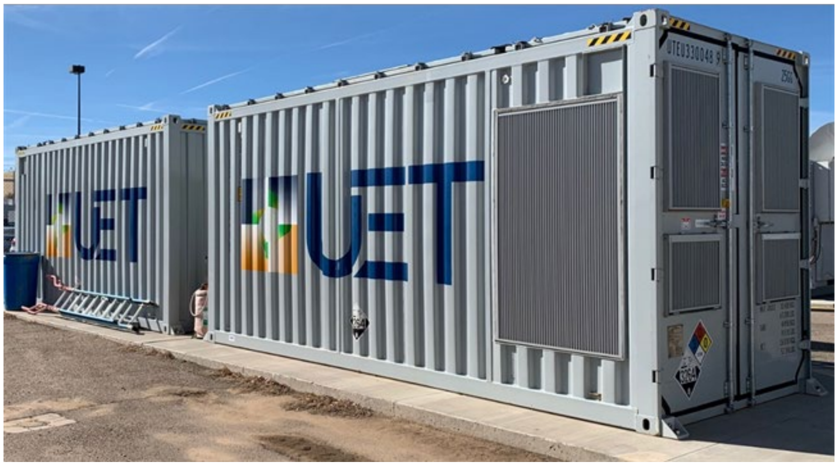

Figure 1. Flow battery at Sandia's Energy Storage Test Pad

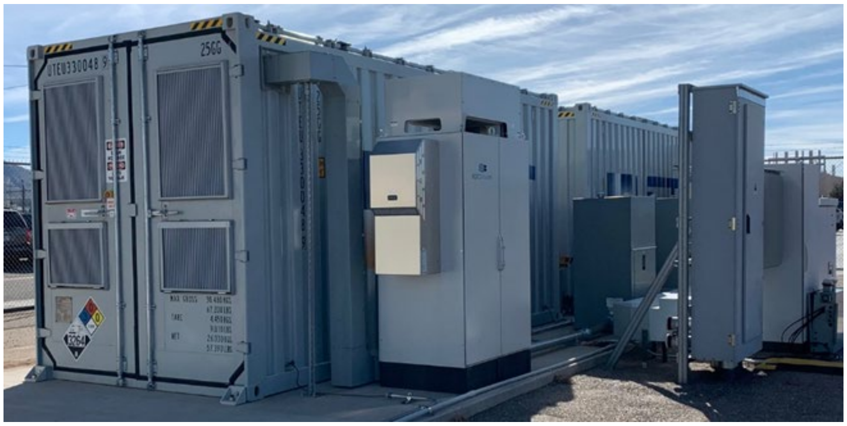

Figure 2. Flow battery containers and enclosures of the power conversion system at Sandia's Energy Storage Test Pad

Siting modular grid-scale ESSs may require significant space and access to medium or high voltage power systems. These systems may be located inside or outside of the fenced or walled area of a substation. Placement, clearance, and fencing of these structures can be impacted by local building codes. Due to fire and gassing risks, indoor BESSs are typically subject to more stringent regulations and size limitations [16]. Outdoor enclosures are installed over a foundation, such as a concrete pad, and secured in place with mechanical (stud anchor) or adhesive (e.g. epoxy-glued bolts) bonds. Buried conduits or wiring gutters protect all cabling, such as communications, main power, and auxiliary power circuits.

Most large-scale compressed-air energy storage (CAES), pumped hydroelectric storage (PHS) and some thermal energy storage (TES) technologies have to be sited on areas with adequate geographical features; unlike BESSs or flywheels, which are typically modular and can be installed mostly without these limitations. CAES and PHS usually comprise reservoirs and a powerhouse. CAES technology requires very large spaces (such as salt caverns) to confine the compressed air (often natural gas), while PHS requires at least two water reservoirs at different elevations. The powerhouse, or compression and power generating facility, is typically a building that houses the compressors, turbines, and power generators employed to store and recover energy from the reservoir. TES systems require a heat source; however the type of heat source will put constraints on their siting. For example, ESSs using a solar tower have a very large footprint and are typically sited in sunny locations. Systems that use a heat pump and engine have fewer siting constraints.

Security and safety risks inherent to ESS make it necessary to implement physical access controls. For outdoor systems, locks, padlocks, doors, walls, gates, and fences are the customary means of avoiding unauthorized entry. Indoor systems are sited where access is restricted by locked doors. ESSs co-located with substations benefit from other security systems, such as thermal cameras, movement sensors, and video surveillance.

2.2. Physical Security Practices

The objective of the physical protection system is to prevent sabotage resulting in damage to an asset, theft of valuable resource, loss of service or, in the worst-case scenario, an electric grid system cascading failure. The physical protection system is designed to provide timely detection and assessment using various sensing methodologies, followed by a delay to threat actions so that it can complete an adequate threat neutralization or system loss mitigation. In many cases, an ESS is located in a rural environment or at a remotely operated location which impacts the effectiveness of any physical protection system, most notably the response interrupting and neutralizing an adversary. Any effective physical security system contains three equally important components: detection, delay, and response. Additional components of an effective protection strategy should include layered access controls and a risk mitigation plan in case of successful attacks. Ideally, all ESS installations would contain the following components to protect their physical structure:

- **Detection and Assessment.** Detection and assessment for both the outer perimeter and the inner security area of the site may contain fence vibration sensors with either fixed or pan-tilt-zoom video cameras for assessment and surveillance. Some more critical facilities employ passive or active infrared sensors, microwave sensors, or other well-established detection methodologies and camera systems with enhanced modalities such as thermal or infrared. The employment of certain technologies is dictated by existing terrain, weather extremes, facility size and location, facility criticality, facility proximity to an effective response force, and other factors. The exterior of certain vital areas, such as a control house, transformer area, HVAC control building, or battery storage areas, may also have interior motion sensor and fixed cameras.
- **Passive Delay.** A perimeter delay is usually accomplished with a chain link fence with vehicle and personnel gates. In some cases, vehicle barriers such as aircraft cable interwoven into the fence fabric or internal vehicle barriers may provide an additional delay. Typically, the only internal delay in the secure area is the actual distance across the area (time it takes to traverse on foot or in a vehicle) from the perimeter to the vital target area. These barriers offer minimal delay for intruders travelling on foot, typically about 30 seconds. For vehicle penetrations, depending on the crash rating of the barrier system, the layered barriers can be more effective than non-layered barriers. These barrier systems are easily breached, however, through the use of hand and/or power tools. Vital area delays typically consist of the construction of the structure (reinforced concrete vs. wood framing and sheetrock) and hardened security doors. Depending on the breaching method, wall or ceiling construction and security doors offer minimal delay – about 30 seconds. Once inside a control house or vital area structure, there are few if any barrier systems; therefore, the only remaining delay would include adversary task time (e.g., placing and detonating explosives).
- **Response.** For remote locations in rural areas, there is typically no on-site response force capable of interrupting and neutralizing an adversary. These locations rely on an off-site response force consisting of one or two local law enforcement (city police, state police, local county sheriff deputies) with hand-held firearms and response time dependent on dispatch communication times and distance of law enforcement patrol to the location (which can be many miles). For those locations with an on-site security team, these personnel must comply with state and local weapon laws and are typically armed with only submission or active body control devices or a side-arm. Therefore, the probability of an armed response interrupting and neutralizing an adversary attack is unlikely.
- **Access control.** Access controls at the outer perimeter personnel gates are dependent on facility size and location, facility criticality, facility proximity to an effective response force, and other factors. Most smaller facilities control access through security padlocks and chain link fences at vehicle or pedestrian gates; whereas larger or more critical substations or facilities typically employ a badge/card swipe device and may have the

additional security measure of an access PIN associated with the badge/card. Access controls at the outer perimeter vehicle gate usually consist of a chain and padlock security the gate. At smaller facilities, access controls are typically limited to door locks. Although these security access controls may comply with current industry security standards, they are typically considered ineffective against a trained adversary.

- **Mitigation.** Mitigation and resiliency, while not part of the physical security strategy, are vital components of the continuity of operations be it from a malevolent act or an act of nature. If there is a successful attack at an ESS facility, an effective mitigation strategy is vital in preventing a cascading failure event. If any target at a typical ESS facility, other than a control house, is attacked and disabled, the control house can function to reroute power and prevent a cascading failure. If the control house (or control facility) is attacked first, timely detection, assessment, and alarm communication to the transmission control center which will immediately shut down the site while rerouting power to eliminate the possibility of a cascading failure. Internal and external fire suppression are also critical elements of a mitigation and resiliency strategy.

2.3. Physical Security Risks

As noted in the Congressional Research Service report, “Physical Security of the U.S. Power Grid,” there is a general consensus among state and federal government officials, utilities, and manufacturers, that high voltage transformers (and substations) are vulnerable to terrorist attack, with potentially catastrophic and cascading consequences [17]. As power grids evolve and ESS becomes a more important part of power systems operation, storage assets can also become critical. The challenge government and utility professionals have found is accurately identifying the risk to specific target sets – from a regional grid to a specific node in that grid such as a substation or transformer. As a result, the Federal Energy Regulatory Commission (FERC) issued the directive that new reliability standards require grid owners to perform risk and vulnerability assessments to identify critical facilities, nodes, and targets, characterize potential threats and vulnerabilities, and implement physical protection plans to combat identified risks.

The primary risk from a physical attack against the electric power grid is a widespread power outage lasting for days or longer, with the most vulnerable targets being towers and transformers [17]. Typically, any regional or local outage caused by weather or malicious activities is repaired fairly quickly due to system resiliency. An attack generating several simultaneous failures, however, may overwhelm typical risk mitigation protocols and have severe implications across a significant portion of the United States.

ESS facilities are often unmanned with minimal physical security components and ineffective event response capabilities. The consequences of physical attacks to ESSs depend on many factors, including the nature of the attack, system size, siting and ESS technology. Reports documenting fires at grid-connected battery systems [18] [19] show the necessity of factoring in the consequences of an attack-caused fire when establishing appropriate physical security mechanisms. These consequences would be radically different if the BESS is located inside of a building or outdoors (sited within distance of other structures or enclosed by a metal shipping container). For more details about safety risks associated with ESSs, refer to Chapter 20: Safety of Electrochemical Energy Storage Devices.

Even if a certain ESS technology does not pose a significant safety risk, other consequences of physical attacks include capital costs to repair or replace the damaged asset and those caused by its loss of functionality. For microgrids and ESSs used for backup power, an attack to a storage system might result in increased costs of operation and power outages. Large-scale power grids currently rely little on distributed ESSs and operate under security margins and power reserves, however, the loss of one or a few ESSs could result in additional operating costs caused by using those reserves and restoring them to pre-event levels.

Physical attacks on ESSs may become more consequential if/when bulk power grids start relying more on energy storage or if coordinated attacks take out enough resources to reduce security margins or create cascading effects. Distributed energy storage in the future is likely to include home-owner facilities such as vehicle power stations or solar battery storage units. Because of their small size, the disruption of service in these units due to a physical attack could significantly damage the home facility but is unlikely to impact bulk power or distribution systems in any consequential way.

Vital target areas at risk may include battery storage systems and associated HVAC units, transformer stations, control buildings (i.e., control house), and overhead bus systems. Transformers are particularly important because they are critical to the distribution of power and extremely vulnerable to malicious attacks. Functional loss of the control house could also result in a cascade event. Secondary targets are vital but could be bypassed or mitigated following an event.

2.4. Standards

The Federal Power Act defines the separation of regulatory responsibilities between states and federal government. This legislation grants federal jurisdiction over regulation of wholesale sales and transmission in interstate commerce, while regulation of generation, distribution, and retail sales falls under state rule [20].

NERC CIP-014-2 – Physical Security standard only applies to transmission stations, transmission substations, and their associated control centers [9]. These standards cover physical security, cyber security, and other reliability issues for the bulk power system, which apply to bulk equipment (>20 MW) connected at 100 kV or greater. Some utility-scale ESS projects do meet these requirements. For example, the 100 MW Tesla Powerpack, located at the Hornsdale Power Reserve in South Australia, is connected to the transmission system at 275 kV [21].

2.5. Industry Best Practices

Industry best practices can be utilized to update or enhance any physical protection system. An effective physical protection system is designed to counter a specific threat, known as a Design Basis Threat (DBT), and includes detection, delay, and response, implemented with balance across security layers and defense in depth from off-site to the target. The mission of a physical protection system is to quickly detect and assess an adversary attack, with delay measures for an armed response to interrupt the adversary attack and neutralize the threat. The DBT is a thorough threat analysis identifying in detail an adversary's motivations, capabilities, equipment and weapons access, transportation, support, and other aspects that provide a physical protection system designer insight into the robustness required to defeat such a threat. This DBT can be system-wide throughout an entire region or grid, or site specific.

Performance-based design criteria are better than feature-based when measuring overall system effectiveness. The application of resources should be based on a risk and vulnerability analysis, target and consequence analysis, and threat characterization. Other important factors impacting resource allocation include criticality of a site, established mitigation protocols, proximity to urban centers and an effective response force, and size of the facility. To achieve an effective Physical Protection System (PPS), the following best practices should be considered [22] [23]:

- Begin the design with a review and thorough understanding of the protection objectives that the designed PPS must meet.
- Include the criteria against which elements of the design will be evaluated (system performance metrics).
- Integrate people, procedures, and equipment into a system that will protect assets from the defined threat.
- Ensure:
  - The total time for detection, assessment, alarm communication, delay, and response is less than the adversary's total task time.
  - Detection is as far from the target as possible and delays are near the target.
  - Detection is timely and *always* placed before delay so that the system operator knows the cause of the alarm.
- Incorporate separate layers of protection so that an adversary is be required to avoid or defeat a number of protective devices in sequence.
- Incorporate balanced protection so that no matter how adversaries attempt to accomplish their goals, effective elements of the PPS will be encountered with similar delay times and probabilities of detection along each adversary path.

The standard for high risk, high consequence sites employs a robust Perimeter Intrusion Detection and Assessment System (PIDAS), which consists of:

- two fence lines
- multiple sensor modalities within the PIDAS zone
- vehicle barriers along the inner perimeter
- associated fixed assessment cameras

2.6. Research and Development

Enhancements in vehicle barrier technology is allowing for more resilient and cost-effective ASTM F2656-07 M50-P1-rated barrier systems to be deployed at a wider range of facilities. When employed within a perimeter detection layer (such as a fence-mounted sensor system), these barriers offer more effective delays than a perimeter fence-mounted cable system where no detection is present or where the detection and delay systems are at the same security layer.

Fixed-perimeter intrusion detection systems remain the backbone of any adversary detection methodology. However, the incorporation of artificial intelligence, data analytics, video analytics, and advances in sensor detection technologies will continue to improve their performance, reliability, resiliency, and ability to process data accurately. Current trends in enhanced camera technology will also improve the ability to assess the validity of triggered alarms. Video analytics and video motion detection algorithms continue to evolve and increase in accuracy and effectiveness. Also, the use of cost-effective airborne devices (drones) with various imaging systems will provide a rapid assessment capability that can adapt to the security situation on the ground as it develops.

The PIDAS strategy may not be cost effective for smaller, more isolated, or less consequential facilities. Fence-mounted detection systems, such as enhanced fiber mesh for vibration/cutting detection or wireless detection systems, are proving to be a cost-effective trend for smaller facilities. New developments for detection at gate areas utilizing wireless gate sensors, such as a wireless balanced magnetic switch and vibration/cutting detection technologies, are also beneficial for smaller facilities. These new development areas, when combined with vehicle and pedestrian delays in depth, offer cost-effective solutions for risk mitigation.

Several multi-modality sensor systems are being researched that combine two or more detection modalities into a single unit, offering a more cost-effective platform with complimentary detection capabilities (i.e., digital microwave and active infrared). The development of intelligence perimeter lighting is also being researched as a cost-effective dual-capability platform where lighting installed along a perimeter provides uniform illumination for fixed assessment or surveillance camera systems while embedded accelerometers can detect an adversary attempting to cut, climb, or lift/move fence fabric. This smart lighting employing a low-voltage LED illumination system not only keeps operational costs low but also offers enhanced visual capabilities such as intensity adjustment and alarm strobing as a deterrent to the adversary.

Interior space detection is also an area seeing marked improvements in technology. Research is being conducted in self-learning analytics and impulse radar technology, enabling security systems to detect adversaries even when they have stopped moving or are using concealment techniques. The use of wireless technology and secure mesh networks reduces the impact of installing interior detection systems and may offer cost-effective solutions for monitoring interior spaces at remote facilities.

3. Current State of ESS Cybersecurity Technology

3.1. ESS Communications Architectures

Currently, large utility-owned ESSs include communications typical of larger power systems. These are dedicated utility-to-asset connections that provide near real-time operations data-to-grid operators. In the United States, these communications usually use the IEEE 1815 (DNP3) protocol—though other options exist (IEC 61850 protocols, Open Field Message Bus, etc.). Soon, smaller ESSs will also have communications connections back to utilities. The national DER interconnection and interoperability standard, IEEE 1547, was updated in 2018 and now defines standardized device interfaces. Once mandated, all grid-connected DERs, including ESSs, must include one of the following communication protocols: IEEE 2030.5, IEEE 1815, or SunSpec Modbus. Utilities will then be able to communicate directly to the devices or route their communication through DER vendors or DER aggregators to individual devices.

3.1.1. Utility-Scale Energy Storage Communications Systems

Historically, utilities use dedicated communication networks to control large thermal generators. These communications would run over fiber or copper telecommunication lines. However, as more of the generation is becoming distributed, grid operators are turning to cellular networks, radio and microwave communications, and public internet to communicate with their smaller assets. These communications can be represented logically using the Purdue Enterprise Reference Architecture (PERA – commonly referred to as the Purdue Model – wherein the upper tiers represent utility information technology (IT) network devices and the lower layers are ESS site and device operational technology (OT). The IT and OT environments are separated with a demilitarized zone (DMZ) to limit access to the OT operations from the IT environment. One representation of the layers is shown in Figure 3 [24]. More information on this network is presented in *Roadmap for Photovoltaic Cyber Security* [25].

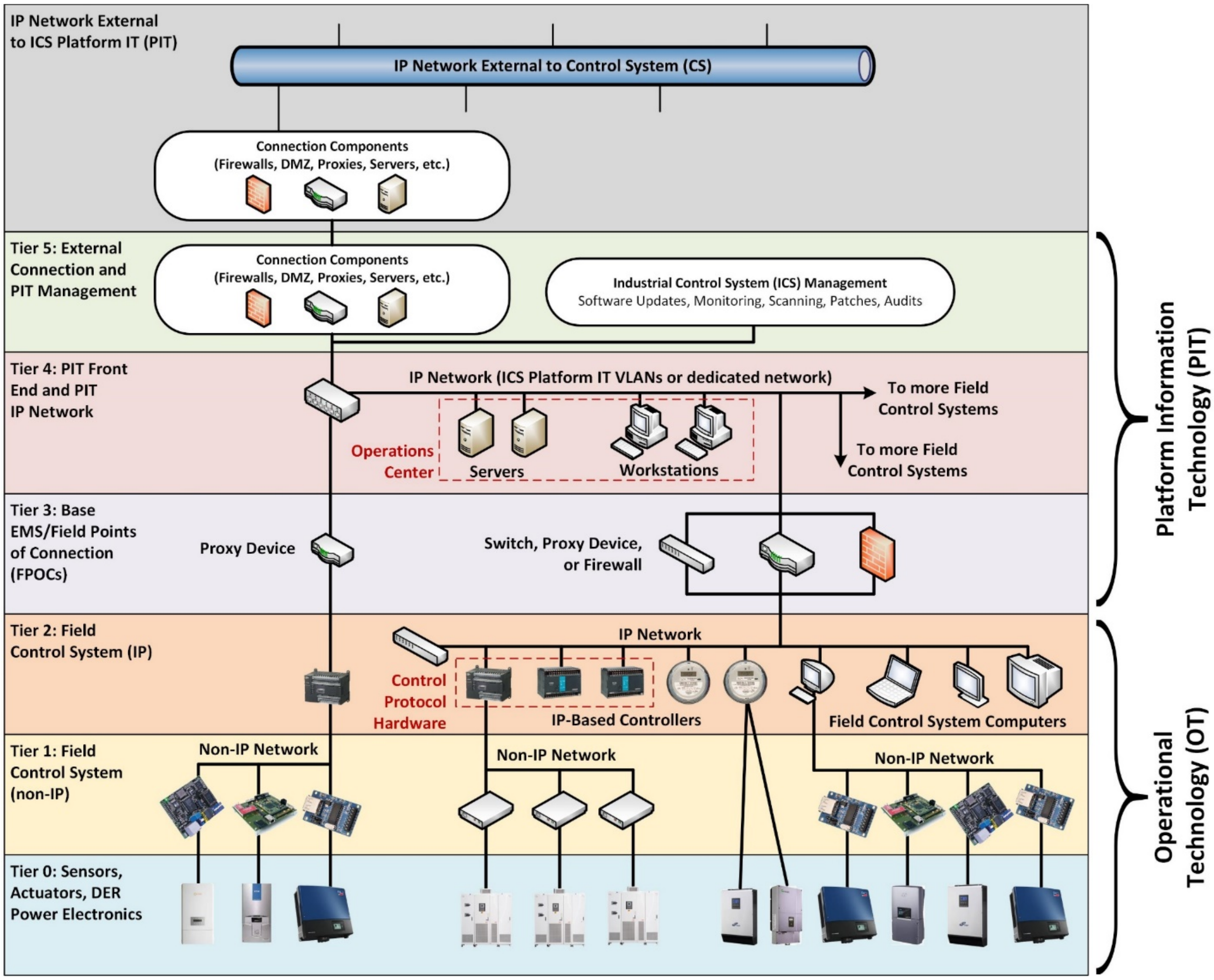
IP Network External to ICS Platform IT (PIT)
IP Network External to Control System (CS)
Connection Components (Firewalls, DMZ, Proxies, Servers, etc.)
Tier 5: External Connection and PIT Management
Connection Components (Firewalls, DMZ, Proxies, Servers, etc.)
Industrial Control System (ICS) Management
Software Updates, Monitoring, Scanning, Patches, Audits
Tier 4: PIT Front End and PIT IP Network
IP Network (ICS Platform IT VLANs or dedicated network)
To more Field Control Systems
To more Field Control Systems
Operations Center
Servers
Workstations
Tier 3: Base EMS/Field Points of Connection (FPOCs)
Proxy Device
Switch, Proxy Device, or Firewall
Tier 2: Field Control System (IP)
IP Network
Control Protocol Hardware
IP-Based Controllers
Field Control System Computers
Tier 1: Field Control System (non-IP)
Non-IP Network
Non-IP Network
Non-IP Network
Tier 0: Sensors, Actuators, DER Power Electronics
Platform Information Technology (PIT)
Operational Technology (OT)

Figure 3. Purdue model for energy storage system communications

3.1.2. Distributed Energy Resources Communications Systems

DER communications requirements in the United States have been evolving rapidly. In 2018, DER interconnection standard, IEEE 1547, was updated to require standardized communications interfaces on all DER equipment. Further, the California Public Utilities Commission mandated that by 2020, all newly installed DER equipment include communications pathways to the three California Investor Owned Utilities (IOUs) in Electric Rule 21. Many other states are expected to follow California. These new communication pathways, in addition to those previously established by DER vendors to monitor DER/ESS equipment and push firmware updates, represent new cybersecurity attack vectors.

A schematic of communications pathways and protocol options between grid operators and distributed ESSs is shown in Figure 4. At the top of the figure are related grid operator systems that are used to monitor and control DER equipment, including the DER management system (DERMS), outage management system (OMS), advanced distribution management system (ADMS), and geographic information system (GIS). The grid operator employs an IEEE 2030.5 server, IEEE 1815 master, or some other server/system to communicate either directly to the DER equipment (purple pathway) or to an aggregator, which passes the command on to the DER equipment (blue and red pathway). The utility will most likely use IEEE 2030.5 or IEEE 1815 to communicate with the equipment or aggregator. The aggregator uses either IEEE 2030.5, IEEE 1815, or Modbus with transport layer security (TLS). There is also a connection the DER vendor maintains with the equipment for monitoring and firmware updates (green pathway) that may be a proprietary protocol. Within the home, site, or facility, the communications reach a gateway that may or may not be physically integrated with the ESS device. The gateway then passes the information to the communication processor in the ESS to parse the data and respond accordingly. The protocol stacks for each of these connections is shown on the right of the image.

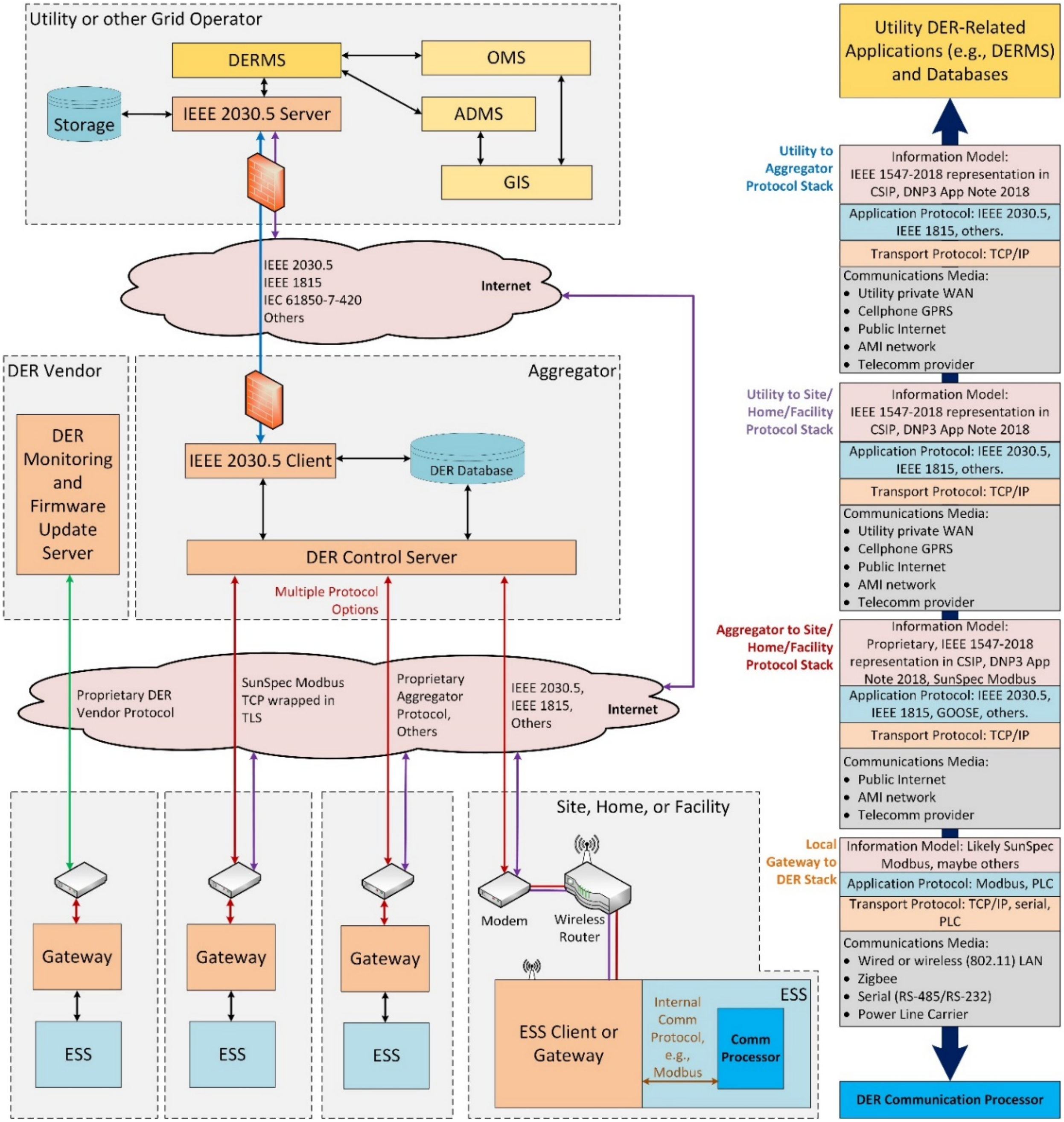
Utility or other Grid Operator
DERMS
OMS
Storage
IEEE 2030.5 Server
ADMS
GIS
IEEE 2030.5
IEEE 1815
IEC 61850-7-420
Others
Internet
DER Vendor
Aggregator
DER Monitoring and Firmware Update Server
IEEE 2030.5 Client
DER Database
DER Control Server
Multiple Protocol Options
Proprietary DER Vendor Protocol
SunSpec Modbus TCP wrapped in TLS
Proprietary Aggregator Protocol, Others
IEEE 2030.5, IEEE 1815, Others
Internet
Site, Home, or Facility
Modem
Wireless Router
Gateway
Gateway
Gateway
ESS
ESS
ESS
ESS Client or Gateway
Internal Comm Protocol, e.g., Modbus
ESS
Comm Processor
Utility DER-Related Applications (e.g., DERMS) and Databases
Utility to Aggregator Protocol Stack
Information Model: IEEE 1547-2018 representation in CSIP, DNP3 App Note 2018
Application Protocol: IEEE 2030.5, IEEE 1815, others.
Transport Protocol: TCP/IP
Communications Media:
• Utility private WAN
• Cellphone GPRS
• Public Internet
• AMI network
• Telecomm provider
Utility to Site/ Home/Facility Protocol Stack
Information Model: IEEE 1547-2018 representation in CSIP, DNP3 App Note 2018
Application Protocol: IEEE 2030.5, IEEE 1815, others.
Transport Protocol: TCP/IP
Communications Media:
• Utility private WAN
• Cellphone GPRS
• Public Internet
• AMI network
• Telecomm provider
Aggregator to Site/ Home/Facility Protocol Stack
Information Model: Proprietary, IEEE 1547-2018 representation in CSIP, DNP3 App Note 2018, SunSpec Modbus
Application Protocol: IEEE 2030.5, IEEE 1815, GOOSE, others.
Transport Protocol: TCP/IP
Communications Media:
• Public Internet
• AMI network
• Telecomm provider
Local Gateway to DER Stack
Information Model: Likely SunSpec Modbus, maybe others
Application Protocol: Modbus, PLC
Transport Protocol: TCP/IP, serial, PLC
Communications Media:
• Wired or wireless (802.11) LAN
• Zigbee
• Serial (RS-485/RS-232)
• Power Line Carrier
DER Communication Processor

Figure 4. ESS communication pathways and associated protocols Internal ESS Communications

Several companies manufacture ESSs commonly composed of devices integrated into a single system. These subsystems are equipped with communication and processing capabilities to enable coordination between them, forming a complete industrial control system (ICS). The main components of a grid BESS are:

- Battery modules (or battery packs)
- Power conversion system (PCS)
- Battery management systems (BMS)

- Energy storage management systems (ESMS), also known as supervisory system control [26]
- Environmental control system (heating, ventilation and air-conditioning system)
- Fire suppression system or fire control system
- Human machine interface (HMI)
- Electrical disconnects, circuit breakers, and switches
- Communications networking switches and cables

An example of how these subsystems are connected is shown in Figure 5. Other ESSs such as flow-batteries, flywheels, CAES, PHS, and TES have distinct technology-specific topologies, controls, and monitoring systems.

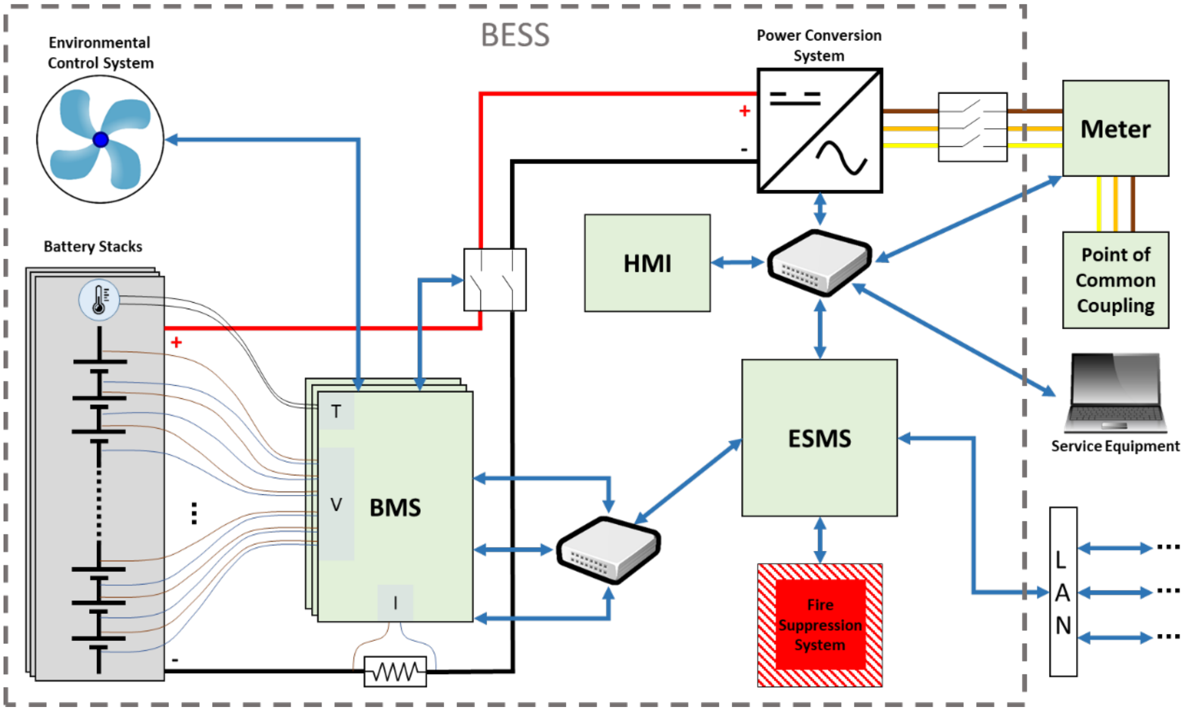

Figure 5. Example of communications between components of utility-scale BESS

BMSs measure cell and stack voltages, stack current, temperature, and electrolyte ion concentration in flow batteries. With that information, BMSs can detect faults and estimate key parameters such as battery state of charge, state of health, and internal resistance, among others. BMSs also control cell charge balancing circuits and contactors. BMSs might also communicate with or control temperature control systems, including battery module fans. Commonly used communications technologies and standards found in ESS include HTTP, CAN Bus, Modbus-TCP, Modbus-RTU, SunSpec Modbus, MESA. WiFi, USB and RS232.

Implementation of ESMSs and BMSs may vary depending on manufacturers. A single device might perform both functions in small BESS, while these functions are implemented by multiple specialized building blocks in large-scale systems. ESMS are typically the point of connection with the site local area network (LAN). More details on ESMSs can be found in Chapter 17: Energy Storage Management Systems. BMSs might be dedicated for a given battery technology or they can be parameterized to work with a wider range of battery technologies. Commonly, there is one

BMS per battery stack. BMSs might measure and balance individual cell voltages or voltages of a few cells connected in parallel. Large systems can have dozens of battery stacks connected in parallel, therefore IP networks are necessary to connect all BMSs to ESMSs and PCSs. Because module, air or cell temperature are typically measured by BMSs, there is commonly a connection between them and environmental control systems. A second network switch can be used to connect the ESMS to PCS, service equipment, power meter, HMI, system historian, and other subsystems.

Figure 5 shows a diagram of a small-sized grid BESS. Large systems are typically modular, having several PCSs connected in parallel. Smaller systems, such as BESSs for homes or small commercial and industrial applications have much simpler layouts. For these smaller systems, the functions of HMIs, BMSs, and ESMSs can be implemented by the same device, typically without environmental control and fire suppression systems.

Flywheels also require specific devices to monitor their critical operating parameters. In addition to controlling power exchanges with the grid, control modules are used to monitor their rotational speed and temperature, as well as controlling cooling systems and power converters.

3.2. Current Cybersecurity Practices

ESS security standards, guidelines, and R&D typically will mirror other DER systems, except in the case of large utility-owned ESSs that fall under the NERC Critical Infrastructure Protection (CIP) requirements and need to be protected like large central generators. Fortunately, extensive work has been done to outline photovoltaic (PV) cybersecurity recommendations that are applicable to ESS equipment. In 2017, Sandia National Laboratories published a roadmap for photovoltaic cybersecurity that focused on a pathway to improve PV cybersecurity by recommending five-year milestones in stakeholder engagement, R&D, standards development, and industry best practices [25]. Each of these recommendations were further subdivided into three strategic areas that align with the NIST Cybersecurity Framework [27]:

1. Identifying and protecting assets
2. Detecting cyber intrusions
3. Responding and recovering from cyberattacks

These recommendations were aligned with the 2011 Energy Sector Control Systems Working Group, “Roadmap to Achieve Energy Delivery Systems Cybersecurity,” [28] and included steps that would help reach the three goals presented in the March 2018, “DOE Multiyear Plan for Energy Sector Cybersecurity” [29]:

- Strengthen energy sector cybersecurity preparedness
- Coordinate cyber incident response and recovery
- Accelerate game-changing research, development and demonstration of resilient energy delivery systems

As a result, the following cybersecurity R&D discussion heavily leverages these prior reports to provide a summary of cybersecurity considerations for ESS. Section 3.3 discusses the cybersecurity risks that exist for energy storage systems; Section 3.4 covers applicable codes and standards; Section 3.5 discusses industry best practices; and Section 3.6 explores applicable R&D topics for ESS cybersecurity.

3.3. Cybersecurity Risks

There are cybersecurity risks to ESS components and the power system. If an adversary could adjust the operations of certain ESS components, spoof internal measurements, and/or disarm alarms, the equipment could malfunction and damage hardware or injure bystanders. Furthermore, if the ESS is connected to critical infrastructure components—e.g., in power plants, natural gas systems, water treatment facilities, or defense critical installations—disruptions or destruction of the ESS could result in cascading failures [30].

Similarly, there are many concerns that DER equipment could impact grid operations, especially when controlled as an aggregate resource. In fact, there have been multiple studies that have looked at the impact of controlling demand response assets, electric vehicle chargers, and DER equipment on the grid at the distribution and transmission levels [31]–[34]. As DER penetrations increase and DER equipment is controlled maliciously, there is a growing impact on the power system. In the August 2019 report, "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid," the Government Accountability Office recommended FERC address a risk presented by a combination of geographically dispersed systems that individually fall below the compliance threshold of NERC CIP standards [35]. The risk posed by thousands of small, unregulated DER devices is the same in aggregate as that of a large generator with the same nameplate capacity. Fortunately, as described in the following sections, there are several efforts underway to improve DER cybersecurity standards and create new security technologies. Additionally, the industry can follow many well-established best practices to improve their cybersecurity posture.

3.4. Standards

Cybersecurity standardization is essential in this highly interconnected and interoperable energy environment in which ESSs are operating. While standards cannot evolve at the same pace as cyber adversaries, they provide a common baseline for the industry and establish fixed criteria to enter the market.

3.4.1. Transmission-Connected ESS Cybersecurity Standards

There are many cybersecurity codes and standards for transmission-connected BES devices and others in development for medium- and low-voltage-connected DER equipment. As stated earlier, BES equipment that is >20 MW connected at 100 kV or greater falls within the NERC CIP requirements, which include the following:

- CIP-002-5.1a: Cyber systems and asset categorization
- CIP-003-6: Security management controls
- CIP-004-6: Personnel training and security awareness
- CIP-005-5: Electronic security perimeters for critical assets and border access point protections
- CIP-006-6: Physical security
- CIP-007-6: Security system management
- CIP-008-5: Incident reporting and response planning

- CIP-009-6: Recovery plans
- CIP-010-2: Configuration change management and vulnerability assessments
- CIP-011-2: Information protection

These, along with the forthcoming CIP-013-1 (Supply chain management) and CIP-014-2 (Physical security for transmission stations, substations, and control systems), provide the basis for mandatory power system security requirements. They are monitored and enforced through NERC audits, spot checks, and self-certifications of utilities and power system operators. The operators of large ESSs will be required to adhere to the NERC CIP requirements. These systems generally are connected to grid operators like other large generators and should be protected in the same way.

3.4.2. Distribution-Connected ESS Cybersecurity Standards

There are currently no cybersecurity standards for smaller DER equipment. Acknowledging this gap, the DOE Solar Energy Technologies Office provided funding to establish the SunSpec/Sandia DER Cybersecurity Workgroup in August 2017 [36]. For more than two years, this group has brought together DER interoperability and cyber security experts to discuss security for DER devices, gateways, aggregators, utilities, and the US power system. The group is primarily focused on generating a collection of best practices that act as basis for or input to national or international DER cybersecurity standards. The group has also facilitated DER cybersecurity discussions between stakeholders and exchanged perspectives on implementation and technical solutions. Within the workgroup, cybersecurity subgroups were established to address:

- Standardized test procedures for DER cyber vulnerabilities – A subgroup established a test protocol for DER equipment that included 11 test cases used to verify authentication, authorization, confidentiality and data integrity for TCP/IP communications to grid operators [37]. This subgroup is currently working with Underwriters Laboratories (UL) to determine if there is industry interest in converting this into an American National Standards Institute (ANSI) standard.
- DER network architectures – This subgroup, led by Electric Power Research Institute (EPRI), established a reference architecture for DER communications networks and requirements and compliance checklists for DER networks based on the resource criticality levels [38]. The requirements cover network segmentation, boundary protections, service protections, integrity mechanisms, etc.
- Data-in-flight – This subgroup investigated the possibility to harmonize the cybersecurity requirements of the IEEE 1547-2018 communication protocols (SunSpec Modbus, IEEE 2030.5, and IEEE 1815). A common set of protocol requirements for encryption, authentication, and key management within the DER communication ecosystem is helpful in establishing a baseline set of security features. While the final recommendations are not released from this active subgroup yet, a collection of recommendations for trust and encryption was included in a Sandia report [39].
- Access controls – A newly formed subgroup is investigating a role-based access control taxonomy, password control, and data privacy expectations for IEEE 1547-2018 functionality.

In the future, the SunSpec/Sandia DER Cybersecurity Workgroup is planning to address patching requirements and auditing procedures.

There are many other standards organizations that provide the basis for the recommendations produced by the SunSpec/Sandia DER Cybersecurity Workgroup. These include encryption requirements, cipher suites, and internet protocols established by the Internet Engineering Task Force (IETF) and the NIST Federal Information Processing Standards (FIPS). NIST also provides a range of guides for IT and OT systems. In addition to the "Framework for Improving Critical Infrastructure Cybersecurity," [27] there is also the NIST 800-53 "Security and Privacy Controls for Information Systems and Organizations" [40] and NIST 800-82 "Guide to Industrial Control Systems (ICS) Security," [41] which include over 100 security controls and the defense of Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs). While not widely used in the United States, perhaps the most comprehensive standards for power systems communications is the IEC 62351 series [42]. Furthermore, IEEE 1815 (DNP3) has a more secure version called DNP3 Secure Authentication (DNP3-SA) codified in IEC 62351-5. Where applicable, these standards should be referenced to improve DER and ESS communications requirements.

In addition to these best practices, there are many other guides from government and private agencies, including International Organization for Standardization (ISO), IEC, UL, NIST, International Council on Large Electric Systems (CIGRE), and the International Society for Automation (ISA) that should be included in a suite of cybersecurity requirements for ESS equipment and communication networks.

3.5. Industry Best Practices

There are several industry best practices that will improve ESS cybersecurity. Principal among them is defense-in-depth approaches, where multiple security features are layered in the asset or network. National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) outline several defense-in-depth elements including network architecture, network perimeter security, host security, security monitoring, and vendor management [43]. Cybersecurity practices from NIST 800-82, as it relates to these areas, include:

- Controlling logical access with unidirectional gateways, DMZs, unique OT authentication mechanisms, defense-in-depth methodologies with multiple security layers
- Restricting physical access
- Minimizing DER exploits by:
- Regular patches,
- Disabling unused ports and services,
- Adopting the principle of least privilege,
- Monitoring audit trails,
- Using anti-virus programs,
- Applying encryption or cryptographic hashes for data storage and communications, etc.
- Minimizing data-in-transit manipulation, falsification, or spoofing
- Employing intrusion detection and prevention systems
- Maintaining functionality under duress—redundant critical components, restorations plans, fault tolerant systems, and graceful degradation without cascading failures—whereby the equipment can transition to emergency operations

3.5.1. Cybersecurity Self-Evaluations and Audits

ESS vendors and network operators should conduct cybersecurity self-evaluations either with an internal team or using an outside contractor. DHS US-CERT Cyber Security Evaluation Tool (CSET) [44] systematically evaluates the network security, identifies and ranks gaps based on ICS-CERT threat information, and reports on the assessment to recommend high-priority improvements. Another self-evaluation tool is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [45], which tailors the C2M2 to the power industry. The C2M2 model provides a method of ranking an organization using maturity indicator levels in 10 different domains:

1. Risk management
2. Asset, change, and configuration management
3. Identity and access management
4. Threat and vulnerability management
5. Situational awareness
6. Information sharing and communications
7. Event and incident response, continuity of operations
8. Supply chain and external dependencies management
9. Workforce management
10. Cybersecurity program management

Once areas of improvement have been targeted, risk management frameworks [46] [47] should be applied to mitigate the exposure to these risks.

3.5.2. Patching

It is also critical that the ICS/OT/ESS systems are patched from known vulnerabilities. An unpatched firewall was the culprit in the DoS attack that prevented sPower, a Utah-based renewable energy company, from accessing 500 MW of their wind and solar assets for 12 hours [15]. ESS vendors also need to adopt a rigorous program to push updates and patches to their equipment to avoid risks to the equipment and power system. Formalized mechanisms for developing and deploying patches is a current industry gap.

3.5.3. Supply Chain Risk Management

It is also essential to minimize the risk to ESS equipment through effective supply chain risk management approaches. ESS devices are assembled from hundreds of components manufactured from many different suppliers in a range of national and international locations. This exposes the equipment to new risks, as control equipment could be changed remotely with backdoor attacks or other entry points into equipment or a system. The SANS Institute has provided recommendations for combatting supply chain cyber risks by establishing recommendations for people, process, and technology elements [48]. There are also several supply chain risk management standards and best practices that apply to aerospace (SAE ARP9134 [49]), electrical equipment/medical imaging (NEMA CPSP 1-2015 [50]), and automotive industries (SAE AS5553A [51], SAE AS5553B [52]). DER equipment vendors should reference these best practices and establish Cyber Supply Chain Risk Management (C-SCRM) programs to reduce the supply chain cyber risk.

3.5.4. *Insider Threat Mitigation*

ESS vendors and network operators must consider the risk presented by disgruntled or malicious employees. These actors are especially dangerous because they have legitimate access to equipment and DER control networks. In "Common Sense Guide to Mitigating Insider Threats," the authors recommend many practices to mitigate insider threats of ESS equipment, including [53]:

- Inventory and document assets with associated functionality and prioritization/criticality
- Develop a formal insider threat program and adding training for all employees
- Document policies and controls
- Monitor and respond to suspicious or disruptive behavior
- Consider insider and business partners threats in enterprise-wide risk assessments
- Avoid harmful social media disclosures
- Implement strict password and account management practices
- Use stringent access controls and monitor privileged users
- Monitor employee actions with correlated data from multiple sources
- Monitor and control remote access from all devices, e.g., cell phones and tablets
- Establish baseline behavior for networks
- Establish baseline behavior for employees
- Enforce separation of duties and principle of least privilege
- Create explicit security agreements for cloud services
- Institute change controls
- Implement secure backups and recovery processes
- Prevent data exfiltration from wired and wireless networks, portable media, etc.

3.6. Opportunities and Emerging Technologies

Maintaining a robust cybersecurity R&D program to is critical to defending ESS assets and networks from evolving cybersecurity threats. Technology development efforts must span the NIST Cybersecurity Framework functions (identify, protect, detect, respond, recover) though many technologies are crosscutting and could be applied to multiple areas. A depiction of malicious cyber activities being thwarted with different technologies in the Framework functions is shown in Figure 6, which was adopted from the National Science and Technology Council (NSTC) Federal Cybersecurity Research and Development Strategic Plan [54]. There are some obvious relationships between each of these elements – e.g., you must detect the threat to respond to it—but the basic concept of layering security defense technologies is well represented in Figure 6. The defensive R&D for each of these functions is shown below each of the functional areas, and includes:

- Identifying cybersecurity assets, policies, organizational support, vulnerabilities, threats, and risk management strategies at the system and personnel levels to prepare the organization and deter adversaries
- Protecting ESS assets by developing safeguards to prevent or contain cyber- attacks

- Detecting malicious activities at the device and network level to provide awareness of adversary actions and understand the potential risk of intrusions
- Responding to cyberattacks to mitigate impact to operations with forensic analysis, impact calculations, and appropriate response
- Recovering from attacks to restore system and asset operations

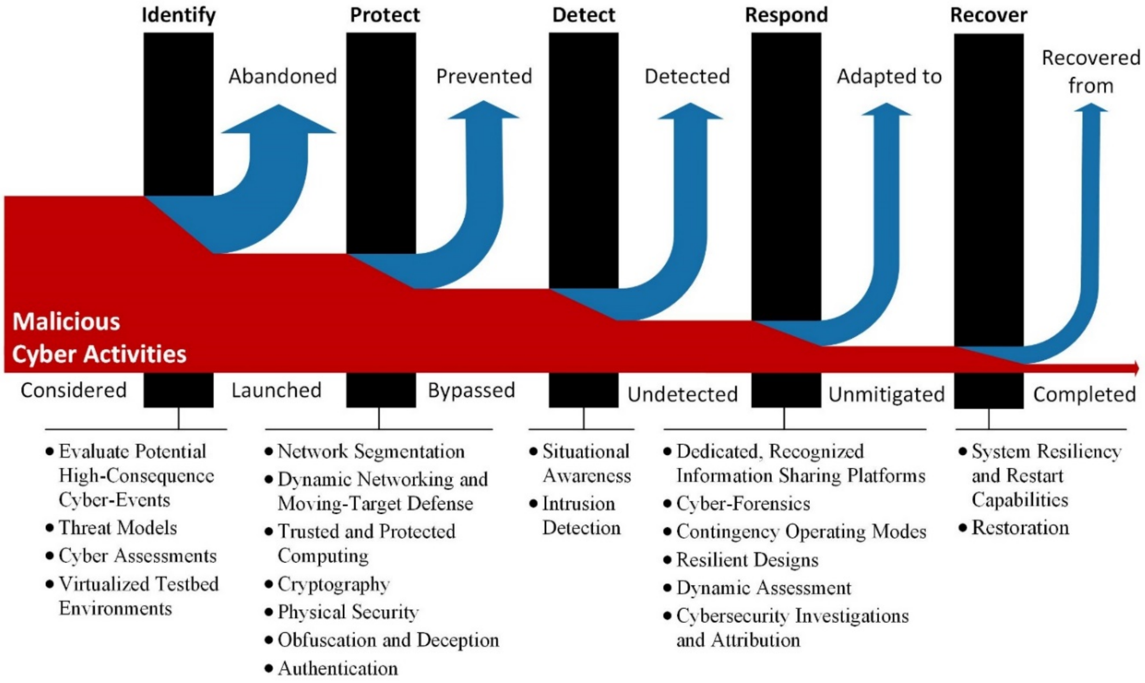
Identify
Protect
Detect
Respond
Recover
Abandoned
Prevented
Detected
Adapted to
Recovered from
Malicious Cyber Activities
Considered
Launched
Bypassed
Undetected
Unmitigated
Completed
• Evaluate Potential High-Consequence Cyber-Events
• Threat Models
• Cyber Assessments
• Virtualized Testbed Environments
• Network Segmentation
• Dynamic Networking and Moving-Target Defense
• Trusted and Protected Computing
• Cryptography
• Physical Security
• Obfuscation and Deception
• Authentication
• Situational Awareness
• Intrusion Detection
• Dedicated, Recognized Information Sharing Platforms
• Cyber-Forensics
• Contingency Operating Modes
• Resilient Designs
• Dynamic Assessment
• Cybersecurity Investigations and Attribution
• System Resiliency and Restart Capabilities
• Restoration

Figure 6: Thwarting malicious cyber activities with defensive R&D categorized using the five NIST Cybersecurity Framework functions

The following sections include cybersecurity R&D topics in each of the functional areas. These topics are aligned with the R&D research areas identified in the *Roadmap for Photovoltaic Cyber Security* [25] and the *Roadmap for Wind Cybersecurity* [55].

3.6.1. Identify

To effectively defend ESS equipment and control networks, it is essential to identify hardware and software assets and determine possible vulnerabilities and risks to those system components. Organizations also must establish cybersecurity policies, risks management strategies, and asset and supply chains programs. This process reduces the attack surface and potential impact to ESSs.

- **Evaluate potential high-consequence cyber events** – ESS converter studies and power system modeling can help quantify critical infrastructure risk from cyberattacks [56]–[59]. Understanding which types of attacks are benign or catastrophic helps engineers prioritize which defensive solutions should be implemented first and which assets are most critical.
- **Threat models** – Threat modeling identifies high-value assets, attack vectors, and potential vulnerabilities to determine credible threats. Systematically identifying and enumerating the threats to ESS devices and communication systems can help direct the design of appropriate security features for utilities, ESS aggregators, and ESS vendors.

- **Cyber assessments** – Penetration testing or "red teaming" by internal or external organizations can identify weaknesses in cybersecurity posture in the design phase. Cyber assessments should follow standardized methodologies provided by NIST SP 800-82 [41], ICS-CERT Cyber Security Evaluation Tool [44], or custom assessment techniques like the Information Design Assurance Red Team (IDART^{TM}) methodology [60] that identifies multiple attack vectors (DoS, packet replay, man-in-the-middle attacks, vulnerabilities scans, and modified firmware uploads) and inspects password handling and log management [61].
- **Virtualized testbed environments** – The construction of virtualized testbeds is useful across all the NIST Cybersecurity Framework functions as it can be used to analyze, evaluate, and demonstrate cyber security resilience and develop preventative and protective measures, analytic tools, and security strategies. By virtualizing the network, devices, and power system, it is possible to quickly assess different cyber security approaches and their compliance with standards [62].

3.6.2. Protect

One of the more active areas of cybersecurity R&D is focused on creating new protection technologies to defend ESS systems from cyberattacks. These technologies include:

- **Network segmentation** – Segmenting control networks using firewalls, VPNs, proxies, or other networking technologies minimizes traffic between enclaves and isolates attacks. EPRI recommended DER networks be segmented based on the criticality of the equipment [38]. In the case of utility-owned assets this is relatively straightforward, but for internet-connected ESSs it is more challenging and research in this area is warranted [31].
- **Dynamic networking and moving-target defense** – Moving target defense secures control networks against cyberattacks by rotating network addresses, network parameters, application libraries, or applying other cryptographic tools, without noticeably affecting system performance. This approach uses software-defined networks to eliminate a class of adversaries that rely on known static addresses for attacks. Dynamic networking could also be used to automatically reconfigure network settings and dynamically randomize application communications when an attack is detected [63].
- **Trusted computing** – Many computing products include tamperproof Trusted Platform Modules (TPMs) or similar integrated circuits, designed to secure private keys and function alongside the main processor for cryptographic operations.
- **Protected computing** – Protected computing requires two processors: one trusted and one untrusted. The public is not allowed to access the protected processor, but the application code is divided between the two processors in a mutually dependent way such that any tampering is detected.
- **Cryptography** – Encryption of data-at-rest and data-in-flight ensures confidentiality and integrity of the information. Public Key Infrastructure (PKI) to encrypt ESS transmissions is being rolled out in California as they deploy IEEE 2030.5 utility-to-DER communication networks. There are still several open questions regarding appropriate trust and encryption improvements in DER communication standards [39].
- **Physical security (for cybersecurity)** – Physical security is necessary to secure cybersecurity operations of ESSs. At the device-level the microprocessor chip type and manufacturer should be masked with an opaque conformal coating or some other

obfuscation method so that the architecture and associated vulnerabilities are hidden from adversaries. Anti-tamper protections should also be employed on utility-owned and customer-owned ESSs.

- **Obfuscation and deception** – Deceiving an adversary may disrupt reconnaissance and attack attempts. Methods include generating false network traffic to disguise legitimate traffic or creating intentionally complex programs. Similarly, honeypots and honeynets (device decoys or networks of decoys) can be inserted into the network to confuse attackers and capture their actions prior to attacks on physical systems.
- **Authentication** – Research must continue on multi-factor authentication mechanisms, one-time-use tokens, and other technologies that prevent brute force password attacks.

3.6.3. Detect

Once an adversary has penetrated a device or network, quick detection of their presence is necessary to mitigate damage. Some emerging technologies to accelerate the detection process include:

- **Situational awareness** – Advanced ESS cybersecurity systems must include tools to capture, analyze, and visualize near-real-time data from all networks. These tools enable the monitoring, detection, alerting, remediation, and accounting of benign anomalies or hazardous incidents. NIST SP 1800-7 "Situational Awareness for Electric Utilities" [64] describes the tools to enable situational awareness as comprising:
    - Logging software or a security incident and event management system
    - Bump-in-the-wire devices for OT encryption and logging
    - Commercial or open source software for collecting, analyzing, visualizing, and storing network data, e.g., historians, outage management systems, distribution management systems, and HMIs
    - Products that ensure telemetry and end-device data integrity
- **Intrusion detection** – Detecting adversarial actions on ESS control networks is necessary to implement appropriate countermeasures. There are a range of technologies that can be used for intrusion detection systems (IDSs) but generally can be divided into three approaches:
    - Signature-based – The IDSs monitor data for specific patterns indicative of known malware signatures previously observed. The signatures can be in the form of a specific string match, a match on binary data, or a match on a sequence of events occurring within the data.
    - Anomaly-based – Focus on recognizing abnormal patterns in data when compared to a baseline. Anomaly-based approaches can be trained on pre-existing data or by an operator, often using statistical machine learning algorithms.
    - Policy-based – Leverage a logical security policy and an execution trace validation algorithm to identify legal and illegal information flows between the objects of a system.

3.6.4. Respond

Appropriate countermeasures must be designed to minimize the duration and impact of a cyberattack. The following capabilities should be developed to respond effectively to an ESS cyber event:

- **Dedicated, recognized information sharing platforms** – Cybersecurity threat data need to be shared among ESS stakeholders to learn of adversary actions and potential compromise. Sharing this data has privacy, proprietary data, classification, and indemnification challenges. However, with properly structured information sharing programs and software platforms, cybersecurity threat data can be shared between government agencies and the private sector, including Department of Defense (DoD) Defense Industrial Base (DIB) Cybersecurity Program (DIBNet), Department of Homeland Security (DHS) NCCIC, DHS Automated Indicator Sharing (AIS), DHS Cyber Information Sharing and Collaboration Program (CISCP), and DOE Cybersecurity Risk Information Sharing Program (CRISP).
- **Cyber-forensics** – Following a cyber-attack, it is necessary to dissect the events that led to the breach. Incident response frameworks with forensics are helpful in patching holes in the security system, determining the source of leaked data, conducting periodic health checks of the system state, and isolating malware attacks.
- **Contingency operating modes** – ESS operators must establish adaptive response mechanisms to withstand the cyberattack and quickly recover to a known operable state. Temporary contingency modes allow time for forensics, restoration operations, or other recovery systems to take over while still maintaining critical functionality. For ESSs, this could be reverting to default, low risk operating modes.
- **Resilient designs** – ESS cyber-resilience is the ability of the system to maintain critical operations in the presence of adversary actions. This is typically performed using adaptive systems with components that fail gracefully so that backup, fail-over, and recovery equipment may be brought online.
- **Dynamic assessment** – Dynamic assessment technologies conduct real-time analytics on data streams to understand the tactics and approach of the adversary. This information is used to assess system damage, avoid future compromises, and plot a recovery course.
- **Cybersecurity investigations and attribution** – It is also necessary to identify those responsible of cyberattacks to begin criminal proceedings. Log file inspection tools for attribution and other forensics technologies are necessary to begin the judicial processes, and reverse engineering malware can determine the creator, the target equipment, and accessed data.

3.6.5. Recover

After responding to the adversary, the system should be returned to normal operation. Ideally, this recovery process is quick, coordinated, and pre-planned.

- **System resiliency and restart capabilities** – ESS networks and devices should be designed with the capability to ride through cybersecurity attacks by removing inherent weaknesses and building in attack responsiveness. Even if cyberattacks are successful, the ESS should be able to rebound from the event quickly. Not only should the ESS restart normal operations quickly, but utility-scale ESSs should be designed to provide black start capabilities so that the ESSs can support the re-energization of the power system.

- **Restoration** – Maintain rusted “gold master” firmware, software, and virtual machines to enable the restoration and recovery following a cyber-incident. Even if the firmware and software is wiped from the equipment, there should be a backup version that can be rapidly reinstalled on OT devices and control systems.

4. Concluding Remarks

This chapter presented an overview of the current state and future trends of ESS physical security and cybersecurity, including fundamental security concepts, security standards, state-of-the-art of physical security and cybersecurity technology, and ongoing R&D efforts to make energy storage more secure.

Including security as a fundamental component in energy storage industry culture is paramount, even for early development grid-connected ESS technologies. The experience of related power systems industries shows that ignoring security during the new product development cycle may lead to costly and ineffective security solutions when added in later stages of product development. The reports of physical and cybersecurity incidents in power systems and DERs send a clear message about how seriously the energy storage community should take security.

Fortunately, many efforts to create and disseminate best practices are under way. This chapter cites many standards and reports on best practices from several organizations that can serve as a guide to improving the security posture of ESS. Many of them recommend taking simple actions, such as enforcing physical access restrictions, observing password policy best practices, and applying other basic cybersecurity measures to communication networks. However, the lack of observance of these practices indicates that it is necessary to further disseminate the value of security to ESS owners and operators. There are still improvements to be made in terms of revising current standards and broadening their scope, but the industry is progressing.

Jay Johnson is a Principal Member of Technical Staff at Sandia National Laboratories. Jay is the co-convener of the SunSpec DER Cybersecurity Workgroup and leads several multidisciplinary research projects focused on power systems control, secure electric vehicle charging, and renewable energy cybersecurity. Mr. Johnson has seven patents and authored over 100 technical publications. He received a B.S. in Mechanical Engineering from the University of Missouri-Rolla in 2006 and a M.S. in Mechanical Engineering from the Georgia Institute of Technology in 2009.

Jeffrey Hoaglund is a Principal Member of the Technical Staff at Sandia National Laboratories. Mr. Hoaglund is a project lead in the Secure Commerce and Border Systems department, currently leading border security projects supporting the Department of State and the Threat Analysis Group supporting the Department of Energy's Global Material Security nonproliferation efforts. He has led vulnerability analyses at critical nuclear and energy infrastructure locations throughout the United States, Kingdom of Saudi Arabia, Russia, and other locations in the Middle East. Mr. Hoaglund graduated from the Naval Postgraduate School in 2002 with a M.S. in Information Technology Management and a M.S. in Software Engineering. He earned his B.S. in Oceanography in 1994 from the U.S. Naval Academy. Mr. Hoaglund also served 10 years as an Intelligence Officer in the U.S. Marine Corps.

Rodrigo D. Trevizan is a Postdoctoral Appointee at Sandia National Laboratories. Rodrigo authored research papers on the subjects of control of energy storage systems and demand response for power grid stabilization, power system state estimation, and detection of nontechnical losses in distribution systems. Dr. Trevizan received a B.S. and M.Sc. degree in Electrical Engineering from the Federal University of Rio Grande do Sul, Brazil, in 2012 and 2014, respectively, a M.Sc. in Power Systems Engineering from the Grenoble Institute of Technology (ENSE3) in 2011 and a Ph.D. in Electrical Engineering from the University of Florida in 2018.

Tu A. Nguyen is a Senior Member of the Technical Staff at Sandia National Laboratories. He is also a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE) and an editor of IEEE Transactions on Sustainable Energy. He received his B.S in Power Systems from Hanoi University of Science and Technology, Vietnam in 2007 and his Ph.D. in Electrical Engineering from Missouri University of Science and Technology in 2014. Before joining Sandia National Laboratories in September 2016, he worked as a Postdoctoral Research Associate at University of Washington. His research interests include energy storage analytics, microgrid modeling and analysis, and the integration of distributed resources into power grids.

References

[1] United States Code, vol. 44.

[2] M. D. Hogan and E. M. Newton, “Supplemental Information for the Interagency Report on Strategic US Government Engagement in International Standardization to Achieve US Objectives for Cybersecurity,” NISTIR 8074, 2015.

[3] U.S. Army, “The Army Physical Security Program,” AR 190-13, 2019.

[4] M. Nieles, K. Dempsey, and V. Pillitteri, “An introduction to information security,” National Institute of Standards and Technology, Jun. 2017. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-12r1.

[5] Jim Peppard, “Reward offered in power transformer shooting,” WTSP News (Tampa), Tampa, FL, Oct. 17, 2005.

[6] Chelsea J. Carter, “Arkansas man charged in connection with power grid sabotage,” CNN, Oct. 12, 2013.

[7] Federal Bureau of Investigation, “Jason Woodring Pleads Guilty to Federal Charges Related to Attacks on Power Grid,” Mar. 10, 2015.

[8] R. A. Serrano and E. Halper, Sophisticated but low-tech power grid attack baffles authorities. Los Angeles Times, 2014.

[9] “Critical Infrastructure Protection Standard CIP-014-2 – Physical Security,” North American Electric Reliability Corporation, Standard, Oct. 2015.

[10] J. Battis, M. Kurtovich, and Arthur O’Donnell, “Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699,” California Public Utilities Commission, Physical Security R.15-06-009, Jan. 2018.

[11] Industrial Control Systems Cyber Emergency Response Team, “Cyberattack against Ukrainian critical infrastructure,” ICS-CERT, IR-ALERT-H-16-056-01.

[12] Andy Greenberg, “‘Crash Override’: The Malware That Took Down a Power Grid,” Wired, Jun. 2017.

[13] Joe Slowik, “CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack,” Dragos, Inc., 2019.

[14] G. Bade, Russian Hackers infiltrated utility control rooms, DHS says. 2018.

[15] Robert Walton, “First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say,” Utility Dive, Nov. 04, 2019.

[16] NYSERDA, “New York Battery Energy Storage System Guidebook for Local Governments,” Jan. 2020.

[17] P. W. Parfomak, Physical security of the US power grid: high-voltage transformer substations. Congressional Research Service Washington, DC, 2014.

[18] Eric Wesoff, “Battery Room Fire at Kahuku Wind-Energy Storage Farm,” Greentech Media, Aug. 03, 2012.

[19] Julian Spector, “The Arizona Battery Explosion Is Changing Conventional Wisdom on Safety,” Greentech Media, Oct. 10, 2019.

[20] J. S. Dennis, S. G. Kelly, R. R. Nordhaus, and D. W. Smith, “Federal/State Jurisdictional Split: Implications for Emerging Electricity Technologies,” Lawrence Berkeley National Lab. (LBNL), Berkeley, CA (United States), 2016.

[21] “Hornsdale Power Reserve Project: Tesla’s largest utility-scale battery,” Global Infrastructure Hub, Sep. 2019. Accessed: Dec. 08, 2020. [Online]. Available: https://cdn.gihub.org/umbraco/media/2765/gih_showcaseprojects_hornsdale_2019_web_art.pdf.

[22] M. L. Garcia, Vulnerability assessment of physical protection systems. Elsevier, 2005.

[23] M. L. Garcia, Design and evaluation of physical protection systems. Elsevier, 2007.

[24] J. E. Stamp, J. E. Quiroz, and A. Ellis, “Cyber Security Gap Analysis for Critical Energy Systems (CSGACES).,” Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), 2017.

[25] J. Johnson, “Roadmap for photovoltaic cyber security,” Sandia Natl. Lab., 2017.

[26] M. T. Lawder et al., “Battery Energy Storage System (BESS) and Battery Management System (BMS) for Grid-Scale Applications,” Proc. IEEE, vol. 102, no. 6, pp. 1014–1030, Jun. 2014, doi: 10.1109/JPROC.2014.2317451.

[27] “Framework for Improving Critical Infrastructure Cybersecurity v1.1,” National Institute of Standards and Technology, Standard, Apr. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[28] E. S. C. S. W. Group and others, “Roadmap to achieve energy delivery systems cybersecurity,” Energ. Inc, 2011, [Online]. Available: https://www. controlsystemsroadmap. net/ieRoadmap$\backslash$% 20Documents/roadmap. pdf.

[29] “Multiyear Plan for Energy Sector Cybersecurity,” US DOE Office of Electricity Delivery and Energy Reliability, Mar. 2018.

[30] M. G. Angle, S. Madnick, J. L. Kirtley, and S. Khan, “Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems,” IEEE Power Energy Technol. Syst. J., vol. 6, no. 4, pp. 172–182, 2019.

[31] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, “Power system effects and mitigation recommendations for DER cyberattacks,” IET Cyber-Phys. Syst. Theory Appl., Jan. 2019, [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-cps.2018.5014.

[32] A. Chavez et al., “Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems,” in 2019 IEEE CyberPELS (CyberPELS), 2019, pp. 1–6.

[33] J. T. Johnson, “Securing Vehicle Charging Infrastructure APR.,” Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), 2019.

[34] S. Ghosh, M. H. Ali, and D. Dasgupta, “Effects of Cyber-Attacks on the Energy Storage in a Hybrid Power System,” in 2018 IEEE Power & Energy Society General Meeting (PESGM), 2018, pp. 1–5.

[35] U. S. G. A. Office, “Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid: Report to Congressional Requesters,” US Government Accountability Office, Report to Congressional Requesters, Aug. 2019.

[36] “SunSpec/Sandia DER Cybersecurity Work Group.” [Online]. Available: https://sunspec.org/cybersecurity-work-group/.

[37] D. Saleem and C. Carter, “Certification Procedures for Data and Communications Security of Distributed Energy Resources,” National Renewable Energy Lab.(NREL), Golden, CO (United States), 2019.

[38] Candace Suh-Lee, “EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-based Approach for Network Design,” 3002016781, Oct. 2019.

[39] J. Obert et al., “Recommendations for Trust and Encryption in DER Interoperability Standards,” Sandia Technical Report, 2019.

[40] R. S. Ross, “Security and Privacy Controls for Information Systems and Organizations,” National Institute of Standards and Technology, Sep. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5.

[41] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” NIST Spec. Publ., vol. 800, p. 82, 2015.

[42] F. Cleveland, “Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure,” White Pap., 2012.

[43] U. I. C. E. R. Team, “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,” Dep. Homel. Secur. Wash. DC USA Www Ics-Cert Us-Cert Govsitesdefaultfilesrecommended Pract.-CERTDefenseinDepth2016S508C Pdf, 2016.

[44] US-CERT, CSET. .

[45] U.S. Department of Energy, “Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.1,” Feb. 2014. [Online]. Available: https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

[46] J. T. F. T. Initiative and others, “Guide for applying the risk management framework to federal information systems: A security life cycle approach,” National Institute of Standards and Technology, 2014.

[47] N. DOE, “NERC, Electricity Subsector Cybersecurity Risk Management Process,” Tech. Rep. May, 2012.

[48] D. Shackleford, “Combatting cyber risks in the supply chain,” 2015.

[49] SAE International, “Supply Chain Risk Management Guideline,” ARP9134A, Feb. 2014. [Online]. Available: https://saemobilus.sae.org/content/arp9134a.

[50] “Supply Chain Best Practices,” National Electrical Manufacturers Association, NEMA CPSP 1:2015, Aug. 2015.

[51] SAE International, “Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria,” AS5553A, Aug. 2014.

[52] SAE International, “Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition,” AS5553B, Sep. 2016.

[53] M. Theis et al., “Common Sense Guide to Mitigating Insider Threats,” Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-2018-TR-010, 2019. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644.

[54] “Federal cybersecurity research and development strategic plan,” National Science and Technology Council, Feb. 2016.

[55] “Roadmap for Wind Cybersecurity,” 2020, doi: 10.2172/1647705.

[56] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, “Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks,” IEEE Trans. Smart Grid, vol. 9, no. 5, pp. 4702–4711, 2017.

[57] D. D. Sharma, S. Singh, J. Lin, and E. Foruzan, “Agent-based distributed control schemes for distributed energy storage systems under cyber attacks,” IEEE J. Emerg. Sel. Top. Circuits Syst., vol. 7, no. 2, pp. 307–318, 2017.

[58] A. Farraj, E. Hammad, and D. Kundur, “On the impact of cyber attacks on data integrity in storage-based transient stability control,” IEEE Trans. Ind. Inform., vol. 13, no. 6, pp. 3322–3333, 2017.

[59] S. Sahoo, T. Dragičević, and F. Blaabjerg, “Cyber security in control of grid-tied power electronic converters–challenges and vulnerabilities,” IEEE J. Emerg. Sel. Top. Power Electron., 2019.

[60] D. P. Duggan, “The IDART Methodology,” Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), SAND2017-2205B, 2017.

[61] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, “Cyber security assessment of distributed energy resources,” in 2017 IEEE 44th Photovoltaic Specialist Conference (PVSC), 2017, pp. 2135–2140.

[62] I. Onunkwo et al., “Cybersecurity Assessments on Emulated DER Communication Networks,” Sandia Technical Report, 2018.

[63] A. R. Chavez, J. Hamlet, and W. Stout, “Artificial Diversity and Defense Security (ADDSec) Final Report.,” Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), SAND2018-4545, 2018.

[64] J. McCarthy et al., “Situational Awareness for Electric Utilities,” NIST Special Publications 1800–7, Feb. 2017.