IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 4, 2022, accepted May 22, 2022, date of publication June 2, 2022, date of current version June 9, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3178987

Cyberphysical Security of Grid Battery Energy Storage Systems

RODRIGO D. TREVIZAN[1], (Member, IEEE), JAMES OBERT[1], (Senior Member, IEEE), VALERIO DE ANGELIS[1], (Member, IEEE), TU A. NGUYEN[1], (Senior Member, IEEE), VITTAL S. RAO[2], (Life Senior Member, IEEE), AND BABU R. CHALAMALA[1], (Fellow, IEEE)

[1]Sandia National Laboratories, Albuquerque, NM 87123, USA
[2]Department of Electrical and Computer Engineering, Texas Tech University, Lubbock, TX 79409, USA

Corresponding author: Rodrigo D. Trevizan (rdtrevi@sandia.gov)

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2022-7469 J.

ABSTRACT This paper presents a literature review on current practices and trends on cyberphysical security of grid-connected battery energy storage systems (BESSs). Energy storage is critical to the operation of Smart Grids powered by intermittent renewable energy resources. To achieve this goal, utility-scale and consumer-scale BESS will have to be fully integrated into power systems operations, providing ancillary services and performing functions to improve grid reliability, balance power and demand, among others. This vision of the future power grid will only become a reality if BESS are able to operate in a coordinated way with other grid entities, thus requiring significant communication capabilities. The pervasive networking infrastructure necessary to fully leverage the potential of storage increases the attack surface for cyberthreats, and the unique characteristics of battery systems pose challenges for cyberphysical security. This paper discusses a number of such threats, their associated attack vectors, detection methods, protective measures, research gaps in the literature and future research trends.

INDEX TERMS Battery energy storage systems, battery management systems, cybersecurity, energy storage, industrial control systems, power systems.

NOMENCLATURE

ACRONYMS

AES	Advanced Encryption Standard
AGC	Automatic Generation Control
AID	Anomaly-based Intrusion Detection
AMI	Advanced Metering Infrastructure
APT	Advanced Persistent Threat
AUV	Autonomous Underwater Vehicle
BESS	Battery Energy Storage System
BMS	Battery Management System
BoL	Beginning-of-Life
BTM	Behind-the-Meter
CAN	Computer Area Network
CC	Constant Current
CIP	Critical Infrastructure Protection
CNN	Convolutional Neural Network
CP	Constant Power
CV	Constant Voltage
CPS	Cyberphysical System
CRM	Charge Reservoir Model
CUSUM	Cumulative Sum
DDoS	Distributed Denial-of-Service
DER	Distributed Energy Resource
DERMS	DER Management System
DNP3	Distributed Networking Protocol 3.0
DMS	Distribution Management System
DMZ	Demilitarized Zone
DoD	Depth-of-Discharge
DoS	Denial-of-Service
ECM	Equivalent Circuit Model
ECU	Electronic Control Unit
EIS	Electrochemical Impedance Spectroscopy
EKF	Extended Kalman Filter
EMS	Energy Management System
EoL	End-of-Life
ERM	Energy Reservoir Model
ESMS	Energy Storage Management System

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

ESS	Energy Storage System
EV	Electric Vehicle
FDIA	False Data-Injection Attack
FERC	Federal Energy Regulatory Commission
FTM	Front-of-the-Meter
HAN	Home Area Network
HEV	Hybrid Electric Vehicle
HIDS	Host-based Intrusion Detection System
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heat, Ventilation and Air Conditioning
IAM	Information security Assessment Methodology
ICS	Industrial Control System
IDART	Information Design Assurance Red Team
IDS	Intrusion Detection System
IEM	Information Security Evaluation Methodology
INFOSEC	Information Security
IoT	Internet-of-Things
IP	Internet Protocol
IT	Information Technology
IVVC	Integrated volt/VAR control
KF	Kalman Filter
LAN	Local Area Network
LCO	Lithium Cobalt Oxide
LFP	Lithium Iron Phosphate
Li-ion	Lithium-ion
LMO	Lithium Manganese Oxide
MESA	Modular Energy Storage Architecture
MITM	Man-in-the-middle
ML	Machine Learning
Modbus	Modicon communication bus
MOSFET	Metal-oxide-semiconductor field-effect transistor
MQTT	Message Queue Telemetry Transport
NaS	Sodium-Sulfur
NERC	North American Electric Reliability Corporation
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Regulations
NMC	Nickel Manganese Cobalt oxide
NMH	Nickel-Metal Hydride
NSA	National Security Agency
OCV	Open-Circuit Voltage
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
OT	Operational Technology
P2P	Peer-to-peer
PCS	Power Conversion System
PDS	Power Distribution System
PKI	Public Key Infrastructure
PLC	Programmable logic controller
PLL	Phase-locked loop
PV	Photovoltaic
RBAC	Role-Based Access Control
RC	Resistor Capacitor
RES	Renewable Energy Source
RL	Reinforcement Learning
RLS	Recursive Least-Squares
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SEI	Solid Electrolyte Interface
SID	Signature-based Intrusion Detection
SoC	State-of-charge
SoH	State-of-health
SoL	State-of-life
SPAN	Switched Port Analyzer
TCP	Transmission Control Protocol
TEP	Technical Evaluation Plan
TLS	Transport Layer Security
UAV	Unmanned Aerial Vehicle
UKF	Unscented Kalman Filter
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRLA	Valve-Regulated Lead-Acid
WAN	Wide Area Network
WBMS	Wireless Battery Management System
ZnMn	Zinc-Manganese

MATHEMATICAL SYMBOLS

$\mathbf{A}$	state matrix of linear system
$\mathbf{B}$	input matrix of linear system
$\mathbf{C}$	output matrix of linear system
$C_{1,2}$	capacitances of equivalent RC circuit parameters
C_{cap}	battery capacity
$\mathbf{D}$	feedthrough matrix of linear system
$g_{k\|k}$	chi-squared detector
$h(\varsigma)$	function that maps SoC to OCV
i_{bat}	electric current going into the battery
i_c	charge current
i_d	discharge current
$\mathbf{K}_k$	Kalman gain matrix at time k
$\mathbf{P}_{k\|k-1}$	predicted state covariance
$\mathbf{P}_{k\|k}$	updated state covariance
q	reactive power injected by the PCS
$\mathbf{Q}$	covariance matrix of process noise
$q_{\max}$	upper reactive power injection capacity of PCS
$q_{\min}$	lower reactive power injection capacity of PCS
$\mathbf{R}$	covariance matrix of output noise
R_0	series internal resistance
$R_{1,2}$	resistances of equivalent RC circuit parameters
$\mathbf{u}_k$	vector of system control input at time k
$\mathbf{u}'_k$	attacked input vector
v	AC voltage measured by the PCS
$v_{1,2}$	voltage drops on equivalent RC circuits of cell

$\mathbf{v}_k$	vector of output noise at time k
v_{oc}	battery cell OCV
$V_{1,2,3,4}$	voltage parameters of droop controller
$\mathbf{w}_k$	vector of process noise at time k
$\mathbf{x}_k$	vector of system states at time k
$\hat{\mathbf{x}}_{k\|k-1}$	vector of predicted state estimates at time k
$\hat{\mathbf{x}}_{k\|k}$	vector of updated state estimates at time k
$\mathbf{y}_k$	vector of system output at time k
$\hat{\mathbf{y}}_{k\|k}$	updated estimate vector of system output at time k
$\mathbf{y}'_k$	attacked output vector
$\mathbf{z}_{k\|k}$	updated residuals at time k
$\alpha_{y,u}$	input or output false data injection scaling factor
$\beta_{y,u}$	input or output false data injection additive factor
γ_k	probability of false alarm of the χ^2 detector
η_c	charging efficiency coefficient
η_d	discharging efficiency coefficient
η_s	self-discharging coefficient
ϱ	state-of-life
ς	battery SoC
$\mathcal{T}_a$	FDIA period

I. INTRODUCTION

As the Electric Power industry transitions from centralized, fossil fuel-based generation to a paradigm with increased adoption of distributed, Renewable Energy Sources (RESs), the importance of Energy Storage Systems (ESS) in grid operation increases. ESS' flexibility and ability to shift renewable energy generation and stabilize the grid has attracted investments and attention from policymakers. As of August 2020, seven USA states had passed laws and regulations establishing goals for energy storage capacity in the near future [1].

The United States has currently approximately 24.5 GW of ESS in operation, most of which is pumped hydropower [2]. Recent reports on new projects have indicated the pace of ESS adoption in the USA is accelerating, with record 476 MW new deployments in the third quarter of 2020 and an expected annual 7.5 GW growth by 2025 [3]. Siting a pumped hydro plant, however, depends on a combination of specific geographical, geological and hydrological features that are very limited, such as soil providing strong foundation, narrow river passages like gorges or canyons, and abundance of water resources, to name a few.

Battery energy storage systems (BESS), on the other hand, are modular systems that can be deployed in a much broader range of locations. One of the earliest examples of the grid-scale application of BESS was Battery Energy Storage Test [4], [5]. It was composed of a 500 kWh developmental zinc-chloride BESS connected to a 300 kW converter, a 500 kWh lead acid battery and a 1.8 MWh calcium-grid lead-acid battery interfaced via a 2.5 MW converter. The utility application cycles included peak-shaving, spinning reserve, load following and special customer applications. After more than 30 years of this pioneering project, grid BESS have finally become a commercially viable technology. The increase in electric vehicle (EV) production has driven economies of scale and technology advancement that reduced the costs of lithium-ion (Li-ion) battery packs by 85% between 2010 and 2018 [6]. Consequently, the prices of lithium-based grid BESS have decreased significantly. The power capacity of BESS in the United States is projected to increase from 859 kW in 2018 [7] to 17 GW in 2050 [8].

BESS are flexible power systems assets capable of providing a plethora of services for bulk energy systems, transmission infrastructure, distribution infrastructure, consumer energy systems, and ancillary services [9]. From performing energy arbitrage through compensating voltage regulation due to RES volatility in distribution systems to minimizing electric frequency deviations via frequency regulation, ESS are expected to be a critical asset for ensuring reliable and cost effective power systems operation [10].

Many BESS' applications include distributed controls and intensive communications capabilities. For instance, some ESS applications require responding to remote price or control signals [10] and vendors offer remote software and firmware updates as well as advanced monitor and diagnostics in platforms through remote servers or cloud technology [11]. In the USA, the recently passed Federal Energy Regulatory Commission (FERC) Order No. 2222 will allow distributed energy resources (DERs) to participate in wholesale markets, which will demand bidirectional and frequent communications between aggregators that participate in markets and the fleets of DER they control [12]. The latest revision to the DER interconnection standard IEEE 1547 [13] will accelerate the adoption of grid-support functions performed by DER, which will present challenges for cybersecurity [5].

If on the one hand the adoption of Information and Communication Technologies can improve electrical system security and reliability by allowing higher flexibility and participation of small power generation and storage assets in grid operations, on the other hand, the extensive communication infrastructure necessary also increases the surface for cyberattacks, which creates concerns with respect to the cybersecurity of these systems [14]. The U.S. Government Accountability Office has found that the electric grid is increasingly vulnerable to cyberthreats, especially due to grid-connected Internet-of-Things (IoT) devices [15]. Similarly, the Electric Reliability Organization has identified cybersecurity vulnerabilities as one of its identified risks and cybersecurity as one of the priorities for improving grid reliability [16]. Recent intrusions to small infrastructure companies highlight the need for increased cybersecurity training and solutions for organizations that cannot afford specialized personnel [17].

When compared to other DER such as solar photovoltaic (PV), wind, and demand response, battery-based energy storage presents unique security, reliability, and safety challenges. BESS are currently used in reliability-focused

applications, such as backup power or black start, and can provide a wider range of ancillary services than other DER, which demands an increased level of resiliency and reliability and more complex communications infrastructure [18]. Furthermore, in a future scenario where most of the energy mix is composed of low-inertia and intermittent power sources like wind and solar PV, the importance of grid BESS for energy security and grid stability is expected to grow significantly. Some of the safety risks associated to BESS are common to other DER, such as susceptibility to natural disasters, arc flash due to large DC currents, and high voltages. However, batteries can pose additional safety risks if improperly handled or operated. Damaged or overcharged battery cells can produce toxic and flammable fumes and are susceptible to thermal events [19]. Therefore, dedicated protection and monitoring devices to ensure batteries operate within safe limits are imperative for grid BESS. These electronic devices are often managed remotely over the public internet, which increases BESS system complexity and vulnerability to cyberattacks. This combination of reliability, safety and cybersecurity risks makes grid BESS a higher-consequence target for malicious actors when compared to other DER.

While grid BESS is a maturing technology starting to prove cost-effective in several applications, recent research shows security of battery storage systems needs improvements [11]. The importance of BESS cyberphysical security is expected to grow significantly in the near future. This paper presents a comprehensive literature survey on the safety and security risks specific to BESS. To fully understand the cyberphysical risks associated BESS, applications, interactions between electronic components with batteries and the grid, and structure of grid BESS are reviewed in depth. While most cyberphysical security issues are common to other DERs that share similar power grid and communications interfaces, BESS present unique challenges that have received little attention in the current literature. Because cybersecurity of BESS is still an incipient research area, many aspects of BESS security are currently not yet covered in specific research works, so investigation on closely related areas, such as EVs, mobile systems, and other DERs, as shown in Fig. 1, were also included for completeness. The goal of this paper is to survey BESS state-of-the-art cyberphysical security information, describe risks, current research gaps and future trends.

A. CYBERATTACKS TO CRITICAL INFRASTRUCTURE

Currently, the technical literature has no records of cyberattacks targeting grid BESS. However, multiple federal agencies and other U.S. government-associated entities have been reporting cybersecurity incidents [20]–[22] and issuing warnings about potential cyberattacks to critical infrastructure, operational technology (OT), and industrial control systems [15], [23], [24]. Recently, media outlets have covered multiple instances of cyberattacks to the power grid and other closely related systems. In December 2015, a coordinated attack on three Ukrainian regional power distribution utilities remotely disconnected seven substations, causing a power interruption that affected approximately 225,000 customers [22]. The perpetrators also took actions to make operators unaware of the situation and to hinder system restoration. Another service interruption caused by a cyberattack happened in 2016 in Ukraine [25]. This attack was more automated than its predecessor and it used a sophisticated malware known as *Crashoverride* or *Industroyer*. The malicious actors targeted multiple power transmission control systems in an attempt to create a sequence of events leading to a catastrophic outcome that included permanent damage of power system equipment. On the physical side, the attack started by opening circuit breakers to cut power delivery and then exploited a vulnerability of protective relays to disable overload or fault protection capabilities. Then the attackers anticipated that the power utility would follow the commonly adopted procedure of manually restoring service. Should a power system fault occur in this moment, such event could result in permanent damage to power system equipment due to uncleared faults and lead to sustained and large-scale power interruption, possibly requiring replacement of power transformers or lines. Fortunately, because the attackers lacked a deep understanding of how the target system worked and were not fully aware of the system vulnerabilities during this event, a large scale power outage was avoided. The attack was more ambitious than the previous year's, but it failed to cause major sustained grid disruption.

The literature on consequences of cyberattacks to power grids is very rich in examples of attacks that are much more complex than those to the Ukrainian power grid in 2015 and 2016. The Aurora Generator Test has shown that a remote attack on a digital relay protecting a generator or spinning machine can reclose the relay to create an out-of-phase condition with the power grid, causing serious damage to the rotating machine due to over-torque stress [26]. This vulnerability could be exploited through several attack vectors, including manual reclosing of a circuit breaker, malicious code injection into the relay's firmware, manipulation of programmable digital relay parameters through a connected computer, accessing the device's front panel to change relay parameters and disable protection mechanisms, or malicious command injection through compromised communications channels such as modem, internet, wireless, or supervisory control and data acquisition (SCADA) system [27]. The concept of using distributed denial-of-service (DDoS) [28] or false data injection attacks (FDIA) [29] to mislead power systems operators into taking actions that can lead to cascading failures has also been shown in simulations.

In 2018, it was reported that control rooms of US power utilities have been targets of cyberintrusions [30]. 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[1] firewall led to loss of visibility of 500 MW of generation assets in the US [31]. The affected power company

[1] A patch is a software or firmware update aimed at fixing a vulnerability.

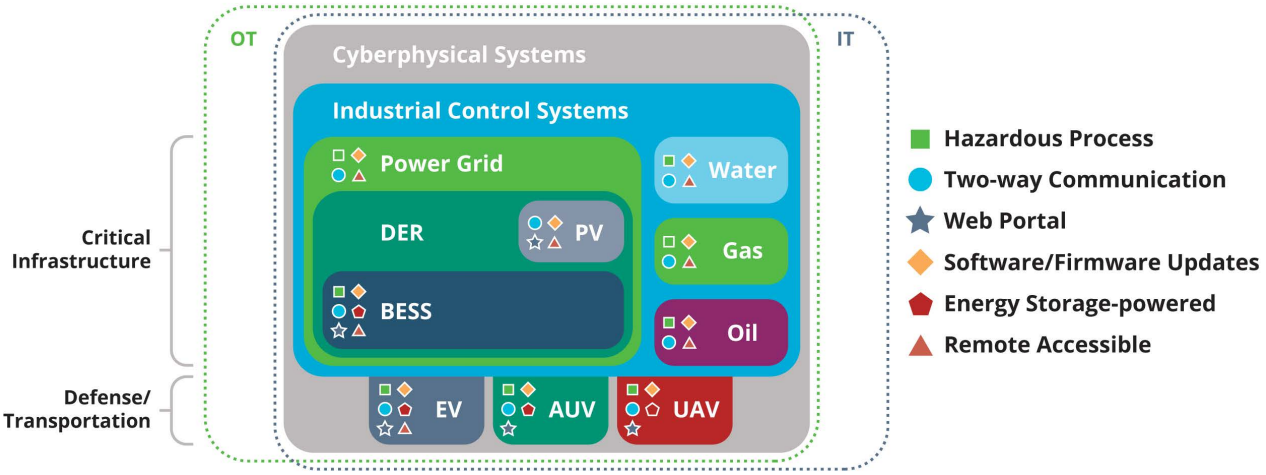


FIGURE 1. Relationship between areas closely related to BESS and relevant security features.

experienced intermittent service due to frequent reboot of the firewall, which only ended after the patch was applied. More recently, a cyberattack to the industrial control systems (ICS) of a natural gas compression facility caused a two-day shutdown of a gas pipeline [20]. The threat actor obtained access to the company's Information Technology (IT) network through a spearphishing attack and later gained access to the OT network due to lack of network segmentation. In 2021, a major fuel pipeline in the USA had its operations halted due to a ransomware attack [32]. These incidents highlight that there is cybersecurity education gap within the ICS operation community.

B. RELATED LITERATURE

Even though the subject of energy storage cyberphysical security is still new, many review papers have been dedicated to describing security measures for closely related areas, such as Smart Grids [29], [33]–[53], particularly for DERs [54], energy storage systems in general [55], and more broadly for cybersecurity of cyberphysical systems (CPS) [56]–[60]. However, BESS have unique features and safety subsystems that increase risks and the complexity of cybersecurity when compared to other DERs or even other ESS. Reviews of cybersecurity exclusively for Battery Managements System (BMS) threats and defenses implemented following an IoT paradigm are presented in [61], [62]. These publications have a strong focus on Blockchain-based cyberdefense strategies.

A perspective on cybersecurity of battery systems of the IoT is presented in [63], where security threats to BMS are classified in three layers: physical, battery management and application. High-level descriptions of attack vectors for all layers and cross-layer attacks are presented, as well as a proposed taxonomy of Battery System Attacks that classifies them according to targeted layers, action characteristics and attack mediums. The focus of that paper is not on grid BESS, but on solar power management system, mobile communications devices, and vehicles such as EV, unmanned aerial vehicles (UAVs), and autonomous underwater vehicles (AUVs). Several aspects of the literature on cyberphysical security of EVs have been reviewed in [64]. EVs and BESS share very similar batteries, BMS, and power conversion system (PCS) components, which make them a relevant benchmark.

In [11], the authors have performed security assessment of home BESS, reporting the vulnerabilities and exploits necessary to perform some attacks to those systems. A literature survey on attacks to BESS and detection methods during operation with a focus on approaches based on machine learning (ML) is presented in [65]. The pioneering work [66] has discussed several hypothetical cyberattacks to grid BESS. The authors have also used real hardware in a laboratory environment to demonstrate that, given access to the local BESS communications network, a malicious actor could manipulate real and reactive power outputs of a BESS despite authentication controls.

From a more applied perspective, [5] presents a review on basics of cybersecurity, communications systems, cybersecurity guidelines and standards applied to DER, as well as recommendations for DER networks in a format intended as an introductory document for informing DER vendors, aggregators, and grid operators. This report focuses on current best practices and state-of-the-art for DER in general and does not emphasize on ongoing research on the area.

This paper aspires to closing some gaps of the current literature. None of these surveys have provided a comprehensive literature review focused on grid BESS. For instance, [55] does not cover battery-specific risks, does not cover risks associated with all BESS on a component level, and focuses on IT-based solutions for securing ESS. Also, several categories defenses applied to CPS are not covered in [66] either. Additionally, important aspects of BESS necessary to understand threats and risks, such as applications and detailed

overview of all system components have not been reviewed in detail.

C. PAPER ORGANIZATION

The remainder of the paper is organized as follows. The next three sections provide information necessary to understand BESS risks and system criticality. An overview of BESS grid applications and their relevance to risk analysis is presented in Section II. Section III discusses battery operation and the safety risks of the most common BESS technologies. Section IV details relevant aspects and cybersecurity vulnerabilities of all major components of a grid BESS, with a focus on supervisory and management systems (IV-A), BMS (IV-B), PCS (IV-D), communications (IV-C), and gas and fire protection (IV-E) with a focus on Li-ion BESS that are currently the most pervasive systems. Following the discussion on BESS risks, the following two sections provide more insights into cyberthreat mitigation in the forms of technology and processes. Section V presents BESS cyberphysical security in the broader context of Smart Grids and other DER, with a focus on proposed cyberphysical security controls and countermeasures. Section V-A provides a review on relevant cybersecurity concepts applicable to CPS. An overview of applicable standards is presented in Section VI. The conclusion of the work and a compilation of research gaps are presented in Section VII.

II. CLASSIFICATION OF GRID BATTERY ENERGY STORAGE SYSTEMS

Battery technology, application, and size of BESS are fundamental aspects to consider when assessing the cybersecurity risks involved with any BESS. This section will present a discussion on the latter two classification criteria of BESS and discuss their implications. The intent of classifying BESS is to better understand how critical a system so well-informed decisions on security investments and system hardening can be made. The cost-effective implementation of security controls should to be informed by risk assessment and by understanding asset criticality. More details on battery technology are left to Section III.

A. CLASSIFICATION BASED ON APPLICATIONS

Over the last few years, given the favorable policies and the improvement of battery technologies, the application space for BESSs has grown significantly. The use cases of BESSs can typically be classified as power or energy applications. A summary of BESS applications are given in Table 1. Power applications involve charging and discharging large amount of power over short periods (seconds to minutes). Energy applications require charging and discharging large amounts of energy over long periods, often several hours [10]. As more and more BESSs are deployed at different places on the grid, their applications can also be categorized based on their locations. The terms Front-of-meter (FTM) and Behind-the-meter (BTM) are often used to specify the location of a BESS relative to a revenue meter. While BTM systems are often owned by the end customers (e.g., residential homes, commercial and industrial facilities) and used for customers' benefits (e.g., time-of-use management, demand charge reduction), FTM systems are often owned by the utilities and operated for grid services (e.g., transmission and distribution deferral, peak shaving).

TABLE 1. Applications of grid BESS.

Application	Power or Energy?	FTM or BTM?
General Energy Applications		
Energy Arbitrage	Energy	FTM
Renewable Energy Firming	Energy	FTM and BTM
Renewable Smoothing	Power	FTM and BTM
Ancillary Services		
Frequency Regulation	Power	FTM
Operating Reserve	Energy	FTM
Frequency Response	Power	FTM
Voltage support	Power	FTM
Ramp support	Power	FTM and BTM
Black Start	Power	FTM
Transmission Services		
Upgrade Deferral	Energy	FTM
Congestion Relief	Energy	FTM
Stability Damping Control	Power	FTM
Distribution Services		
Peak shaving	Energy	FTM and BTM
Voltage regulation	Power	FTM and BTM
Reliability and Resilience	Energy and Power	FTM and BTM
End customers' services		
Time-of-use management	Energy	BTM
Power Quality	Power	BTM
Resilience (Back-up power)	Energy	BTM

The application of a BESS is a determining factor of risks caused by loss of data confidentiality, asset integrity, or availability. For instance, the consequences of loss of availability of a BESS providing energy arbitrage-type services are loss of revenue, while disabling a system providing black-start or backup power services will impact reliability, continuity of service, and power grid resiliency.

B. CLASSIFICATION BASED ON SIZE

Similarly to the nomenclature used by the solar PV industry [67], grid-connected BESS can be classified in three categories according to size: utility, commercial and consumer. Utility-scale BESS are typically multi-megawatt systems connected to distribution or transmission grids. These systems can provide significant power and energy capacity for bulk power systems and they might fit the definition of bulk electric systems [68] (more details in Section VI). Failure to provide ancillary or transmission services to the bulk power grid could have severe consequences for large areas. The loss of availability of BESS applied to power

distribution system can impact power quality or continuity of service for hundreds of consumers. However, the size of the organizations that operate those devices allow them to support the implementation of enterprise cybersecurity policies, in addition to enforcement of regulations, both of which can provide a high level of cyberprotection.

Commercial-scale systems are rated from tens of kilowatts to a few megawatts. They are usually owned by power utilities, industrial, or large commercial enterprises and are used to support microgrids and buildings, provide services to power distribution systems, provide backup power for industrial loads, or in other BTM applications. Those systems fall under the DER class, however, might be owned by smaller organizations that cannot support specialized cybersecurity functions or even by end consumers. Therefore, those systems are not subject to the same rigorous cybersecurity requirements of utility-scale BESS [69].

Finally, consumer-scale BESS are smaller and much simpler systems than the previous two classes, having only a few kilowatts of capacity. Typically consumer-scale BESS provide behind-the-meter services used primarily by residential and small business applications. It is not expected that these systems are maintained nor operated by specialized personnel, therefore common physical security and cybersecurity controls could be insufficient or nonexistent. This lack of security calls for turnkey, system-level cybersecurity solutions that will enable consumer-scale DER to securely play an increasingly important role in power systems operations.

III. BATTERY TECHNOLOGIES

The goal of this section is to present an overview of the most relevant battery technologies being used for grid applications and how they relate to cyberphysical security of BESS. Knowing the modes of failure and overall safety characteristics inherent to each battery chemistry is important for understanding the risks associated with the overall BESS.

Rechargeable battery technology has driven the development of large markets in the 20th century. Until 1910,internal combustion engine cars did not use any electrical components and were started using a cranking handle. It was not until 1912 that Cadillac introduced a car with a starter and a lead-acid battery, and by 1920 lead-acid batteries were used in almost every car. Until Li-ion batteries were developed, consumer electronics used primary alkaline batteries and portable computers used low-capacity and low-density Nickel-Metal Hydride (NMH) batteries. The first Li-ion battery was introduced by Sony in 1991 and accelerated the adoption of laptop computers, camcorders, and cell phones, paving the way for the personal communication devices that we all carry today [70].

Over the years, the same lead-acid and Li-ion batteries developed for low-voltage applications, have been used in higher-voltage applications. Lead-acid batteries are used in 500 V power backup systems used in datacenters, providing power grid applications like renewable integration, and transmission and distribution services [9], and Li-ion batteries are applied to 400 V or higher battery packs used in electric cars. As the voltages of the battery systems increase, so does the need for monitoring and maintenance. Lead-acid batteries in uninterruptible power supply (UPS) applications operate on float for most of the time and are maintained by specialized technicians who check the batteries for signs of degradation every 6 months. Li-ion batteries in EVs are subject to continuous charge and discharge regimes and are monitored and rebalanced in real time by BMS.

The probability of failure of individual battery cells equipped with safety devices is very low. However, in large-scale systems that operate a large quantity of cells, the probability of failure is increased significantly [71]. For instance, a single cell going into thermal runaway will dramatically increase the temperature of nearby cells within the same battery module, thus propagating the failure. This highlights the importance of battery, gas, and fire protection systems to large-scale grid BESS [72].

Vulnerabilities in the protection systems can be leveraged by malicious actors to cause cyber-induced safety incidents. Batteries hazards have been documented extensively in the technical literature and by the media. Incidents involving fires and explosions of battery cells have been reported many times recently. Fire in battery-powered consumer electronics such as smartphones [73]–[75], e-cigarettes [76] and ''hoverboards'' [77] received significant coverage from the press. In the transportation sector, fires in airplanes [78] and electric vehicles [79] have also been documented. With the advent of grid BESS, incidents involving fire and explosion of utility-scale systems have also been reported all over the world [80]–[82]. Accidents in BESS have been linked to defects in battery cells, insufficient battery management capabilities (e.g. no overvoltage or overcurrent protection), environmental conditions (e.g. humidity, dust), and lack of experience in BESS integration [83].

As the percentage of RES on the grid increases, the number of stationary ESSs and the sophistication of their control will increase making them targets for cyberattacks. Such attacks can severely damage ESSs by tampering with the operating parameters or by simply disabling the battery monitoring system while a battery is being operated. Sometimes the last-resort action of turning the system off during an attack can cause catastrophic failures depending on the operation and state-of-charge (SoC) of the battery at the time. For example, for Li-ion systems, depending on how the system is designed, emergency shutdown might halt energy redistribution of cells and turn off sensing and control of battery cells. Because the chances of thermal runaway grows with SoC, that can pose a significant safety risk when cells are fully charged. As an additional example, for water-based systems, gas evolution can occur if a system is stopped at the top of charge and that can lead to high concentration of toxic or flammable gasses.

Therefore, the analysis of the cybersecurity of energy storage systems is dependent on an understanding of the nonlinear behavior of batteries and of their failure and degradation

TABLE 2. Batteries commonly used in grid applications and their key characteristics [9], [84]–[87].

Type	Voltage[a]	Voltage range	Temperature range	Energy density	Efficiency[b]	Cycle life	Safety	Charging
LFP	3.3 V	2.5 - 3.6 V	-30 - 60 °C	60-110 Wh/kg	95%	>1000	◔	CC-CV
NMC	3.7 V	2.5 - 4.2 V	-20 - 60 °C	100-240 Wh/kg	95%	>500	○	CC-CV
Lead-Acid	2.0 V	1.75 - 2.1 V	-40 - 60 °C	10-40 Wh/kg	70-75%	200 - 1500	◓	CC-CV, Float
Redox flow	1.4 V	1 - 1.6 V	0 - 40 °C	10-50 Wh/kg	85%	>10,000	◕	CC-CV [88]
NaS	2.076 V	1.78 - 2.1 V	270 - 350 °C	117 Wh/kg	86%	4,500	◔	CP
Zn/MnO_2	1.5 V	0.9 - 1.5 V	-20 - 40 °C	100 Wh/kg	50-90%[c]	20-3000[c]	◔	CV/CP

[a]Nominal voltage.

[b]Round-trip efficiency.

[c]Highly dependent on depth of discharge [87], [89].

modes. The rest of this section will focus on the most common and promising types of grid-scale energy storage technologies, Lithium-ion, aqueous batteries, like flow batteries, and liquid metal batteries, like sodium-sulfur. First, we will establish some common nomenclature and then discuss the vulnerability to cyberattacks of each of the chemistries.

A. DESIGN OF BATTERY SYSTEMS

Battery systems are assembled from cells connected in series and parallel to build voltage up to 400-1000 V and current up to 40 - 50 A. Cells of different chemistries operate in dissimilar voltage ranges (Table 2). For example, 12 V lead-acid batteries are made of 6 cells. Each cell operates between 2.5 V and 1.6 V. As the SoC of the cells changes from 0 to 100% the voltage also changes. For a given SoC, the voltage during charging is higher than the voltage during discharging. The discharge voltage curves are also a function of the charge and discharge current.

Fig. 2 shows the discharge curves for a lithium iron phosphate (LFP) battery at different discharge rates as a function of the SoC. Even commercial cells exhibit some cell-to-cell variation that increases with the age of the cell (as shown in Fig. 3). The energy capacity of batteries also changes over time (as shown in Fig. 3), and its variation is dependent on the operation of the battery. In many cases, a correct modeling of loss of capacity is necessary to ensure the safe operation of battery cells as they age and degrade.

With this background, we can now analyze the safety risks associated to different battery chemistries. Although there are several emerging battery technologies, and several incumbents (like nickel-zinc, NiZn), the discussion is limited to five types of batteries. Li-ion batteries are taken as an example of modular battery that requires a BMS and thermal control. Lead-acid batteries are a mature technology used in backup power applications. Zinc manganese technology utilizes low-cost materials and has good safety characteristics. Redox flow batteries are taken as an example of large-scale long duration batteries that require complex balance-of-system components like pumps and tanks. Sodium-sulfur (NaS) batteries are taken as an example of batteries that operate at high temperature. Each of the type

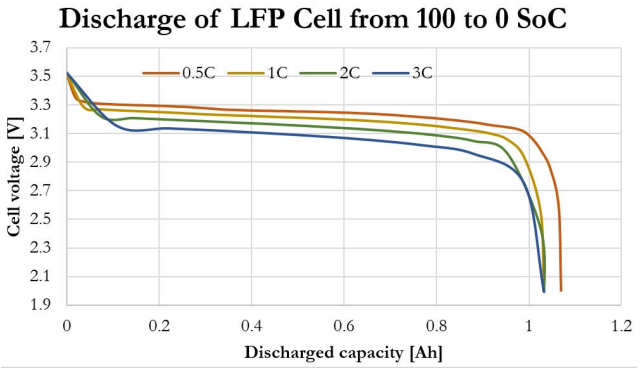


FIGURE 2. Discharge curves from LFP cells under different discharge currents [90].

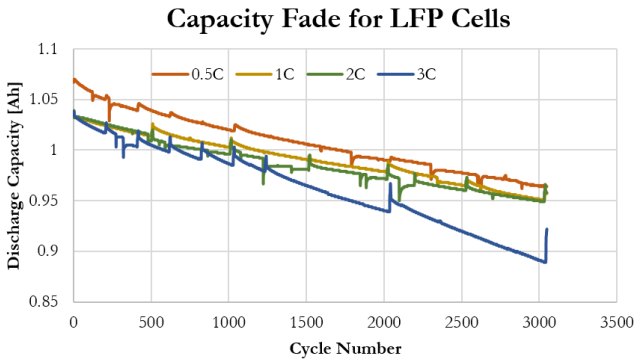


FIGURE 3. Capacity fade as a function of cycle number for LFP cells [90].

of batteries discussed in this section presents different degradation and safety risks if a malicious agent tampers with the BMS. A summary of relevant characteristics of select battery technologies is shown in Table 2.

B. MODULAR BATTERIES: LITHIUM-ION

Li-ion batteries are the most common choice for ESS of up to 4 hours of capacity. In other words, the battery contains enough capacity (kWh) to be used at a rated power (kW) for 4 hours. Li-ion technology is very popular due to its unmatched energy density, which theoretically can reach 1.5 MJ/kg [71]. The most common Li-ion batteries have

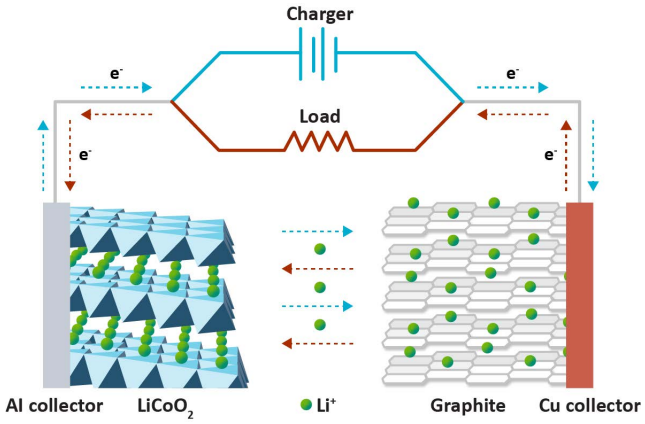


FIGURE 4. Illustration of the chemical reactions within a lithium-ion battery.

a graphite anode. The most common cathodes are lithium cobalt oxide (LCO), lithium manganese oxide (LMO), nickel manganese cobalt oxide (NMC), and LFP. A picture showing how Li-ion cells work is shown in Fig. 4. Lithium ions move from the anode to the cathode during discharge (red arrows) and reverse the flow during charge (blue arrows).

Safety is often cited as drawback of the technology since Li-ion cells are subject to thermal runaway [91], [92]. In some cases, thermal runaway is caused by construction defects. In other cases, internal shorts develop as the cells are cycled. The most relevant cause of thermal runaway for this paper is abuse conditions such as overcharge. A comprehensive review of failure modes that can lead to thermal runaway can be found in the literature [93]–[95] and it is outside the scope of this review.

To prevent thermal runaway, Li-ion cells are operated in a narrow voltage range (˜2.5-4 V) using complex BMSs that can detect out-of-bounds conditions in cell-to-cell voltage and SoC [96]. The industry has also developed methods for the early detection of thermal runaway that include a combination of cell voltage sensing, surface temperature or internal temperature monitoring, detection of gas venting, and electrochemical impedance spectroscopy (EIS) [97].

Any cyberattack that stops cell monitoring during charge/discharge, tampers with the parameters of a few cells, or impairs the cooling system can lead to catastrophic failures even when the string is seemingly operating in nominal conditions. To prevent thermal runways from a single cell to propagate to the system, the industry has developed thermally and mechanically insulating battery pockets that however increase the cost and decrease the energy density of the systems.

C. AQUEOUS BATTERIES: LEAD-ACID

Lead-acid batteries are a mature technology with low cost and widely available. The first practical designs date to 1860, following the work of Raymond Gaston Planté. Current designs use lead dioxide in the cathode and lead in the anode with an aqueous solution of sulfuric acid as the electrolyte [84]. A recent study has found that 99% of lead-acid batteries were recycled between 2014 and 2018 [98].

The two major types of lead-acid batteries are sealed or valve-regulated lead-acid (VRLA) and open or vented. Open-vented batteries are the older technology that require regular routine maintenance, can release hydrogen gas on charge, spill sulfuric acid, and need to be stored and used in vertical orientation. The safety issues related to possible gassing and spilling make the open design of lead-acid batteries ill-suited for applications in closed spaces with people. VRLA technology requires little to no maintenance due to the very low loss of electrolyte, are safe for use in confined spaces and can be used and stored in any orientation [99].

Lead-acid batteries are used in a wide range of applications. The most common of application is starting, lighting and ignition of internal combustion engines, including automobiles, marine vessels, and aircraft, but also stationary power (e.g. substation switching power, diesel generators). This application takes advantage of the good performance for high-rate discharge and float charge. Traction and propulsion of vehicles and vessels are another application, which includes the use of lead-acid batteries as the primary power source of vehicles, such as EVs, submarines, and industrial trucks. Stationary applications include standby power such as UPS, grid energy storage, communication utility backup power, to name a few examples. Lead-acid batteries can also be found in portable electronics and consumer products [84].

Overcharge leads to oxygen and hydrogen evolution and the consequent loss of water. In open systems these gases escape the battery while in VRLA designs minimize the hydrogen evolution and promote recombination of oxygen with the negative plate. Energy density is relatively low, which limits its application in vehicles and portable devices, areas where Li-ion systems have been prevalent recently [84]. Leaving lead-acid batteries in a discharged state can lead to sulfation, which creates irreversible damage. Temperature effects include reduced expected float life for temperatures higher than 20°C, reduced output capacity for temperatures under 20°C, and sensitivity of open circuit voltage of −3 mV per °C per cell [99]. For standby power source applications where the battery has to operate over a large temperature range, temperature compensation should be applied to float current and charge. To make temperature compensation more effective, battery and charger should be kept at the same temperature [100]. Lead-acid batteries are managed using dedicated chargers and inverters that control the charging sequence and the discharging limits. The typical charging sequence include a bulk charging step (Constant Current – CC), followed by an absorption step (Constant Voltage – CV), followed by float charging that is required to compensate for self-discharge. Lead-acid batteries used with solar energy or in grid applications can require a more complex control firmware, which could increase its vulnerability to attacks that, for example, can increase charging voltage during CV or extend the CC charging portion and cause gas generation. Prolonged periods of high float current

can deplete the water in lead-acid batteries, leading to a collapse in internal resistance that generates significance heat and potentially fire. This compounding process is also called thermal runaway but is entirely different from the process by that name in Li-ion batteries.

D. AQUEOUS ALKALINE BATTERIES: ZINC MANGANESE

Rechargeable alkaline zinc–manganese oxide ($ZnMnO_2$) batteries utilize a zinc anode (positive terminal) and a manganese dioxide (MnO_2) cathode (negative terminal). These batteries derive from primary cells that use a strongly basic electrolyte like potassium hydroxide (KOH) introduced in the 1950's [87]. This alkaline primary $ZnMnO_2$ chemistry has been used in primary batteries used in portable electronics for more than 3 decades. Efforts to design rechargeable $ZnMnO_2$ have met challenges with zinc dendrite formation and degradation of the MnO_2 material after just a few cycles [101]. The need for large, low-cost, safe energy storage has prompted a renewed interest in the chemistry [102]. Furthermore, rechargeable $ZnMnO_2$ are used as replacement for lead-acid and alkaline batteries and consumer electronics applications [84].

Several characteristics make alkaline $ZnMnO_2$ batteries a potential alternative to current grid-storage battery technologies [87]. These batteries have low cost, good capacity retention, good safety features, and no maintenance requirements due to their sealed design. Zinc has low cost, it is not toxic, has high theoretical capacity and low standard electrode potential. Furthermore, zinc metal is relatively stable in aqueous electrolytes [87], [103].

Current commercially available rechargeable $ZnMnO_2$ batteries for grid storage have 100 Wh/L of energy density and a cycle life of up to 300 cycles [87]. To achieve extended cycle life, however, it is necessary to limit significantly the depth-of-discharge (DoD). Cyberattacks that induce high-current rates and high DoD can decrease significantly the cycle life of $ZnMnO_2$ batteries. Alkaline batteries are charged using a sequence of CC and CV steps driven by the voltage of the battery. If the charging and voltage limits are exceeded, gas generation can occur.

E. FLOW BATTERIES: VANADIUM REDOX

There are several types of aqueous batteries. They are not subject to thermal runaways. However, side reactions that are not significant when batteries operate within nominal voltage and temperature ranges can lead to failure and safety issues when the batteries are operated outside their normal range of operations. In this section we discuss in more details the safety risks associated with redox flow batteries.

Flow batteries use an electrolyte, ion-selective membrane stack, and two large tanks. Electrolyte from each tank flow through the membrane stack and exchanges ions with the electrolyte flowing from the other tanks. Vanadium Redox Flow batteries are the most common flow batteries in the market. The electrolyte is strongly acidic and made by dissolving vanadium pentoxide in sulfuric acid. The battery

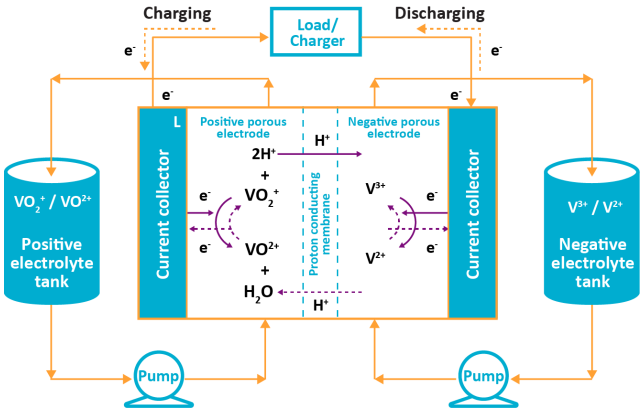


FIGURE 5. Vanadium flow redox battery [104].

string is made of several cells connected in series. Each cell operates between 1 V and 1.6 V. Flow batteries are subject to corrosion and gas evolution. At the top of charge (>1.6 V), gas evolution becomes significant with H_2 evolving from the negative electrode and CO_2 and O_2 evolving from the positive electrode. The release of these gases can create explosive conditions. In addition, pump operation is important to prevent self-discharge from shunt currents and keeping the battery operational.

A cyberattack that disabled the BMS during charging can lead to gas generation and explosions. An attack that disables the pumps operation or tampers with their set point can render the system unusable.

F. MOLTEN METAL: SODIUM-SULFUR

The development of NaS battery technology started in the 1960's within the automobile industry. The first grid applications of the NaS batteries developed by NGK and Tokyo Electric Power Company (TEPCO) in Japan dates to 2002 [105]. The normal operating temperature regime of NaS cells during discharge/charge cycles is in the range of 300 °C to 350 °C. These batteries are used in stationary applications and in heavy transportation vehicles. NaS batteries have been used in grid energy storage products, and currently there are more than 200 products and more than 600 MW/4.2 GWh [106]. Room temperature NaS batteries are a promising technology but the research and development is still in an early stage [107].

NaS batteries are unique as they use liquid electrodes and a solid electrolyte. During discharge, the sodium (negative electrode) is oxidized at the sodium/beta alumina interface, forming Na^+ ions. These ions migrate through the beta alumina solid ceramic electrolyte and combine with sulfur that is being reduced at the positive electrode to form sodium pentasulfide (Na_2S_5). The Na_2S_5 is immiscible with the remaining sulfur, thus forming a two-phase liquid mixture.

The characteristics of NaS make them good candidates for power grid applications. These batteries are potentially low-cost systems, made from inexpensive raw materials, with high cycle life, high round-trip efficiency, and high power

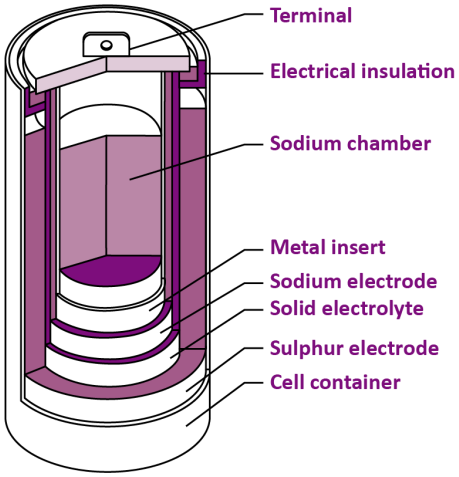


FIGURE 6. Sodium-sulfur battery [108].

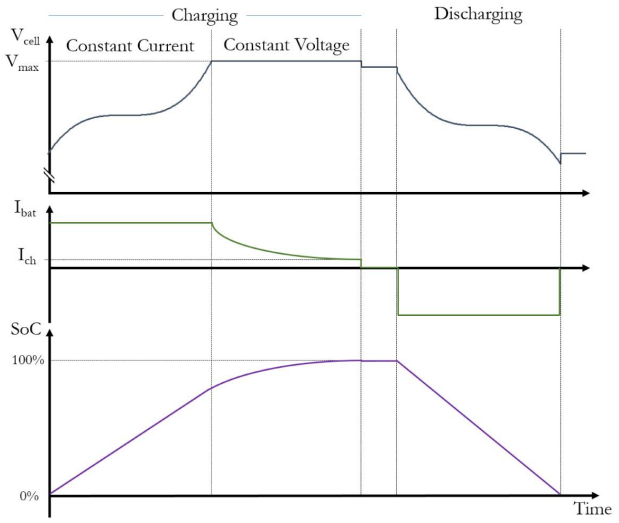


FIGURE 7. Charging cycle of a battery cell.

density. The cells' enclosures are sealed, which makes them insensitive to ambient conditions [84]. In spite of temperature increases during discharge, resistance heaters might be necessary to maintain cell temperature above 290 °C during standby [105]. The cells need to be well sealed or the electrode material can ignite in contact with open air and humidity. A cyberattack that disrupts the heating element of the a NaS battery will render it unusable.

G. CHARGING AND DISCHARGING

Each type of cell requires specific charging protocols. For example, the most commonly used method for charging a Li-ion battery is the CC-CV [84], shown in Fig. 7. Starting from a fully depleted cell, first the battery is charged with constant current until it reaches the maximum operational voltage of the cell. This stage is responsible for most of the charge. As the voltage increases, the power drawn from the charger also increases and reaches the peak at the end of the constant current stage. After this point, the cell enters constant voltage mode and the current starts decaying exponentially as the cell recharges. The battery is considered completely charged when this current reaches a very low value. Constant voltage mode usually takes a long time to complete. Some manufacturers speed up the constant voltage charging mode by slightly increasing the voltage in this mode. Since the open-circuit voltage of many batteries is temperature-dependent, care must be taken if the cell chemistry has low overcharge tolerance.

In standby power source applications, lead-acid batteries use two-step CV charging or charge compensation method. In the two-step CV method, a CC stage is followed by two CV stages, the first one having a higher voltage level than the second. For instance, for a 6-cell VRLA lead-acid battery, the first CV step could be set to 14.7 V and in the second trickle charge CV step the voltage is kept at 13.7 V at 25 °C. The transition between both CV stages occurs when the current falls below a certain threshold [100]. During float charge, the battery is constantly being charged, thus maintaining full charge in spite of self-discharge [84], [89]. The charge compensation method, also known as float charge or trickle charge, following a CC and a CV steps, the battery is disconnected from the load and a small current is injected into the battery to compensate for self-discharge. Lead-acid batteries used in applications where it is the main power source and constant cycling is required, also use a CV or CV-CC recharging cycle [100]. Zinc-manganese oxide batteries can be minimized by the used of pulsed DC and AC charging protocols [87]. The NaS batteries are charged using a near CV protocol and require an initial formation step that depends on the details of the NaS electrolyte composition. Despite any optimal or vendor-recommended charging cycles, often practical charging and discharging cycles are dictated by the application, so constant power (CP) cycles are often used [105], [109], [110].

H. STATE-OF-CHARGE ESTIMATION

The SoC of a battery is defined as the fraction between the remaining capacity in its maximum available capacity [111]. In the BMS, SoC is a key parameter that controls charging and discharging cycles which determines the useful operational life of battery. An accurate estimation of SoC is required for safety and effective charge management during operation of BESS. Therefore, from a cyberphysical security perspective, SoC estimation is important for mitigating risks of damaging battery cells due to overcharge or overdischarge. Furthermore, as shown in sections V-J3 and V-K, anomaly detection cybersecurity-aware control methods utilize mathematical models of physical systems.

It is a very challenging task to estimate SoC due to nonlinear behavior of electrochemical properties of the batteries based on internal operating conditions and external grid interactions. Furthermore, key parameters of batteries are often not known precisely and vary depending on environmental

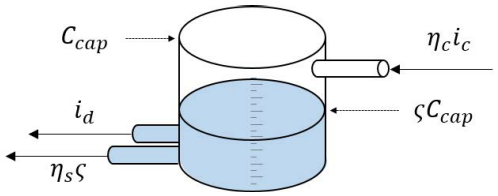


FIGURE 8. Depiction of charge reservoir model.

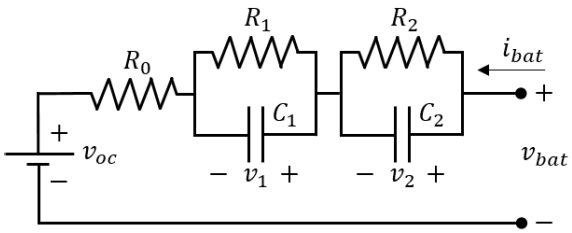


FIGURE 9. Example of second-order equivalent circuit model.

or operational conditions. Battery capacity and impedance are affected by aging and are also temperature-dependent. Battery operational conditions such as type of cycle profile it operates under, including depth of discharge, temperature, charge and discharge rates are factors that contribute to the speed of battery degradation [112]. Open-circuit voltage (OCV) is also dependent on temperature, which poses additional challenges to parameter estimation.

Primary SoC estimation approaches can use Coulomb counting, a method in which the SoC of a cell is estimated by calculating the integral of the battery current [113]. In recent papers, Xiong *et al.* [114] and Rosewater *et al.* [111] have provided an extensive overview of the SoC models and discussed various advantages and disadvantages of each method for a given application. These SoC models play a very crucial role in implementing the optimal control strategies. Many methods are available in the literature for estimation of the SoC using battery models. Models that define capacity in units of energy can be classified as energy reservoir models (ERM), those which define in units of charge as charge reservoir models (CRM), and those which define units of concentration as concentration-based models. An example of a charge reservoir model is shown in Fig. 8. In addition, the thermal effects of heat generation in the batteries and heat transmission to external enclosures on the battery models must be taken into consideration. A succinct summary of the all the important methods for the battery models is available in [111].

The SoC estimation methods can be classified as direct methods, in which the parameters of the models are determined using the physical relationships between the SoC and the measured quantities such as voltage, current, and temperature. In general, these methods are open loop in nature and introduce significant errors in the estimation of the SoC. Whereas in indirect methods, such as model-based estimation algorithms minimize estimation errors by employing high-fidelity battery models that capture the behavior of the system under various operating conditions and applying various forms of state estimation techniques, such as extensions of the Kalman Filter (KF) for nonlinear dynamic systems. The model-based methods have the capability to estimate in real time and can integrate both electrical and thermal equations in the estimation algorithms. Hence these algorithms attracted the attention of many research investigators [115]. In addition to direct and indirect methods, data-driven SoC estimation methods are being investigated for battery systems in which mathematical models are not available. These can be used for prognostics of end-of-discharge time or run-time [116].

In the BMS, the model-based estimation algorithms have become common for SoC and parameter estimation purposes. The equivalent circuit models (ECMs) are being used for capturing the dynamic behavior of the battery systems, due to their simplicity and accuracy. These models are often used to develop the model-based SoC estimation methods used in commercial BMS [117]. The OCV of a battery cell is represented as an SoC-dependent voltage source, sometimes modeled using a nonlinear function or using a lookup table. The phenomena of polarization of the cell due to passage of current, double-layer capacitance due to accumulation of charge carriers, and diffusion are represented by series resistance and parallel resistor-capacitor (RC) circuits, a model known as Randles cell [118]. Several pairs of RC circuits can be connected in series to represent cell polarization. The parameters of the cell might differ during charge and discharge [118]. A depiction of a second-order ECM of a Lithium-ion battery is shown in Fig. 9 [111].

$$i_{\text{bat}}(t) = i_c(t) - i_d(t)$$
$$i_c(t) \geq 0, \quad i_d(t) \geq 0 \tag{1}$$
$$\frac{dv_1(t)}{dt} = \frac{-1}{R_1 C_1} v_1(t) + \frac{1}{C_1} i_{bat}(t) \tag{2}$$
$$\frac{dv_2(t)}{dt} = \frac{-1}{R_2 C_2} v_2(t) + \frac{1}{C_2} i_{bat}(t) \tag{3}$$
$$v_{\text{bat}}(t) = v_{\text{oc}}(t) + R_0 i_{\text{bat}}(t) + v_1(t) + v_2(t) \tag{4}$$
$$v_{\text{oc}}(t) = h(\varsigma(t)) \tag{5}$$
$$\frac{d\varsigma(t)}{dt} = \frac{1}{C_{\text{cap}}}\left(\eta_c i_c(t) - \frac{i_d(t)}{\eta_d}\right) - \eta_s \varsigma(t) \tag{6}$$

where

i_{bat} is the electric current going into the battery,
i_c is the charge current,
i_d is the discharge current,
ς is the battery SoC,
v_{oc} represents the battery OCV,
$h(\varsigma)$ is the (nonlinear) function that maps SoC to OCV,
R_0 is the series internal resistance,
$v_{1,2}$ are voltage drops on equivalent RC circuits,
$R_{1,2}$ are resistances of equivalent RC circuit parameters,
$C_{1,2}$ are capacitances of equivalent RC circuit parameters,
C_{cap} is the battery capacity,

η_c charging efficiency coefficient,
η_d discharging efficiency coefficient,
η_s self-discharging coefficient.

Due to uncertain battery parameters, noisy measurements and errors introduced in simplifications employed to obtain practical battery models, state estimation methods are commonly applied to battery monitoring. Those include KFs [119], Extended KFs (EKFs), Sigma-point KFs [120], [121], Sliding Mode Observers [122], [123], among others. A review on these methods is presented in [124]. SoC estimation becomes particularly challenging when batteries approach end-of-life (EoL) and their parameters change significantly from those of new batteries [125]. Common features of aged batteries are capacity fade and increased internal impedance (power fade). To overcome these challenges, authors have proposed joint state and parameter estimation algorithms such Dual Extended Kalman Filter [125] and Fuzzy Unscented Kalman Filters [126]. In spite of reduced estimation errors when compared to EKF estimation, DEKF has shown limitations in terms of observability of parameters. Joint estimation of states and parameters has also been proposed for concentration-based models, which are more detailed and complex battery models than ECMs and CRMs [127]. Manufacturers of BMS systems, however, are opaque when it comes to their SoC estimation algorithms.

I. STATE-OF-HEALTH AND DEGRADATION

The state-of-health (SoH) is typically used to quantify battery degradation with respect to known or predefined EoL and beginning-of-life (BoL) parameters. A common definition of SoH is the ratio between current (degraded) battery energy capacity and its BoL value [128], known as capacity fade. Typically it is considered that batteries reach EoL when they lose 20% of their BoL capacity. The use of batteries beyond this limit is known as second life and is common with repurposed EV batteries. Cyberattacks can be designed to reduce battery life by leveraging cell degradation mechanisms, as internal temperature increase, for example. Early battery degradation can harm the economic performance of BESS by increasing the need for maintenance, increasing the cost of cell replacement, or even reducing the life of the BESS.

SoH based on energy capacity degradation can be measured directly by performing a full charging and discharging cycle to estimate current battery capacity and then comparing it to BoL and EoL capacities. A more general definition of SoH, ϱ, expands this concept to change in the state-of-life (SoL) of any critical parameter, y (e.g. impedance, resistance, round trip efficiency, number of cycles, etc.), with respect to its BoL and the difference this parameter's value in BoL and EoL, as shown in (7) [111].

$$\varrho = 1 - \left| \frac{y_{\text{BoL}} - y_{\text{SoL}}}{y_{\text{BoL}} - y_{\text{EoL}}} \right| \tag{7}$$

Battery resistance monitoring is a feature of many BMS, sometimes associated with capacity fade to estimate SoH [129]. Battery internal resistance is an important parameter to monitor since it is known to increase when Li-ion batteries are subject to overcharge [96]. This method, however, might require interrupting battery normal operation so that its resistance or impedance can be measured [130]. Measurement of cell internal resistance might be done by observing variation in cell voltage when a significant load (or charge) is applied to a cell [129]. However, not all battery technologies exhibit a clear correlation between capacity fade and impedance [128]. Cycle count is another simple method used by some BMS manufacturers to estimate battery SoH [131].

Long term monitoring of battery strings using infrared images and voltage measurements has been proposed as a means of monitoring battery health and detect overcharged batteries [132]. This method however, requires thermal imaging of the batteries, which might be very hard to achieve in commercial batteries assembled inside of compact modules. Model based approaches, such as [133], can be used to track battery model parameter variations due to overcharge or overdischarge conditions. These methods, however, require precise knowledge of battery parameters, including possibly EIS tests, to achieve good signature matching.

Sophisticated degradation methods include semi-empirical approaches, which leverage rainflow cycle counting algorithms and stress factor models [134]. This method includes solid electrolyte interface (SEI) film formation, calendar aging, temperature, SoC, time, and depth-of-discharge stress factor models. This method, however, is intended for offline applications, requires tuning of several parameters and does not take into account other degradation factors. Researchers have proposed a method using ensemble learning to estimate SoH of batteries from the point of view of capacity and power fade [135]. This method, however, requires applying current pulses to batteries and are not dedicated for overcharge detection. A data-driven method based on an ensemble learning method has been proposed for detecting overcharge conditions on time-series battery cycling data [136].

J. SUMMARY OF BATTERY NEEDS

The management of a battery system includes, as discussed, several components. As batteries are built out of cells in series or parallel, the cells need to be kept balanced. A discussion on cell balancing methods is found in Section IV-B3. The cells need to be kept within a safe SoC. SoC estimation has to consider environmental conditions (like temperature), application conditions (like rate of discharge), and aging that causes the available capacity (SoH) to decrease and impedance to increase. Although these basic principles of battery management apply to all types of batteries, in the remainder of the document, the discussion with focus on the security of the most prevalent technology, Li-ion.

IV. STRUCTURE OF BATTERY ENERGY STORAGE SYSTEMS

In order to perform all of its functions, grid BESSs require dedicated safety, security, controls, power conversion and

FIGURE 10. Basic elements of a utility-scale BESS [137], [138].

communications subsystems. It is possible to group these devices in four subsets: storage module, integration, PCS, and energy management system (EMS) (see Fig. 10) The complex architecture of BESS depends on requirements dictated by several factors, including the battery technology, size of system, and applications. These will be discussed in detail in the next sections. A more detailed and functional list of the typical components and functions of a small-sized battery-based grid ESS is itemized below:

- Storage Module:
  - Battery modules (or battery packs);
  - Battery Management Systems (BMS);
  - Gas Detection System;
- Integration:
  - Environmental Control System (Heating, Ventilation and Air-Conditioning System);
  - Fire Suppression System (Fire Control System);
  - Communications networking devices, including network switches, routers, firewalls, and cables;
  - Electrical disconnects, circuit breakers and relays;
- Power Conversion System (PCS);
- EMS:
  - Energy Storage Management Systems (ESMS), also known as Supervisory System Control;
  - Human Machine Interface (HMI);

Consumer battery systems might have simpler architectures, composed of battery cells, a BMS, a PCS and a control unit (ESMS) [11]. On the other end of the spectrum, multi-megawatt utility-scale BESS can have a much larger number of devices, including dedicated stabilization control remote terminal units (RTUs), local monitoring systems, networked protection relays and fault recorders, video monitoring systems, power quality devices, to name a few [18].

From the point of view of information security, it is particularly important to understand how the pieces of equipment that compose a BESS exchange information and the networks involved in the communications. Fig. 11 shows a diagram of a grid BESS. Large systems are typically modular, having several PCSs connected in parallel. Smaller systems, such as BESS for home or small commercial and industrial applications have much simpler layouts. For these smaller systems, the functions of HMI, BMS and ESMS can be implemented by the same device, typically without Environmental Control and Fire Suppression Systems. These systems exchange information among themselves and with grid operators. Cybersecurity vulnerability can exist between any endpoints of communication. The BESS components are discussed in the following section.

A. ENERGY STORAGE MANAGEMENT SYSTEMS

Implementation of ESMS and BMS might vary depending on manufacturers. A single device might perform both functions in small BESS, while for large-scale systems these functions are implemented by multiple specialized building blocks. ESMS are often implemented by embedded computers hosting web interfaces serving users and maintenance, as well as providing communications with remote servers from vendors. At each ESS, there is a local EMS, the ESMS, that interfaces with the higher level management system and manages different ESS components including the PCS and the storage devices [10].

Communication is essential for ESMSs to work. In a hierarchical ESMS architecture, operating data need to be sent from devices to local ESMS and then to central ESMS while control commands go in the opposite direction. For example, in the case of a BESS, the battery packs are managed by a BMS that provides operating data such as the SoC, the SoH, the battery cell temperature. These data together with the operating data of the PCS are given to the ESMS and the central EMS in order to calculate the charge or discharge power at each time period, which then are passed to the PCS as power commands. While delivering these required powers, the PCS also interfaces with the BMS to ensure that none of the battery limits are violated. Fundamental requirements for a communication interface of an ESS can be found in existing standards such as IEC61850-7-420 and Modular Energy Storage Architecture (MESA) (Fig. 12). However, current standards often focus on the operational requirements of a communication interface rather than the necessary cybersecurity requirements. The lack of a cybersecurity layer in ESMS can make the communications (between different ESSs and subsystems within each ESS) vulnerable to cyberattacks.

1) ATTACKS ON ESMS

Within a BESS, ESMS are the most critical subsystem from a cybersecurity standpoint. ESMS are often outward-facing systems, often hosting web interfaces for local access, providing an interface between internal and external communication systems. Consequently the exposure of such systems like ESMS of consumer BESS have exhibited vulnerabilities and poorly implemented security measures (e.g. static default passwords) or absence of basic access control mechanisms [11]. This is a source of great concern because ESMS can monitor and control BESS' subsystems such as PCS and BMS. Furthermore, ESMS might manage remote firmware updates and can be used to change BESS operational

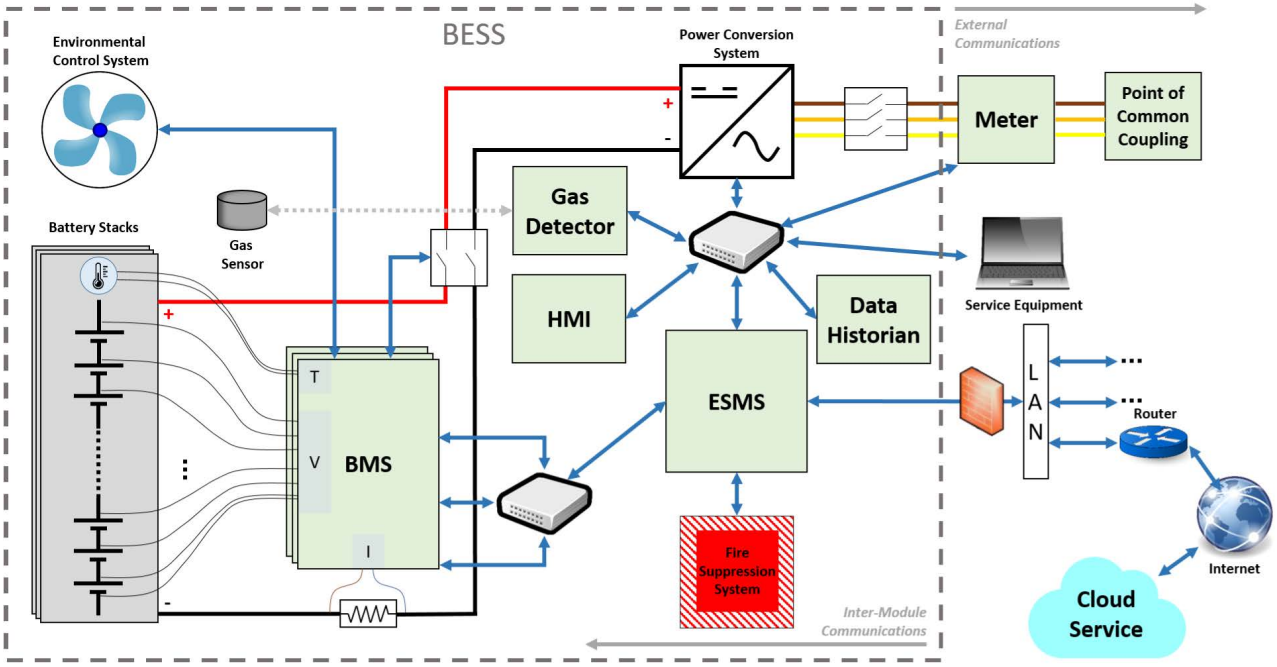


FIGURE 11. Example of communications between components of utility-scale BESS.

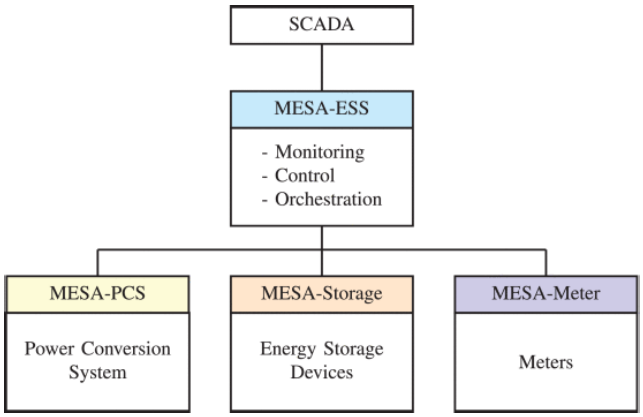


FIGURE 12. MESA communication basic structure [139].

constraints, which if improperly handled can lead to safety concerns.

An attacker in control of a large enough fleet of grid BESS could potentially create several power grid instability scenarios, such as over and under-voltage events, or even shift grid frequency [66]. Due to the similarity between the structure of grid BESS and EV or HEV, it is possible to draw parallels between many of the attacks documented in the technical literature of EVs and BESS. Attacks on EMS algorithms of HEV targeting battery health degradation and reduction of system energy efficiency have been proposed [140]. The attack strategies for accelerating battery degradation are based on long-term cyberattacks increasing the battery throughput by manipulating parameters and sensor data, while reduction of energy efficiency attacks have the goal of increasing fuel and battery energy consumption. The attack vectors are based on manipulating parameters and signals within the EMS such as SoC, vehicle speed data, and gear ratio. The attacks are constrained to maintaining torque requirements from the driving cycle so the driver cannot notice changes in utilization. A summary of attacks applicable to ESMS found in the technical literature is found in Table 3. Definitions of those attacks can be found in Sections V-A1 and V-A2.

B. BATTERY MANAGEMENT SYSTEMS

BMS implement safety and sensing functions, which are fundamental for BESS operation. Additionally, BMS measure cell and string voltages, string current, temperature, and electrolyte ion concentration in flow batteries. Safe operation of BESS requires thermal management of cells and modules, operation within voltage and current limits, detection of faults, and battery shutdown. Other monitoring functions include SoC and SoH estimation, run-time, among others. BMS can also perform control functions such as cell charge balancing circuits, open or close contactors and pre-charge circuits, control of electrolyte flow rate in redox flow batteries, and some BMS implementations include control of fans. In large systems, many battery packs with individual BMS are combined [128].

While BMS are designed to prevent batteries from operating in unsafe conditions, the protection mechanisms might fail in some scenarios. Overcharge might occur due to battery charger malfunction [147] or heterogeneous cell capacity, impedance, or SoC in battery strings [132], [148], [149].

TABLE 3. Summary of potential attacks on ESMS found in the literature.

Attack	Target	Origin	References
Eavesdropping	Confidentiality	Remote, Local	[11], [62]
Hardware Trojan Horse	Confidentiality, Integrity	Supply Chain	[63]
Remote code execution	Confidentiality, Integrity	Remote	[11]
Unauthorized access	Confidentiality, Integrity	Remote	[11]
Replay attack	Integrity	Remote, Local	[113]
Packet injection	Integrity	Remote, Local	[66], [113], [141], [142]
Attacks on setpoints	Integrity	Remote	[55], [66], [143], [144]
False Update	Integrity	Remote	[11]
Remote Exploitation of ECU	Integrity	Remote	[142]
Attacks on algorithms	Integrity	Remote	[140]
Denial-of-Service (DoS)	Availability	Remote, Local	[62], [145]
Distributed DoS (DDoS)	Availability	Remote	[146]

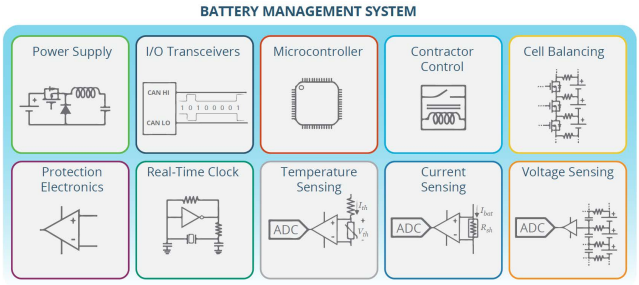


FIGURE 13. Hardware functions found within battery management systems [63].

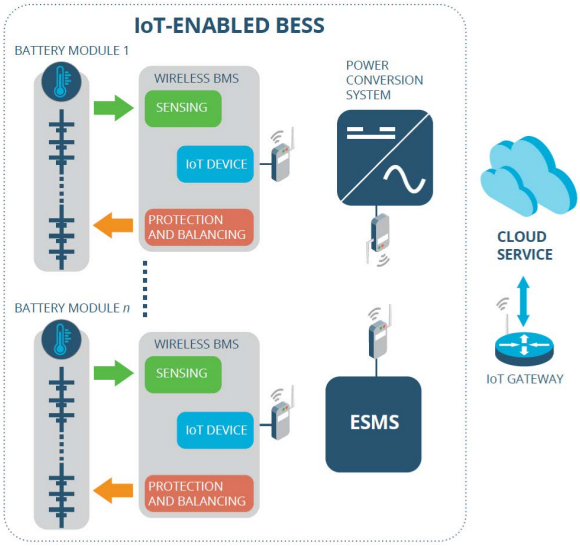


FIGURE 14. Overview of an IoT-enabled BESS with cloud-based analytics [157].

Failure in protection electronics or in cell balancing circuits might lead to failure in protection functions [147]. Because many modern BMS and battery chargers are controllable and parameterizable, a cyberattack can cause BMS malfunction, which can result in battery damage [150]. Furthermore, fires caused by defects in battery cells cannot necessarily be avoided by protection mechanisms implemented by BMS [76].

1) BMS ARCHITECTURE

Some manufacturers adopt modular designs where BMS are composed of two pieces of hardware: a primary device does data processing, communications and controls, and a secondary device that contains data acquisition hardware for voltage, current and temperature measurement as well as cell balancing circuits [131], [151]. Isolating those devices enables a more scalable and flexible design capable of supporting several battery modules.

In order to enforce safety constraints and collect performance data, the BMS must run protection, control, and estimation algorithms in real time. Additionally, these systems often host HMI applications, such as web portals with graphical interfaces for users. BMS are embedded systems with limited memory and processing power with low energy consumption requirements. All this computational burden might place a constraint on fidelity of models and advanced diagnostics.

Capabilities of BMS can be extended by utilizing cloud technology and IoT communications, as shown in Fig. 14, where wireless BMS (WBMS) replace traditional wired technologies. One example is the application of the concept of digital twin. A digital twin is a virtual representation, or equivalent, of a physical product [152]. In BESS, digital twins can be implemented by high-fidelity simulation models of batteries, which would allow advanced monitoring and diagnostics algorithms to run in servers using cloud technology [153], [154]. Digital twins have been proposed to provide anomaly detection, intrusion detection and online monitoring of cyberphysical systems [155], [156]. These high-fidelity models of physical and cyber systems can be applied in the context of cyberphysical security as a means of detecting anomalous or unexpected behavior of physical plants by comparing measurements and other data sources obtained from real plants and signals collected from the digital twin.

As shown in Fig. 11, BMS need to communicate with several other BESS devices. Some BMS communicate with, or control, environmental control systems, including battery module fans. Commonly there is one BMS per battery string or per battery module. BMS might measure and balance individual cell voltages or cells connected in parallel. Large

systems can have dozens of battery strings connected in parallel, therefore Internet Protocol-based (IP) networks are a commonly used solution to connect all BMS to ESMS and PCS. Since module, air or cell temperature are typically measured by BMS, 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, among other subsystems.

2) SENSING AND PROTECTION

Usually BMS measure cell voltages, but some systems include additional battery string voltage measurements. Some BMS provide redundancy for each cell, with highly accurate cell voltage measurements and comparator circuits intended to flag violations of safe cell voltage operation ranges. Fault-tolerant designs allow BMS to continue to monitor voltages in all cells even if one of the voltage sensors fail. Granular voltage measurement capabilities and redundancy can allow BMS to identify damaged battery cells and defects in voltage sensors [97].These voltage measurements are implemented by dedicated integrated circuits that can be configurable to work with any cell chemistry or dedicated to a given type of battery cell [151].

Current sensing is typically performed on battery strings or at the module level. Current sensors can be galvanically connected or isolated. Galvanically connected technologies include shunt resistors, typically placed in the low-voltage side of the battery string to avoid high common-mode voltages. Isolated current sensors include Hall, magneto-resistive and flux-gate technologies that measure the magnetic field to obtain the DC current that circulates through the battery string [151]. SoC is often estimated based on cell voltage and current measurements (more on SoC estimation in Section III-H)

Typically, temperature sensors are used to obtain cell surface, battery pack, and battery module air temperature using negative temperature coefficient, positive temperature coefficient, or digital sensors [151]. Most commercial BMS surveyed in this research are equipped with less temperature sensors than the number of cells they are intended to monitor, which indicates that in practice the temperature of most cells cannot be measured individually. Cell surface and internal temperatures are very useful for early detection of thermal runaway events [97]. Internal temperature sensing in batteries is challenging due to the harsh environment, which requires chemically and electrically inert materials, such as fiber Bragg gratings [158].

Several BMS safety functions establish thresholds based on temperature measurements as well as cell and string voltages, current, and SoC. Cell and battery string operational limits are often programmable and their implementation is dependent on the equipment manufacturer. In general, there are two types of constraints: operational constraints and interrupt constraints. If normal operational constraints are violated, BMS can issue alarms and send out warning messages to inform PCS controller and EMS. If the battery's interrupt constraints are violated, then the BMS can enter a fault state and disconnect the battery string by actuating circuit-breakers, contactors or solid-state relays. Pre-charging circuits can also be controlled by a BMS to avoid inrush currents when a battery string is connected to a DC bus or PCS [118], [159]. It is common to derate the maximum charge current (maximum discharge current) when a battery is almost fully charged (discharged). A notional depiction of the cell voltage and current limits enforced by the BMS is shown in Fig. 15. For safety and reliability reasons, BMS can also limit power or current during charge or discharge modes based on temperature [129], [159], [160] and SoC measurements [111], [129].

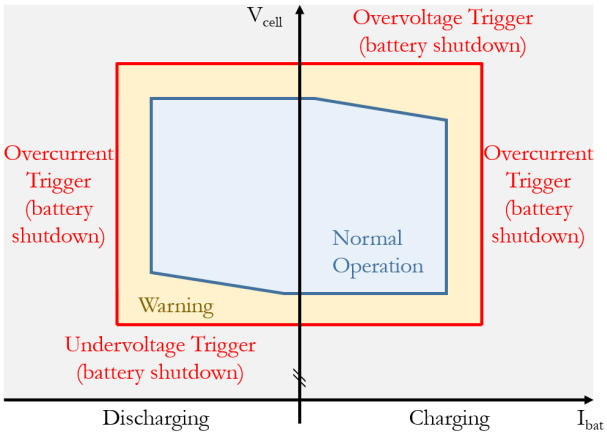


FIGURE 15. Current and voltage limits enforced by BMS [131].

3) CELL BALANCING

Because battery capacity, internal resistance, cell temperature and self-discharge rates are not always perfectly homogeneous among cells in the same string, the cells that have the lower capacity in the string charge and discharge faster. BMSs typically implement interrupt constraints or fault conditions based on cell voltages, therefore if there is a cell that charges or discharges much faster than the others it would trigger such protections thus decreasing the overall usable capacity of the battery string. Consequently, to avoid unnecessary interruption of operation, BMS employ cell balancing methods. Passive cell balancing uses resistors to dissipate excess energy of cells as heat. Active balancing schemes are capable of transferring excess charge from overly charged cells to cells with lower SoC using capacitive and inductive charge pump circuits [149].

There are several strategies for cell balancing. Average SoC cell balancing aims at keeping cell SoCs within a range around the average SoC of the string. Excess charge of cells that reach the upper limit of the SoC band is dissipated or are transferred to the cells that are closer to the lower limit of the band if the BMS is equipped with active balancing circuits. This method requires that the SoC of each

cell is estimated. Similarly, the goal of voltage-based charge equalization algorithms is to maintain uniform cell voltages throughout the string [161]. Voltage-based charge balancing is not very effective for batteries that have a very flat voltage profile. To minimize cell overequalization, balancing strategies based on model-predictive control have also been proposed [162]. Overequalization is undesirable because cell balancing causes energy losses, which harm system energy efficiency.

4) ATTACKS ON BMS

A cyberattack on a BMS can be designed to cause system malfunction, disable battery protection mechanisms, or even change parameters that set normal operational limits of battery cells (see Fig. 15) [150]. If protection mechanisms are not engaged and the BMS fails to report its SoC, continued operation can result in temporary or permanent battery damage. Furthermore, some chemistries experience accelerated capacity fade under higher depth and rate of discharge operation cycles [112]. The batteries are typically the most costly part of a BESS and replacing them following an attack would probably require several days or weeks depending on supply chain conditions. A partial list of cyberattacks applicable to BMS can be found in Table 4.

a: BATTERY EXHAUSTION ATTACKS

In battery-powered mobile devices, the concept of ''sleep deprivation torture'' attack is a type of denial of service threat where the threat actor forces the mobile device to constantly process information, never allowing it to enter power-saving (sleep) mode, ultimately leading to battery exhaustion [165]. For battery-powered vehicles such as EVs, UAVs, and AUVs, this type of attack is especially harmful because it can lower system range [63]. In EVs, an estimated 20% of battery discharge can be obtained by operating vehicle systems such as air conditioning, fans, power steering, and others [142]. In [166], several stealthy attack vectors targeting parked EVs have been identified. Those include increasing current consumption by frequently waking up ECUs, injecting controls that increase battery consumption (e.g. direct or indirect activation of lights, repeatedly open and close door locks, change the vehicle's power mode).

In comparison to mobile devices, grid BESS have a much larger battery capacity and often BESS are powered by an auxiliary power source. A more effective version of an attack designed to increase self-discharge of batteries could include continuous operation of passive cell balancing circuits.

b: DEEP DISCHARGE

Overdischarging Li-ion cells decomposes the SEI layer and the dissolution of the copper from the current collector. Subsequent copper deposition can lead to internal battery short circuits and [167]. Internal cell short circuits can lead to total battery failure.

c: OVERCHARGE

Lithium-ion battery overcharge can accelerate the degradation of a battery and, in extreme cases, lead to catastrophic failure. Overcharging is discussed in Section III-I.

d: TEMPERATURE

Depending on the chemistry, the degradation of battery cells present high sensitivity to ambient temperature. For instance, it has been shown that LFP batteries degrade faster when cycled at 35 °C than at 15 °C [112]. If compromised BMS fail to manage cell or module temperature adequately, accelerated battery degradation can occur. A hypothetical attack on automobiles cooling fans activated by Computer Area Network (CAN) protocol messages and re-flashing BMS has been proposed as a means to induce thermal runaway in batteries [142], [164].

C. COMMUNICATIONS ARCHITECTURE OF UTILITY-SCALE BESS

Utility-scale BESS are complex systems whose operation depends on the communications of alarms, measurements, control setpoints and other critical pieces of information between several electronic devices, such as BMS, PCS, ESMS, HMI, gas sensors, data historians, service equipment and others. An example of how these subsystems are connected and communicate is shown in Fig. 11. It is also common to see topologies where BMS communicate directly with PCS and fire suppression systems instead of relaying commands first to the ESMS. Flow-batteries have distinct technology-specific topologies, control and monitoring systems.

1) EXTERNAL COMMUNICATIONS

Utility-scale BESS typically provide grid services that require two-way communications over a SCADA-type communications system that serves as an interface between the utility application servers and control center with field devices and substations. As highlighted in Section II-A, BESS applications require communications between the local ESMS with power grid markets (e.g. arbitrage), power systems frequency control systems (e.g. frequency regulation and other ancillary services), or simply to take setpoint commands and report system status (e.g. active status, available capacity, SoC, other local measurements) to utility-owned DER management systems or DER aggregators providing some centralized. As a consequence, BESS might interact with several different systems that support the power grid. An illustration of a privately-owned Smart Grid Communication System and where BESS fit is shown in Fig. 16. In a broader context, BESS can also be found within transmission systems [168], power plants [169], [170] and microgrids, to name a few.

IEEE 1815 (also known as distributed networking protocol 3.0, DNP3) and Modicon communication bus (Modbus) are very commonly used for DER communications [172], both of which present security deficiencies.

TABLE 4. Summary of potential attacks on BMS found in the literature.

Attack	Target	Origin	References
Electromagnetic sensor spoofing of hall sensors	Integrity	Supply chain	[163]
Packet injection	Integrity	Remote and local	[66], [113], [141], [142]
Packet replay	Integrity	Remote and local	[113]
Denial-of-Service	Availability	Remote and local	[62], [145]
Accelerate battery degradation	Integrity	Remote and local	[142], [150]
Disable temperature management	Integrity	Remote and local	[142], [164]
Battery depletion/sleep deprivation	Availability	Remote and local	[62], [63], [142], [165], [166]

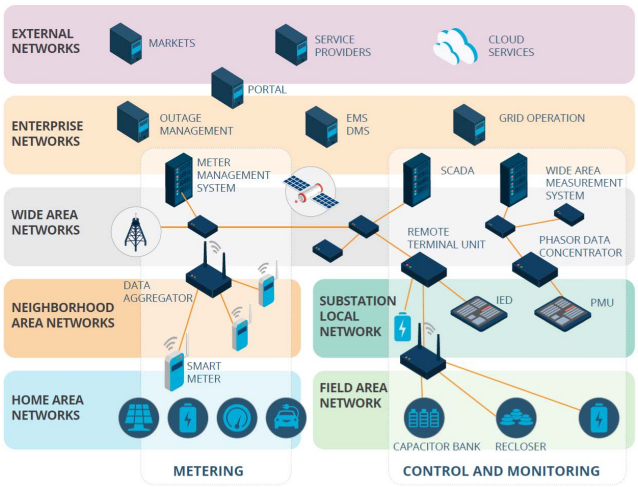


FIGURE 16. BESS within Smart Grid communications infrastructure. Adapted from [171].

IEEE 1547-2018, a standard covering specifications for interoperability between electric utility operators and DERs preconizes communications over Sunspec Modbus, DNP3 and IEEE 2030.5 IoT protocol [173]. DNP3 can utilize Transport Layer Security (TLS) to secure DER communications through cryptography (see Section V-F1), and provide access control features (see Section V-I) following Role-Based Access Control (RBAC) methods, but both are optional features. The earlier versions of the Modbus protocol were not built with native cybersecurity features, so legacy systems might need to use bump-in-the-wire encryption devices[2] to provide confidentiality for Modbus messages. Later versions of Modbus that supporting TCP/IP protocol can use TLS encryption. IEEE 2030.5 (SEP2) also supports TLS 1.2 [5]. IEC 61850 is another standard commonly used for DER communications.

Message Queue Telemetry Transport (MQTT) is a popular IoT protocol designed for reduced bandwidth and applications. MQTT uses a publish-subscribe paradigm where a *broker* manages distribution lists of messages to be sent and received by the clients [174]. The application of MQTT for BMS has been proposed in the literature [61], [62], [175], but commercial IoT-based BMS systems are not yet available. MQTT does not have built-in security features such as access control, mutual authentication and control message security [176]. As a consequence, the protocol allows malicious subscribers to communicate with other devices [62], among other security problems.

Because BESS are incorporated in many different configurations and often require remote control and communications, many of the smart grid communication security protocols can be utilized. When smart devices are deployed in home area networks (HANs), utilization of Zigbee and Z-wave protocols may be employed [177]. BESS incorporated into neighborhood area networks, BESS could be connected via IEEE 802.11,[3] IEEE 802.15.4[4] or IEEE 802.16[5] [177]. In wide area networks (WANs) it is possible to utilize industrial applications protocols including DNP3 and Modbus [177]. Most recently there has been research into using the cognitive radio protocol IEEE 802.22 which provides coverage when WAN wireless resource availability is limited [178]. When battery banks are controlled at the substation level, IEC 61850 is used [44].

All of the above-mentioned protocols possess vulnerabilities. Modbus and DNP3 vulnerabilities are discussed in [179], [180], and Zigbee, Z-Wave, IEC 61850 protocol vulnerabilities are detailed in [181]. Specific communications security vulnerabilities for cognitive radio are described in [182]–[184]. Modbus is one of the most heavily utilized protocols within a WAN environment due to its ease of use. Generally, Modbus communications are unencrypted and unauthenticated when used across a WAN. In 1979 when the protocol was originally developed, the overhead that encryption imposed was a vital consideration with the limited computational resources of the time [185]. Encryption and authentication is now available on Modbus to enforce data privacy and proper authentication. DNP3 version 3.0 will work over IP and encapsulating encrypted data in Transmission Control Protocol (TCP) or User Datagram Protocol packets.

2) INTER-MODULE COMMUNICATIONS

Commonly used communications protocols found in communications between BESS components and subsystems include I2C, SPI, CAN Bus, Modbus, TCP/IP, Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol

[2]Those are devices that can be inserted into the communication endpoints of legacy systems to provide cybersecurity features such as encryption.

[3]Used in Wi-Fi [171].

[4]Defines the physical and medium access control layers of Zigbee [171].

[5]Used in WiMAX technology [171].

Secure (HTTPS) and MESA [5], [118], [129], [131], [186]. I2C and SPI are used to communicate between chips within the same printed circuit board or over short distances of up to one meter, which makes SPI suitable for distributed BMS architectures [118]. CAN, Modbus, and serial communications using RS-232, RS-485 more robust communication protocols that are better suited for intermodule communications, as BMS to PCS or BMS to ESMS. Other physical layer protocols include Universal Serial Bus (USB) and IEEE 802.11 (Wi-Fi). CAN is common communication interface in BMS due to its wide use in the automotive industry for communications between electronic computing units (ECUs), including EV's BMS. Further, CAN offers robustness to electromagnetic interference and allows near real-time performance. DER can communicate with aggregators and utilities over IEEE 1815, IEEE 2030.5 and IEC 61850 [5], [55], [173]. A list of communication protocols and standards found in BESS is shown in Table 5.

Some of these communication protocols have been deemed insecure. In [11], the authors have found that malicious actors with local network access could adulterate parameters of home BESS. Because of lack of authentication mechanisms and access control, any node in a CAN bus can listen to all messages sent in that network, which means that the confidentiality of data is at risk especially since message encryption is not a common feature in CAN networks. Due to the same reasons, any node, authentic or malicious, can also send messages to all nodes in the same CAN bus, including replay attacks [113]. Frame-injection attacks to CAN-based communications along with exploitation of security vulnerabilities have been applied to remotely control a passenger car [141]. Even though frame analysis-based anti-threat systems such as IPS and IDS could effectively stop these attacks, it is still possible to exploit CAN fault confinement and error handling vulnerabilities to perform an effective DoS attack if physical access to OBD-II diagnostics port is obtained [145].

3) ATTACKS ON BESS COMMUNICATIONS

a: MAN-IN-THE-MIDDLE AND EAVESDROPPING

An attacker could exploit unsecured communications between BESS components (e.g. CAN bus, HTTP, Modbus, other plaintext messaging) to read their content or even perform man-in-the-middle attacks (MITM). In this type of attack, the threat actor has access to the communication channel between sender and receiver, allowing the attacker to intercept and read communication packets between them, as well as deceptively craft packets to mimic a message to any receiver. With this capability, an attacker is capable of performing traffic analysis (or packet sniffing), steal critical information or disrupt communications in the link or bus [62]. A security assessment of several models home BESS has shown that most devices have inadequate encryption and authentication procedures for communications over the internet, which exposes these devices to eavesdropping or MITM attacks [11].

b: DEVICE COMMUNICATIONS DENIAL-OF-SERVICE

Exploiting vulnerabilities in communication channels (e.g CAN fault confinement and error handling [145]) can lead to interruption in the communications between devices. That can create a risky situation when warning or fault messages have to be communicated by safety equipment (e.g. BMS, gas sensors) and the system must respond by a coordinated action between BESS devices.

c: BESS DENIAL-OF-SERVICE

Several BESS applications such as energy arbitrage, demand response, or frequency regulation rely on communications with external entities. Loss of communications between the BESS and a power system balancing authority, for example, would lead to loss of frequency regulation service.

d: COMMUNICATIONS DISTRIBUTED DENIAL OF SERVICE

BESS or any of its devices (e.g. BMS) implemented following an IoT paradigm might be infected by malware to create large-scale botnets used to perform distributed denial of service (DDoS) attacks. An example of such is the 2016 Mirai cyberattack [146].

D. POWER CONVERSION SYSTEMS

PCS condition and mediate bidirectional electric power flows between BESS and the power grid. These devices transform direct current (DC) power native to batteries to alternating current (AC) used in the electric grid and vice-versa. This type of DC-to-AC converter is known as an inverter. Grid BESS inverters are bidirectional, with the DC side functioning as both as a battery charger and load to the battery. The management of the PCS often requires two levels of control: primary and secondary. The secondary control receives power commands (e.g., real and reactive power) from the ESMS and the energy storage states (e.g., SoC and temperature) from the BMS and calculates the operating modes for the PCS such as charge mode, discharge mode, and standby mode. The primary control includes the module level controllers that generate the drive signals for the power converters given the operating modes, the power command references and the state of the PCS.

1) POWER CONVERTER TOPOLOGY AND MODULATION

Power inverter manufacturers are not explicit with respect to what power converter topology is used in their PCS. Often these are patented or proprietary circuits designed to operate in a reliable and efficient way, frequently regarded as a source of competitive advantage. Many converters are marketed as ''true sine wave'' or ''modified sine wave'', and their commercial documentation states other key information such as their power factor. Modified sine wave can be obtained with low-frequency modulation techniques and can be implemented with thyristors [190] or even with metal-oxide-semiconductor field-effect transistors (MOSFETs) [191]. However, these topologies cannot provide high power

TABLE 5. Security features of communication protocols used in BESS [173].

Protocol	Data flows	Physical Medium	Encryption	Node Authentication	References
I2C	BMS - BMS	twisted pair	No	-	[118]
SPI	BMS - BMS	twisted pair	No	-	[118], [186]
CAN	BMS - PCS, BMS - ESMS	twisted pair, DB9	No	No	[118], [129], [131], [187], [188]
Modbus/RTU	PCS - BMS - ESMS	RS485, RS232	No	No	[118], [131], [173]
Modbus/TCP[a]	BMS - ESMS - Operator	Ethernet	No	No	[118], [131], [159], [173]
HTTP	Server - ESMS - BMS	Ethernet, Wi-Fi	No	No	[131], [159]
IEEE 2030.5	ESMS - Utility/Aggregator	Ethernet, Wi-Fi[b]	Yes (TLS 1.2)	Yes	[5], [55], [173]
MQTT	Server - ESMS - BMS	Ethernet, Wi-Fi	No[c]	Optional	[174], [175]

[a] A variant called Modbus/TCP Security features x.509v3 certificate-based identity and authentication with TLS v1.2 [189].
[b] Any that supports TCP/IP [173].
[c] Not required by standard but several open-source MQTT implementations incorporate TLS security features [174].

quality, therefore they cannot power sensitive loads. True sine wave means that the voltage output of the converter will have a waveform very close to a sinusoid [192], [193]. Consequently, the Total harmonic distortion should be low. To achieve such, a high-switching frequency modulation technique must be used, which can only be implemented with some switches and power converter topologies.

A commonly applied technique for obtaining true sine wave outputs is pulse-width modulation. However, many techniques such as hysteresis, sine-triangle, third-harmonic injection, space-vector modulation and delta modulation exist [194]. Because of the diversity of converters and modulation techniques available (which are likely unique for each inverter model), for power systems dynamic analysis purposes, inverters are commonly modeled using modulation and topology-agnostic equations [195].

Due to those requirements for power quality, most modern power electronic converters within BESS utilize transistor-based technologies. However, mentions to circuits that use thyristors, such as three-phase fully controlled rectifiers are found in the literature [196]. Another advantage of transistor-based over thyristor-based inverters is the independent control of active and reactive power, which allows operation in all four quadrants under constraints such as power factor, maximum and minimum real and reactive power output and others (see Fig. 17) [13], [134]. There exist a large number of power converter topologies implemented with fast-switching transistors that can handle the task or providing true sine waves. The most common is probably the two-level three-phase bridge converter [194] using MOSFET or insulated-gate bipolar transistor switches. Oftentimes this converter is modeled as a Voltage Source Inverter, which implies that a constant voltage, low-impedance source is available. In addition, the peak AC voltage output of the inverter is limited to half of the DC bus voltage [194]. This topology is considered low-cost, easy to control and reliable due to its low complexity [197]. The application of such converter to BESS can be supported by the use of a bi-directional DC-DC converter acting either as a battery charger or load in the DC side to regulate the battery and DC link voltage [134], [198]. Similar structures having a buck-boost converter and a two-level inverter can be found for Hybrid Electric Vehicles [199].

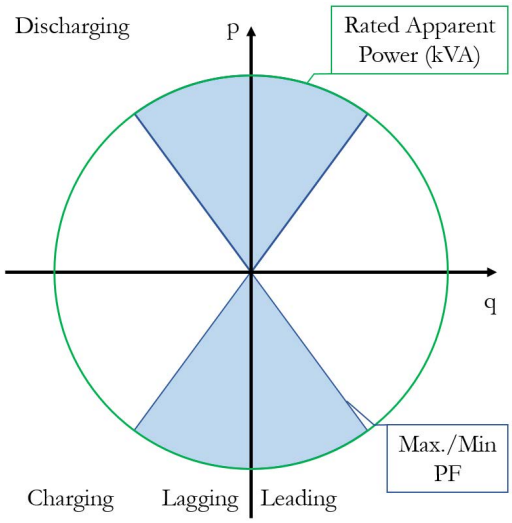


FIGURE 17. Four-quadrant operation of inverters with apparent power and power factor constraints.

2) VOLTAGE AND POWER CONTROL

A PCS is implemented with several layers of feedback control loops whose goal is to ensure that all voltages, electrical currents and power follow predefined setpoints. Additionally, control algorithms determine how the PCS responds to disturbances like voltage and power frequency events. For example, standards like IEEE 1547-2018 provide guidelines for control loops such as volt/VAR (voltage-reactive power) control, frequency-power, voltage ride-through, operation under islanding, and others [13].

The two most common operation modes of smart inverters are grid-following and grid-forming. Power electronic converters operating in grid-following mode calculate their current setpoints based on voltage magnitude and frequency measured from the grid. Active and reactive power setpoints are typically defined based on the application and can either be calculated locally or broadcasted from a hierarchically superior controller. This is the most common mode of operation for small DERs that do not operate in islanded mode. Grid-forming mode of operation requires an internal oscillator so that the converter has a reference for the voltage signal. Then, the inverter controls local voltage magnitude

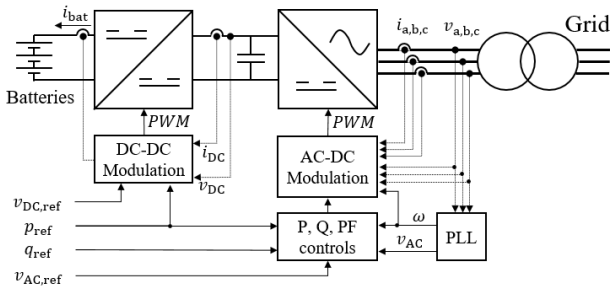


FIGURE 18. Control signals and main components of a generic two-stage PCS. Adapted from [134], [195], [202].

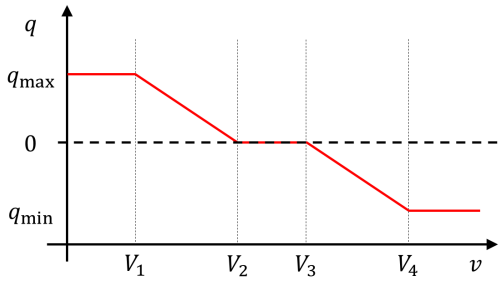


FIGURE 19. Voltage-reactive power (or volt/VAr) power characteristic. Adapted from [13].

and frequency by modulating its real and reactive power outputs. This mode of operation allows inverters to function in islanded mode (disconnected from an electric grid) [200] and is necessary in BESS applications such as black start and backup power. The inverters of large DERs typically operate in grid-forming mode.

A high-level depiction of the control loops, setpoints and sensors of a two-stage PCS is shown in Fig. 18. Grid frequency estimation is typically done using phase-locked loops (PLLs), but other methods such as those based on the KF [201] are also used. Most of the control loops of the PCS are local controls whose objective is to ensure that the power converters follow voltage and power setpoints and can be interconnected successfully with the grid. Several BESS applications, such as some BTM uses, volt/VAr control, frequency-power and backup power, do not necessarily require communications with a remote entity, such as an Advanced Distribution Management System.

For instance, volt/VAr (Fig. 19) local droop controls executed by grid following smart inverters within BESS or any other DER can be described by (8). These functions allow decentralized sharing of control efforts necessary to maintain voltage magnitude within normal operating range.

$$q = \begin{cases} q_{\max}, & v < V_1 \\ q_{\max} - \dfrac{q_{\max}}{V_2 - V_1}(v - V_1), & V_1 \le v \le V_2 \\ 0, & V_2 \le v \le V_3 \\ \dfrac{q_{\min}}{V_4 - V_3}(v - V_3), & V_3 \le v \le V_4 \\ q_{\min}, & v > V_4, \end{cases} \tag{8}$$

where v is the voltage measured by the PCS, $V_1 < V_2 \le V_3 < V_4$ are voltage parameters, and $q_{\max}$ and $q_{\min}$ are the upper and lower reactive power injection capacity of a PCS.

When integrated with power systems operations, BESS must be equipped with two-way communications. For instance, frequency regulation applications require that the BESS reports several pieces of information including injected power, its capacity, which might be dynamic due to SoC constraints, and other information while responding to control commands that update real power injection setpoints. For effective integration to the Automatic Generation Control (AGC) closed-loop control system that includes frequency regulation, all assets must respond almost instantaneously to the fast-changing control commands broadcasted every 2 to 4 seconds [203]. Some microgrids using hierarchical control schemes might also have secondary control loops that require communications between a central microgrid controller and DERs [200].

3) ATTACKS ON PCS

Just like other CPS, PCS are subject to DoS, data replay, and data deception attacks (e.g. FDIA) [204]. These attacks can target sensor data, state estimators or observers, and control signals or systems [64]. A list of PCS attacks is shown in Table 6. Older inverter technologies that use insecure Hall sensors are vulnerable to electromagnetic spoofing attacks capable of disrupting their operation [163]. A cyberattack capable of compromising ESMS or PCS control parameters or signals can have a severe impact on the power grid. Incorrect design or tuning of PLL parameters can lead to harmonic resonance or even instability [205], [206]. Incorrect setting of inverter control parameters and communications delays can also lead to undesirable operation of DER and power system instability [54], [207], [208].

Attacks to current setpoints of inverters within EV powertrains can cause large torque variations, which could cause mechanical vibrations and vehicle instability. Additionally, a similar attack could overload a power converter causing premature failure [64]. Similar attacks in BESS PCS could harm grid power quality and accelerate battery degradation through high ripple currents.

In [143], droop and inertial response controls have reduced the frequency deviation induced by an FDIA on a BESS of an emulated microgrid. A method based on control of fast-responding ESS and power system state estimation-based bad data processing has been proposed to mitigate the effects of FDIA in grid voltage measurements [209]. Attacks to volt/VAR [54] and volt/Watt [144] controls of smart inverters have shown that malicious actors capable of changing parameters of those devices can cause voltage deviations in PDS to outside of normal levels, which can potentially damage power system equipment or loads.

In addition to methods based purely on IT cybersecurity techniques to protect from attacks, many researchers have

proposed feedback control methods to mitigate the effects of maliciously designed controllers or control signals. It has been discussed that if a subset of DER are compromised and can be remotely controlled by the malicious actor, it is possible to create grid disruptions that range from local power quality issues to large-scale power outages. A reinforcement learning-based DER control method for mitigating effects of a cyberattack on a subset of grid DER has been proposed [210]. This technique should enable each individual uncompromised smart inverters to adjust their voltage control loop gains to neutralize cyberattacks targeting the voltage stability of power grids.

E. GAS AND FIRE PROTECTION

Grid-scale BESS are often equipped with gas sensors and fire protection equipment, which are typically absent of small battery systems. Gas sensors provide signals that allow fast and clear detection of thermal runaway events [211]. The composition of gases expelled by cells depend on several factors, including their chemistry and mode of operation. Li-ion batteries can generate gases during normal operation [212]. Cost-effective gas sensors are typically sensitive to a narrow spectrum of molecules, therefore the choice of gas sensors must be informed by understanding the failure mechanisms of each battery technology. For instance, an experiment using a commercial LFP cell has shown that in early stages of battery overcharge, vented gasses are rich in dimethyl carbonate,ethyl methyl carbonate, methane, carbon monoxide and carbon dioxide, while other gases like ethylene and hydrogen fluoride acid appear later in the process [213]. Practical gas sensing mechanisms can communicate with ESMS and other systems through common industrial communications protocols (e.g. Modbus) to send warning messages.

BESS have multiple levels of protection against fire. The design of battery cells, modules and enclosure play a role in mitigation of fire hazards. The materials of battery electrolyte, anode, and cathode can be chosen and engineered for improved thermal stability. Cells can be built with safety features such as pressure relief vents, current interrupts, and positive temperature coefficient devices that can shutdown the cell if abnormal conditions are detected, avoiding cell overheating and damage. Thermal management systems prevent incidents by maintaining optimal battery pack temperatures. Battery enclosures must be built to resist high temperatures and equipped with fire suppression and pressure relief mechanisms. Fire systems must not only extinguish fires but, more importantly, cool battery cells to avoid re-ignition [212], [214]. The fire suppressants most recommended by battery manufacturers are water, carbon dioxide, and chemical or dry powder [215].

V. SYSTEM-LEVEL CYBERSECURITY OF GRID BESS

In previous sections all major subsystems of BESS were presented and possible vulnerabilities and examples of cyberattacks were listed. However, vulnerabilities might exist across multiple subsystems or stem from the integration of subsystems, therefore it is necessary to employ methods like threat analysis to obtain an holistic analysis of risk. This section discusses how BESS can be made secure. Several of these systems contain microprocessors and are connected to external networks. Therefore, one or more of the components can be subject to the same vulnerability. The section summarizes vulnerabilities, prevention, and remediation for each component considering both physical and cyberattack points. This section starts with an introduction of key concepts covering cybersecurity of CPS. Then, a discussion on risk analysis starts by a presentation of techniques used for threat assessment and the enumeration of entry points common to BESS. The remaining of the section is dedicated to the discussion of several classes of methods and practices aimed at improving cybersecurity posture of grid BESS.

A. CYBERSECURITY OF CYBERPHYSICAL SYSTEMS

The fundamental objectives of information security are to guarantee the confidentiality, integrity, and availability of information, commonly referred to as the ''CIA triad''. A fourth concept found in the literature is non-repudiation, which is the requirement to accept data when the communication is authorized or legitimate. The concept of confidentiality implies that the content of a given piece of information can only be known by authorized parties. Mechanisms such as access control policies and encryption are common ways of enforcing confidentiality. Integrity of information is related to the authenticity of data and its origin, meaning that neither the content of a given message nor its source can be inadvertently or intentionally altered in an unauthorized manner. Preventing information integrity violation can be done by employing sound authentication and access control methods, for example. Hashing and verification bits are common processes employed for verifying data integrity. Availability is related to the capability to use resources or having access to information. Uptime metrics of a system can be impacted by hardware failures and software bugs, so availability can be improved by, for instance, the use of redundant systems, failover mechanisms, data backups, and system monitoring [216].

The cybersecurity of ICS is a relatively new concept when compared to mature areas such as computer and communication systems [33]. One major difference between IT and OT systems is the distinct priority between the three security objectives. OT systems typically prioritize availability. For instance, the metrics for assessing reliability of power systems are directly related with continuity of service, such as system average interruption frequency, system average duration, consumer average interruption duration indices (SAIFI, SAIDI, and CAIDI, respectively). On the other hand, IT systems have higher tolerance to downtime, but breaches in data integrity and confidentiality are unacceptable [38].

1) DEFINITIONS OF CYBERATTACKS ON CYBERPHYSICAL SYSTEMS

In general terms, cyberattacks are defined as a sequence of actions that generate a violation of security. Those violations

TABLE 6. Summary of potential attacks on PCS found in the literature.

Attack	Target	Origin	References
Electromagnetic sensor spoofing of hall sensors	Integrity	Supply chain	[163]
Packet injection	Integrity	Remote and local	[66], [113], [141], [142]
DoS	Availability	Remote and local	[62], [145]
Replay attack	Integrity	Remote and local	[113], [204]
Tampering sensor, state estimator, controls	Integrity	Remote and local	[64], [209]
Power converter setpoint tampering	Integrity	Remote and local	[64]

can be intentional or unintentional, as well as perpetrated by persons from within (i.e. insider threat) or from outside of the organization. Vulnerabilities stem from failures in the implementation of procedures, technology, or management of security controls in computer systems. Cyberattacks stem from the exploitation of vulnerabilities by malicious actors [216]. A vulnerability is called *zero-day* if it is unknown or if it has not yet been fixed. A *zero-day attack* is a cyberattack that exploits a zero-day vulnerability. *Attack vectors* describe the means used by an attacker to access the target system [217].

The literature on CPS security often classifies cyberattacks in three broad categories: DoS, data replay, and data deception [59], [204]. The goal of *DoS* attacks is to harm the availability and non-repudiation of data or system resources, such as interrupting a communication link, or disabling any other CPS device. A variation of this attack is called DDoS when data packets come from multiple sources. Repetition or delay of data is used in *replay attacks*, which target the integrity of data. Replay attacks can be launched with no detailed knowledge of the system they target and they might be successful applied to communications using encryption protocols that are not equipped with adequate security features [59], [216].

Finally, *deception attacks*, which includes FDIA, are those in which an attacker crafts false data signals to deceive its target system. Stealthy FDIA typically require knowledge of the target system to avoid detection. The literature on computer security places deception attacks within the class of *modification* attacks. *Man-in-the-middle (MITM)* is a type of modification attack in which a malicious actor intercept messages from a sender and modifies their content before forwarding them to the receiver [216]. Attacks that violate integrity of the data by changing setpoints of the control systems of CPS and by tampering with algorithm code also fit within the definition of modification attacks. Attackers can craft communications packets and send them to receivers, a practice known as *packet injection*, to implement some types of cyberattacks, such as MITM and DoS. Modification attacks targeting widely used software or libraries can be used to perform *supply chain* attacks, where, for instance, a vulnerability is introduced to a given library used to develop software.

2) DEFINITIONS OF OTHER CYBERTHREATS

In addition to the previously mentioned class of attacks applicable to CPS, other attacks more commonly mentioned in the broader cybersecurity literature are worth of mention. *Eavesdropping* attacks target the confidentiality of data by unauthorized interception of data, including accessing files in a system and listening to communications. *Spoofing or masquerading* attacks occur when a malicious actor violates the integrity of the source of information, impersonating another entity [216]. This includes attacks where the malicious actor uses stolen credentials to obtain remote access to a computer system. *Remote code execution*, or arbitrary code execution, vulnerabilities allow a malicious actor to run any commands or code in the target system [11]. *False update* attacks occur when an attacker tampers with a legitimate software or firmware update, or when an unauthorized system update is issued by the malicious actor. This type of attack is complex and is composed of several violations of integrity of code and source of data. *Side-channel* attacks leverage pieces of information from a system that an attacker can have access to and that can be used to extract confidential information. Power consumption and program execution time are examples of side channels that an attack can observe to, for example, infer cryptographic keys [217]. *Watering hole* is a type of attack in which threat actors observe the websites regularly accessed by their target and infects them with malware, which will eventually infect the target system.

Cyberattacks or some of their steps can be performed autonomously by computer programs. *Malware* is a set of computer instructions that can cause computer security violations. Because they are run by an authorized entity, access control methods cannot avoid their execution [216]. A *backdoor* is a hidden feature of a computer program that allows bypassing common authentication or encryption procedures [217]. Backdoors are often used to obtaining *unauthorized remote access* to computers. A *Trojan horse* is a type of malware that has a covert purpose unknown by the user [216]. Similarly, a *hardware Trojan horse* is a piece of hardware that performs functions that are secret to the user. Software and hardware implementations of Trojan Horses can be used to perform eavesdropping or to implement back doors, for example. A computer *virus* is a Trojan horse that is capable of making copies of itself and inserting those in other files. A *ransomware* is a malware that locks computer systems until a ransom is paid to the attack perpetrators [216].

Very often, the weakest link in the cybersecurity chain is human. *Social engineering* methods aim at using deception strategies in order to extract valuable information necessary to carry out a cyberattack campaign. *Phishing* is a specific

type of spoofing attack, where the attacker impersonates an entity, such as a website, in order to obtain unauthorized access to sensitive information such as passwords. A *spearphishing* attack is a phishing attack targeted at a specific victim [216].

3) CYBERSECURITY RISKS

Securing any given system requires allocation of capital and human resources, which puts cybersecurity in competition for funds with other activities within an organization. Prioritization resource allocation requires assessing risks and the criticality of assets. Security risks are typically quantified as the product of the consequence of a given contingency and the probability of is occurrence. This definition is well suited for system failure causes that are random, but there is discussion as if it is a good representation of scenarios where risks are driven by adversarial action, such as cybersecurity. For instance, FERC order 706 that mandated cybersecurity standards to be adopted to the bulk power grid notes that risk-based assessment methodologies should be used but due to insufficient data on cyber incidents, frequency cannot be determined and it should be assumed that an event will happen. Therefore risk assessment should focus more on consequences of a cyberattack, not on the likelihood of its occurrence [218]. Based on this definition, the classification of a BESS asset in terms of its application (Section II-A) and size (Section II-B), as well as the safety risks it poses (Section III) become valuable tools for risk assessment.

4) CYBERATTACK STRATEGIES

Untargeted cyberattacks try to reach as many targets as possible expecting to exploit vulnerabilities that are expected to exist in several systems. Common attack methods include phishing, waterholing, ransomware, and scanning [219]. Targeted cyberattacks are more complex endeavors that focus on a given entity. Those typically require a preparation step that can take several months [219]. The Cyber Kill Chain is a framework used for describing the steps of targeted cyberattacks that is based on the military concept of kill chains [220]. This framework was initially developed for modeling advanced persistent threats (APTs), which are highly capable adversaries that can conduct multi-year intrusion campaigns targeting valuable sensitive information. This framework defines seven steps for a cyberattack:

1) **Reconnaissance:** The attack campaign starts by identification and selection of the targets. For instance, threat actors can gather intelligence by exploring public information on the internet to find a suitable vulnerable target.
2) **Weaponization:** The second step is to use information obtained in the reconnaissance step to develop means to perform a system intrusion. Those might include infecting a file (the ''payload'') with a Trojan horse enabling remote access to the victim's computer system.
3) **Delivery:** In this phase the malware developed in the previous step is transmitted to the targets. For instance, a spearphishing campaign can be crafted to deliver the infected files to potential targets as email attachments. Additional means of spreading the malware include watering hole websites, and USB drives. It is also possible that a hacker can gain access to an organization's system by exploiting vulnerabilities in internet-facing websites.
4) **Exploitation:** After the victim receives the malware or enters the watering hole website, the attacker can start to get remote access to the target's computer system or receives sensitive information such as usernames and passwords. Malicious code might run by exploiting known system vulnerabilities or by leveraging auto-execution features of the host operating system. The malware can may inform the intruder that it has been successfully run in the target system and begin system and network recognition tasks.
5) **Installation:** After getting a foothold in the target's system, the attacker moves on to securing access by installing a backdoor allowing persistent access. In this step system modifications including disabling network defenses can be made. The malicious actor can also use control over systems or stolen credentials or create administrator accounts in the network to consolidate its presence.
6) **Command and control:** In this step the attacker is capable of fully controlling the target's system, can impersonate users in the network. The attacker can establish a command and control channel to issue commands manually to the target system.
7) **Actions on Objectives:** After completing the previous six stages the attacker can accomplish their goals. Those can include stealing confidential information, disrupting the company's operations, locking users out or encrypting data to demand ransom, or even use the compromised target system as a starting point to progress towards other systems. If a malicious actor gains access to ICS networks and engineering stations, they can disable system protections and alarms, halt physical processes, change setpoints, reprogram programmable logic controllers (PLCs), to name a few examples.

Following a successful attack malicious actors typically act to remove evidence of their presence, such as deleting logs and any information used to investigate the attack, including protecting their identity and exploits. Backdoors can be left in place to facilitate new intrusions.

B. THREAT MODELING AND RISK ASSESSMENT

Threat modeling is a part of product design cycle intended to understand its threat environment and defend against potential attacks [221]. Threat modeling is a useful tool for understanding security requirements, design secure products from the development stage, and to address current security flaws

of systems in a structured and formal way. The process of threat modeling can be divided in four steps [222]:

1) Model system;
2) Find threats;
3) Address threats;
4) Validate.

Cyberthreat analysis of BESS has been the subject of some research [11], [63]. Additionally, the technical literature provides examples of vulnerability assessments in related areas such as UAVs [223], and electric drive systems [224].

1) THREAT MODELING METHODS

Threat models are typically classified as graphical or formal [225]. Graphical methods rely on tables and graphs, such as attack trees and fault trees, to model threats. Formal methods are based on mathematical models of threats. A very popular threat modeling framework is STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege) [226].

Another leading security assessment methodology is the Information Design Assurance Red Team (IDART) [227] is a NIST-recognized method in SP800-115, Technical Guide to Information Security Testing. The IDART methodology is a guide for conducting threat assessments with the goal of guiding system stakeholders in reducing the attack surface and implementing mitigations within their systems. One major goal of the IDART methodology is presenting an adversarial perspective to the vulnerabilities in their system.

The IDART process includes creating a plan for accomplishing the assessment, collecting the data from the stakeholders to best identify critical system components and potential consequences. A threat model that captures potential attack scenarios is developed in the characterization stage. Using the threat models as a guide, various network and host-based penetration testing and vulnerability scanning tools are used to collect system data during reconnaissance, vulnerability scanning and penetration testing activities. Penetration and vulnerability scanning data is analyzed and summarized in a report along with mitigation strategies and risk-based choices where risk tolerance, attack difficulty and relative consequences are carefully considered.

Another well recognized threat modeling and assessment methodology is the National Security Agency (NSA) Information Security (INFOSEC) Assessment Methodology (IAM) [228] which is coupled with the NSA INFOSEC Evaluation Methodology (IEM) [229]. The IAM's goal is to help the system stakeholders improve their INFOSEC posture. The first step in the IAM is the pre-assessment step which entails gathering information on the stakeholder's organization and environment including key staff members, mission statement, requirement and constraints. In this phase critical information assets and information systems of the organization are discussed. Next, on-site activities where the systems reside are conducted and include understanding the security policies, procedures and the formation of information criticality matrices, listing of impact attributes of the systems under analysis. In the post-assessment phase of the IAM, the findings of the pre-assessment and on-site visits are documented, and considerations are made for the IEM phase are made. In the IEM, a technical evaluation plan (TEP) is formulated which includes the technical steps based on the IAM criticality matrices and impact attributes. During the on-site evaluation phase, the TEP is used as a guide while various network, host-based penetration testing and vulnerability scanning tools are used to collect system data during reconnaissance, vulnerability scanning and penetration testing activities. The final phase of the IEM is the post-evaluation phase which entails drafting a report with the findings gathered during the on-site evaluation phase. In the final report mitigation strategies and risk-based choices based on the IAM criticality matrices are carefully considered.

To understand the threats and risks, it is necessary to have a good knowledge of communications architecture, entry points, vulnerabilities and critical information an attacker might want to access or damage it might want to cause. Risk analysis can be performed based on component models [223].

C. BESS REMOTE ATTACK SURFACE

One of the biggest sources of concern with respect to cybersecurity of DERs and the power grid are massive coordinated attacks operated remotely [15]. A successful attack would require exploiting the attack surface of DER and gaining a foothold in their ICS network or by accessing remote control systems, such as a utility SCADA or DER management system (DERMS), or aggregator control network. Security of enterprise SCADA and enterprise IT systems is critical and could be subject to regional regulations (see Section VI) but is out of the scope of this paper.

An entry point is any device that would allow an attacker located remotely to communicate with the system. Detailed threat models of BESS were not found in the literature, but closely related systems dedicated for end-consumers such as electric vehicles have numerous wireless connection methods such as Bluetooth, Wi-Fi, cellphone data and others [150], which create a large attack surface. The entry points of BESS can be limited through many protection layers, including physical security, and by policies limiting the communications capabilities of such devices. In a typical BESS, it is common to find the following entry points:

- Service equipment;
- Local Area Network (LAN);
- Meter;
- WiFi or Bluetooth-connected devices;
- Vendor cloud service or server;
- Software and firmware upgrades;
- Public-Facing Infrastructure (e.g. web portals);
- Remote access technologies (e.g Virtual Private Network (VPN), Virtual Network Computing (VNC)).

Intrusion into ICS networks through internet connections have been reported [230]. Lack of authentication for accessing internet connected PLCs is a security flaw commonly

found in ICS [21]. Threat actors operating in the ICS domain have historically targeted remote access technologies such as Remote Desktop Protocol and VPN. VPN is often used by vendors and system integrators to access OT networks and, if compromised, can allow hard-to-detect adversary access into operation environments [230]. Remote connection capabilities are commonly used to monitor the OT assets, perform software updates, or perform maintenance [172], [231]. Complex systems like large power plants are often supported by multiple equipment manufacturers and other specialized service providers that may access the ICS network to monitor or remotely control devices, which multiplies the risk of exploitation in vulnerabilities present in remote connection systems. If these remote connection capabilities are compromised, the OT network might be exposed to cyberphysical attacks capable of disabling or damaging the plant.

Human online activity is another major point of attacks. For instance watering hole attacks have been used to harvest credentials, later used to exploit vulnerabilities in Windows Servers, such as ZeroLogon [230], [232]. Spearphishing attacks have been used as a common way for accessing IT networks and then advancing into OT systems [21].

A penetration test applied to several home BESS has found multiple vulnerabilities and several examples of lack of implementation of standard cybersecurity controls [11]. The researchers identified missing or weak access control mechanisms allowing remote access to BESS local web portals over LAN, as well as connection to internet-hosted web portals. Inadequate authentication practices including static (immutable) passwords, standard passwords, or complete lack of authentication allowed device access and remote code execution from local networks. Flaws in the protection of data-in-flight privacy were identified, with some devices lacking adequate encryption and authentication of messages transmitted over the internet to remote vendor servers, which could allow MITM attacks. Update practices were also found inadequate from a security point of view, without digital signatures or other integrity controls, possibly allowing attackers to inject manipulated system updates. Poor manufacturer web portal implementation allowed connection between any BESS from the same manufacturer though standard passwords used for accessing VNC server and access to expert mode, which is a type of privilege elevation. This attack could allow a malicious actor to perform emergency shutdown of a BESS, manipulate operational limits and modes of operation. Deployment of ransomware is also a common type of attack from threat actors seeking financial benefits.

D. PHYSICAL SECURITY

Restricting physical access to BESS is very important from a cybersecurity standpoint of both large and small BESS. An attacker with physical access to a system or facility can steal devices, recover discarded devices, connect spy or hacking devices (e.g. plug key loggers or other devices to USB and debug ports), physically destroy system components [217], access removable data storage, perform physical connection to restricted computer networks, or circumvent IT cybersecurity controls. The main goals of physical security controls are to detect threats (e.g. motion sensors, cameras), control access (e.g. gates, fences, locks, badge readers), delay action of threat actors (e.g. vehicle barriers), and responding to threats (e.g. security personnel, law enforcement) [55].

For IoT devices, some of the recommendations include protection to access and availability of physical medium of data storage. Those include: applying encryption to data-at-rest, guarding against removal of data storage physical medium; ensuring external ports cannot be used to maliciously access the device; designing devices that are tamper-proof or cannot be easily disassembled; disabling or physically removing any external ports that are not required for the product to function; enabling limiting roles of users [233].

In utility-scale modular systems, it is likely that there will be electrical connections and communications wires in between modules, which are typically buried. Therefore, physically damaging or having physical access to any of the components shown in Fig. 11 would require an inside actor [234], breaching physical barriers such as chain link fences or gates. For all components physically inside of a BESS, an external malicious actor would additionally have to defeat door locks to access them. Other physical threats to BESS are out of the scope of this paper, and discussions regarding various attacks using vehicles, firearms, etc., will be omitted.

The communications architecture of BESS depicted in Fig. 11 shows two network switches physically inside of the system. For commercial or utility-scale systems, it is safe to assume that physically accessing them or any other service ports in any of the devices listed would require an inside actor or defeating at least two physical layers or protection: module door locks and site fences or gates. Additionally, an attacker would have to escape detection by security cameras and other alarm sensors to avoid confrontation with security and law enforcement [55]. Furthermore, if any of these networks have a wireless implementation such as Wi-Fi or Bluetooth (piconet), connecting to or eavesdropping into these networks could be performed from a short distance.

Protecting communication assets such as cables, switches and other devices from inadvertent and intentional damage reduces the risk of losing data availability caused by a physically-induced failure in communications, such as disconnecting a cable or asset theft. Insufficient physical access controls can also allow malicious actors to alter system settings through an unprotected HMI, manipulate system calibration or damaging equipment [172]. Furthermore, very often DER communicates do not encrypt data, which might allow a malicious actor wiretapping a physical communications device to access the data being transmitted [173]. Unprotected local networks can be an effective attack vector for malicious actors targeting home BESS, therefore in some cases physical security might be the only protection of systems with improper access controls or measures for

TABLE 7. Summary of potential attacks on batteries found in the literature.

Attack	Target	Origin	References
Device swap	Integrity	Supply chain	[63]
Kinetic	Integrity	Local	[239]
Counterfeit devices	Integrity	Supply chain	[63]

protecting privacy and integrity of data [11]. It has been shown recently that given enough physical access to devices and software, cryptographic keys can be extracted from mobile payment systems and Digital Rights Management devices, which can harm security of data-in-flight [235].

E. SUPPLY CHAIN ATTACKS AGAINST BATTERIES

Counterfeit devices supplied to BESS can lead to several security problems. Counterfeiters can resell rebranded (or rewrapped) degraded battery cells [76] or knockoff batteries that do not have protection circuits [236]. Counterfeit items can go over carefully engineered falsification processes that can be hard to detect [237]. Those items have inferior quality in terms of capacity and safety.

One means of detecting counterfeit batteries is through authentication. In [238], a wireless hardware module based on secure hash algorithm was proposed for authentication of batteries by BMS. This approach could be used to detect counterfeit batteries or to protect against battery swap-type attacks [63]. A summary of attacks on batteries can be found on Table 7.

F. SECURE COMMUNICATIONS

1) ENCRYPTION

The main goal of cryptography is to preserve the confidentiality of information. A cryptosystem uses keys and enciphering functions to transform a message (plaintext) into an unintelligible piece of information called a cyphertext. The same cryptosystem can use a key to decipher the cyphertext in plaintext again. Cryptographic techniques can also be used to verify the integrity of a message (e.g. hashing) and identity of message senders [216]. In spite of the relevant computational burden of cryptographic algorithms, modern embedded systems have enough processing power to encipher and decipher messages [113]. For instance, current generation of microprocessors used in automotive ECUs can perform Advanced Encryption Standard (AES) encryption on the application layer of CANbus in reasonable time for automotive applications [188].

The use of Public Key Infrastructure (PKI)[6] has been long ago pointed out as a suitable solution for Smart Grid cybersecurity [35]. However, that can only be possible through standardization of Smart Grid communication protocols and the development of appropriate tools. Many recently developed or updated standard communication protocols do support encrypted communications, such as IEEE 2030.5 [173].

While much attention is focused in protection of data-in-transit, encryption is also a powerful tool for security of data-at-rest. A typical solution for protecting confidentiality of data-at-rest is to physically isolate the servers where data is stored and to encrypt that data. However, if the identity and credentials of the account that has access to this data is stolen, then it is possible defeat such protection measures.

2) AUTHENTICATION

Authentication can be defined as the process of verifying the integrity of the origin of data by relating the data source to a known identity [216]. Typically, authentication process relies on one or more of four factors: who you are (e.g. biometrics like retinal pattern or fingerprints), where you are (e.g. geolocation, IP address), what you have (e.g. token, badge, or card), and something you know (e.g. password). Verification of message authenticity can impede actions from a malicious actor capable of communication with a target system by rejecting the messages from a source whose authenticity cannot be verified [66].

Insufficient or nonexistent authentication methods supporting access controls have been detected in commercial home BESS, exposing these systems to intrusions from attackers with access to local networks [11]. It is possible to retrofit devices to incorporate authentication mechanisms. In [240], a bump-in-the-wire device was designed to append a message authentication code to IEC61850 GOOSE messages used in electrical substation communications.

Another measure used to harden CPS is to employ secure communications protocols or to add security features to existing systems. In [176] the authors have proposed an improved version of the MQTT by implementing several security features on top of the existing protocol capable of performing mutual authentication, access control, data security, control message security, and end-to-end security. The popular ICS communications protocol has a variant called Modbus/TCP Security that features x.509v3 certificate-based identity and authentication with TLS v1.2 [189].

G. NETWORK SEGMENTATION

Network segmentation refers to the logical or physical separation of a communications networks. This approach is an effective method for reducing the impact of a cyberattack exploiting common vulnerabilities to devices connected to the same network [241]. Segmentation can be particularly useful for obtaining separate network enclaves for critical and noncritical devices, or devices featuring entry points. Use of firewalls can be done in the interface between the network of critical devices and others.

Isolation of OT networks, known as ''air gapping'', is an extreme case of network segmentation. This practice was once thought to provide a very high level of security against remote attacks, but this has been proven incorrect in several cases. For instance, the system targeted by Stuxnet was

[6]PKI provides management of digital certificates and public-key encryption. Public-key cryptography uses one-way encryption using a public key (available to anyone) to encrypt plaintext, which can only be decrypted by a private (or secret) key.

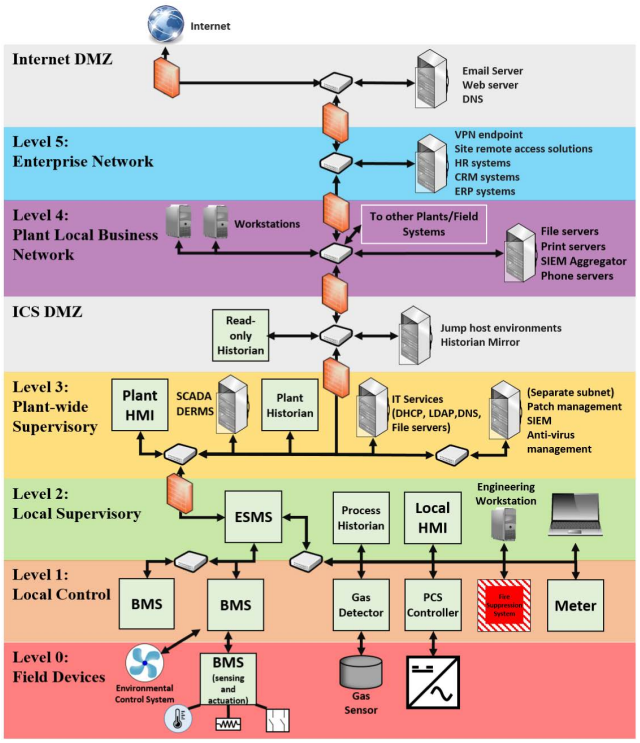


FIGURE 20. BESS IT and OT networks and the Purdue model [55], [244].

thought to be air-gapped, which would have been circumvented in the attack [242]. Also, it is often found that incorrect cybersecurity practices and training of personnel can lead to breaches in the air gap [231]. Systems not connected to the internet are hard to patch and very often use legacy software that is no longer supported by their vendor, which carries vulnerabilities that could be exploited by an attacker capable of breaching the air gap. Air-gapped systems also have limited remote monitoring and unpractical maintenance. Furthermore, some ICS require communications with other systems for maintenance and operation, which impedes complete system isolation. One way of preventing access to restricted network while keeping monitoring capabilities is by using unidirectional security gateways, also known as data diodes. The unidirectional nature of communications comes with restrictions of protocols, so often more flexible technologies are used in ICS [243].

Fig. 20 shows an example of communication system connecting a utility-scale BESS to the corporate environment. A classification of these networks can be done through the Purdue Enterprise Reference Architecture, also known as Purdue model. This model has 6 levels, with the lower three representing OT systems and the higher three representing IT systems. Separation between IT and OT environments is typically done through a demilitarized zone (DMZ) [55].

A DMZ is a segment of the network that divides the network in an internal and external part [216]. The goal of the DMZ is to separate the traffic between these network segments. In an ICS-type network such as the one a utility-scale BESS is typically located, there should be at least one DMZ in between the enterprise network and the ICS network as well as a DMZ between the internet and the enterprise network [245].

Network segmentation presents some drawbacks in terms of increased communications latency and increased complexity of network administration. These can prove particularly challenging for DER operations since some applications might be sensitive to latency and the communications infrastructure might be owned by several entities. Logical segmentation can be done through firewall rules and Virtual Local Area Networks, to name a few examples [241].

1) FIREWALLS

For communications systems owned by a single entity, firewall rules are a good choice for network segmentation. Firewalls are pieces of networking software or hardware that provide rule-based control of data traffic. Firewall software running in a computer to block messages to this machine are called host-based firewalls. Stateless firewalls, also known as packet filters, block or let packets through based on their IP and port, which correspond to Open Systems Interconnection (OSI) layers 3 and 4. Stateful firewalls have state tables that are used to keep track of network connections and are deemed more secure. For instance, if one machine inside the corporate network establishes communication over TCP with an external computer, a stateful firewall at the edge of the corporate network would be aware of such connection. There are reports of employment of commonly used ports and protocols by attackers as the means of circumventing firewall protection [21].

Application firewalls using deep packet inspection, also known as Next Generation Firewalls are able to analyze data from higher layers in the OSI stack, namely session, presentation, and application. Those evaluate the payloads of network packets and are equipped with software able to distinguish between normal and abnormal communications, possibly allowing them to detect cyberattacks. While application firewalls are already commercial products, applications for DER are still incipient. Deep packet inspection has been considered an important technique for detection of cyberattacks [246].

Firewall rules allow the creation of network enclaves. The best practice is to block all traffic and only allow data from exceptions. In DERMS that could involve allowing communications originating from known sources such as DER in HAN. For large numbers of DERs, this approach could prove resource intensive in terms of network management [241].

2) VIRTUAL PRIVATE NETWORKS

VPNs have been adopted as a solution for securing DER communications with aggregators and utilities [247]. As the name suggests, this technology allows the connection between a remote device (or LAN) and another private network[7] over

[7]Private networks support a limited amount of authorized users that can communicate using private IP addresses. In traditional private networks, all data traffic between machines in the network is isolated and passes only through devices that are connected to the private network.

public or shared infrastructure (e.g. the internet) in a manner that emulates the direct connection between the aforementioned device and private network. With this virtual extension of the private network, the remote device gets most benefits of being connected to a private network, such as access to resources in the network (e.g. access to local data repositories or servers that do not communicated with the internet) [248]. Typically, this network extension is implemented by what is sometimes called a "VPN tunnel",[8] which is an encrypted connection over public network infrastructure between a remote device and a VPN server located within the private network, which functions as a bridge between the private network and VPN-connected users.

VPNs offer a multitude of advantages. Encrypted VPN links offer improved protection of data confidentiality and integrity for communications over the internet, which is an enabler of remote work. Further, VPNs are more cost effective and can be setup much more quickly than traditional private networks, especially if network infrastructure needs to be deployed to connect networks over large distances. VPNs, however, present some technical drawbacks and security concerns. Unlike in traditional private networks, data transmitted over VPNs passes through links owned by third parties, which could allow malicious actors to eavesdrop packets if vulnerabilities are exploited. VPNs have shown vulnerabilities [249], including zero-day exploits [250]. Also, routing data traffic over public infrastructure exposes communications to quality of service problems that might affect overall system performance. Further, the encryption algorithms are computationally expensive, which can increase costs and reduce data throughput [248].

In most use cases, once a device is connected through VPN, all of its communications traffic is routed through the virtual network. If a device is communicating several data types that should be segmented, the use of VPN could pose a security risk. In these cases, a possible solution could be the use of per-application VPN, when device establishes a VPN connection for a specific communication application. This technology is still under development for mobile devices, but it could allow inverter manufacturers to develop downloadable smart inverter applications for their platforms, and allow that application to be run in a per-application VPN [173].

H. BLOCKCHAIN

Blockchain is the name given to a class of electronic distributed databases that contain logs (or ledgers) of timestamped digital transactions. These logs are combined into blocks, which are stored in distributed public ledgers that can be accessed through digital networks. The blocks are sequential and time-stamped, signed by private keys. A one-way function produces a short sequence of bits, called the hash, that is dependent on all of the items that are placed in the log. This hash works as a digital fingerprint, which is designed to be virtually unique given a certain log. Consequently, when adding new entries to the log, its hash will change. The hash and the log are published so that they can be audited by independent third-parties using public keys. The maintenance of the blockchain is divided between many entities and its integrity is verified by distributed consensus algorithms [173], [251]. A visual summary of the blockchain technology is shown in Fig. 21.

The blockchain structure offers several advantages. The distributed architecture achieved through consensus algorithms eliminates single points of failure, avoids performance bottlenecks, and reduces infrastructure costs. The continuous validation of transactions that are permanently stored and linked allows auditability and identification of illegitimate transactions. Some of the disadvantages of blockchain are its intense computational and storage requirement, which are major challenges for embedded systems, as well as vulnerabilities in the consensus algorithms [173].

A key concept enabled by blockchain technology are smart contracts. In theory, a smart contract [252] is a digital set of clauses, typically in the form of computer software, that can be executed automatically, i.e., without human intervention. When implemented using blockchain technology, smart contracts regulate changes made to a ledger [251]. Further, the blockchain framework provides transparency that allows the parties involved in a smart contract to verify their counterparts' performance of the contract while the distributed verification of transactions allows the mediation necessary for unknown and untrusted parties to enforce their contracts [251].

In the energy sector, blockchain has been deemed a disruptive technology, potentially enabling several applications. Peer-to-peer (P2P) energy trading through smart contracts can enable the participation of small energy producers and consumers in localized, energy-efficient micro-markets. Blockchain can provide a framework for secure and decentralized management of intelligent devices [251]. Blockchain has been proposed as a means to ensure data integrity in Smart Grids through distributed ledger-enabled multi-factor verification [253]. This framework can support anomaly detection and detection of unauthorized modification of critical Smart Grid data, including configuration information, telemetry and commands. While the technology would provide little protection against unauthorized network access, it could generate timestamped data logs used for incident analysis. A recently proposed architecture developed by NIST for securing communications between DER, aggregators and utilities uses a distributed ledger for logging all information exchanges between those entities, which can be used for auditing [247].

IoT devices, such as BMS, can use blockchain technology to improve their security in many ways. By using blockchain's PKI, BMS could have an ID and asymmetric key, allowing packet encryption, which would assure data integrity and privacy even if insecure communication protocols are used [62]. Blockchain technology can also help to keep integrity of stored data by leveraging its

[8]More generally, tunneling refers to the practice of encapsulating one protocol in another protocol.

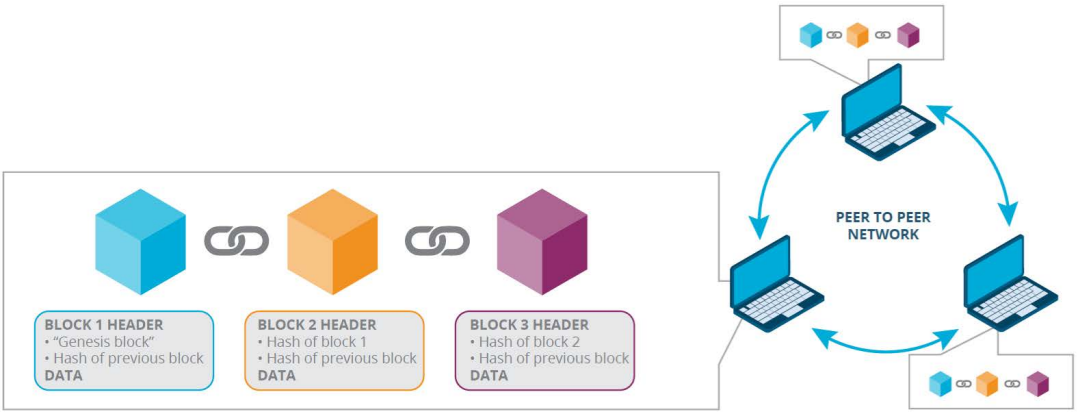


FIGURE 21. Overview of blockchain technology.

distributed ledger. If data is manipulated by a malicious actor, its integrity can be verified by consensus algorithms analyzing the data in public ledgers [62], [254]. Smart contracts can provide automatic integrity verification of firmware version and updates by leveraging version hashes stored in blockchain ledgers. If a firmware has been illegally changed, a smart contract can request the latest firmware via a distributed P2P filesystem [255]. A blockchain-based IoT firmware update technology has been developed [256]. Blockchain's smart contract-based access control can also be leveraged to guarantee data privacy [62], [257].

Furthermore, blockchain technology for supply chain management can help identify and trace system components such as electronics, batteries and others [62]. Examples of such technologies include TrustChain [258] and POMS [259].

In [260], battery monitoring system using IoT-enabled WBMS and a blockchain server was implemented. The blockchain network uses Hyperledger Fabric [261] system. The WBMS are IoT devices which interact through an IoT gateway with a cloud-based battery monitoring and diagnosis system [157], which is the blockchain server. This blockchain-based technology allows scalability and processing power through the IoT network and cloud service. In terms of security, the blockchain technology implements communication and data security. Some limitations of this technology include memory limitations of embedded devices under growing blockchain ledgers, latency of the system, possibility of compromise of blockchain accounts due to private keys with limited randomness and lack of a consensus protocol that can be scalable and simple [62].

Most applications of blockchain technology in energy storage, or even in the energy sector in general, have been on small research or demonstration projects. There are still concerns with respect to security, scalability, and speed of large energy projects [251]. Further, security risks exist due to poor system design or cyberattacks. Many blockchain implementations are not yet mature technologies, therefore it is expected that vulnerabilities and software bugs might be common [251]. Digital wallets holding Ethereum, a major cryptocurrency, have been successfully attacked by cybercriminals in the past [262]. Energy consumption of blockchains that operate in untrusted environments remains a significant drawback. For example, Bitcoin consumes approximately 119.22 TWh per year (0.53% of energy consumption worldwide) [263].

I. ACCESS CONTROL

Access control is especially challenging for consumer-owned BESS. Asset owners monitor their system, which is usually more conveniently made over a phone application or web portal. Vendors need to push firmware updates, provide advanced analytics (e.g. health monitoring and schedule maintenance). Grid operators and aggregators need to monitor the systems and control their fleet of BESS. Under those conditions, establishing a process for controlling the access to information and processes in information systems [264] can be very hard to implement. Furthermore, from the point of view of information security, it is necessary to have robust mechanisms able to restrict access to system resources. In a DER that has reconfigurable control settings, unauthorized users can maliciously change those parameters and compromise equipment operation.

RBAC has been advocated as an appropriate solution for DER applications [69]. RBAC is a popular method in complex organizations where assigning permissions for each system user individually is a labor-intensive process. The underlying idea of RBAC is that the need to access or modify information depends on the function each user needs to perform in the systems [216]. The same access control policy has been used in IEC's family of standards for securing power system communications (IEC 62351-8) [69].

The example solution for protecting DER communications developed at NCCoE uses gateways to control access based on identity tokens. These are inserted into the header of the first packet sent to open a TCP connection. If the identity is not recognized or unauthorized, the request is ignored [247].

J. INTRUSION DETECTION SYSTEMS

Traditional Intrusion Detection Systems (IDS) applied to IT systems monitor network traffic and packet content and report results to system administrators. From the point of view of CPS, the concept of IDS can be expanded to OT systems. These physical IDS can monitor not data traffic but physical quantities measured by sensors or calculated by controllers and search for anomalies.

The example solution presented in the NIST Cybersecurity Practice Guide for DER communications [247] uses a NIDS that learns the topology and behavior of devices on the OT communications network. This system can perform communications monitoring, traffic analysis, and detection of anomalies in multiple points of the system.

1) INTRUSION DETECTION SYSTEM FOR BATTERIES

There exist several examples of IDS applied to battery-based mobile systems. In [265], a battery-based intrusion detection system has been proposed to detect the exploitation of battery power via DoS attacks. In [266] an IDS framework to mitigate the impact of battery depletion DoS attacks in mobile devices and laptops. In [267], the authors have proposed a hybrid scheme named multi-vector portable IDS that monitors the host-based device instantaneous current and traffic signatures. The framework recognizes any significant change in the instantaneous current of the device and correlates it to the anomaly or increase in Wi-Fi or Bluetooth traffic. Model-based anomaly detection [268] or signature matching [242] can be used to detect anomalies in sensor readings.

2) NETWORK INTRUSION DETECTION SYSTEMS

Generally, a BESS is composed of common OT [269] network and computing components and therefore commercial IDS can be applied to BESS to monitor and detect internal and external threats. Network threats are present within network communications traffic, and host computing systems threats are present in the form of malware. Network threats can affect the proper operation of devices communicating in the network and include routers, switches, and endpoint systems. A network IDS (NIDS) is placed at the network layer, they are typically connected directly to a Switched Port Analyzer (SPAN) port so that the IDS can observe and monitor all communications traversing the network switch. NIDS use anti-threat software and is only installed in specific points of the network. An endpoint IDS which is termed as a host-based IDS (HIDS) is typically provides access to host-based data such as system calls, event logs, and system files. HIDS include multiple anti-threat software applications that are installed on every network computer that can perform two-way communications with the outside of the network.

Both an NIDS and a HIDS use signature-based and anomaly-based intrusion detection (AID) techniques. Signature-based intrusion detection (SID) inspects data for specific patterns that are indicative of known malware and network attack sequences. 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 approaches focus on recognizing abnormal patterns in data and compared to baseline data or detect when specific portion of the observed data is a statistical outlier. In the case of supervised learning [270] anomaly detection, the IDS is trained using baseline data that does not contain attack events. An unsupervised learning [271] anomaly detection IDS does not require training, but instead identifies segments of monitored data that are statistical outliers. Supervised and unsupervised learning anomaly detection systems are often implemented using statistical machine learning algorithms. A third approach is policy-based intrusion detection, where a logical security policy and an execution trace validation algorithm identify legal and illegal information flows between the objects of a system [29].

Several commercially available NIDS and HIDS products [272] are implemented with SID and AID, and each intrusion detection type has its own set of benefits and drawbacks. SID techniques require the use of threat pattern catalogs that contain known malware and attack signatures. An attacker can evade detection by a SID based system by slightly modifying its attack signature. Additionally, SID techniques are not useful on zero-day attacks where an attack is launched for the first time. SID techniques are particularly useful when dealing with fixed malware and attack patterns that do not often change. Polymorphic and metamorphic malware [273]–[275] are types of malware that vary their attack signatures dynamically and are thus not able to be detected by SID systems. Additionally, network attack sequences can be varied and temporally staggered dynamically to avoid direct signature matching by the SID system.

Unlike SID systems, AID systems can detect dynamically varying and zero-day attack patterns using supervised and unsupervised learning algorithms. The detection sensitivity and accuracy of AID systems based on supervised learning, are highly dependent on the amount and quality of the detection training data. The detection sensitivity and accuracy of AID systems based on unsupervised learning depends primarily on the chosen data outlier metrics.

Simultaneous implementation of SID and AID systems can benefit from their complementary characteristics, with SID being the most accurate for known and static threat patterns and AID systems detecting dynamically varying and zero-day threats. AID and SID systems are generally configured within WAN and LAN monitoring nodes as illustrated in Fig. 22. The WAN monitoring node samples TCP/IP packets via a network tap and samples firewall log data within the DMZ located between the WAN and LAN networks.

The LAN monitoring node is typically connected to a switch spanning port and samples TCP/IP packets on the BESS subnet. Generally, a grid-based BESS will contain operational logs which can be sampled as well by the LAN monitoring node. In a robust WAN and LAN threat monitoring configuration, nodes utilize the AID and SID system algorithms described in the following sections to detect threats and decide on a set of optimal mitigations.

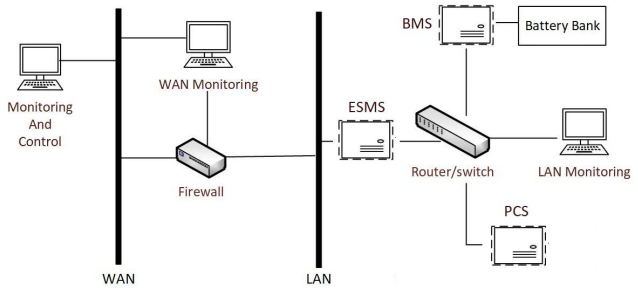


FIGURE 22. Example of application of NIDS to BESS.

a: SUPERVISED LEARNING ANOMALY DETECTION

Supervised learning is a category of machine learning which maps labeled training data feature vectors to individual classes. Once trained, the supervised learning algorithm can be used to classify new unlabeled data samples that did not appear in the training data. The supervised learning algorithm can generalize patterns and relations based on the training data and classify previously unobserved data. Some of the more common supervised learning algorithms include support vector machines, linear and logistic regression, decision trees, neural networks, Naive Bayes and K-Nearest neighbors which are explained in [276], [277].

b: UNSUPERVISED LEARNING ANOMALY DETECTION

In unsupervised learning, the training data are not labeled with their classifications. As such, unsupervised learning models must identify relationships between elements of the training data without being provided with knowledge about which elements belong to which class. Unsupervised learning is often referred to as cluster analysis or clustering, though strictly speaking clustering is only one type of unsupervised learning. Some of the more commonly utilized algorithms include K-means clustering, hierarchical clustering and unsupervised neural networks which are explained in [278]–[280].

c: SEMI-SUPERVISED MACHINE LEARNING

In supervised machine learning it is often challenging to find a complete set of labeled data with which to train the models. Semi-supervised machine learning on the other hand facilitates training by using a large amount of unlabeled data in conjunction with a small amount of labeled data to train the IDS anomaly detection models. It has been found that semi-supervised as compared to unsupervised learning exhibits higher learning accuracy [281]. In semi-supervised learning computational complexity of threat classification can be greatly reduced by observing a subset of a dataset and then inferring a decision boundary within unlabeled data samples.

d: REINFORCEMENT LEARNING

Reinforcement learning (RL) uses an iterative method where feedback is provided to a learning agent that can derive an optimal policy for domain specific actions. RL does not require labeled data but does require an operational environment for the learning agent to gather information. As a learning agent takes actions within the operating environment, a state and reward for each action is determined. The learning agent will form an optimal actions policy where the largest reward is received for each action made [282]. Applied to classification problems in an anomaly detection-based IDS, an optimal actions policy is derived such that observations are optimally assigned labels based on the learning agent's actions within the environment. RL techniques can be slow to converge on optimal policies and thus require more computational resources than supervised learning algorithms. The types of RL methods for deriving an optimal actions policy such as value functions and policy gradients are explained in [270], [283]–[285].

3) PHYSICS MODEL-BASED ANOMALY DETECTION

Successful attacks on ICS have compromised control systems and situational awareness of monitoring, protection and control systems to achieve their goals. Stuxnet, for example, compromised situational awareness of operators by leveraging measurement recalibration and replaying data from normal operations to HMI, alarm systems, and the legitimate control code. At the same time, the malware induced overspeed and ovepressure on nuclear fuel centrifuges, eventually damaging some of them [242]. Modification of control logic and parameters have also been reported as attack vectors, which could cause malfunction of physical plants [21]. FDIA have emerged as a source of stealthy attacks on CPS, where the attacker attempts to cause damage or alter the operation of the system by manipulating the values of measurements or control signals. In such a scenario, the attacker designs an attack vector that maximizes damage to the system and minimizes the probability of detection by traditional methods. Because BESS are a type of CPS, one should consider that similar types of attacks could be designed to target energy storage systems or some of its subsystems, such as a BMS. From the point of view of cybersecurity defense, there is typically no situational awareness for communications at Purdue levels 0 and 1 (see Fig. 20), whose traffic is rarely monitored and where accurate analysis tools are lacking [242].

Research in power systems state estimation produced several methods for generating a stealthy attack vector for static state estimation if the physical model is known by the attacker [286], [287]. These FDIA can circumvent the bad data detection algorithms utilized for detecting tampered measurements. The physical models for battery systems are dynamical in nature, hence these static bad data detection methods are not applicable. Furthermore, CPS might require complex models to provide an adequate representation of the system dynamics. CPS typically integrate physical systems, which are naturally modeled in continuous time, with electronic controls and sensors signals processed by discrete time algorithms. Therefore, hybrid system model approaches might be used. Alternatively, CPS can be modeled as distributed parameter systems [59].

The work [268] presented a method for detecting FDIA on CPS. Let's consider the state-space model of a linear time-invariant dynamic system, where its state transition dynamics are described by (9) and its state-dependent output (or measurement) function is given by (10).

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \mathbf{w}_k \tag{9}$$

$$\mathbf{y}_k = \mathbf{C}\mathbf{x}_k + \mathbf{D}\mathbf{u}_k + \mathbf{v}_k \tag{10}$$

The matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ and $\mathbf{D}$ model the dynamics of the system and might be time-dependent [120]. It is assumed that the CRM process noise is a random vector with $\mathbf{w}_k \sim \mathcal{N}(\mathbf{0}, \mathbf{Q})$ and $\mathbf{v}_k \sim \mathcal{N}(\mathbf{0}, \mathbf{R})$. More information on battery modeling can be found in Section III-H.

FDIA targeting sensor integrity and control signal attack can be represented as (11) and (12) respectively [64], [224].

$$\mathbf{y'}_k = \alpha_y \cdot \mathbf{y}_k + \beta_y, \quad k \in \mathcal{T}_a \tag{11}$$

$$\mathbf{u'}_k = \alpha_u \cdot \mathbf{u}_k + \beta_u, \quad k \in \mathcal{T}_a \tag{12}$$

Following this generalized FDIA model, $\mathbf{y'}_k$ and $\mathbf{u'}_k$ are the tampered sensor measurement and control input vectors, respectively. $\mathcal{T}_a$ denotes the period when the attack is performed. Scaling attacks and additive attacks can be performed by selecting $\alpha_y, \alpha_u \neq 1$ and $\beta_y, \beta u \neq 0$, respectively. These attack coefficients can be of any format chosen by the attacker, such as white noise, decaying high-frequency harmonics injection, periodic function, periodic pulse injection, constant value, to name a few [64], [224].

If the pair ($\mathbf{A}$, $\mathbf{C}$) is observable, one can estimate its state variables given that input and output are known. A KF can be developed to compute a minimum mean squared error state estimate using the following recursive relationships:

$$\hat{\mathbf{x}}_{k+1|k} = \mathbf{A}\hat{\mathbf{x}}_{k|k} + \mathbf{B}\mathbf{u}_k \tag{13}$$

$$\hat{\mathbf{x}}_{k|k} = (\mathbf{I} - \mathbf{K}_k\mathbf{C})\,\hat{\mathbf{x}}_{k|k-1} + \mathbf{K}_k\mathbf{y}_k \tag{14}$$

$$\mathbf{P}_{k|k-1} = \mathbf{A}\mathbf{P}_{k|k-1}\mathbf{A}^\mathsf{T} + \mathbf{Q} \tag{15}$$

$$\mathbf{P}_{k|k} = \mathbf{P}_{k|k-1} - \mathbf{K}\mathbf{C}\mathbf{P}_{k|k-1} \tag{16}$$

$$\mathbf{K}_k = \mathbf{P}_{k|k-1}\mathbf{C}^\mathsf{T}\left(\mathbf{C}\mathbf{P}_{k|k-1}\mathbf{C}^\mathsf{T} + \mathbf{R}\right)^{-1} \tag{17}$$

The estimates $\hat{\mathbf{x}}_{k|k-1}$ and $\hat{\mathbf{x}}_{k|k}$ represent *a priori*, or predicted, and *a posteriori*, or updated, state estimates, respectively. Similarly, $\mathbf{P}$ is the covariance of the state estimation error and $\mathbf{K}$ represents the so-called Kalman gain used in the state correction step, (14). The measurement residual $\mathbf{z}_k = \mathbf{y}_k - \mathbf{C}\hat{\mathbf{x}}_{k|k-1} - \mathbf{D}\mathbf{u}_k$ is defined as the difference between actual measurement and estimated measurement. Let us define the measurement post-fit residual as,

$$\mathbf{z}_{k|k} = \mathbf{y}_k - \hat{\mathbf{y}}_{k|k}, \tag{18}$$

where the post-fit estimated output is given by

$$\hat{\mathbf{y}}_{k|k} = \mathbf{C}\hat{\mathbf{x}}_{k|k} + \mathbf{D}\mathbf{u}_k. \tag{19}$$

The covariance matrix of post-fit measurement residual is given by

$$\mathbf{P}_{\mathbf{z}k|k} = \mathbf{C}\mathbf{P}_{k|k}\mathbf{C}^\mathsf{T} + \mathbf{R}. \tag{20}$$

Since the measurement residual, $\mathbf{z}_k$ is a Gaussian random variable, the quantity $g_{k|k} = \mathbf{z}_{k|k}^\mathsf{T}\mathbf{P}_{\mathbf{z}k|k}^{-1}\mathbf{z}_{k|k}$ follows a χ^2 (chi-squared) distribution. In [268], a χ^2 detector can be used to detect anomalies in CPS. The alarm will be initiated if the value $g_{k|k}$ exceeds a preselected threshold value of η. η can be chosen based on the number of degrees of freedom (function of number of measurements and state variables) and a probability of false alarm $\gamma_k = Pr(g_{k|k} \geq \eta)$. It is important to note that this probability does not take into account any characteristic of FDIA, but stems from assumptions about model correctness and noise variance and mean. Such detector can be used both for detection of errors in sensors as well as detecting FDIA attacks [288]. To deceive a state estimator with such capability, a malicious actor would need to know the system parameters and manipulate several measurements in order to design a stealthy attack. Alternatively, other FDIA detection approaches, such as the cumulative sum algorithm (CUSUM) might be applied to residuals of, for example, an EKF [289], to determine any biases in measurements.

Approaches based on state estimation and CUSUM have also been proposed for sensor fault detection and isolation in BMS. Similarly to FDIA, faulty sensors can cause malfunction of BMS, who might fail to protect the battery cells. In [290], a CUSUM algorithm applied to the log-likelihood ratio of the residuals obtained by an adaptive EKF was used to detect and identify sensor faults in BMS monitoring battery cells connected in series. The hypothesis test used for identification of fault modeled the residuals of each cell voltage measurement as a Gaussian random variable that follow either distribution for normal behavior (null hypothesis) or faulty behavior (alternative hypothesis). Following a sensor defect detection, the fault identification process assumed that only one sensor error occurs at a time for a given battery string. If only one sensor fault is detected, then it is assumed that the cell voltage sensor has a defect. If multiple CUSUM detectors identify faults simultaneously, it is assumed that there is a defect in the string current sensor. In [291], absolute value of residuals of estimated SoC and battery capacity were identified as the feature of choice for detection of errors in BMS sensors. The residual of SoC corresponds to the difference between the SoC estimations obtained by two distinct methods: Coulomb counting and an Unscented Kalman Filter (UKF) using a first-order ECM. The UKF uses a battery model with parameters identified by recursive least-squares (RLS). So called battery capacity residuals are defined the difference between the reference battery capacity and the estimated capacity calculated by the RLS-EKF method.

The CUSUM detector is designed to detect persistent attacks, therefore intermittent attacks can be designed to remain undetected by this class of anomaly detection methods. In [292], online CUSUM-based attack detection and estimation algorithm, a generalized Shewhart test and a sliding-window χ^2 test have been for detection of intermittent and persistent FDIA. The method estimates the attack parameters based on a few additive attack models. The authors also

propose a type of persistent stealthy attacks targeting CUSUM algorithms with positive control chart only. These attacks consist in manipulating the probability density function of the post-attack tampered signal to avoid detection.

Conditions for designing undetectable cyberattacks capable of introducing estimation errors on KFs have been defined in [293]. It is shown that it is not possible to induce an infinite state estimation error only by attacking the actuators. Additionally, it is proven that an attack on measurements can increase indefinitely the state estimation error in certain systems. More specifically, if the transition matrix has at least one unstable eigenvalue, its associated eigenvector is in the range space of the system controllability matrix and if the product of this same eigenvector and the measurement matrix is in the range space of the measurement attack matrix. In practice, this can be seen as an exploitable vulnerability of the system that is due to its own dynamics. This result can be taken into consideration when security features are being designed for such system.

A measurement encoding strategy was developed in [294] to increase the residuals obtained by the KF applied to the attack sequence defined in [293]. The larger values of residuals allow successful error detection. The encoding scheme is implemented by designing an invertible matrix that multiplies the vector of measurements. Attackers with knowledge of dynamical model of the system can launch stealthy cyberattacks using zero-dynamics property of systems. The authors also propose some methods to detect those attacks, including changing system dynamics (adding or removing measurements and actuators, change system topology) [295]. More generalized models for CPS attacks, in addition to conditions for detectability and identifiability of malicious actions, and monitors for detectable and identifiable attacks have also been proposed [296].

Cyberattacks and physical faults on CPS can lead to similar outcomes and affect the same systems. Additionally, ICS communications networks are often not monitored properly [230]. Consequently, making distinction between faults and some types of cyberattacks, especially deception and replay attacks, can be very challenging. In [64] it is argued that physical faults in EV powertrains tend to follow a pattern imposed by the cause of the failure (e.g. short circuit impedance), while cyberattacks can have a much more random nature. Furthermore, the same authors have identified different frequency signatures for replay attacks in phase current setpoints and short circuits between motor phases and ground.

The goal of an FDIA might go beyond introducing an error in state estimation to harm situational awareness. These types of attacks might introduce instability in closed loop systems. Stealthy FDIA against charging EVs have been discussed in [297]. The authors have demonstrated that given some knowledge of the battery dynamics and the capability of tampering with voltage sensor and current sensor data, it is theoretically possible to induce undetectable overcharge and denial-of-charging in EVs. Due to the similarities with EVs, it is possible that analogous attacks could produce similar outcomes on BESS.

4) DATA-DRIVEN ANOMALY DETECTION

The physics model-based FDIA approaches have a few drawbacks that create challenges in their application. Statistics-based anomaly detection methods require the selection of sensitivity parameters and thresholds to indicate the presence of a failure or attack. Mathematical models rely on parameters that are often assumed constant but can change over time (e.g. due to battery degradation). Also, systems can have unmodeled dynamics (e.g. effect of temperature variations) that can create a state prediction error. KF-type approaches rely on the knowledge of noise statistics, which can be hard to determine. Tracking all those parameters can be a very challenging task and possibly lead to the failure of the FDIA detection methods.

Alternatively, data-driven approaches can be applied to FDIA detection or sensor failure identification problems. ML algorithms do not rely on the same assumptions of model-based methods and learn system dynamics from training data presented to them. In [298], the authors propose a Convolutional Neural Network (CNN)-based method for detecting false sensor data in BMS. The authors consider three sensor failure modes: constant offset (additive bias), stuck fault (sensor data is not updated), and time-delay fault (sensor data transmission is delayed). In [299] the authors have extended their CNN-based approach and they have included replay faults as another class of sensor data failures and replaced temperature readings by SoC as their inputs. They have also validated their results using different cells and have compared their method to other ML approaches. In [136] the authors have used a stacked ensemble learning method to characterize and quantify deviations between a normal battery charging cycle and a battery cycles where overcharging happened. The method uses charging cycle divergence as the metric to correlate thermal and electrical stress a cell experiences during a charging cycle.

Those data-driven methods present some drawbacks. They do not incorporate knowledge of the dynamic models and it is uncertain how sensitive they are to small magnitude or stealthy FDIA. Also, as with any ML method, quality of the detector is a function of the quality of data. Because there are no real datasets available, so the authors of research papers rely on assumptions and simulations to create datasets for training and validation. Also, there are no clear limits for defining how a cyberattack can affect a system, therefore the capability of the cyberattack detection will depend on the assumptions made by the authors when defining the attacks a given BESS would be subject to when obtaining the datasets for training the ML-based method.

K. CYBERSECURITY-AWARE CONTROLS

Many types of CPS often rely on remote sensing and telemetry to control distributed systems. One example of such is the power grid, which is operated using SCADA systems and

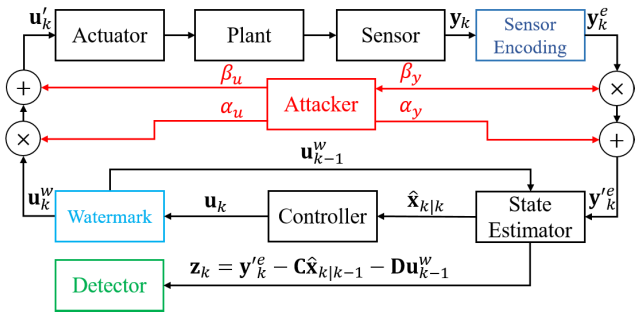


FIGURE 23. Model of deception and replay cyberattacks and defenses in closed loop-controlled CPS [294], [305]–[308].

phasor measurement units. As introduced in Section II-A, grid BESS do participate in many control loops of the power grid depending on the application they are intended to perform. Some of these control functions rely on telemetry capabilities, such as volt/VAR optimization [54], while others are time-critical and require fast and reliable communications, such as load frequency control, frequency response [10], [300], oscillations damping control [301] and power imbalance reserves [302]. These communications links between sensor, controller, and actuators might suffer from poor quality of service, which is impacted by latency, packet loss, bandwidth limitations, and change in communication topology, to name a few [303]. Very poor quality of communications can lead to system instability [301].

Many methods have been proposed to mitigate the effects of poor communications quality of service and a summary of the attack models and cybersecurity defenses is shown in Fig. 23. In [304], the authors have proposed a robust control method applied to transient stability of power systems using fast-acting BESS. This feedback control approach is designed to compensate for delays on sensor data communications. In [303], the authors have studied the impacts of problems in the quality of service of communication infrastructure and their effects on power system for load frequency control application. The proposed distributed control has shown robustness to errors in communications. A criterion for the design of proportional controllers that modulate real power output of BESS performing oscillation damping control was proposed in [301].

An attacker capable of injecting false control signals and modifying sensor readings is capable of launching undetectable replay attacks on systems operating in steady state. These attacks can disrupt the operation of a feedback controlled system by replaying sensor readings of the system in steady state while modifying the system control input. Much work has been dedicated to detect such attacks. Watermarking has been proposed as a strategy to detect cyberattacks on CPS by adding a signal sequence to a controller input such that, if a replay attack is present, an error detector can identify the replay attack. In [305], a χ^2 error detector was used to detect the replay attack using a Gaussian random watermark signal. Stochastic techniques for encoding control inputs degrade the feedback controller performance and might cause undesired effects. To mitigate the loss of controller performance, a method based on pseudo-inversion calculates deterministic watermarking signals that have guaranteed performance [308]. Game-theoretic approaches designed to find a balance between controller performance and detectability of replay attacks have also been proposed [306].

Another strategy for minimizing the effects of attacks in control inputs is to use algorithms that predict sequences of controls over a time horizon and store those values within the actuator. In [309] an attack-resilient receding-horizon control law was proposed to mitigate the effects of replay or DoS attacks in control signals of networked CPS. Whenever an attack on plant control inputs is detected, it is assumed that the signal sent from the controlled to the actuator was tampered with, and stored control signals are applied to the plant.

L. PATCHING

Unlike IT systems, OT systems have little to no tolerance to downtime. Furthermore, OT equipment is often specialized and costly, so often it is impractical or very expensive to deploy redundant systems to allow patching. Consequently, patching these systems can be challenging and will almost surely require a scheduled outage. Despite technical challenges inherent to patching of OT systems such as smart inverters, remote firmware upgrade of DER is a reality. In 2015, hundreds of thousands of smart inverters have been patched in the Hawaiian islands in a collaboration between the local utility and a microinverter manufacturer to achieve desired fault ride-through performance [310], [311].

To prevent downtime due to ICS software patching or upgrading, a scheme based on parallel deployment and execution of the updated software has been proposed [312]. The concept allows seamless transition between old and new versions of the software used to control a given industrial process by feeding operational input data and process states to both versions of the software while keeping the outdated version controlling the process until a critical point is reached. In that instant, there is a transition of operation to the latest piece of software while the first one can be deactivated without risk of halting the process.

Software downloads and program editing can be used to attack ICS [21]. Standard methods for verifying the integrity of firmware or software updates and security patches include hashes and digital signatures[9] [11].

M. CYBERPHYSICAL SECURITY OF POWER SYSTEMS

As shown in previous sections, grid BESS and the power systems are intertwined both in terms of electrical interactions as well as ICT interactions. Consequently, attacks to power systems can also affect BESS security, and vice-versa.

Problems related with cybersecurity of power systems have been raised multiple times in the past. Concerns with respect

[9]Digital signatures provide authentication of data integrity and origin in a manner that is provable for a third party [216]

to confidentiality, integrity, availability and accountability of Advanced Metering Infrastructure (AMI) communication systems have been expressed in the literature [33]. Privacy concerns are also expressed, especially concerning the unauthorized commercial use of consumer data collected by smart meters [34]. Furthermore, there is a concern with respect to consumer fraud and energy cost manipulation through smart meter hacking and cyberattacks to the physical infrastructure by exploiting vulnerabilities that give access to control capabilities of the meters [34]. Because it is very hard to implement physical security and cybersecurity controls to impede malicious actors from capturing or tampering with CPS sensors, CPS design should incorporate security features that mitigate effects of attacks on sensors [56].

Traditionally, distributed management systems (DMS) are comprised of disconnected applications, such as: fault detection, isolation, and service restoration; integrated volt/VAR control (IVVC); topology processor; distribution power flow; load modeling/load estimation; optimal network reconfiguration; contingency analysis; switch order management; short-circuit analysis; relay protection coordination; optimal capacitor placement/optimal voltage regulator placement; and dispatcher training simulator. The paradigm of distribution system operation is changing, with distributed generation, consumer demand response and power generation, two-way power flows. Future DMS will feature more detailed monitoring capabilities with the integration of AMI Interoperability of DMS applications and subsystems is an expected feature of Smart Grids, which will demand adoption of industry standards and open systems [313]. Cybersecurity of such systems had not been prioritized on its design and on the design of all elements that compose them [57].

Smart inverters are one more modern device that can introduce exploitable vulnerabilities for malicious actors. Changes in control gains and protection schemes such as Volt-VAr, Voltage-Power and others can lead to undesired operation of smart inverters [144]. It is believed that if a critical amount of smart inverters are maliciously controlled, it might be possible to cause a voltage collapse [314].

Power systems applications that have been identified as vulnerable to cyberattacks include state estimation, AGC, voltage control and energy markets [51]. Power system state estimators are vulnerable to FDIA, which is an integrity attack that modifies the values of measurements, circuit breaker statuses, and other critical data. These attacks can be perpetrated at the meter or communication system levels, and their goal is to harm the situational awareness of power system operators and to induce errors in the operation of applications that rely on state estimates. AGC can also suffer from integrity attacks that can corrupt frequency or tie-line power flow measurements. These induced errors affect the Area Control Error, which is the input to the AGC signal that controls the setpoint of generators and frequency regulation assets.

Energy markets rely on access to real time prices and operator's assessment of the correct state of the system. A cyberattack that harms the integrity of these types of information (e.g.: FDIA) or compromises their availability to some market participants (e.g.: DoS) can be used to obtain advantages in the market. Voltage control loops of distribution systems rely on remote measurements to change position of transformer taps that change the transformation ratio of distribution transformers to regulate voltage. Cyberattacks can cause inefficient operation of distribution systems when remote measurements are modified by the attacker such that on-load tap changers are set to increase system voltage. An adversary can launch a similar data integrity attack on measurement signal data in a high loaded feeder scenario. Such an attack can lower the transformation ratio and results in a voltage collapse [51]. Attacks on limited sets of voltage measurements associated with IVVC [315] or volt-watt controls [144] can induce sub-optimal voltage control, possibly leading to power quality issues including violations of voltage limits and increased losses in power distribution systems.

In [316] the authors have proposed methods for characterizing vulnerability of power grids to cyberattacks in DER in terms of voltage and power vulnerability indices. Control policies based on peak-shaving and placement of distributed ESS are evaluated. Power and voltage indices are based on power flow convergence. Power flow convergence, however, might not be a reliable proxy for stability or for quantifying vulnerability since convergence depends on the power flow algorithm [317] and implementation. A test on a hardware-in-the loop platform has shown that a simulated FDIA on a power setpoint of an ESS could cause significant frequency deviations on an islanded microgrid [143].

N. R&D RESEARCH GAPS AND FUTURE RESEARCH

Bridging the gap between the IT and OT areas remains a challenging topic for any CPS, and BESS are no exception. Because BESS security analysis and solutions are in their infancy, gaps in security risk assessment have been identified. BESS security will benefit greatly with the development of threat models and risk assessment methodologies. Threat models can be used by vendors in the design stage of product development and during consumer procurement requirements formulation. As explained previously, the consequences of cyberattacks in small and large systems are expected to have very different consequences to grid applications. Furthermore, smaller systems are less likely to experience battery safety incidents than large ones. It is necessary to know in detail all BESS components and the consequences of their malfunction or loss of operation to BESS safety and grid operations security. It is necessary to know the risks associated with battery technologies and the criticality of BESS applications to have a good understanding of attack consequences.

Another area where threat models can be important is when defining the level of security of communication systems. While it would make less sense to use encryption to secure the inter-module communications for smaller consumer-owned systems with sound physical security features built in, large modular utility-owned battery systems are certainly at higher

risk and could use secure communications protocols. For DERs communication over public communication infrastructure with utilities and system aggregators, blockchain frameworks with low power and processing requirements could be transformative for small and large BESS networked operations. Lightweight blockchain technology tailored for IoT systems could provide several layers of cybersecurity controls, including auditability of data traffic and controls, a framework for securing communications, verification of integrity of updates, among others. Application firewalls with deep packet inspection capabilities designed for DER and BESS operation could provide additional security for the ICS network enclaves where BESS live. Technologies for patching firmware of ICS with minimal or no-downtime are starting to appear but those could also be explored further by the research community.

Secure and robust control of distributed BESS can be further explored to both reduce occurrence of safety incidents on batteries and to avoid power grid disturbances caused by cyberattacks. Published research on robust control and monitoring of battery systems in the component level is still incipient. Analysis of redundant and fail-safe systems for BESS safety and security is another area of interest for research. While standard and robust filtering approaches for battery state estimation and advanced monitoring have been proposed, more research should be done to minimize the risks of battery incidents by providing fast detection of anomalous operation. Typically most publicly available BMS algorithms rely on current and voltage measurements, while temperature and gas data could also be utilized. Once detected, incidents on BESS must find appropriate response to minimize risks to the power grid and batteries. We find that error processing in SoC and SoH estimation algorithms could be used to identify FDIA and sensor failures, and provide information to define the adequate mitigation actions once battery safety issues appear.

VI. CYBERSECURITY STANDARDS AND REGULATIONS

Internationally, several laws and guidelines exists for power supply equipment and its cybersecurity. Some examples include IEC62443, IEC 62351, and ISO/IEC 27000. In the United States, grid BESS that integrate the power grid might be subject to federal and state regulations that regulate transmission, distribution or generation of electric power [318]. In 2013, the Presidential Policy Directive/PPD-21 identified the Energy sector as one of the 16 designated critical infrastructure sectors [319]. Along with Natural Gas and Oil, Electricity is one of Energy's three subsectors. Following the Cybersecurity Act of 2014 [320], the National Institute of Standards and Technology (NIST) has been tasked with identification and development of cybersecurity risk frameworks, which has resulted in the Framework for Improving Critical Infrastructure Cybersecurity [321]. This is a document that outlines practices and processes related with cybersecurity to be adopted in a voluntary way by organizations that operate critical infrastructure. The NIST Framework for Improving Critical Infrastructure Cybersecurity lists five functions: identify, protect, detect, respond and recover [321].

A. APPLICABLE REGULATIONS

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) are mandatory standards applied to the power grid in North America. Standards 2 to 11 cover cybersecurity areas, including system categorization [68], security management controls [322], training [323], security perimeters [324], physical security [325], system security management [326], incident reporting and response planning [327], recovery plans [328], configuration change management and vulnerability assessment [329], information protection [330], communications between control centers [331], and supply chain risk management [332]. NERC CIP standards apply to Bulk Electric Systems, which comprises transmission elements that are operated at 100 kV or higher, and might include in some cases generators, transformers, black start resources, dispersed generation resources, and devices dedicated to absorbing or injecting reactive power [333]. Since the NERC CIP standards do not explicitly mention energy storage, it is not clear what standards should be applied to ESS. Under the interpretation that ESS might be analogous to NERC's definition of ''generating resources'' or ''dispersed power producing resources'', it is possible CIP standards might apply to single systems larger than 20 MVA or aggregate of smaller systems that add up to more than 75 MVA. Excluding systems connected at lower voltages or from smaller sizes from compliance with CIP standards neglects the potential risk of coordinated cyberattacks on smaller DER [15].

B. STANDARDS AND GUIDES

BESS are subject to several safety standards, including overarching codes for BESS, electric safety, operation and maintenance, installation, commissioning, incident preparedness, battery fire, and ESS components [19], [91], [337].[10] While there are no cybersecurity standards directly applicable exclusively to BESS, there are several standards for DER that have cybersecurity requirements. IEEE 1547 is a standard for interconnection and interoperability of DER [13]. Not a cybersecurity standard, but contains some elements of cybersecurity. Any system that complies with IEEE 1547 must have at least one of the following protocols: IEEE 2030.5 (SEP2), IEEE 1815 (DNP3), and Sunspec Modbus. The annex D.4 of IEEE 1547-2018 presents list of cybersecurity requirements. The focus on these requirements is on local DER communication interface security and it also provides some guidelines on system architecture and interfaces.

IEEE 1547.3-2007 is the Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems [334]. Its Clause 9 provides security guidelines for distributed resources

[10]For a more comprehensive review on Smart Grid cybersecurity standards, the reader can refer to [338].

TABLE 8. Summary of cybersecurity-related standards and regulations applied to grid BESS.

Standard/Regulation	Scope	Enforcement Status	References
NERC-CIP	Systems over 20 MVA in North America	Mandatory	[68], [322]–[327], [327], [329]–[332]
IEEE 1547-2018	Interconnection between DER and grid	Optional	[13], [334]
IEEE 2030	Interoperability between EPS devices	Optional	[335], [336]

implementations. The guide discusses security issues and lists options for securing communications. There is an ongoing effort from IEEE Standards Coordinating Committee 21 to get a new version of the guide soon. The new version of 1547.3 Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems will provide more detailed requirements for cybersecurity, a broadened scope and will picture cybersecurity as an organization-wide effort.

IEEE 2030 is a guide for Smart Grid interoperability [335]. It covers energy technology and information technology of electric power systems, end-use applications and loads. This document defines the Smart grid interoperability reference model, which organizes the data exchanges between power systems, communications and information technology. The subclause 4.5 briefly discusses security and privacy and makes many mentions to ISO/IEC 27000 series NISTIR 7628, ''Guidelines for Smart Grid Cyber Security''.

IEEE 2030.2-2015 is a guide for the interoperability of grid ESS [336]. It discusses how discrete and hybrid energy storage systems can be integrated with electric power infrastructure. The Clause 8 discusses security and privacy issues related to interoperability. Even though it is more specific than 2030-2011, it is still a high level document that contains a compilation of security issues, standards, security requirements, risk management, security design, and others. It contains examples of storage applications in bulk generation, transmission, distribution and BTM along with their data flows.

VII. CONCLUSION

Along with other energy storage technologies, BESS are a fundamental component of the power grid of the future, which will be dominated by inverter-based DER. Cyberphysical security of BESS is a complex topic that involves not only information security concepts, but also needs bridging gaps between the knowing impacts of cyberattacks to ICS and their consequences to safety, security, and integrity of batteries, PCS, IT systems, and power systems.

Even though the area of cybersecurity of grid BESS is still incipient, there are papers in the literature that show vulnerabilities in commercial systems, most of which were based on lack of the adequate implementation of basic cybersecurity controls, such as authentication and encryption, among others. These security flaws stem from lack of application of well established cybersecurity best practices. Fortunately, guidelines and standards related with cybersecurity have become more common and the power industry has recognized cybersecurity as a priority.

The research interest on cybersecurity of BESS has also increased. While research on DER security in general was a more active research area, very few papers were found Since the start of the research for this review article new publications have explored the subject. There are still very few examples of cyberphysical security defenses tailored for grid BESS. There are methods developed for CPS in general and for areas where CPS security is more mature, such as EVs, that could be adapted to provide additional protection to BESS that require a very high level of reliability or that are deemed high-risk or critical for a power system. Threat models for BESS need to be further developed to support risk assessment of these assets.

Cybersecurity controls are usually costly and increase the complexity of the implementation of BESS. On the utility side, companies have improved their security posture by increasing investment in system security, employing specialized cybersecurity teams, and adopting standards and best practices. However, the weaker link on the grid cybersecurity chain might be in the smaller organizations that operate DER systems and have limited capacity to implement strong cybersecurity controls, or even in assets used for demand-side response owned by end consumers. It is possible that if those distributed assets are not well secured, systematic attacks on a large number of DER might become a realistic scenario given the vulnerabilities found in security assessments of home BESS. As a consequence, it is imperative that vendors design their products with sound cybersecurity controls that mitigate systematic, internet-borne attacks to the power grid resulting in damage to battery systems and power system instability.

While standards and regulations provide minimum security requirements for organizations operating these devices and for equipment manufacturers, risk assessment should be implemented to identify assets at risk, find vulnerabilities in deployed systems, and prioritize implementation of additional cybersecurity requirements and controls. For BESS manufacturers and large system operators, risk assessment methodologies are effective tools in performing benefit-cost analysis for each system. Such analyses must be driven by the system criticality, the consequences of system loss, the risk of personal injuries, among other relevant aspects.

ACKNOWLEDGMENT

The authors would like to thank Dr. Imre Gyuk, Director of Energy Storage Research, Office of Electricity Delivery and Energy Reliability for his funding and guidance on this research. They would also like to thank Dr. David Rosewater, Victoria O'Brien, and Dr. Reed Wittman for their valuable input.

REFERENCES

[1] A. Colthorpe. (Jun. 2020). *The Magnificent Seven: U.S. States With Energy Storage Mandates, Targets and Goals*. Accessed: Aug. 17, 2020. [Online]. Available: https://www.energy-storage.news/blogs/the-magnificent-seven-us-states-with-energy-storage-mandates-targets-and-go

[2] Sandia National Laboratories. (Aug. 2020). *DOE Global Energy Storage Database*. [Online]. Available: https://www.sandia.gov/ess-ssl/global-energy-storage-database/

[3] Wood Mackenzie Power & Renewables and U.S. Energy Storage Association. (Dec. 2020). *U.S. Energy Storage Monitor Q4 2020 Executive Summary*. [Online]. Available: https://www.woodmac.com/research/products/power-and-renewables/us-energy-storage-monitor/

[4] A. Pivec, B. M. Radimer, and E. A. Hyman, "Utility operation of battery energy storage at the best facility," *IEEE Trans. Energy Convers.*, vol. EC-1, no. 3, pp. 47–54, Sep. 1986.

[5] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, "Cyber security primer for DER vendors, aggregators, and grid operators," *Tech. Rep.*, vol. 12, 2017.

[6] Bloomberg New Energy Finance. (2019). *Electric Vehicle Outlook*. [Online]. Available: https://about.bnef.com/electric-vehicle-outlook/

[7] U. S. Energy Information Administration, *Battery Storage in the United States: An Update on Market Trends*, U.S. Department of Energy, Washington, DC, USA, 2020.

[8] *Annual Energy Outlook 2020 With Projections to 2050*, U.S. Department of Energy, Washington, DC, USA, 2020.

[9] A. A. Akhil, G. Huff, A. B. Currier, B. C. Kaun, D. M. Rastler, S. B. Chen, A. L. Cotter, D. T. Bradshaw, and W. D. Gauntlett, *DOE/EPRI 2013 Electricity Storage Handbook in Collaboration With NRECA*. Albuquerque, NM, USA: Sandia National Laboratories, 2013.

[10] R. H. Byrne, T. A. Nguyen, D. A. Copp, B. R. Chalamala, and I. Gyuk, "Energy management and optimization methods for grid energy storage systems," *IEEE Access*, vol. 6, pp. 13231–13260, 2017.

[11] I. Baumgart, M. Borsig, N. Goerke, T. Hackenjos, J. Rill, and M. Wehmer, "Who controls your energy? On the (In)Security of residential battery energy storage systems," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, doi: 10.1109/SmartGridComm.2019.8909749.

[12] Federal Energy Regulatory Commision. *FERC Order no. 2222: Fact Sheet*. [Online]. Available: https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet

[13] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*, The Institute of Electrical and Electronics Engineers, IEEE Standard 1547-2018, Feb. 2018.

[14] Y. Aillerie, S. Kayal, J. Mennella, R. Samani, S. Sauty, and L. Schmitt, "Smart grid cyber security," Intel Corporation, McAFee, and ALSTOM, Santa Clara, CA, USA, White Paper, 2013.

[15] *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid: Report to Congressional Requesters*, U.S Government Accountability Office, Report to Congressional Requesters, Washington, DC, USA, Aug. 2019.

[16] *2019 ERO Reliability Risk Priorities Report*, North American Electric Reliability Corporation, Atlanta, GA, USA, Nov. 2019.

[17] The Economist. (Aug. 2021). *A Cyber-Attack on an American Water Plant Rattles Nerves*. [Online]. Available: https://www.economist.com/united-states/2021/02/09/a-cyber-attack-on-an-american-water-plant-rattles-nerves

[18] X. Li and S. Wang, "Energy management and operational control methods for grid battery energy storage systems," *CSEE J. Power Energy Syst.*, vol. 7, no. 5, pp. 1026–1040, 2021.

[19] *Operational Risk Management in the U.S. Energy Storage Industry: Lithium-Ion Fire and Thermal Event Safety*, Energy Storage Association, Sep. 2019.

[20] Cybersecurity and Infrastructure Security Agency. (Mar. 2018). *Ransomware Impacting Pipeline Operations*. Accessed: Sep. 17, 2020. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-049a

[21] Cybersecurity and Infrastructure Security Agency and National Security Agency. (Oct. 2020). *NA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems*. Accessed: Jul. 6, 2021. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-205a

[22] Industrial Control Systems Cyber Emergency Response Team. (Feb. 2016). *Cyber-Attack Against Ukrainian Critical Infrastructure*. Accessed: Feb. 19, 2019. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[23] Cybersecurity and Infrastructure Security Agency, Washington, DC, USA. (Mar. 2018). *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*. Accessed: Dec. 20, 2021. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/TA18-074A

[24] R. J. Campbell, "Electric grid cybersecurity," Congressional Res. Service, Washington, DC, USA, Tech. Rep. R46959, Nov. 2021.

[25] A. Greenberg. (Jun. 2017). *Crash Override Malware Took Down Ukraine's Power Grid Last December*. [Online]. Available: https://www.wired.com/story/crash-override-malware/

[26] J. Meserve. (Sep. 2007). *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*. [Online]. Available: http://edition.cnn.com/2007/U.S./09/26/power.at.risk/

[27] M. Zeller, "Myth or reality—Does the aurora vulnerability pose a risk to my generator?" in *Proc. 64th Annu. Conf. Protective Relay Eng.*, Apr. 2011, pp. 130–136.

[28] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA cyber security testbed development," in *Proc. 38th North Amer. Power Symp.*, Sep. 2006, pp. 483–488.

[29] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on smart grid," in *Proc. 2nd IEEE PES Int. Conf. Exhib. Innov. Smart Grid Technol.*, Dec. 2011, pp. 1–7, doi: 10.1109/ISGTEurope.2011.6162722.

[30] G. Bade. (Jul. 2018). *Russian Hackers Infiltrated Utility Control Rooms, DHS says*. [Online]. Available: https://www.utilitydive.com/news/russian-hackers-infiltrated-utility-control-rooms-dhs-says/528487/

[31] R. Walton. (Nov. 2019). *First Cyberattack on Solar, Wind Assets Revealed Widespread Grid Weaknesses, Analysts Say*. [Online]. Available: https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/

[32] C. Bing and S. Kelly. (May 2021). *Cyber Attack Shuts Down U.S. Fuel Pipeline 'Jugular' Biden Briefed*. Accessed: May 14, 2021. [Online]. Available: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

[33] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *Proc. IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–5, doi: 10.1109/PES.2008.4596535.

[34] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, Jun. 2009.

[35] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proc. Innov. Smart Grid Technol. (ISGT)*, Jan. 2010, pp. 1–7, doi: 10.1109/ISGT.2010.5434760.

[36] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Feb. 2010.

[37] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–5, doi: 10.1109/PES.2010.5589829.

[38] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Cyber security challenges in smart grids," in *Proc. 2nd IEEE PES Int. Conf. Exhib. Innov. Smart Grid Technol.*, Dec. 2011, pp. 1–8, doi: 10.1109/ISGTEurope.2011.6162695.

[39] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[40] R. J. Campbell, "Electric grid cybersecurity," Congressional Res. Service, Washington, DC, USA, Tech. Rep. R45312, Sep. 2018.

[41] D. C. Smith, "Enhancing cybersecurity in the energy sector: A critical priority," *J. Energy Natural Resour. Law*, vol. 36, no. 4, pp. 373–380, Oct. 2018, doi: 10.1080/02646811.2018.1516362.

[42] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, 4th Quart., 2012.

[43] S. M. Amin, "Smart grid security, privacy, and resilient architectures: Opportunities and challenges," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2012, pp. 1–2, doi: 10.1109/PESGM.2012.6345767.

[44] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613000042

[45] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Proc. Comput. Sci.*, vol. 34, pp. 532–537, Aug. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050914009193
[46] I. Onyeji, M. Bazilian, and C. Bronk, "Cyber security and critical energy infrastructure," *Electr. J.*, vol. 27, no. 2, pp. 52–60, Mar. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1040619014000268
[47] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *Proc. SoutheastCon*, Apr. 2015, pp. 1–6, doi: 10.1109/SECON.2015.7132891.
[48] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815001388
[49] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.
[50] T. B. Rasmussen, G. Yang, A. H. Nielsen, and Z. Dong, "A review of cyber-physical energy system security assessment," in *Proc. IEEE Manchester PowerTech*, Jun. 2017, pp. 1–6, doi: 10.1109/PTC.2017.7980942.
[51] K. Chatterjee, V. Padmini, and S. A. Khaparde, "Review of cyber attacks on power system operations," in *Proc. IEEE Region 10 Symp. (TENSYMP)*, Jul. 2017, pp. 1–6, doi: 10.1109/TENCONSpring.2017.8070085.
[52] M. M. Pour, A. Anzalchi, and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," in *Proc. SoutheastCon*, Mar./Apr. 2017, pp. 1–4, doi: 10.1109/SECON.2017.7925278.
[53] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.
[54] 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.*, vol. 4, no. 3, pp. 240–249, Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-cps.2018.5014
[55] J. Johnson, R. D. Trevizan, J. Hoaglund, and T. Nguyen, "Cybersecurity and physical security of energy storage systems," in *U.S. DOE Energy Storage Handbook*. Albuquerque, NM, USA: Sandia National Laboratories, 2020, ch. 18.
[56] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Security challenges in next generation cyber physical systems," in *Proc. Nat. Meeting Beyond SCADA, Networked Embedded Control Cyber Phys. Syst.*, Pittsburgh, PA, USA, 2006, Paper 33.
[57] C. Neuman, "Challenges in security for cyber-physical systems," in *Proc. DHS Workshop Future Directions Cyber-Phys. Syst. Secur.*, 2009, pp. 22–24.
[58] H. Sandberg, S. Amin, and K. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Syst.*, vol. 35, no. 1, pp. 20–23, Feb. 2015.
[59] D. Ding, Q.-L. Han, Y. Xiang, C. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231217316351
[60] Y. Zacchia Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," *J. Syst. Softw.*, vol. 149, pp. 174–216, Mar. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0164121218302681
[61] S. Kumbhar, T. Faika, D. Makwana, T. Kim, and Y. Lee, "Cybersecurity for battery management systems in cyber-physical environments," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2018, pp. 934–938.
[62] T. Kim, J. Ochoa, T. Faika, H. A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1270–1281, Feb. 2022.
[63] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. Al Faruque, "A security perspective on battery systems of the Internet of Things," *J. Hardw. Syst. Secur.*, vol. 1, no. 2, pp. 188–199, Jun. 2017, doi: 10.1007/s41635-017-0007-0.
[64] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4639–4657, Aug. 2021.
[65] N. Kharlamova, S. Hashemi, and C. Traholt, "The cyber security of battery energy storage systems and adoption of data-driven methods," in *Proc. IEEE 3rd Int. Conf. Artif. Intell. Knowl. Eng. (AIKE)*, Dec. 2020, pp. 188–192.
[66] M. Culler and H. Burroughs, "Cybersecurity considerations for grid-connected batteries with hardware demonstrations," *Energies*, vol. 14, no. 11, p. 3067, May 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/11/3067
[67] D. Feldman, V. Ramasamy, R. Fu, A. Ramdas, J. Desai, and R. Margolis, "U.S. solar photovoltaic system and energy storage cost benchmark: Q1 2020," Nat. Renew. Energy Lab. (NREL), Golden, CO, USA, Tech. Rep. NREL/TP-6A20-77324, Jan. 2021.
[68] *Cyber Security—BES Cyber System Categorization*, North American Electric Reliability Corporation, Standard CIP-002-5.1a, Dec. 2016.
[69] J. Johnson, "Recommendations for distributed energy resource access control," Sandia Nat. Laboratories, Albuquerque, NM, USA, Tech. Rep. SAND2021-0977, Jan. 2021.
[70] T. Nagaura and T. Tozawa, "Lithium ion rechargeable battery," *Prog. Batteries Sol. Cells*, vol. 9, no. 217, p. 209, 1990.
[71] J. C. Hewson and S. P. Domino, "Thermal runaway of lithium-ion batteries and hazards of abnormal thermal environments," in *Proc. 9th U.S. Nat. Combustion Meeting*, May 2015, pp. 1–9.
[72] J. Lamb and J. A. Jeevarajan, "New developments in battery safety for large-scale systems," *MRS Bull.*, vol. 46, no. 5, pp. 395–401, May 2021.
[73] M. Pittman. (Mar. 2016). *Girl's Iphone Bursts Into Flames Mid-Flight: 'I Thought we Were Going Down'*. [Online]. Available: https://komonews.com/news/local/girls-iphone-bursts-into-flames-mid-flight-i-thought-we-were-going-down
[74] S. Hollister. (Oct. 2016). *Here's Why Samsung Note 7 Phones are Catching Fire*. [Online]. Available: https://www.cnet.com/news/why-is-samsung-galaxy-note-7-exploding-overheating/
[75] S. Tibken and R. Cheng. (Jan. 2017). *Samsung Answers Burning Note 7 Questions, Vows Better Batteries*. [Online]. Available: https://www.cnet.com/news/samsung-answers-burning-note-7-questions-vows-better-batteries/
[76] S. Saxena, L. Kong, and M. G. Pecht, "Exploding E-cigarettes: A battery safety issue," *IEEE Access*, vol. 6, pp. 21442–21466, 2018.
[77] T. Mohinian. (2015). *Why Hoverboards Keep Exploding*. [Online]. Available: https://www.wired.com/2015/12/why-hoverboards-keep-exploding/
[78] "Auxiliary power unit battery fire Japan airlines Boeing 787–8, JA829J, Boston, Massachusetts," Nat. Transp. Saf. Board, Washington, DC, USA, Tech. Rep. NTSB/AIR-14/01, Jan. 2013.
[79] S. Anthony. (2016). *Tesla Model S Battery Bursts Into Flames, Car Totally destroyed in 5 Minutes*. [Online]. Available: https://arstechnica.com/cars/2016/08/tesla-model-s-france-battery-fire/
[80] A. Colthorpe. (Jun. 2019). *Korea's ESS Fires: Batteries Not to Blame But Industry Takes Hit Anyway*. [Online]. Available: https://www.energy-storage.news/news/koreas-ess-fires-batteries-not-to-blame-but-industry-takes-hit-anyway
[81] E. Nakamoto-White and R. Randazzo. (Apr. 2019). *8 Firefighters Hurt in Explosion at APS Facility in Surprise; 3 Flown to Phoenix Burn Center*. [Online]. Available: https://www.azcentral.com/story/news/local/surprise-breaking/2019/04/19/firefighters-hurt-battling-transformer-fire-surprise/3527645002/
[82] Electric Power Research Institute. (Jul. 2021). *BESS Failure Event Database*. Accessed: Dec. 20, 2021. [Online]. Available: https://storagewiki.epri.com/index.php/BESS_Failure_Event_Database
[83] InfoLink. (Aug. 2021). *Fires Raise Concern Over Energy Storage Battery Safety in South Korea*. Accessed: Dec. 23, 2021. [Online]. Available: https://www.infolink-group.com/en/storage/energy-storage-market-trends/fires-raise-concern-over-energy-storage-battery-safety-in-south-korea
[84] T. Reddy, *Linden's Handbook of Batteries*, 4th ed. New York, NY, USA: McGraw-Hill, 2010.
[85] P. Alotto, M. Guarnieri, and F. Moro, "Redox flow batteries for the storage of renewable energy: A review," *Renew. Sustain. Energy Rev.*, vol. 29, pp. 325–335, Jan. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032113005418
[86] U. Koehler, "General overview of non-lithium battery systems and their safety issues," in *Electrochemical Power Sources: Fundamentals, Systems, and Applications*. Cambridge, MA, USA: Elsevier, 2019, ch. 2, pp. 21–46.

[87] M. B. Lim, T. N. Lambert, and B. R. Chalamala, "Rechargeable alkaline zinc–manganese oxide batteries for grid storage: Mechanisms, challenges and developments," *Mater. Sci. Eng., R, Rep.*, vol. 143, Jan. 2021, Art. no. 100593. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0927796X20300516
[88] M. Akter, Y. Li, J. Bao, M. Skyllas-Kazacos, and M. Rahman, "Optimal charging of vanadium redox flow battery with time-varying input power," *Batteries*, vol. 5, no. 1, p. 20, Feb. 2019. [Online]. Available: https://www.mdpi.com/2313-0105/5/1/20
[89] E. Banguero, A. Correcher, Á. Pérez-Navarro, F. Morant, and A. Aristizabal, "A review on battery charging and discharging control strategies: Application to renewable energy systems," *Energies*, vol. 11, no. 4, p. 1021, Apr. 2018. [Online]. Available: https://www.mdpi.com/1996-1073/11/4/1021
[90] Sandia National Laboratories Grid Energy Storage Department. *Battery Archive*. Accessed: Jun. 30, 2021. http://www.batteryarchive.org
[91] D. Rosewater and A. Williams, "Analyzing system safety in lithium-ion grid energy storage," *J. Power Sources*, vol. 300, pp. 460–471, Dec. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S037877531530327X
[92] E. P. Roth and C. J. Orendorff, "How electrolytes influence battery safety," *Electrochem. Soc. Interface*, vol. 21, no. 2, p. 45, 2012.
[93] C.-H. Doh, D.-H. Kim, H.-S. Kim, H.-M. Shin, Y.-D. Jeong, S.-I. Moon, B.-S. Jin, S. W. Eom, H.-S. Kim, K.-W. Kim, D.-H. Oh, and A. Veluchamy, "Thermal and electrochemical behaviour of C/Li_xCoO_2 cell during safety test," *J. Power Sources*, vol. 175, no. 2, pp. 881–885, Jan. 2008.
[94] P. Arora, R. E. White, and M. Doyle, "Capacity fade mechanisms and side reactions in lithium-ion batteries," *J. Electrochem. Soc.*, vol. 145, no. 10, p. 3647, 1998.
[95] P. Biensan, B. Simon, J. Peres, A. De Guibert, M. Broussely, J. Bodet, and F. Perton, "On safety of lithium-ion cells," *J. Power Sources*, vols. 81–82, pp. 906–912, Sep. 1999.
[96] M. Ouyang, D. Ren, L. Lu, J. Li, X. Feng, X. Han, and G. Liu, "Overcharge-induced capacity fading analysis for large format lithium-ion batteries with $LiyNi_{1/3}Co_{1/3}Mn_{1/3}O_2$+ $LiyMn_2O_4$ composite cathode," *J. Power Sources*, vol. 279, pp. 626–635, Apr. 2015.
[97] Z. Liao, S. Zhang, K. Li, G. Zhang, and T. G. Habetler, "A survey of methods for monitoring and detecting thermal runaway of lithium-ion batteries," *J. Power Sources*, vol. 436, Oct. 2019, Art. no. 226879. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378775319308729
[98] SmithBucklin Statistics Group, *National Recycling Study*, Battery Council International, Chicago, IL, USA, Nov. 2019.
[99] "The Yuasa little red book of batteries," Yuasa Battery Sales, Ebbw Vale, U.K., Tech. Rep., 2010.
[100] *VRLA Batteries: Charging Methods*, Panasonic, Osaka, Japan, Feb. 2002.
[101] K. Kordesch, J. Gsellmann, M. Peri, K. Tomantschger, and R. Chemelli, "The rechargeability of manganese dioxide in alkaline electrolyte," *Electrochim. Acta*, vol. 26, no. 10, pp. 1495–1504, Oct. 1981.
[102] V. De Angelis, G. Yadav, J. Huang, A. Couzis, and S. Banerjee, "Rechargeable Zn-MnO_2 batteries for utility load management and renewable integration," in *Proc. Int. Symp. Power Electron., Electr. Drives, Autom. Motion (SPEEDAM)*, Jun. 2018, pp. 50–54.
[103] N. Wang, H. Wan, J. Duan, X. Wang, L. Tao, J. Zhang, and H. Wang, "A review of zinc-based battery from alkaline to acid," *Mater. Today Adv.*, vol. 11, Sep. 2021, Art. no. 100149. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2590049821000199
[104] L. J. Small, C. H. Fujimoto, and T. M. Anderson, "Redox flow batteries," in *U.S. DOE Energy Storage Handbook*. Albuquerque, NM, USA: Sandia National Laboratories, 2020, ch. 6.
[105] A. Bito, "Overview of the sodium-sulfur battery for the IEEE stationary battery committee," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, vol. 2, Jun. 2005, pp. 1232–1235.
[106] NGK Insulators. *Products: NaS Solutions*. Accessed: Dec. 22, 2021. [Online]. Available: https://www.ngk-insulators.com/en/product/nas-solutions.html
[107] D. Kumar, S. K. Rajouria, S. B. Kuhar, and D. K. Kanchan, "Progress and prospects of sodium-sulfur batteries: A review," *Solid State Ionics*, vol. 312, pp. 8–16, Dec. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167273817306501
[108] E. D. Spoerke, M. M. Gross, L. J. Small, and S. J. Percival, "Sodium-based battery technologies," in *U.S. DOE Energy Storage Handbook*. Albuquerque, NM, USA: Sandia National Laboratories, 2021, ch. 4.
[109] Z. Hussien, A. Ismail, W. Lee, A. Busrah, and M. Siam, "Voltage Sag mitigation using NAS battery-based standby power supply," in *Proc. Int. Conf. Power Electron. Drives Syst.*, vol. 2, Nov./Dec. 2005, pp. 1317–1321.
[110] E. M. G. Rodrigues, C. A. S. Fernandes, R. Godina, A. W. Bizuayehu, and J. P. S. Catalao, "NaS battery storage system modeling and sizing for extending wind farms performance in Crete," in *Proc. Australas. Universities Power Eng. Conf. (AUPEC)*, Sep. 2014, pp. 1–6, doi: 10.1109/AUPEC.2014.6966547.
[111] D. M. Rosewater, D. A. Copp, T. A. Nguyen, R. H. Byrne, and S. Santoso, "Battery energy storage models for optimal control," *IEEE Access*, vol. 7, pp. 178357–178391, 2019.
[112] Y. Preger, H. M. Barkholtz, A. Fresquez, D. L. Campbell, B. W. Juba, J. Romàn-Kustas, S. R. Ferreira, and B. Chalamala, "Degradation of commercial lithium-ion cells as a function of chemistry and cycling conditions," *J. Electrochem. Soc.*, vol. 167, no. 12, Sep. 2020, Art. no. 120532, doi: 10.1149/1945-7111/abae37.
[113] L. Marques, M. Silva, and V. Vasconcelos, "CAN based network for modular battery bank with security features," in *Proc. 15th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2020, pp. 1–2.
[114] R. Xiong, J. Cao, Q. Yu, H. He, and F. Sun, "Critical review on the battery state of charge estimation methods for electric vehicles," *IEEE Access*, vol. 6, pp. 1832–1843, 2017.
[115] Z. Zou, J. Xu, C. Mi, B. Cao, and Z. Chen, "Evaluation of model based state of charge estimation methods for lithium-ion batteries," *Energies*, vol. 7, no. 8, pp. 5065–5082, Aug. 2014.
[116] A. Saxena, J. Celaya, I. RoyChoudhury, S. Saha, B. Saha, and K. Goebel, "Designing data-driven battery prognostic approaches for variable loading profiles: Some lessons learned," in *Proc. Eur. Conf. Prognostics Health Manage. Soc.*, 2012, pp. 1–11.
[117] G. L. Plett, *Battery Management Systems: Battery Modeling*, vol. 1. Norwood, MA, USA: Artech House, 2015.
[118] P. Weicker, *A Systems Approach to Lithium-Ion Battery Management*. Norwood, MA, USA: Artech House, 2013.
[119] D. Rosewater, S. Ferreira, D. Schoenwald, J. Hawkins, and S. Santoso, "Battery energy storage state-of-charge forecasting: Models, optimization, and accuracy," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2453–2462, May 2019.
[120] G. L. Plett, "Sigma-point Kalman filtering for battery management systems of LiPB-based HEV battery packs: Part 1: Introduction and state estimation," *J. Power Sources*, vol. 161, no. 2, pp. 1356–1368, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378775306011414
[121] G. L. Plett, "Sigma-point Kalman filtering for battery management systems of LiPB-based HEV battery packs: Part 2: Simultaneous state and parameter estimation," *J. Power Sources*, vol. 161, pp. 1369–1384, Oct. 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378775306011438
[122] I.-S. Kim, "The novel state of charge estimation method for lithium battery using sliding mode observer," *J. Power Sources*, vol. 163, no. 1, pp. 584–590, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378775306018349
[123] I.-S. Kim, "A technique for estimating the state of health of lithium batteries through a dual-sliding-mode observer," *IEEE Trans. Power Electron.*, vol. 25, no. 4, pp. 1013–1022, Apr. 2010.
[124] J. Rivera-Barrera, N. Muñoz-Galeano, and H. Sarmiento-Maldonado, "SoC estimation for lithium-ion batteries: Review and future challenges," *Electronics*, vol. 6, no. 4, p. 102, Nov. 2017. [Online]. Available: https://www.mdpi.com/2079-9292/6/4/102
[125] N. Wassiliadis, J. Adermann, A. Frericks, M. Pak, C. Reiter, B. Lohmann, and M. Lienkamp, "Revisiting the dual extended Kalman filter for battery state-of-charge and state-of-health estimation: A use-case life cycle analysis," *J. Energy Storage*, vol. 19, pp. 73–87, Oct. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352152X18301786
[126] M. Zeng, P. Zhang, Y. Yang, C. Xie, and Y. Shi, "SOC and SOH joint estimation of the power batteries based on fuzzy unscented Kalman filtering algorithm," *Energies*, vol. 12, no. 16, p. 3122, Aug. 2019. [Online]. Available: https://www.mdpi.com/1996-1073/12/16/3122
[127] Z. Deng, X. Hu, X. Lin, Y. Kim, and J. Li, "Sensitivity analysis and joint estimation of parameters and states for all-solid-state batteries," *IEEE Trans. Transp. Electrific.*, vol. 7, no. 3, pp. 1314–1323, Sep. 2021.

[128] M. T. Lawder, B. Suthar, P. W. C. Northrop, S. De, C. M. Hoff, O. Leitermann, M. L. Crow, S. Santhanagopalan, and V. R. Subramanian, "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.

[129] *Orion 2 BMS Operation Manual*, 1st ed. Carol Stream, IL, USA: Ewert Energy Systems, 2018.

[130] C. T. Love and K. Swider-Lyons, "Impedance diagnostic for overcharged lithium-ion batteries," *Electrochem. Solid-State Lett.*, vol. 15, no. 4, p. A53, 2012.

[131] *Nuvation BMS Software Reference Manual: Single Stack*, 2nd ed. Sunnyvale, CA, USA: Nuvation Energy, 2018.

[132] T. Vantuch, J. Fulneček, M. Holuša, S. Mišák, and J. Vaculík, "An examination of thermal features' relevance in the task of battery-fault detection," *Appl. Sci.*, vol. 8, no. 2, p. 182, 2018.

[133] A. Sidhu, A. Izadian, and S. Anwar, "Adaptive nonlinear model-based fault diagnosis of li-ion batteries," *IEEE Trans. Ind. Electron.*, vol. 62, no. 2, pp. 1002–1011, Feb. 2015.

[134] B. Xu, A. Oudalov, A. Ulbig, G. Andersson, and D. S. Kirschen, "Modeling of lithium-ion battery degradation for cell life assessment," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1131–1140, Mar. 2018.

[135] J. Meng, L. Cai, D.-I. Stroe, J. Ma, G. Luo, and R. Teodorescu, "An optimized ensemble learning framework for lithium-ion battery state of health estimation in energy storage system," *Energy*, vol. 206, Sep. 2020, Art. no. 118140.

[136] J. Obert, R. D. Trevizan, L. Torres-Castro, and Y. Preger, "Ensemble learning, prediction and li-ion cell charging cycle divergence," *IEEE Open Access J. Power Energy*, vol. 8, pp. 303–315, 2021.

[137] B. Chalamala and V. Sprenkle, "Tutorial ES04: Grid-scale energy storage materials and systems," presented at the Mater. Res. Soc. Fall Meeting, Boston, MA, USA, 2017.

[138] R. Baxter, I. Gyuk, R. H. Byrne, and B. R. Chalamala, "Engineering energy-storage projects: Applications and financial aspects [Viewpoint]," *IEEE Electrific. Mag.*, vol. 6, no. 3, pp. 4–12, Sep. 2018.

[139] *MESA-PCS Specification D2,* MESA Standards Alliance, Standard (Draft), 2014.

[140] L. Guo, J. Ye, and L. Du, "Cyber–physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyber-attacks," *IEEE Trans. Transp. Electrific.*, vol. 7, no. 2, pp. 636–648, Jun. 2021.

[141] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, p. 91, Aug. 2015. [Online]. Available: https://www.academia.edu/download/53311546/Remote_Car_Hacking.pdf

[142] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of electric vehicle battery packs to cyberattacks," 2017, *arXiv:1711.04822*.

[143] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5, doi: 10.1109/PESGM.2016.7741747.

[144] T. S. Ustun, "Cybersecurity vulnerabilities of smart inverters and their impacts on power system operation," in *Proc. Int. Conf. Power Electron., Control Autom. (ICPECA)*, Nov. 2019, pp. 1–4, doi: 10.1109/ICPECA47973.2019.8975537.

[145] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*. Bonn, Germany: Springer, 2017, pp. 185–206.

[146] Industrial Control Systems Cyber Emergency Response Team. (Oct. 2016). *Heightened DDoS Threat Posed by Mirai and Other Botnets*. Accessed: Apr. 26, 2021. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/TA16-288A

[147] J. Wen, Y. Yu, and C. Chen, "A review on lithium-ion batteries safety issues: Existing problems and possible solutions," *Mater. Exp.*, vol. 2, no. 3, pp. 197–212, Sep. 2012.

[148] N. Lotfi, P. Fajri, S. Novosad, J. Savage, R. G. Landers, and M. Ferdowsi, "Development of an experimental testbed for research in lithium-ion battery management systems," *Energies*, vol. 6, no. 10, pp. 5231–5258, 2013.

[149] Z. B. Omariba, L. Zhang, and D. Sun, "Review of battery cell balancing methodologies for optimizing battery pack performance in electric vehicles," *IEEE Access*, vol. 7, pp. 129335–129352, 2019.

[150] F. Sagstetter, M. Lukasiewycz, S. Steinhorst, M. Wolf, A. Bouard, W. R. Harris, S. Jha, T. Peyrin, A. Poschmann, and S. Chakraborty, "Security challenges in automotive hardware/software architecture design," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, 2013, pp. 458–463.

[151] M. Lelie, T. Braun, M. Knips, H. Nordmann, F. Ringbeck, H. Zappen, and D. Sauer, "Battery management system hardware concepts: An overview," *Appl. Sci.*, vol. 8, no. 4, p. 534, Mar. 2018, doi: 10.3390/app8040534.

[152] M. W. Grieves, "Digital twin: Manufacturing excellence through virtual factory replication," Michael W. Grieves, LLC, White Paper, 2014.

[153] W. Li, M. Rentemeister, J. Badeda, D. Jöst, D. Schulte, and D. U. Sauer, "Digital twin for battery systems: Cloud battery management system with online state-of-charge and state-of-health estimation," *J. Energy Storage*, vol. 30, Aug. 2020, Art. no. 101557. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352152X20308495

[154] B. Wu, W. D. Widanage, S. Yang, and X. Liu, "Battery digital twins: Perspectives on the fusion of models, data and artificial intelligence for smart battery management systems," *Energy AI*, vol. 1, Aug. 2020, Art. no. 100016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2666546820300161

[155] A. Pokhrel, V. Katta, and R. Colomo-Palacios, "Digital twin for cybersecurity incident prediction: A multivocal literature review," in *Proc. IEEE/ACM 42nd Int. Conf. Softw. Eng. Workshops*, New York, NY, USA, Jun. 2020, pp. 671–678, doi: 10.1145/3387940.3392199.

[156] S. S. Adams, R. J. Bruneau, N. Jacobs, N. Murchison, D. R. Sandoval, and B. E. Seng, "Enhancing power plant safety through coupling plant simulators to cyber digital architecture," Sandia Nat. Laboratories, Albuquerque, NM USA, Tech. Rep. SAND2018-13459, Nov. 2018.

[157] T. Kim, D. Makwana, A. Adhikaree, J. Vagdoda, and Y. Lee, "Cloud-based battery condition monitoring and fault diagnosis platform for large-scale lithium-ion battery energy storage systems," *Energies*, vol. 11, no. 1, p. 125, Jan. 2018.

[158] S. Novais, M. Nascimento, L. Grande, M. Domingues, P. Antunes, N. Alberto, C. Leitão, R. Oliveira, S. Koch, G. Kim, S. Passerini, and J. Pinto, "Internal and external temperature monitoring of a li-ion battery with fiber Bragg grating sensors," *Sensors*, vol. 16, no. 9, p. 1394, Aug. 2016.

[159] *Nuvation BMS Software Reference Manual (Multi-Stack): Nuvation BMS Grid Battery Controller*, 2nd ed. Sunnyvale, CA, USA: Nuvation Energy, 2018.

[160] Q. Wang, B. Jiang, B. Li, and Y. Yan, "A critical review of thermal management models and solutions of lithium-ion batteries for the development of pure electric vehicles," *Renew. Sustain. Energy Rev.*, vol. 64, pp. 106–128, Oct. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032116301435

[161] Y. Zheng, M. Ouyang, L. Lu, J. Li, X. Han, and L. Xu, "On-line equalization for lithium-ion battery packs based on charging cell voltages: Part 1. Equalization based on remaining charging capacity estimation," *J. Power Sources*, vol. 247, pp. 676–686, Feb. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S037877531301522X

[162] L. Zheng, J. Zhu, G. Wang, D. Dah-Chuan Lu, P. McLean, and T. He, "Model predictive control based balancing strategy for series-connected lithium-ion battery packs," in *Proc. 19th Eur. Conf. Power Electron. Appl. (EPE ECCE Europe)*, Sep. 2017, p. 8, doi: 10.23919/EPE17ECCEEurope.2017.8099189.

[163] B. Bell. (Aug. 2020). *UCI Cyber-Physical Security Researchers Highlight Vulnerability of Solar Inverters*. [Online]. Available: https://news.uci.edu/2020/08/18/uci-cyber-physical-security-researchers-highlight-vulnerability-of-solar-inverters/.

[164] C. Smith, *The Car Hacker's Handbook: A Guide for the Penetration Tester*. San Francisco, CA, USA: No Starch Press, 2016.

[165] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proc. Int. Workshop Secur. Protocols*. Cambridge, U.K.: Springer, 1999, pp. 172–182.

[166] K.-T. Cho, Y. Kim, and K. G. Shin, "Who killed my parked car?" 2018, *arXiv:1801.07741*.

[167] R. Guo, L. Lu, M. Ouyang, and X. Feng, "Mechanism of the entire overdischarge process and overdischarge-induced internal short circuit in lithium-ion batteries," *Sci. Rep.*, vol. 6, no. 1, pp. 1–9, Sep. 2016.

[168] M. Bahrman and P.-E. Bjorklund, "The new black start: System restoration with help from voltage-sourced converters," *IEEE Power Energy Mag.*, vol. 12, no. 1, pp. 44–53, Jan./Feb. 2014.

[169] M. Swierczynski, R. Teodorescu, C. N. Rasmussen, P. Rodriguez, and H. Vikelgaard, "Overview of the energy storage systems for wind power integration enhancement," in *Proc. IEEE Int. Symp. Ind. Electron.*, Jul. 2010, pp. 3749–3756.
[170] J. Marcos, O. Storkël, L. Marroyo, M. Garcia, and E. Lorenzo, "Storage requirements for PV power ramp-rate control," *Sol. Energy*, vol. 99, pp. 28–35, Jan. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0038092X13004672
[171] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[172] A. Sundararajan, A. Chavan, D. Saleem, and A. Sarwat, "A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security," *Energies*, vol. 11, no. 9, p. 2360, Sep. 2018. [Online]. Available: https://www.mdpi.com/1996-1073/11/9/2360
[173] J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, and R. Ih, "Recommendations for trust and encryption in DER interoperability standards," Sandia Nat. Laboratories, Albuquerque, NM, USA, Tech. Rep. SAND2019-1490, 2019.
[174] G. Perrone, M. Vecchio, R. Pecori, and R. Giaffreda, "The day after mirai: A survey on MQTT security solutions after the largest cyber-attack carried out through an army of IoT devices," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, 2017, pp. 246–253.
[175] A. Adhikaree, T. Kim, J. Vagdoda, A. Ochoa, P. J. Hernandez, and Y. Lee, "Cloud-based battery condition monitoring platform for large-scale lithium-ion battery energy storage systems using Internet-of-Things (IoT)," in *Proc. IEEE Energy Convers. Congr. Expo. (ECCE)*, Oct. 2017, pp. 1004–1009.
[176] C.-S. Park and H.-M. Nam, "Security architecture and protocols for secure MQTT-SN," *IEEE Access*, vol. 8, pp. 226422–226436, 2020.
[177] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," *IEEE Syst. J.*, vol. 9, no. 1, pp. 31–44, Mar. 2015.
[178] N. Kaabouch, *Handbook of Research on Software-Defined and Cognitive Radio Technologies for Dynamic Spectrum Management*. Hershey, PA, USA: IGI Global, 2014.
[179] R. Al-Dalky, O. Abduljaleel, K. Salah, H. Otrok, and M. Al-Qutayri, "A modbus traffic generator for evaluating the security of SCADA systems," in *Proc. 9th Int. Symp. Commun. Syst., Netw. Digit. Sign (CSNDSP)*, Jul. 2014, pp. 809–814.
[180] N. R. Rodofile, K. Radke, and E. Foo, "DNP3 network scanning and reconnaissance for critical infrastructure," in *Proc. Australas. Comput. Sci. Week Multiconference*, Feb. 2016, pp. 1–10, doi: 10.1145/2843043.2843350.
[181] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2012.
[182] M. Riahi Manesh and N. Kaabouch, "Security threats and countermeasures of MAC layer in cognitive radio networks," *Ad Hoc Netw.*, vol. 70, pp. 85–102, Mar. 2018.
[183] M. Bouabdellah, N. Kaabouch, F. El Bouanani, and H. Ben-Azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey," *J. Inf. Secur. Appl.*, vol. 38, pp. 40–49, Feb. 2017.
[184] W. F. Fihri, H. E. Ghazi, N. Kaabouch, and B. A. E. Majd, "Bayesian decision model with trilateration for primary user emulation attack localization in cognitive radio networks," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, May 2017, pp. 1–6, doi: 10.1109/ISNCC.2017.8071979.
[185] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls Into the Modern Power Infrastructure*. Waltham, MA, USA: Elsevier, 2013.
[186] M. Kultgen and G. Zimmer. *Maximizing Cell Monitoring Accuracy and Data Integrity in Energy Storage Battery Management Systems*. Accessed: Feb. 19, 2019. [Online]. Available: https://www.analog.com/en/technical-articles/maximizing-cell-monitoring-accuracy-and-data-integrity-in-energy-storage-battery-management-systems.html
[187] R. Buttigieg, M. Farrugia, and C. Meli, "Security issues in controller area networks in automobiles," in *Proc. 18th Int. Conf. Sci. Techn. Autom. Control Comput. Eng. (STA)*, Dec. 2017, pp. 93–98.
[188] B. Groza and P. Murvay, "Security solutions for the controller area network: Bringing authentication to in-vehicle networks," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 40–47, Mar. 2018.
[189] "MODBUS/TCP security: Protocol specification," Modbus Organization, Hopkinton, MA, USA, Tech. Rep. MB-TCP-Security-v21_2018-07-24, Jul. 2018.
[190] J.-M. Kim, S.-K. Pak, E.-C. Jung, C.-J. Kim, and J.-M. Lee, "High-voltage and high-power stabilized DC power supply using modified sine wave output 3-phase inverter," U.S. Patent 5 652 699, Jul. 29, 1997.
[191] S. Sheng, P. Li, and B. Lehman, "Parallel operation of digital controlled modified sine wave inverters," in *Proc. IEEE Energy Convers. Congr. Expo.*, Sep. 2013, pp. 3440–3447.
[192] W. Koczara and R. Seliga, "High quality sinusoidal voltage inverter for variable speed AC drive systems," in *Proc. 3rd Int. Power Electron. Motion Control Conf. (IPEMC)*, vol. 3, Aug. 2000, pp. 1181–1184.
[193] J. Doucet, D. Eggleston, and J. Shaw, "DC/AC pure sine wave inverter," PFC Worcester Polytecnic Inst., Worcester, MA, USA, Tech. Rep., 2007.
[194] P. C. Krause, O. Wasynczuk, S. D. Sudhoff, and S. Pekarek, *Analysis of Electric Machinery and Drive Systems*, vol. 2. Hoboken, NJ, USA: Wiley, 2002.
[195] P. Pourbeik, S. E. Williams, J. Weber, J. Sanchez-Gasca, J. Senthil, S. Huang, and K. Bolton, "Modeling and dynamic behavior of battery energy storage: A simple model for large-scale time-domain stability studies," *IEEE Electrific. Mag.*, vol. 3, no. 3, pp. 47–51, Sep. 2015.
[196] C. F. Lu, C. C. Liu, and C. J. Wu, "Dynamic modelling of battery energy storage system and application to power system stability," *IEE Proc.-Gener., Transmiss. Distrib.*, vol. 142, no. 4, pp. 429–435, Jul. 1995. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/ip-gtd_19951858
[197] J. A. Mueller, M. Ropp, and S. Atcitty, "Power conversion systems," in *2020 U.S. DOE Energy Storage Handbook*. Albuquerque, NM, USA: Sandia National Laboratories, 2020, ch. 13.
[198] W. W. Chen, "Bidirectional three-phase AC–DC power conversion using DC–DC converters and a three-phase unfolder," Ph.D. dissertation, Dept. Elect. Comput. Eng., Utah State Univ., Logan, UT, USA, 2017.
[199] T. A. Burress, S. L. Campbell, C. Coomer, C. W. Ayers, A. A. Wereszczak, J. P. Cunningham, L. D. Marlino, L. E. Seiber, and H.-T. Lin, "Evaluation of the 2010 Toyota Prius hybrid synergy drive system," Oak Ridge Nat. Lab. (ORNL), Oak Ridge, TN, USA, Tech. Rep. ORNL/TM-2010/253, 2011.
[200] H. Bevrani, B. François, and T. Ise, *Microgrid Dynamics and Control*. Hoboken, NJ, USA: Wiley, 2017.
[201] F. Wilches-Bernal, J. Wold, and W. H. Balliet, "A method for correcting frequency estimates for synthetic inertia control," *IEEE Access*, vol. 8, pp. 229141–229151, 2020.
[202] C. Shah, J. D. Vasquez-Plaza, D. D. Campo-Ossa, J. F. Patarroyo-Montenegro, N. Guruwacharya, N. Bhujel, R. D. Trevizan, F. A. Rengifo, M. Shirazi, R. Tonkoski, R. Wies, T. M. Hansen, and P. Cicilio, "Review of dynamic and transient modeling of power electronic converters for converter dominated power systems," *IEEE Access*, vol. 9, pp. 82094–82117, 2021.
[203] W. Kempton, V. Udo, K. Huber, K. Komara, S. Letendre, S. Baker, D. Brunner, and N. Pearre, "A test of vehicle-to-grid (V2G) for energy storage and frequency regulation in the PJM system," Univ. Delaware, Newark, Delaware, USA, Tech. Rep., 2008, vol. 32.
[204] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, Apr. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231219301924
[205] M. Cespedes and J. Sun, "Impedance shaping of three-phase grid-parallel voltage-source converters," in *Proc. 28th Annu. IEEE Appl. Power Electron. Conf. Expo. (APEC)*, Feb. 2012, pp. 754–760.
[206] C. Zhang, X. Wang, F. Blaabjerg, W. Wang, and C. Liu, "The influence of phase-locked loop on the stability of single-phase grid-connected inverter," in *Proc. IEEE Energy Convers. Congr. Expo. (ECCE)*, Sep. 2015, pp. 4737–4744.

[207] R. J. Concepcion, F. Wilches-Bernal, and R. H. Byrne, "Effects of communication latency and availability on synthetic inertia," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Apr. 2017, pp. 1–5, doi: 10.1109/ISGT.2017.8086010.

[208] F. Wilches-Bernal, R. Concepcion, J. Johnson, and R. H. Byrne, "Potential impacts of misconfiguration of inverter-based frequency control," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5, doi: 10.1109/PESGM.2018.8586272.

[209] M. Ayar, R. D. Trevizan, S. Obuz, A. S. Bretas, H. A. Latchman, and N. G. Bretas, "Cyber-physical robust control framework for enhancing transient stability of smart grids," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 8, pp. 198–206, Dec. 2017. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-cps.2017.0017

[210] J. Benet, "IPFS–content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*.

[211] S. Koch, K. Birke, and R. Kuhn, "Fast thermal runaway detection for lithium-ion cells in large scale traction batteries," *Batteries*, vol. 4, no. 2, p. 16, Mar. 2018. [Online]. Available: https://www.mdpi.com/2313-0105/4/2/16

[212] L. Kong, C. Li, J. Jiang, and M. G. Pecht, "Li-ion battery fire hazards and safety strategies," *Energies*, vol. 11, no. 9, p. 2191, 2018.

[213] Y. Fernandes, A. Bry, and S. de Persis, "Identification and quantification of gases emitted during abuse tests by overcharge of a commercial li-ion battery," *J. Power Sources*, vol. 389, pp. 106–119, Jun. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378775318302581

[214] M. Ghiji, V. Novozhilov, K. Moinuddin, P. Joseph, I. Burch, B. Suendermann, and G. Gamble, "A review of lithium-ion battery fire suppression," *Energies*, vol. 13, no. 19, p. 5117, Oct. 2020. [Online]. Available: https://www.mdpi.com/1996-1073/13/19/5117

[215] K. Wilkens, B. Johnsen, A. Bhargava, and A. Dragsted, "Project blue battery, Part II: Assessment of existing fire protection strategies and recommendation for future work," Danish Inst. Fire Secur. Technol., Hvidovre, Denmark, Tech. Rep., Dec. 2017.

[216] M. Bishop, *Computer Security: Art and Science*. Reading, MA, USA: Addison-Wesley, 2018.

[217] J.-M. Flaus, *Cybersecurity of Industrial Systems*. Hoboken, NJ, USA: Wiley, 2019.

[218] *Final Rule Order No. 706: Mandatory Reliability Standards for Critical Infrastructure Protection*, U.S. Federal Energy Regulatory Commission, document 122 FERC ¶ 61,040, Jan. 2008.

[219] National Cyber Security Centre. (Jun. 2016). *How Cyber Attacks Work*. Accessed: Feb. 21, 2022. [Online]. Available: https://www.ncsc.gov.U.K./information/how-cyber-attacks-work

[220] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Lockeed Martin Corp., Bethesda, MD, USA, White Paper, 2011.

[221] P. Torr, "Demystifying the threat modeling process," *IEEE Secur. Privacy*, vol. 3, no. 5, pp. 66–70, Sep. 2005.

[222] A. Shostack, *Threat Modeling: Designing for Security*. Hoboken, NJ, USA: Wiley, 2014.

[223] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks—An approach to the risk assessment," in *2013 5th Int. Conf. Cyber Conflict (CYCON)*, 2013, pp. 1–23.

[224] B. Yang, L. Guo, F. Li, J. Ye, and W.-Z. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3301–3310, May 2020.

[225] W. Xiong and R. Lagerström, "Hreat modeling–A systematic literature review," *Comput. Secur.*, vol. 84, pp. 53–69, Jul. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818307478

[226] L. Kohnfelder and P. Garg, "The threats to our products," *Microsoft Interface*, Apr. 1999.

[227] (2021). *Information Design Assurance Red Team*. [Online]. Available: https://idart.sandia.gov.

[228] R. Rogers, *Security Assessment: Case Studies for Implementing the NSA IAM*. Rockland, MA, USA: Syngress, 2004.

[229] R. Rogers, E. Fuller, G. Miles, and B. Cunningham, *Network Security Evaluation Using the NSA IEM*. Amsterdam, The Netherlands: Elsevier, 2005.

[230] *ICS Cybersecurity Year in Review 2020*, Dragos, 2021.

[231] 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, Dec. 2019.

[232] T. Tervoort, "Zerologon: Unauthenticated domain controller compromise by subverting netlogon cryptography," Secura, Eindhoven, The Neterlands, Tech. Rep. (CVE-2020-1472), 2020.

[233] OWASP. (2018). *Top IoT Vulnerabilities*. [Online]. Available: https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf

[234] M. Theis, R. Trzeciak, D. Costa, A. Moore, S. Miller, T. Cassidy, and W. Claycomb, "Common sense guide to mitigating insider threats," Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2018-TR-010, 2019. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644

[235] L. Goubin, P. Paillier, M. Rivain, and J. Wang, "How to reveal the secrets of an obscure white-box implementation," *J. Cryptograph. Eng.*, vol. 10, no. 1, pp. 49–66, Apr. 2020.

[236] B. Charny. (Jun. 2004). *Verizon Recalls Cell Phone Batteries*. [Online]. Available: https://www.cnet.com/news/verizon-recalls-cell-phone-batteries/

[237] U.S. Immigration and Customs Enforcement. (Apr. 2014). *Former Simi Valley CEO Convicted of Selling Navy Knock-Off Batteries Used on Subs and Aircraft Carriers*. [Online]. Available: https://www.ice.gov/news/releases/former-simi-valley-ceo-convicted-selling-navy-knock-batteries-used-subs-and-aircraft.

[238] A. Al Khas and I. Cicek, "SHA-512 based wireless authentication scheme for smart battery management systems," in *Proc. 8th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Nov. 2019, pp. 968–972.

[239] R. A. Serrano and E. Halper. (Feb. 2014). *Sophisticated But Low-Tech Power Grid Attack Baffles Authorities*. [Online]. Available: https://www.latimes.com/nation/la-na-grid-attack-20140211-story.html.

[240] D. Ishchenko and R. Nuqui, "Secure communication of intelligent electronic devices in digital substations," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo. (T&D)*, Apr. 2018, pp. 1–5.

[241] I. Onunkwo, B. Wright, P. Cordeiro, and N. Jacobs, "Cybersecurity assessments on emulated DER communication networks," Sandia Nat. Laboratories, Albuquerque, NM, USA, Tech. Rep. SAND-2019-2406, Feb. 2019.

[242] J. Baeckel, "Collection and analysis of serial based traffic in critical infrastructure control systems," SANS Inst. Inf. Secur. Reading Room, SANS Inst., Bethesda, MD, USA, White Paper, Jan. 2021, pp. 1–29. [Online]. Available: https://sansorg.egnyte.com/dl/8QqM4NNnnT

[243] B.-S. Jeon and J.-C. Na, "A study of cyber security policy in industrial control system using data diodes," in *Proc. 18th Int. Conf. Adv. Commun. Technol. (ICACT)*, Jan. 2016, pp. 314–317.

[244] J. E. Stamp, J. E. Quiroz, and A. Ellis, "Cyber security gap analysis for critical energy systems (CSGACES)," Sandia Nat. Laboratories, Albuquerque, NM, USA, Tech. Rep. SAND2017-8823, Aug. 2017.

[245] J. E. Stamp, J. Stinebaugh, and D. R. Fay, "Guide for cyber assessment of industrial control systems field devices," Sandia Nat. Lab. (SNL-NM), Albuquerque, NM, USA, Tech. Rep. SAND2017-3386, 2017.

[246] J. Johnson, "Roadmap for photovoltaic cyber security," Sandia Nat. Laboratories, Tech. Rep. SAND2017-13262, Dec. 2017.

[247] J. McCarthy, D. Faatz, N. Urlaub, and J. Wiltberger, "Securing the industrial Internet of Things: Cybersecurity for distributed energy resources (preliminary draft)," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. 1800-32B, Apr. 2021. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/energy-iiot-sp1800-32b.pdf

[248] R. Venkateswaran, "Virtual private networks," *IEEE Potentials*, vol. 20, no. 1, pp. 11–15, Feb. 2001.

[249] National Institute of Standards and Technology. (Aug. 2020). *CVE-2019-11510 Detail*. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-11510

[250] (Apr. 2021). *CVE-2021-22893 detail*. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-22893

[251] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032118307184

[252] N. Szabo, "Smart contracts: Building blocks for digital markets," *EXTROPY: J. Transhumanist Thought*, vol. 18, no. 16, no. 2, 1996.
[253] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *Proc. Resilience Week (RWS)*, Sep. 2017, pp. 18–23.
[254] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, Jan. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804518303473
[255] J. Benet, "IPFS–content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*.
[256] B. Lee and H.-J. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, Sep. 2016.
[257] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.
[258] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17318988
[259] K. Toyod, P. T. Mathiopoulo, I. Sasase, and T. Ohtsuk, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.
[260] T. Faika, T. Kim, J. Ochoa, M. Khan, S.-W. Park, and C. S. Leung, "A blockchain-based Internet of Things (IoT) network for security-enhanced wireless battery management systems," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting*, Sep. 2019, doi: 10.1109/IAS.2019.8912024.
[261] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, New York, NY, USA, Apr. 2018, doi: 10.1145/3190508.3190538.
[262] J. Jay. (Nov. 2019). *Hackers Cart Away $37.6m in Ethereum From South Korean Cryptocurrency Exchange*. Accessed: May 14, 2021. [Online]. Available: https://www.teiss.co.U.K./ethereum-theft-upbit/
[263] Cambridge Center For Alternative Finance. *Cambridge Bitcoin Electricity Consumption Index*. Accessed: May 25, 2022. [Online]. Available: https://cbeci.org/
[264] M. Nieles, K. Dempsey, and V. Pillitteri, "An introduction to information security," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-12, Jun. 2017, doi: 10.6028/NIST.SP.800-12r1.
[265] G. A. Jacoby, R. Marchany, and N. J. Davis, "Using battery constraints within mobile hosts to improve network security," *IEEE Secur. Privacy*, vol. 4, no. 5, pp. 40–49, Sep. 2006.
[266] D. C. Nash, T. L. Martin, D. S. Ha, and M. S. Hsiao, "Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices," in *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2005, pp. 141–145.
[267] B. R. Moyers, J. P. Dunning, R. C. Marchany, and J. G. Tront, "Effects of Wi-Fi and Bluetooth battery exhaustion attacks on mobile devices," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, 2010, pp. 1–9, doi: 10.1109/HICSS.2010.170.
[268] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2618–2624, Sep. 2016.
[269] A. Haider, "Value maximisation from information technology in asset management-A cultural study," in *Proc. ICOMS 2009: Asset Manage. Conf.: Sydney, 1-5 June 2009*, 2009, p. 20.
[270] S. J. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.
[271] V. N. Vapnik, *The Nature of Statistical Learning Theory*. New York, NY, USA: Springer, 2000.
[272] R. C. Newman, *Computer Security: Protecting Digital Resources*. Burlington, MA, USA: Jones & Bartlett Publishers, 2009.
[273] W. Wong and M. Stamp, "Hunting for metamorphic engines," *J. Comput. Virol.*, vol. 2, no. 3, pp. 211–229, Nov. 2006.
[274] U. Payer, M. Lamberger, and P. Teufl, "Hybrid engine for polymorphic code detection," in *Proc. Conf. Detection Intrusions Malware Vulnerability Assessment*, pp. 19–31, 2015.
[275] M. R. Chouchane and A. Lakhotia, "Using engine signature to detect metamorphic malware," in *Proc. 4th ACM Workshop Recurring Malcode (WORM)*, 2006, pp. 73–78.
[276] M. Mohri, A. Rostamizadeh, and A. Talwalkar, *Foundations of Machine Learning*. Cambridge, MA, USA: MIT Press, 2012.
[277] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2016, pp. 785–794.
[278] J. MacQueen, "Some methods for classification and analysis of multivariate observations," in *Proc. 5th Berkeley Symp. Math. Statist. Probab.*, vol. 1, no. 14. Oakland, CA, USA, 1967, pp. 281–297.
[279] L. Rokach and O. Maimon, "Clustering methods," in *Data Mining and Knowledge Discovery Handbook*. New York, NY, USA: Springer, 2005, pp. 321–352.
[280] S. Haykin and N. Network, "A comprehensive foundation," *Neural Netw.*, vol. 2, p. 41, Feb. 2004.
[281] X. Zhu and A. Goldberg, *Introduction to Semi-Supervised Learning*. San Rafael, CA, USA: Morgan & Claypool, 2009.
[282] M. Van Otterlo and M. Wiering, "Reinforcement learning and Markov decision processes," in *Reinforcement Learning*. Berlin, Germany: Springer, 2012, pp. 3–42.
[283] R. Bellman, "A Markovian decision process," *Indiana Univ. Math. J.*, vol. 6, no. 4, pp. 679–684, 1957.
[284] J. Peters and S. Schaal, "Policy gradient methods for robotics," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, Oct. 2006, pp. 2219–2225.
[285] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 1998.
[286] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2009, pp. 21–32, doi: 10.1145/1653662.1653666.
[287] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Dec. 2010, pp. 5991–5998.
[288] R. D. Trevizan, V. O'Brien, and V. Rao, "Detection of false data injection attacks in the state of charge estimation of battery energy storage systems," in *Proc. DOE OE Energy Storage Program Peer Rev. Update Meeting*, Sep. 2020, p. 1.
[289] V. Obrien, R. D. Trevizan, and V. Rao, "Detection of false data injection attacks targeting state of charge estimation of battery energy storage systems," in *Proc. Adv. Energy Conf.*, Jun. 2021, p. 1.
[290] Z. Liu and H. He, "Sensor fault detection and isolation for a lithium-ion battery pack in electric vehicles using adaptive extended Kalman filter," *Appl. Energy*, vol. 185, pp. 2033–2044, Jan. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261915014105
[291] R. Xiongl, Q. Yu, W. Shen, C. Lin, and F. Sun, "A sensor fault diagnosis method for a lithium-ion battery pack in electric vehicles," *IEEE Trans. Power Electron.*, vol. 34, no. 10, pp. 9709–9718, Oct. 2019.
[292] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 498–513, Feb. 2019.
[293] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *Proc. IEEE Amer. Control Conf. (ACC)*, Jun. 2013, pp. 3344–3349.
[294] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding sensor outputs for injection attacks detection," in *Proc. 53rd IEEE Conf. Decis. Control*, Dec. 2014, pp. 5776–5781.
[295] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1806–1813.
[296] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[297] S. Dey and M. Khanra, "Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging," *IEEE Trans. Ind. Electron.*, vol. 68, no. 1, pp. 478–487, Jan. 2021.

[298] H. Lee, G. Bere, K. Kim, J. J. Ochoa, J.-H. Park, and T. Kim, "Deep learning-based false sensor data detection for battery energy storage systems," in *Proc. IEEE CyberPELS (CyberPELS)*, Oct. 2020, pp. 1–6, doi: 10.1109/CyberPELS49534.2020.9311542.

[299] H.-J. Lee, K.-T. Kim, J.-H. Park, G. Bere, J. J. Ochoa, and T. Kim, "Convolutional neural network-based false battery data detection and classification for battery energy storage systems," *IEEE Trans. Energy Convers.*, vol. 36, no. 4, pp. 3108–3117, Dec. 2021.

[300] T. A. Nguyen, R. H. Byrne, R. D. Trevizan, A. F. Bastos, F. Wilches-Bernal, R. Concepcion, R. Tonkoski, and A. J. Headley, "Applications and grid services," in *U.S. DOE Energy Storage Handbook*. Albuquerque, NM, USA: Sandia National Laboratories, 2021, ch. 23.

[301] F. Wilches-Bernal, D. A. Copp, I. Gravagne, and D. A. Schoenwald, "Stability criteria for power systems with damping control and asymmetric feedback delays," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2018, pp. 1–6, doi: 10.1109/NAPS.2018.8600640.

[302] F. W. Bernal, J. C. Neely, R. J. Concepcion, R. H. Byrne, and A. Ellis, "Communication enabled fast-acting imbalance reserve," U.S. Patent 10 574 056, Feb. 25, 2020.

[303] V. P. Singh, N. Kishor, and P. Samuel, "Load frequency control with communication topology changes in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1943–1952, Oct. 2016.

[304] M. Ayar, S. Obuz, R. D. Trevizan, A. S. Bretas, and H. A. Latchman, "A distributed control approach for enhancing smart grid transient stability and resilience," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 3035–3044, Nov. 2017.

[305] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918.

[306] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," in *Proc. 52nd IEEE Conf. Decis. Control*, Dec. 2013, pp. 1854–1859.

[307] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017.

[308] R. Romagnoli, S. Weerakkody, and B. Sinopoli, "A model inversion based watermark for replay attack detection with output tracking," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2019, pp. 384–390.

[309] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[310] P. Fairley. (Feb. 2015.) *800,000 Microinverters Remotely Retrofitted on Oahu-in One Day*. [Online]. Available: https://spectrum.ieee.org/energywise/green-tech/solar/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu

[311] A. Konkar. (Mar. 2015). *'Something Astounding Just Happened': Enphase's Grid-Stabilizing collaboration With Hawaiian Electric*. [Online]. Available: https://enphase.com/en-us/stories/'something-astounding-just-happened'-enphase's-grid-stabilizing-collaboration-hawaiian

[312] A. R. Chavez, K. Phan, J. Hosic, R. M. Birmingham, and J. D. Patel, "Real-time software upgrade," U.S. Patent 10 037 203, Jul. 31, 2018.

[313] J. Fan and S. Borlase, "The evolution of distribution," *IEEE Power Energy Mag.*, vol. 7, no. 2, pp. 63–68, Mar. 2009.

[314] K. Misbrener. (Apr. 2019). *Cyberattacks Threaten Smart Inverters, But Scientists Have Solutions*. [Online]. Available: https://www.solarpowerworldonline.com/2019/04/cyberattacks-threaten-smart-inverters-but-scientists-have-solutions/

[315] A. Teixeira, G. Dan, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures," in *Proc. Amer. Control Conf.*, Jun. 2014, pp. 4372–4378.

[316] M. Tuttle, M. Poshtan, T. Taufik, and J. Callenes, "Impact of cyber-attacks on power grids with distributed energy storage systems," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–6, doi: 10.1109/SmartGridComm.2019.8909736.

[317] P. J. Lagace, "Power flow methods for improving convergence," in *Proc. 38th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2012, pp. 1387–1392.

[318] J. S. Dennis, S. G. Kelly, R. R. Nordhaus, and D. W. Smith, "Federal/state jurisdictional split: Implications for emerging electricity technologies," Lawrence Berkeley Nat. Lab. (LBNL), Berkeley, CA, USA, Tech. Rep. LBNL-1006675, Dec. 2016.

[319] *Presidential Policy Directive/PPD 21–Critical Infrastructure Security and Resilience*, Washington, DC, USA, White House, 2013.

[320] *Cybersecurity Enhancement Act of 2014*, Public Law, U.S. Congress, Washington, DC, USA, 2014, pp. 113–274.

[321] M. P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity V1.1*, Nat. Inst. Standards Technol., Apr. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[322] *Cyber Security—Security Management Controls*, North American Electric Reliability Corporation, Standard CIP-003-8, Apr. 2020.

[323] *Cyber Security—Personnel & Training*, North American Electric Reliability Corporation, Standard CIP-004-6, Jul. 2016.

[324] *Cyber Security—Electronic Security Perimeter(s)*, North American Electric Reliability Corporation, Standard CIP-005-6, Oct. 2020.

[325] *Cyber Security—Physical Security of BES Cyber Systems*, North American Electric Reliability Corporation, Standard CIP-006-6, Jul. 2016.

[326] *Cyber Security—Systems Security Management*, North American Electric Reliability Corporation, Standard CIP-007-6, Jul. 2016.

[327] *Cyber Security—Incident Reporting and Response Planning*, North American Electric Reliability Corporation, Standard CIP-008-6, Jan. 2021.

[328] *Cyber Security—Recovery Plans for BES Cyber Systems*, North American Electric Reliability Corporation, Standard CIP-009-6, Jan. 2021.

[329] *Cyber Security—Configuration Change Management and Vulnerability Assessments*, North American Electric Reliability Corporation, Standard CIP-010-3, Oct. 2020.

[330] *Cyber Security—Information Protection*, North American Electric Reliability Corporation, Standard CIP-011-2, Oct. 2020.

[331] *Cyber Security—Communications Between Control Centers*, North American Electric Reliability Corporation, Standard CIP-012-1, Jul. 2022.

[332] *Cyber Security—Supply Chain Risk Management*, North American Electric Reliability Corporation, Standard CIP-013-1, Oct. 2020.

[333] *Bulk Electric System Definition Reference Document*, Standard, North American Electric Reliability Corporation, Apr. 2014.

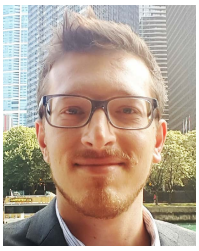
[334] *IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems*, The Institute of Electrical and Electronics Engineers, IEEE Standard 1547.3-2007, Nov. 2007.

[335] *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*, The Institute of Electrical and Electronics Engineers, IEEE Standard 2030-2011, Sep. 2011.

[336] *IEEE Guide for the Interoperability of Energy Storage Systems Integrated With the Electric Power Infrastructure*, The Institute of Electrical and Electronics Engineers, IEEE Standard 2030.2-2015, Mar. 2015.

[337] J. Lamb and M. Paiss, "Codes and standards update winter 2019/2020," Sandia Nat. Laboratories, Pacific Northwest Nat. Lab., Albuquerque, NM, USA, Tech. Rep. PNNL-SA-150383, SAND2019-3258R, Feb. 2020.

[338] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids—A comprehensive survey," *Comput. Standards Interfaces*, vol. 56, pp. 62–73, Feb. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548917301277



RODRIGO D. TREVIZAN (Member, IEEE) was born in Canoinhas, Brazil. He received the Diplôme D'Ingénieur degree in power systems engineering from the Grenoble Institute of Technology (ENSE3), in 2011, the B.S. and M.Sc. degrees in electrical engineering from the Federal University of Rio Grande do Sul, Brazil, in 2012 and 2014, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Florida, in 2018.

From 2015 to 2018, he was a Research Assistant with the University of Florida Power Laboratory. Since 2019, he has been a Researcher with the Energy Storage Technology & Systems Department, Sandia National Laboratories, Albuquerque, NM, USA. He is the author of more than 40 research articles. His research interests include security of energy storage systems, techno-economic analysis of energy storage, control of energy storage and demand response for power grid stabilization, power system state estimation, and detection of nontechnical losses in distribution systems.

JAMES OBERT (Senior Member, IEEE) received the B.S.E.E. degree from the University of Texas, the M.S.E.E. degree from New Mexico State University, the M.S.C.S. degree from California State University, and the Interdisciplinary Ph.D. degree in computer science and electrical engineering from New Mexico State University. He is currently a Computer Scientist at Sandia National Laboratories and is actively involved in machine learning and information theory research. His recent focus has been the research and development of algorithms for the detection of network and host-based cyber/cyber-physical and host-based threats. He has more than 25 years of experience in computer science and cyber security related research in his positions with industry and government research laboratories, including NASA, IBM, and HP.

VALERIO DE ANGELIS (Member, IEEE) received the Ph.D. degree from the UC Santa Barbara. He joined Sandia National Laboratories, in 2020, to work on battery modeling, system integration, advanced manufacturing, and long-duration energy storage. He is currently the Co-Founder of batteryarchive.org, the first public repository for easy visualization and comparison of lithium-ion battery degradation data across institutions. Before joining Sandia National Laboratories, he was the Executive Director of the City University of New York Energy Institute. At the Institute, he expanded the scope of the battery research from the laboratory to large-scale energy storage systems. Several initiatives have spun off from the research, notably Urban Electric Power, of which he was the Co-Founder, CEO, and VP of Product. Previously, he was the CEO and CTO of Mindflash Technologies, a leading provider of online training platforms that he founded when he was a Ph.D. student at the UC Santa Barbara. Mindflash started in 1999 as a tool to put classroom lectures, quizzes, and exams online and maintain a grade book and was used in the spring of 2000 by over half of the students at the UC Santa Barbara. Mindflash became a leading provider of online training platforms for public and private institutions and was acquired by Applied Training Systems.

TU A. NGUYEN (Senior Member, IEEE) received the B.S. degree in power systems from the Hanoi University of Science and Technology, Vietnam, in 2007, and the Ph.D. degree in electrical engineering from the Missouri University of Science and Technology, in 2014. He is currently a Senior Member of the Technical Staff at Sandia National Laboratories. Before joining Sandia National Laboratories, in September 2016, he worked as a Postdoctoral Research Associate at the University of Washington. His research interests include energy storage analytics, microgrid modeling and analysis, and the integration of distributed resources into power grids. He is also an Editor of the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY.

VITTAL S. RAO (Life Senior Member, IEEE) received the M.Tech. and Ph.D. degrees in electrical engineering from the Indian Institute of Technology Delhi. He was a Rutledge-Emerson Distinguished Professor of electrical and computer engineering and the Director of the Intelligent Systems Center, University of Missouri-Rolla (UMR). He worked as the Program Director of the National Science Foundation. He is currently a Professor of electrical and computer engineering with Texas Tech University. His research interests include cyber security of smart grid, energy storage systems, industrial control systems, and distributed energy management systems. He was a recipient of the IEEE Centennial Medal, the Faculty Excellence Awards at UMR, and the NSF Director Award for Program Management Excellence.

BABU R. CHALAMALA (Fellow, IEEE) received the B.Tech. degree in electronics and communications engineering from Sri Venkateswara University and the Ph.D. degree in physics from the University of North Texas.

He is currently the Head of the Energy Storage Technology and Systems Department and the Program Manager for grid energy storage at Sandia National Laboratories. Prior to joining Sandia, in 2015, he was a Corporate Fellow of MEMC Electronic Materials, where he led research and development, and product development in grid scale energy storage for a period of five years. Before that, he founded two startup companies commercializing large format lithium batteries and digital X-ray sources. Earlier, he was a Research Staff Member at Motorola and Texas Instruments, where he made contributions to the development of materials and device technologies for flat panel displays and microelectronics. He authored over 120 published articles and awarded nine U.S. patents.

Dr. Chalamala is a fellow of the American Association for the Advancement of Science and the National Academy of Inventors. He is also a Life Member of the Electrochemical Society and a member of the Materials Research Society. He also serves as the Chair for the Energy Storage and Stationary Battery Committee of IEEE Power and Energy Society and as a Senior Editor of IEEE ACCESS. He has served on the Editorial Board for the PROCEEDINGS OF THE IEEE, IEEE ACCESS, IEEE JOURNAL OF DISPLAY TECHNOLOGY, and *Energy Storage* journal.