[INL/RPT-24-82607]

Application of Cyber-Informed Engineering for Protecting BESS

WHITE PAPER

Emma Stewart, Ben Lampe, Ginger Wright, Megan Culler, and Remy Stolworthy

Idaho National Laboratory

January 2025

Idaho National Laboratory

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Application of Cyber-Informed Engineering for Protecting BESS

White Paper

Emma Stewart, Ginger Wright, Ben Lampe
Megan Culler, and Remy Stolworthy

January 2025

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Cybersecurity, Energy Security, and Emergency Response
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

TABLE OF CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

AC	Alternating current
ACC	Area control center
AOO	Asset owner/operator
BABA	Build America Buy America
BESS	Battery energy storage system
BIL	Bipartisan Infrastructure Law
BMS	Battery management system
CAISO	California Independent System Operator
CATL	Contemporary Amperex Technology Co. Limited
CCE	Consequence-driven Cyber-Informed Engineering
CCP	Chinese Communist Party
CESER	U.S. DOE Office of Cybersecurity, Energy Security, and Emergency Response
CIE	Cyber-Informed Engineering
CONOPS	Concept of operations
DC	Direct current
DER	Distributed energy resource
DERMS	Distributed energy resource management system
DMZ	De-militarized zone
DOE	U.S. Department of Energy
EMS	Energy management system
EV	Electric vehicle
FEOC	Foreign Entity of Concern
FY	Fiscal year
GW	Gigawatt
GWh	gigawatt-hour
HMI	Human-machine interface
HR	Human resources
IBR	Inverter-based resource
INL	Idaho National Laboratory
ISO	Independent system operator
IT	Information technology
LAN	Local area network
LOTO	Lock out tag out

ms	Millisecond
MSC	Minimum state-of-charge
MW	Megawatt
MWh	Megawatt-hour
NDA	Non-disclosure agreement
NDAA	National Defense Authorization Act
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OEM	Original equipment manufacturer
OT	Operational technology
PCS	Power conversion system
PERA	Purdue enterprise reference architecture
PSPS	Public Safety Power Shutoff
PV	Photovoltaic
RF	Radio frequency
SBOM	Software bill-of-materials
SCADA	Supervisory Control and Data Acquisition
SIS	Safety instrumented system
SoC	State-of-charge
SoH	State-of-health
WECC	Western Electricity Coordinating Council
TMS	Thermal management system
U.S.	United States
VPP	Virtual power plant

1. INTRODUCTION AND BACKGROUND

The demand for Li-ion batteries is surging, fueled predominantly by the expanding electric vehicle (EV) and stationary storage systems markets. By 2030, stationary storage alone is projected to require around 1,000 gigawatt-hours (GWh) of battery supply. As seen in Figure 1, United States (U.S.) utility-scale battery capacity totaled around 16 gigawatts (GW) at the end of 2023. In the near term, developers plan to nearly double U.S. battery capacity to more than 30 GW by the end of 2024. This additional 15 GW capacity would exceed other energy sources, such as petroleum liquids, geothermal, wood and wood waste, or landfill gas. A further 9 GW installation is planned for 2025, which could grow as new projects are announced. As of late 2023, about half of the scheduled battery capacity additions were collocated with solar energy generation.

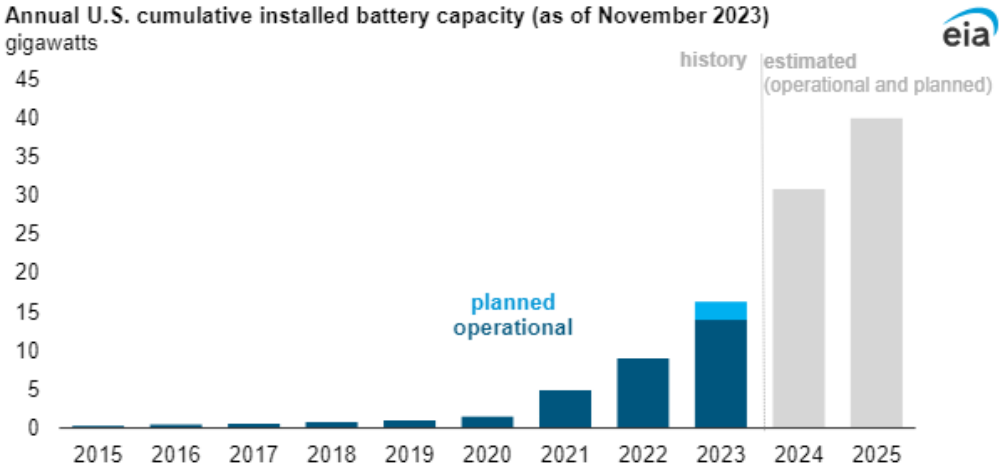

Figure 1: EIA Cumulative Battery Capacity in the U.S. as of November 2023.[1]

There are political, national and cybersecurity concerns stemming from the prevalence of foreign entity of concern (FEOC) components imported to meet the demand for battery energy storage system (BESS) technologies.[2] There is a need to secure existing installations, while a more U.S.-based supply chain for components is developed.

This report serves as an operationalization and implementation roadmap for using Cyber-Informed Engineering (CIE) to deploy domestic controls and enable safe operation while bringing the supply chain to the U.S. and within integrated system design by American vendors. By leveraging CIE principles throughout the energy transition lifecycle, this report recommends an alternative strategy, ensuring optimal resource allocation and enhancing security measures to safeguard the future of energy in the U.S. and extending outside its borders. These proactive mitigations are tested and evaluated against their cost implications, including considerations for non–domestic sourced electric infrastructure, and can be combined into a package of solutions for any BESS owner, operator, or integrator.

1.1. Background

Recent high visibility incidents, such as reporting concerning the disconnection and removal of Chinese-made batteries at Camp Lejeune, have brought these issues into sharp focus.[3] Industry and international reports have raised questions surrounding the intricate connections and delicate relationship between Contemporary Amperex Technology Co. Limited (CATL), the supplier of the BESS at Camp Lejeune and the Chinese Communist Party (CCP), underscoring concerns about China's control over approximately 80% of the global raw materials supply for rechargeable batteries.[4] The situation is exacerbated by the lack of alternative suppliers who can meet the increasing economic and time-based

targets for energy delivery, thus posing a substantial potential and perceived impediment to the nation's energy security due to inconsistent supply and unreliable sources. There are penalties and tax credit limitations now being levied on the use of FEOC batteries in vehicles,[5] and the 2024 fiscal year National Defense Authorization Act (NDAA)[6] mandates six battery companies from which items can no longer be purchased or used with Department of Defense funds by 2027.

The geopolitical landscape further complicates the battery supply chain. With reports of Russia spying on Danish wind farm operations[7] and groups linked to China conducting cyber reconnaissance on entities involved with offshore wind in India and the Straight of Taiwan,[8] the implications for international energy infrastructure and supply chain are clear.[9] In California, for example, batteries have become indispensable assets, as highlighted in a use case for analysis within this report (p.39). Despite their importance, these systems are not yet classified as critical generators, and the adoption of cybersecurity standards for inverters and batteries, such as IEEE 1547.3-2023 and UL2941, are still in their infancy. Additionally, the cybersecurity application to FEOC-sourced assets may be limited by the testing and certification of those assets being physically in FEOC locations.[10] The complexities and eventual implications of these standards are not yet fully understood because they were developed under the domestic supply chain predominance assumption.[11] Current reports from the North American Electric Reliability Corporation (NERC) suggest that existing standards and models may not adequately address real-world scenarios.[12] Therefore, there are both challenges and opportunities to enhance the typical operation of these systems, particularly when considering the ramifications of potentially untrusted devices, especially those from FEOC sources within domestic infrastructure.

With significant investments in BESS and the complexities of the supply chain, the energy sector stands at a crossroads, facing the dual imperative of integrating this accelerated transition to sustainable energy systems and ensuring this integration is secure so that critical device infrastructure and systems are robust and resilient. The energy sector is one of the few sectors by which most, if not all, other sectors rely, so its security and integration are chiefly important. BESS technology is essential to grid support functions, including providing backup power when islanding, maintaining power stability and power quality, and reducing grid congestion concerns. With this integration into the grid and other energy sources, using BESS can introduce a variety of new risks given their complex physical structures and advanced digital and remote-control features, as well as its criticality to grid sustainability.

As demonstrated in the "U.S. Department of Energy (DOE) Battery Supply Chain Security" white paper, the supply chain security required to support these large investments into BESS technology requires improved methods and implementation.[13] Battery systems fulfill various roles contingent on the unique market demands and the specific challenges presented by regional grid infrastructures. These roles also vary due to the differing utility models for ownership and operation, which are adapted to meet regional and local capabilities and requirements. Concerns have been raised regarding the potential for adversaries to exploit knowledge of battery operational patterns to orchestrate decisive attacks. However, the security of operational data for these systems may not be the primary vulnerability, as much of this information is already well-understood within the community. Applying a modest degree of subject matter expertise can often yield valuable predictions regarding how a battery will respond under certain conditions, such as grid emergencies, high or low-temperature days, Public Safety Power Shutoff (PSPS) events, and outages. The operational characteristics of batteries are well-documented, and their capabilities, including the risks associated with misoperation and the resulting consequences, are published and understood within the industry.

CIE practices represent the next step in gaining functional assurance and providing an acceptable level of risk, regardless of whether a battery vendor can support a trusted and validated supply chain. While this issue has exacerbated supply chain challenges, it is not an isolated condition. This foreign supply route is the primary source of BESS for the U.S. market. Significant efforts are underway through the Bipartisan Infrastructure Law (BIL) to change that. Still, strategic short-term operational mitigations

are needed to ensure the security of our operational technology (OT) systems, which are enhanced by instilling trust and are separate from vendors implementing CIE principles.[14]

This white paper synthesizes an array of crucial grid services provided by BESS technology, assesses its architecture and communications, and presents a case study for analysis against the principles introduced by CIE. Furthermore, in walking through the analysis, this paper presents a framework to evaluate risks and solutions when considering BESS components. Asset owners and buyers could perform this analysis to assess their BESS product implementations, alternative inverter-based resources (IBR), and energy management systems (EMS).

2. BESS GRID SERVICES

Batteries, particularly utility-scale batteries, provide a range of possible grid services to the power grid in the U.S. It is necessary to understand the services and functions these systems provide to evaluate the risk associated with their growing penetration, including the impact of the supply chain and FEOC risk. These services are vital for maintaining the grid's stability, efficiency, and reliability, which utilizes BESS to support grid services directly.

2.1. Grid Stability Services

To gain a comprehensive understanding of the integral role that BESS play in the power grid, it is essential to explore the various grid stability services they perform. Some of the key grid stability services performed by BESS include the following: frequency regulation, voltage support, and ramping or spinning reserve.

2.1.1. Frequency Regulation

BESS are commonly used to help maintain the grid's electric frequency within required periods. Frequency often increases when loads are lost and generation remains, while frequency decreases when loads are added and generation remains. BESS systems are well suited for the role of frequency regulation due to their ability to act as both an energy source and load to the grid and to quickly respond to these changes without any startup time, if configured to provide frequency support. This service is crucial because deviations in frequency can lead to instability in the system. This application requires a control algorithm and fast response time. BESS handle the frequency regulation by altering its ability to absorb and release real power, maintaining grid frequency within the required tolerances and close to its target value.

2.1.2. Voltage Support

Similar to frequency support, BESS can help maintain a constant power system voltage by injecting or absorbing reactive power. This can correct voltage droops at the end of lines or help maintain voltage stability, especially during transient events. Voltage support requires quick response times, which is a feature that batteries can provide via their control systems, power electronics in smart inverters, and by having energy capacity on demand.

2.1.3. Ramping or Spinning Reserve

This BESS application involves quickly responding to sudden changes in the grid, such as rapid changes in demand or loss of generation. This is particularly important in regions with a high proportion of renewable or variable energy sources, such as wind and solar, where output can fluctuate with changes in weather conditions. BESS used for ramping or spinning reserves typically responds in a timely manner to sudden changes in grid conditions. Additionally, as the grid undergoes a transition in energy sources, BESS providing this "spinning" reserve through synthesized inertia is an increasingly critical function as traditional modes of "spinning" reserve (inertia) are replaced.

2.2. Grid Congestion Services

Understanding the specific grid congestion functions and services provided by BESS is also essential for evaluating their impact and managing potential risks. These grid congestion services include load following, peak shaving, and congestion relief.

2.2.1. Load Following

BESS can adjust their output to match changes in electricity demand. This capability is valuable for responding to load changes more efficiently and with less stress on the grid compared to mechanical systems. Batteries performing load following adjust their output to match changes in electricity demand. This function generally operates on a scale of minutes to hours, responding to more gradual changes in load throughout the day.

2.2.2. Peak Shaving

By discharging during peak demand periods, batteries can reduce the need for higher cost, seldom-used generation capacity. This often leads to lower wholesale electricity prices, reducing peak demand charges, and providing a more balanced demand on the grid. For peak shaving, batteries discharge during periods of peak demand, which can last for several hours, usually in the late afternoon or early evening when electricity demand is highest. When peak shaving practices are instituted, electricity expenses are reduced with significant market benefits.

2.2.3. Congestion Relief

Energy congestion relief addresses challenges akin to peak shaving but with slightly different objectives. While peak shaving aims to diminish perceived demand at specific points in the system by offsetting periods of high load with local battery discharges, congestion relief involves discharging BESS to serve local loads and alleviate demand on the transmission system. This occurs during times of high load when substantial power must be transferred from generation sources to load centers, straining the transmission system's capacity. There is interdependency between this grid service and the ability to defer infrastructure investments in expanding the transmission system as congestion needs change.

2.3. Market Services

By participating in energy markets, BESS contribute to energy arbitrage, buying electricity when prices are low and selling it when prices are high, which helps in optimizing economic returns and balancing supply and demand.

2.3.1. Reducing End-Use Consumer Demand Charges

For commercial and industrial facilities, onsite energy storage used during peak demand times can lower electricity demand charges, which are based on the highest rates of consumption observed during peak periods. This application typically targets peak demand periods, which can last for a few hours each day, particularly during times when electricity prices are highest.

2.3.2. Storing and Smoothing Renewable Generation

BESS can store excess electricity generated from renewable sources, such as solar and wind, and then supply it back to the grid or to local loads as needed. This reduces curtailment (ceasing energy production from renewable sources because additional generation is unneeded) and helps manage the intermittency of variable renewable sources. The timeframe for this function depends on the variability of the renewable energy source and the BESS installation size. For solar energy, this might involve storing excess energy during midday and releasing it in the evening. For wind energy, it could involve longer or more variable periods, depending on wind patterns.

2.3.3. Deferring Infrastructure Investment

BESS can be used strategically to manage growing electricity demand in specific areas, thus deferring the need for costly new grid infrastructure such as upgraded substations or additional distribution or transmission lines. This is a longer-term application in which batteries might be used intermittently, depending on local demand growth patterns. The focus here is on reducing peak loads over time to delay the need for new infrastructure.

2.3.4. Energy Arbitrage

BESS can store energy when prices are low and release energy back into the grid when prices are high. This process, known as energy arbitrage, helps balance energy supply and demand and leads to economic benefits by capitalizing on variable energy prices. The timeframe for energy arbitrage can vary widely, from hours to a day.

2.4. Backup Power Services

In times of grid failures or planned outages, the importance of reliable backup power cannot be overstated. BESS offer a robust solution to maintain continuous power supply during such disruptions. They ensure that essential services and operations remain uninterrupted, thereby enhancing the resilience of the power infrastructure.

2.4.1. Backup Power

In cases of outages, islanding, or to support electric reliability, BESS can provide backup power to a set of local loads, such as households, businesses, and parts of the distribution grid. They are integral to these advanced microgrid setups, helping maintain power flow during temporary separations from the main grid (i.e. islanding). The duration for backup power can vary significantly based on the BESS capacity and the energy needs of the connected local load. Backup power can range from a few hours to days.

2.4.2. Black Start and Microgrid Grid Forming

BESS can play a pivotal role in black starting the system, initially powering local loads and gradually increasing output or supporting other generation sources as they come online to restore power to the entire system. This complements the use of backup power services, where during outages, prompt detection is crucial to allow local generation sources to swiftly assume the load and facilitate a seamless transition to backup power. However, this is not always feasible, as doing so may risk inadvertently creating unintentional islands, powering loads not intended to be served by backup power. It is important to note that often BESS cannot support as much inrush current as traditional synchronous generators of equivalent capacity, necessitating careful and deliberate reenergization of loads in a black start service profile.

Whether considering grid-connected microgrids like island-able distributed energy resources (DERS) or standalone microgrids that are always isolated from the grid, microgrids serve a defined set of loads, meeting their needs with local generation. In particular, the BESS capability to act as a grid-forming source can enable other resources, such as wind and solar, to come online in a grid-following mode, which is often better suited for variable resources. The primary duty of a grid-forming source is to dynamically adjust the source's output to ensure that the load and generation are always balanced. Some of these grid services have established methodologies for valuing the benefits they provide, allowing those who provide these services to be compensated for their contributions.

Figure 2 shows the battery service types, the timescale in which they must be able to respond, and the market maturity for valuing these services.[15]

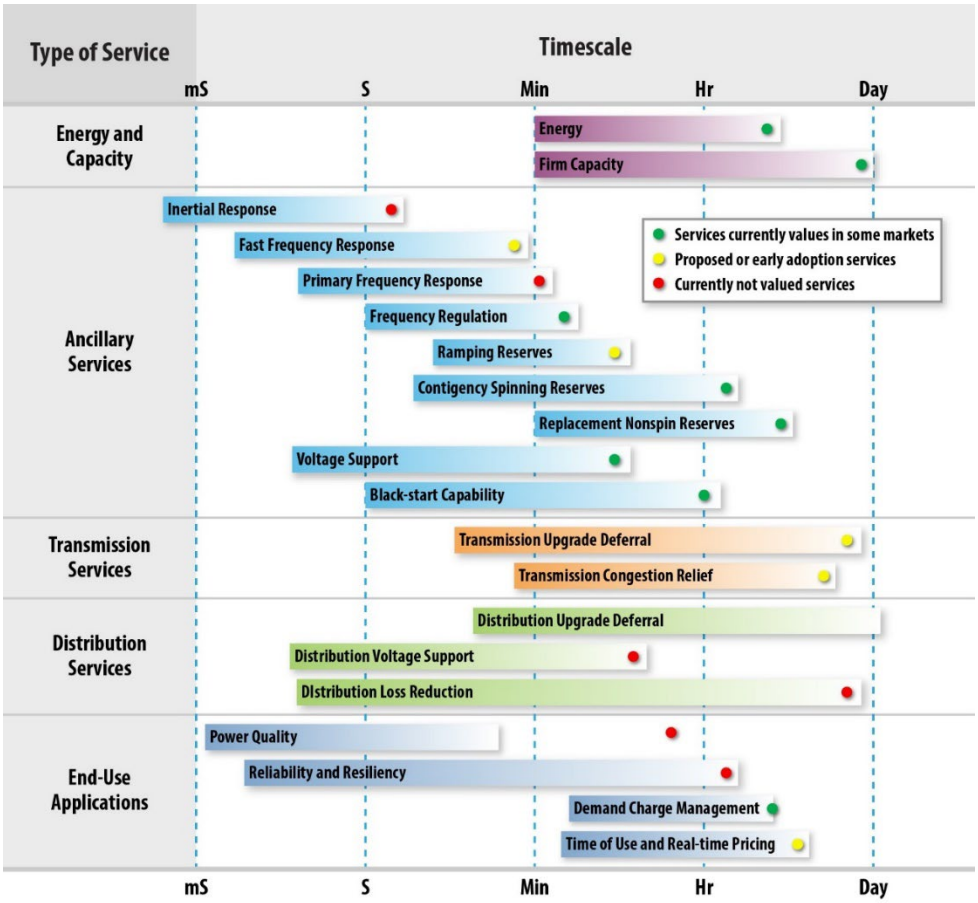

Figure 2: BESS Service Types.[15]

These services demonstrate the variety of BESS installation usage. When considering the adoption rate of BESS technologies, there is increasing importance surrounding battery storage in enhancing the grid's resilience, flexibility, and ability to integrate the diversity of energy sources for the modern grid. As battery storage deployment continues to increase, its role in the U.S. energy grid is likely to also expand and evolve, offering new service modes and solutions for energy management and grid stability. The duration and response time of BESS are greatly influenced by their energy capacity (measured in megawatt-hours, MWh) and power capacity (measured in megawatts, MW). The ratio of these two metrics, known as the battery duration, is a key determinant of how long the battery can perform a particular service. This duration presents a security challenge where the remaining duration variably affects the amount of risk at a given moment a service is required. Additionally, the specific battery technology used (e.g., lithium-ion, lead-acid, and flow batteries) and the temperature of the environment also impact the BESS performance characteristics.

Finally, it is important to note that grid services used for an individual BESS is heavily dependent on the region and the market offerings, and there is no assumption of identical services at all BESS installations. Most utility-scale BESS operators pursue a strategy of revenue stacking, looking for multiple revenue streams to justify the costs of their investment. For instance, in the United Kingdom, many BESS installations revolve around offerings for ancillary services such as frequency control. Italy has successful BESS operators that have won renewables-focused capacity auctions. Meanwhile, German operators have found opportunities to profit by avoiding costly grid upgrades. These examples show that offerings must be customized to installation requirements, the market, and local regulations, a strategy which extends to the U.S. as well.

3. INTRODUCTION TO BESS ARCHITECTURES

Different types of BESS architectures cater to various needs and services. Modular architectures allow for scalability and redundancy by using standardized modules. Most BESS implementations are configured with standardized modules. This report will focus on the most common standardized modules found in BESS installations. The predominant standardized module architecture includes five interrelated subsystems: (1) a battery pack managed by (2) a battery management system (BMS), protected by (3) a thermal management system (TMS) and connected to (4) a central power conversion system (PCS), controlled or monitored by the controls, and communicating with (5) an energy management system (EMS).

Depending on the size of the BESS installation, there may be a multitude of components for each subsystem. For example, a site may house single or multiple battery packs and a single or set of BMS units, each connecting to a single PCS or alternatively having its own PCS and a single or set of controllers while communicating to one or more EMS installations. This modularization and scalability offer increased reliability and flexibility but require more complex algorithms. The battery pack module may additionally combine different battery types to optimize performance and cost. This modular approach to BESS architecture is further challenged by changes in ownership between subsystems and/or within subsystems. The ultimate architecture choice depends on application needs, scalability requirements, ownership, and site conditions.

Figure 3 and Figure 4 show integrator examples of BESS architectures, one in its infancy and another mature integrator. The color variance represents a potentially different supplier, although sometimes there could be vertical integration.

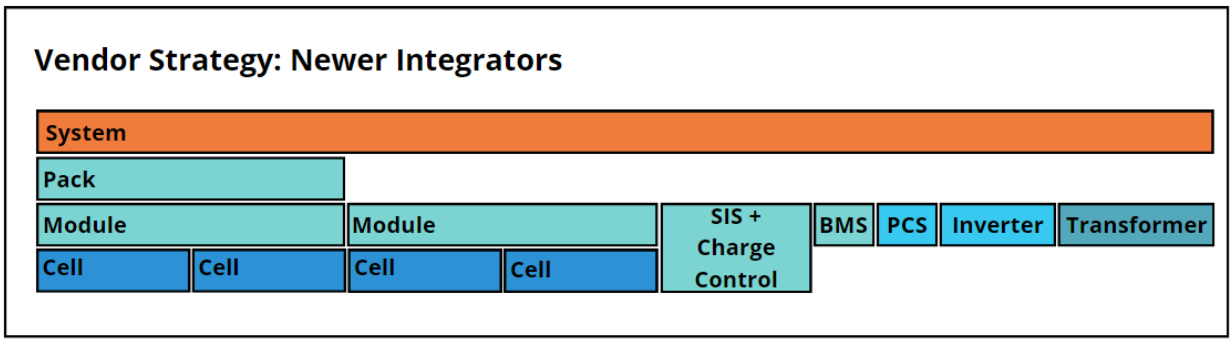

Figure 3: Integrator example of Buy Everything External approach (newer integrators).

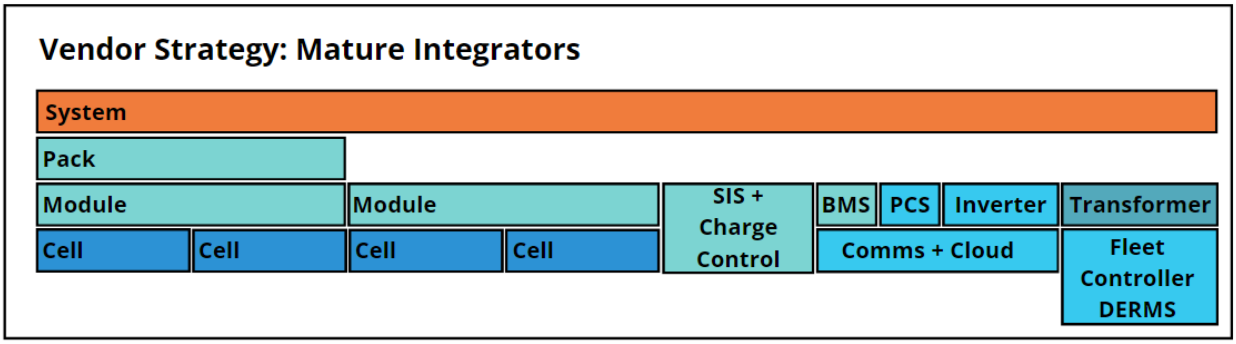

Figure 4: Integrator example of External Equipment, Homegrown Software (mature integrators) and Fleet Control approach.

3.1. Battery Pack Subsystem

The battery pack subsystem consists of individual electrochemical cells. The combination of cells constitutes a module, and a combination of modules comprises the battery pack. Often, vendors provide a battery pack with a set power and energy rating and then use that measure to scale the site's expected power and energy ratings. Traditionally, a certain number of battery packs are installed in a cabinet or set of cabinets, which is then integrated with the BMS, inverters, and PCS subsystem(s). The battery cell is the basic unit that contains the electrochemical components necessary to generate electrical energy through chemical reactions. These cells are then connected in various configurations (series, parallel, or a combination thereof) to form the module.

3.1.1. Risks

While the cells are often free from digital components, flaws in the manufacturing process could lead to degraded performance over time, which may cause the battery to fail when performing key functions. Failure of a single cell can lead to failure of the entire module through thermal propagation or how the cells are wired into a string of batteries. Furthermore, as digitization finds its way into these cells and other elements of the battery packs with microprocessors and memory-bearing elements, this presents a vulnerability and opportunity for manipulation by an adversary.

3.2. BMS Subsystem

The BMS subsystem is the "brain" of the battery modules contained within the BESS. It consists of components (i.e., interface boards, controllers, etc.) whose function is to safeguard and protect the battery cells, battery modules, and, ultimately, battery packs from damage in support of their delivering and receiving power. The BMS maintains parameters such as state-of-charge (SoC), state-of-health (SoH), voltage, temperature, and current. For instance, the BMS monitors and enforces the cells nominal voltage ratings to reduce the possibility of premature battery cell failure. As the size of the BESS system increases, the BMS subsystem is often deployed in a multi-tiered architecture at the cell level and the module, pack, and overall system levels. The algorithms utilized in the BMS are critical to control the battery cell environment, which directly relates to thermal management requirements and protections to prevent thermal runaway. This puts the BMS at higher risk due to the potential consequences if it were to be compromised.

3.2.1. Risks

The BMS is often the first subsystem to have significant digital components. Both firmware (i.e., operating system and setup of the computing system) and software (i.e., programs running on the system to perform operational tasks) may have vulnerabilities. Many of these vulnerabilities are simply flaws in the design or execution of the code, leading to unintended functionality, such as memory overflows that allow for the insertion of arbitrary code. However, particularly for FEOC devices, malicious code could be inserted that causes undocumented activity to occur, such as leaving a backdoor open or sending a beaconing signal to would-be attackers.

3.3. Thermal Management Subsystem

The TMS subsystem consists of the components required to regulate the BESS thermal requirements. There are multiple thermal aspects of the BESS, some of which are not installed on various BESS installations. These include battery cells, module, and pack temperature management, fire protection, and general installation environment temperatures. Frequently, a combination of these thermal aspects is included in a BESS so that in the event of thermal runaway, the numerous layers of protection between thermal management of battery cells, modules, and pack temperature and fire protection participate in mitigating that risk.

3.3.1. Risks

Environmental control safety systems are critical for protecting BESS assets from environmental hazards and fire-related incidents and regulating the thermal characteristics of the battery cells, modules, and packs. Exploitation of vulnerabilities in these systems could compromise overall safety, asset integrity, and operational efficiencies leading to disastrous outcomes.

3.4. Inverters

Inverters are essential for converting direct current (DC) from renewable energy sources like wind turbines and photovoltaic (PV) panels into alternating current (AC) for the power grid. It is typically only used to describe the one-way conversion of power and its injection into the grid. The primary function of an inverter is to ensure that the AC output has the desired characteristics, including voltage, frequency, and waveform. Operational technologies can be vulnerable to cyber-attacks through inverters and control devices.[16] When functioning properly, smart inverters can manage the voltage supplied to the grid, mitigating damaging fluctuations and offering some protection from attacks.

3.4.1. Risks

If adversaries gain control over these inverters, they can change key setpoints, potentially causing severe voltage imbalances. This could lead to brownouts or even blackouts. Smart inverters differ from traditional power generation systems in the bulk power grid due to their unique energy conversion mechanisms and ability to respond to commands much faster than synchronous generators.

The supply chain for inverters, particularly on smaller scales, is predominantly reliant on international and FEOC manufacturers. Dependence on a non-domestic supply chain introduces additional risks, especially if connections to foreign original equipment manufacturers (OEMs) are maintained post-installation. While often in place for legitimate business functions, such as asset health monitoring and proactive maintenance, these digital connections can offer pathways for technical influence over the aggregation and if not managed correctly, could potentially compromise the security and reliability of the entire virtual power plant (VPP) ecosystem.

One of the primary risks associated with the inverter supply chain is the possibility of embedded

vulnerabilities or malicious code within the inverters. Given the geopolitical tensions and differing regulatory standards between countries, there is an inherent risk that inverters sourced from FEOC manufacturers could be exploited as vectors for cyber-attacks. This is particularly concerning if these devices maintain persistent connections to OEMs for updates or monitoring, as these connections could be leveraged for unauthorized access or control. Additionally, if an inverter's software is not updated and secure, its data could be intercepted and manipulated. An attacker could also embed code in an inverter that could spread malware into the larger power system. [16]

Furthermore, online services such as cloud storage, real-time performance evaluation[17], remote code injection and fault diagnosis, all provide critical but potentially exploitable paths that can be targeted for code injection and execution. Smart inverters can also be at risk of cyber-attacks through third parties. In fact, 90% of the world's top energy companies suffered from third-party data breaches in 2023.[18]

While a few inverters with incorrect settings might not significantly affect the entirety of the grid, a large number of compromised inverters, all altering their voltages in unison, could have catastrophic effects and potentially lead to a complete grid failure.[17] A large number of smart inverters are installed at customer sites, which extends the attack surface and makes them more accessible, especially when interconnected with building automation and other public IT networks. DER owners may not have sufficient smart inverter cybersecurity awareness, the expertise, or human capital to combat such issues, which emphasizes the need to introduce CIE.

3.5. PCS Subsystem

The PCS system manages and integrates power conversion with the grid. It is similar to an inverter but includes a bi-directional flow of power. It is a set of components that controls charge and discharge, converting AC to DC and DC to AC, as well as covering additional control and protection functions. The PCS is a combination of devices including inverters, converters, transformers and power control. This configuration is required because although the BESS store and deliver energy via DC, the grid and load operate via AC requiring this transformation. Also, the BESS provides the ability to store and deliver energy while requiring the PCS subsystem to support this bi-directional process. Therefore, because this subsystem acts as the boundary between the BESS and the grid or local loads, the system contains various operational modes. Additionally, the complexity of its algorithms is directly related to the grid services provided by the BESS, which may require optimized power management, intelligent coordination, and load balancing. PCS monitor grid conditions, regulate voltage and frequency, and facilitate smooth transitions between power sources or operational modes. PCS may also perform safety functions such as fault detection, isolation, and protection.

3.5.1. Risks

Many of the legitimate BESS functionalities need to be supported by the PCS. Thus, the PCS is unique in that it is the subsystem in which all power flows in and out of a BESS, and any vulnerabilities in this subsystem can impact the BESS breadth of capabilities. As with battery modules, poor manufacturing could create hardware vulnerabilities that affect PCS performance. Another hardware vulnerability to consider is intentional tampering with the manufacturing or shipping process. China has been accused of tampering with computing equipment destined for the U.S. and of installing backdoors on chips used in military applications, nuclear power plants, and power distribution.[19,20]

3.6. EMS Subsystem

The EMS subsystem consists of the components involved in the supervisory control and data acquisition (SCADA) functions. This subsystem serves as the central control and monitoring hub for the BESS installation and other BESS-related energy sources managed by the EMS. This subsystem also communicates directly with the control cabinet subsystem at either the BESS controller or site controller level to determine when and how to discharge power in relation to the grid service provided, such as voltage regulation, peak shaving, etc. The EMS subsystem often has integrations such as with utility providers, other energy management systems like distributed energy resource management systems (DERMS), balancing authorities, market services, or others to best optimize or forecast BESS performance and return on investment calculations. These optimizations are related to the limitations in the underlying BESS modules such as SoC, SoH, or other parameters. Some of these optimization calculations are distributed to the controller or BMS subsystems. The determination of their location is critical in a successful analysis. Operators interact with the EMS subsystem, typically in a central utility office environment or through other authorized mechanisms such as mobile device applications. Some deployments may include using a local operation station or human machine interface (HMI), detailed in section 3.7, that interacts with the state provided by the EMS subsystem. The localized installations can provide information transparency beyond the local BESS installation due to the scope the EMS may be configured to manage.

3.6.1. Risks

The EMS collects data and may send control signals to batteries based on grid conditions. At this level of the BESS, key considerations include who has access to data and functionalities and how that access is managed. Vulnerabilities, such as weak password policies, hard-coded passwords, improper

authentication, or improper storage of critical information may create attack paths for adversaries to leverage existing functionalities for malicious purposes.

3.7. HMI, Local Controls Subsystem

The HMI acts as the interface between the operator and the BESS controller, which provides state information and control commands that are important to managing the specific BESS installation. While similar to the EMS subsystem, it differs in that its scope is strictly the BESS controller and that controller's purview. The HMI allows local manual operations, such as resets and emergency stops, ensuring compliance with safety protocols and providing direct interaction with the system components. This is especially important if access to the EMS subsystem is lost for any reason to aid with monitoring and control actions. One of the configuration variations of this HMI is implementing it as a client within the larger EMS, but this approach runs the risk of desyncing. If desynchronization happens, the connection between itself and the EMS servers is lost.

3.7.1. Risks

Unauthorized access to legitimate accounts poses a significant risk, emphasizing the importance of robust access control measures and authentication protocols. Unauthorized access to the control logic allows for any alteration in the expected behavior of the other subsystems. These alternations often lead to worst-case scenarios in the BESS system and could lead to the system experiencing extended recovery times and possible replacement due to the inability to recover the control logic without fully replacing the controllers.

3.8. Communication Subsystem

To facilitate communication between the controls subsystem and the EMS subsystem, a communication subsystem is provided, which consists of a gateway device and, optionally, network switching devices are installed (i.e., router, virtual private network (VPN) router, firewall appliance, etc.). Often, cellular, satellite, or other radio frequency (RF) modems are implemented within a controls subsystem and facilitate communication between the BESS and the EMS subsystem, sometimes via a cloud service. This is particularly true in remote or off-grid locations where traditional internet connectivity may be limited or unreliable. Additionally, due to warranty agreements, the BESS vendor utilizes internet connectivity provided or a separate connection via cellular modem to their specific energy management application, monitoring and managing their installation. This is often separate from the energy management application maintained by the asset owner or support company overseeing the BESS.

When utilities are the owners and operators of a BESS installation or partnered with another company, they can rely on dedicated communication networks already in place to manage existing energy sources and substation portfolios. However, with a growing amount of generation transitioning to DERs, grid operators are increasingly turning to cellular networks, radio and microwave communications, and the public internet to communicate with smaller assets and BESS installations. These communications can be conceptualized using the Purdue Enterprise Reference Architecture (PERA), commonly known as the Purdue Model. In this model, the upper tiers represent utility information technology (IT) network devices, while the lower layers encompass the BESS site and device OT. A demilitarized zone (DMZ) segregates IT and OT environments to restrict access to OT operations from the IT environment. A depiction of these layers with BESS components is illustrated in Figure 5.

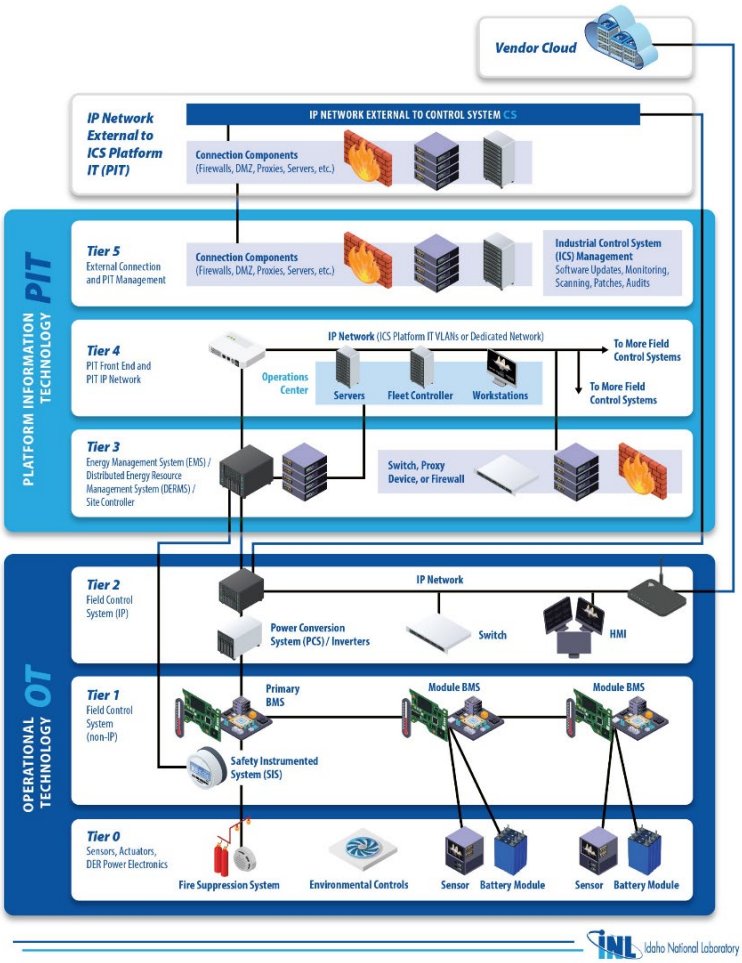

Figure 5: Purdue Model for energy storage system communication.

Typically, architectures following PERA are intended to only connect to the tiers directly above and below the current tier. As seen in Figure 6, many BESS have additional connections that do not align with PERA, most noticeably vendor clouds that are connected directly to OT networks without passing through the asset owner's enterprise network.

Ideally, there are still protections surrounding these connections, including using VPNs, strong access management policies and password requirements, and the appropriate segmentation to limit what service providers have access to if they have a legitimate business need to connect to OT devices. For example, many BESS manufacturers retain connections to the BESS for health monitoring and data collection that will help them to improve their technology. Other third-party services may include maintenance companies that retain persistent connectivity for monitoring purposes or market optimization companies that monitor the current state of assets to make recommendations on how to bid into energy or support function markets. It is worth noting that the BESS PERA figure above displays a typical arrangement of network segmentation, but individual sites may be diverse based on their size, the functions they provide, ownership and grid integration models, and more.

3.8.1. Risks

Unauthorized access to legitimate accounts poses a significant risk, emphasizing the importance of robust access control measures and authentication protocols. It is important to consider not only battery-specific hardware but also the supplementary equipment used in these systems that are not typically considered specialized OT equipment, but as traditional IT equipment. The first publicly disclosed attack

that affected U.S. renewables exploited a known vulnerability in Cisco firewalls, causing them to reboot repeatedly, which blocked the flow of data from several wind and solar sites to the aggregator, sPower.[21,22] More recently, disclosed and zero-day vulnerabilities were exploited on systems belonging to several small Danish utilities.[23]

3.9. Electrical Delivery and Protection Subsystem

This subsystem contains power protection equipment and other electrical elements throughout the BESS system. Types of equipment include circuit breakers, fuses, switches, transformers, and other power electronics that help facilitate the safe and reliable delivery of power.

3.9.1. Risks

Historically, circuit breakers, switches, and other protection devices were manual or electromechanical devices triggered by local sensor readings. Now, digital relays may be used as primary protection for grid systems. Vulnerabilities in these devices have been proven to cause device mis- and mal- operation. Special consideration should be given to digital asset use in the context of protection and other safety functions.

4. EVALUATING BESS USING CYBER-INFORMED ENGINEERING

In the critical infrastructure protection domain, the national laboratories and the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) have pioneered the CIE construct, which represents a critical enhancement to current cybersecurity practices. This construct represents a paradigm shift in how critical infrastructure systems are designed, built, commissioned, maintained, and retired to protect the country's most vital assets from sophisticated cybersecurity threats. The following outlines a CIE methodology applied while performing a risk assessment and employing a mitigation framework, which can be deployed as part of an existing BESS program or as a security assessment tool, assisting asset owners in evaluating consequences and additive mitigation strategies to protect those who may be buying FEOC components for BESS installations (as there are few other accessible vendors).

4.1. Introduction to Cyber-Informed Engineering (CIE)

CIE is a set of principles developed by DOE CESER with the Idaho National Laboratory (INL) to provide engineers and technicians with a strategic approach to defending their engineered systems against cyber-induced impacts in tandem with cybersecurity professionals and traditional cybersecurity practices. The principles are intended to be implemented throughout the system lifecycle. This enables practitioners to go beyond the traditional perspective of cybersecurity with its access control, network segmentation, etc., and embed security considerations and consequence-focused engineered controls directly into the design, operation, and maintenance of the engineered industrial control systems and OT. The goal is to define a cybersecurity protection scheme that implements engineering and traditional cybersecurity controls to ensure that cybersecurity is not just an add-on or afterthought, but an intrinsic part of the design and engineering process.

CIE focuses on identifying and protecting against unacceptable consequential events that could result from cybersecurity adversaries exploiting the digital components of OT process systems. It emphasizes a proactive and preemptive strategy whereby potential pathways for cyber-attacks are eliminated or mitigated during the system design phase. This strategy reduces or removes the likelihood of successful exploitation and mitigates the impact on critical operations. To read more about CIE and its implementation, visit https://inl.gov/cie.

4.2. CIEBAT

The Cyber-Informed Engineering Battery Analysis Tool (CIEBAT)[24] was developed in collaboration with DOE CESER. This tool is designed to enhance the security and resilience of energy infrastructure by integrating Cyber-Informed Engineering (CIE) principles and resilient design into the deployment, operation and management of battery energy storage systems (BESSs), including Hybrid integrations with solar and microgrids.

The tool is being actively deployed through the Grid Deployment Office (GDO) technical assistance (TA) programs[25], providing vital support to utility design and integration engineers, along with cybersecurity teams as they integrate these digital technologies into their energy systems. This deployment ensures that new installations are not only efficient but also secure-by-design. The tailored technical assistance for digital assurance in grid resilience aids utilities in implementing these tools effectively, optimizing their systems' performance. CIEBAT operates through the following structured three-step process designed to provide a thorough and utility-specific analysis:

4.2.1. Analysis of System Services

This initial step involves a detailed examination of the energy system's operational services. For battery systems, this might include energy storage, load balancing, and frequency regulation.

4.2.2. Consequence-Focused Analysis

In this step, the tool conducts a consequence analysis to assess the potential impacts of system failures or cyber incidents. This analysis focuses on identifying high-consequence functions within the system that could lead to significant disruptions if compromised. CIEBAT evaluates the criticality of these functions to prioritize protection efforts.

4.2.3. Cyber-Informed Engineering Mitigation Analysis

The final step involves applying CIE principles to develop and recommend mitigation strategies. This analysis incorporates cybersecurity considerations directly into the engineering process, ensuring that the designed mitigation measures are effective against cyber threats while maintaining system performance.

The output of CIEBAT is highly customized, providing results and recommendations that are specific to the utility's infrastructure and operational context. This tailored approach ensures that the utilities can implement practical and effective measures that align with their unique system configurations and service requirements.

4.3. Applied Methodology to BESS Integration

The following six steps provide a strategic methodology, referred to as the CIE Analysis, for BESS programs to analyze BESS systems for worst-case consequences and rationalize the adoption of cybersecurity and engineering controls. Throughout these steps, the CIE principles inform the decisions and rationale demonstrated.

This CIE analysis is a multi-step workflow for analyzing and enhancing the cybersecurity posture of OT installations such as BESS. This requires a systematic approach with the goal of aligning mitigations to the nuances of a specific installation, and where to direct limited organizational resources (i.e., time and budgetary limitations) for that protection scheme. The five-step methodology is detailed more below but begins with step one where the system definition is defined. Then, step two requires tracing the 'functional threads' through the system that relates to the services provided by the system under consideration. For BESS, this is selecting one or many of the grid services defined above and enumerating the enabling functions that contribute to the successful operation of the grid service(s). Step three is where the consequences are defined and prioritized. When a consequence is deemed unacceptable, it sets the foundation for the remaining methodology. In step four, these consequences are connected through

engineering-informed causal analysis and cyber-informed misuse analysis where a pathway from the functional thread to the unacceptable consequences is documented. Step five involves selecting both CIE and cybersecurity mitigations and positioning them to address the subsystems along the path as defined by the functional thread to the consequence to reduce or eliminate the impact of the consequence (CIE Principle 1 – Consequence-Focused Design). The completion of this analysis provides a collection of mitigations (CIE Principle 5 – Layered Defenses) and their location within the system definition, which defines the system's cybersecurity protection scheme.

4.3.1. Step 1: System Definition

This step provides a user with reference architectures to baseline the system definition for analysis. It is expected that alterations to this baseline will be performed to match the nuances for any specific engineering requirements that may exist. For an example use case, a general BESS reference architecture, provided in Figure 6, is assumed for a baseline analysis. The key to step one is to provide an understanding of the subsystems that are available and support the successful operation of a BESS installation. This understanding contributes to the successful execution of CIE Principle 1, Consequence-focused design, which challenges engineers to understand their critical functions and undesired consequences. To best achieve that, the designer must understand the environment (system) in which they are working. Additionally, CIE Principle 8, Digital Asset Awareness, demands that engineers understand the specifics of their system, more specifically, that they understand where digital assets are involved in the system environment and where a reference architecture provides an initial view of subsystem network interconnectivity. Even if direct network connectivity is not provided to a component, knowing that microprocessor technology is available in a component used in the BESS system is critical to addressing CIE Principle 8. There exists an opportunity when network connectivity is not provided to a component with digital assets as a required element in design to consider the CIE Principle 4, Design Simplification, and replace this component with a simpler electromechanical or alternative format that removes the risk of digitization if the subsequent steps of CIE analysis allow. Finally, the CIE Principle 7 of Interdependency Evaluation also contributes to this step where the reference architecture through the network connectivity demonstrates the possibility of interdependency within the system, which is one of the elements in this CIE principle.

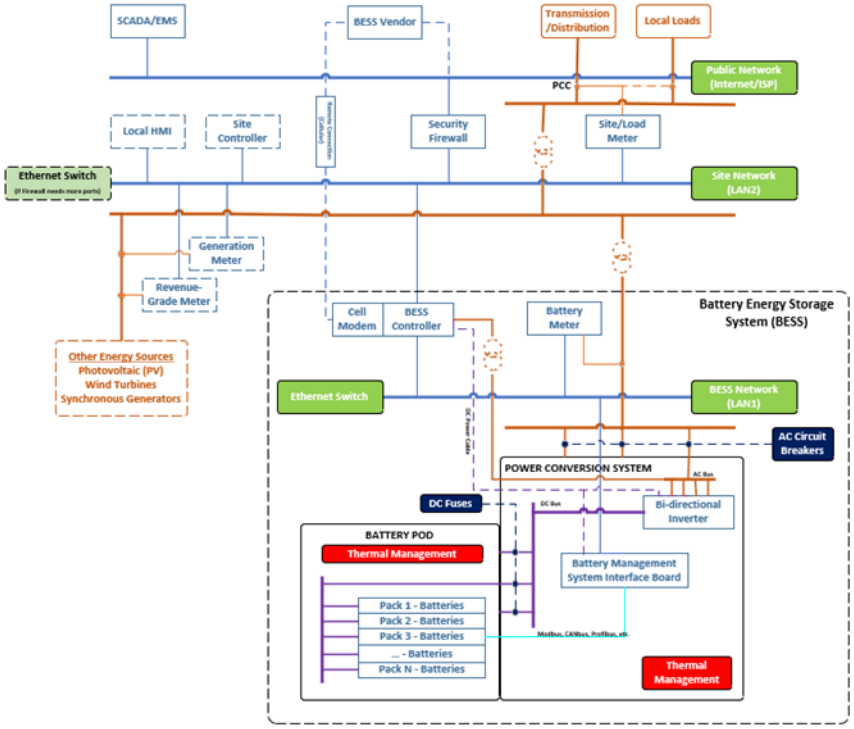

Figure 6: BESS reference architecture.

4.3.2. Step 2: Service Definition

Once the system definition is understood, in step two, the user indicates the services this system is intended to provide. The reason being that systems are often built with one or more services in mind. These services are known for their critical functionality, which must be maintained resiliently, especially if the importance of this system is elevated (see step three). Another key aspect when defining the service (critical function) is to evaluate if its position informs the user performing the analysis of the boundary location for which this service is expected and configured. For example, in the BESS system reference architecture, the voltage support service is provided at the AC bus as a boundary within the PCS subsystem and by which all available Power Conversion System inverters connect. Figure 7 shows an example of a service for the BESS reference architecture provided in the previous step. Completing the definition of the services provided by the BESS CIE analysis helps to frame and finalize CIE Principle 1, which focuses on understanding critical functions and ensuring their operationalization.

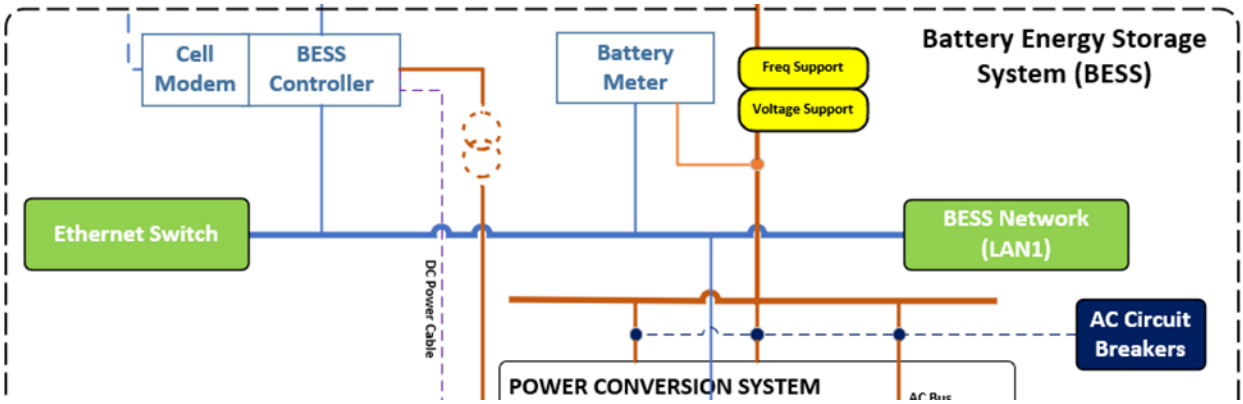

Figure 7: Service identification.

The second half of this step is for the user to describe how the enabling functions and the elements in the reference architecture perform when contributing to providing the service. See Figure 8 for an example of these functional threads for the BESS reference architecture. By defining the enabling functions and the component contributions within the BESS subsystems, the user has the narrative to understand how these services are realized. In the CIE perspective, this understanding will contribute to the success of CIE Principle 3 – Secure Information Architecture, CIE Principle 8 – Digital Asset Awareness, and CIE Principle 7 – Interdependency Evaluation.

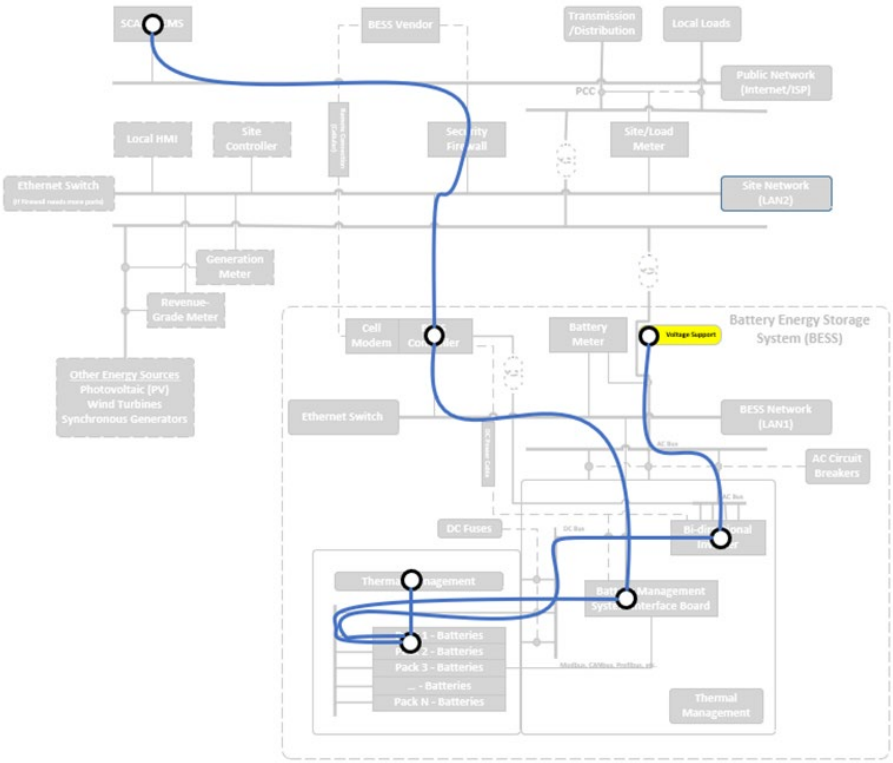

Figure 8: Functional Thread.

These functions play a crucial role in ensuring the safe and efficient operation of the battery, covering aspects such as fire detection, emergency shutdown, temperature management, current monitoring, voltage regulation, and fault detection. Table 1 provides examples of enabling functions that a given component in a subsystem would perform as it contributes to the delivery of the grid service. This list is not meant to be comprehensive but to provide examples of items engineers may find in enumerating the enabling functions available and used to deliver the grid service.

Table 1: BMS and environmental control functions and signals.

Barriers	Function
BMS monitoring (BMS subsystem)	• Current, voltage, SoC: Monitoring the level of charge in the battery storage units to optimize usage and prevent overcharging or discharging, temperature monitoring. • Over Temperature: Monitors and responds to excessive temperatures. • Over and Under Current: Monitors and manages current levels.

Barriers	Function
	• Fault Codes for Over and Under Voltage: Indicates faults related to voltage irregularities. • Cell Over Temperature and Thermal Limits: Monitors individual cell temperatures to prevent overheating. • Overcharge: Prevents excessive charging of the battery. • Voltage Imbalance: Monitors and balances voltage levels across cells.
Cooling system (TMS subsystem)	• Temperature regulation of BESS space
Thermal Insulation (TMS subsystem)	• Minimize heat transfer between battery modules or racks.
Fire and smoke detector (TMS subsystem)	• Detects smoke and produces visual and audible alerts at control center.
Active fire suppression (TMS subsystem)	• Provides fire suppression, extinguishment, and cooling.
Emergency fire response (TMS subsystem)	• Provides firefighter action plan.
Gas detection (TMS subsystem)	• Provides early detection for accumulation of flammable gases before reaching explosive.
Emergency ventilation (TMS subsystem)	• Removes gas before reaching explosive concentration.
Emergency shutdown	• Provides electrical isolation.
Circuit breaker	• Electrical isolation, Insulation Breakdown/Shunt Trip: Trips circuit breakers in case of insulation breakdown.
BESS Controller (Controls Subsystem)	• Frequency Droop Control: Adjusts the output power of the BESS in response to changes in grid frequency, helping to stabilize the grid. • Voltage Droop Control: Modulates the BESS output voltage based on variations in grid voltage, supporting grid stability. • Voltage and Frequency Reference: Sets reference values for grid voltage and frequency to maintain within predefined limits. • Virtual Generator Inertia: Simulates the inertia of traditional generators by controlling the rate of change of power output, enhancing grid stability during disturbances. • Real Power vs. Reactive Power Limiting: Manages the balance between real power (active power) and reactive power (voltage support), ensuring optimal operation of the BESS within grid constraints. • Utility Support Mode: Enables the BESS to provide ancillary services such as frequency regulation, voltage support, and black start capabilities to support grid operations.

Barriers	Function
	• Black Start: Initiates the process of restoring grid operation in the event of a blackout by using stored energy from the BESS to power critical infrastructure.
Metering (Controls Subsystem)	• Voltage: Monitors grid voltage levels to ensure stability and compatibility with the BESS operation. • Frequency: Tracks grid frequency for frequency regulation and synchronization purposes.
Human Machine Interface (HMI) (Controls Subsystem)	• Local SCADA via HMI enables local SCADA operations. • LOTO Compliance: Contributes to Lockout/Tagout (LOTO) compliance by allowing manual disable functions via SCADA. • HMI Manual Reset: Provides the capability to locally reset system components. • HMI Local Only: Restricts operations to local control only, ensuring security and operational integrity. • HMI Local Emergency Stop: Facilitates immediate shutdown of the system in emergencies. • Fire Alarm: Integrates with the fire alarm system for safety and emergency response.
Network Switches	• Communication pathways between subsystems. For instance, the BMS communicates with the BESS controller to maintain optimal environmental conditions for batteries. Meanwhile, battery modules interact with the PCS to regulate power flow based on BMS directives, ensuring battery health. • Metering devices and safety switches are linked to the BESS controller, offering real-time monitoring and control. • The EMS serves as the central control hub, coordinating operations between the BMS, PCS, HMI, and external sources to optimize energy distribution and respond to grid demands. • The Fire Suppression System communicates with the BESS Controller to detect and manage fire incidents swiftly. Service equipment enables remote diagnostics and maintenance, enhancing system reliability and minimizing downtime.

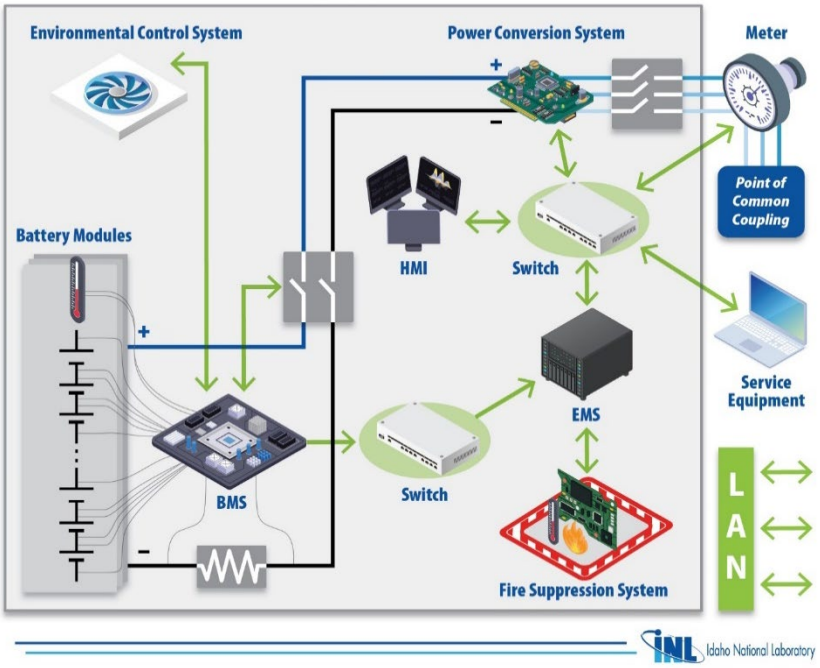

Figure 9: Example of communications between components of utility-scale BESS.

Figure 9 provides an alternate example of the interdependencies in a BESS and how the Local Area Network provides key relationships when identifying the CIE Principle 7 – Interdependency evaluation relationships between the subsystems. Completion of steps 1 and 2 provides complete awareness of both the system design and how that design facilitates the services required.

4.3.3. Step 3: Consequence Definition

Step three provides the user with the ability to describe system consequences. Such consequences are assumed to occur due to digital failure from either misconfiguration or as adversary driven sabotage. The goal is to define and evaluate the worst-case consequences of a BESS installation site during its modes of operation. This requires an awareness of the critical functions of the system (step two), the system of systems dependencies (CIE Principle 7 – Interdependency Evaluation), and the undesired consequences that must be prevented (CIE Principle 1 – Consequence-Focused Design). Safety, local grid impact, local equipment damage, bulk grid impact, bulk damage, reputation, and community impact must be considered for BESS, particularly where physical performance is concerned. Evaluating BESS risks is different than those present in regular generators and power systems.

For example, a BESS can act as both a load and a source of energy during its modes of operation. Additional dependencies exist based on the penetration of the resource, the capability in the market (i.e., what it is being used for or its service), and when it is being used (i.e., emergency, strained, or normal operations). Generally, most systems are designed with the capability to do all the normal functions. Emergency functions are often a special feature. Consider the use case of a BESS in a large independent system operator (ISO) with a high penetration of resources. The first step is to determine the criteria by which the consequence is assessed. This analysis is put into a decision matrix, which is used to rank the consequences with the following parameters:

- **System-Level and Component-Level Consequence Analysis:** Granular consequence-based analysis of the function and repercussions at the system and component levels, which is crucial for identifying specific vulnerabilities and opportunities for enhancement.

- **Grid-Scale and Utility-Scale Operational Consequence:** The report assesses the potential operational consequences of these policies at the grid and utility level, providing a broad view of the systemic impacts and consequences of the penetration and mis- or mal- operation of these components.

In this digital age, the cybersecurity risk profile is often considered. More specifically, batteries can be broken down into traditional risk components of threat, vulnerability, attack exposure, and consequence. While this reasoning is important for planning the misuse analysis and cybersecurity protections in steps four and five, the CIE principles are built on a cyber-attack being assumed, understanding the impact, and focusing CIE protections on reducing or eliminating this impact.

1. System-Level and Component-Level Consequence Analysis and Component Prioritization

The components that have a control, monitoring, or communication function are the most consequential to the BESS operation. Evaluating the criticality of these components and the consequence of their cyber or physical mis- or mal-operation is used to prioritize their evaluation as part of a supply chain analysis and solution development. This report considers the system functions, modes in which it can or should operate, and modes by which it can mis-operate. The operational functions of concern are shown in Table 2 below.

Table 2: Ability and negative impact of component mis- and mal-operation.

Component Name	Function	Negative Impact of Misoperation
PCS/Inverter	Charge and discharge management	Power system coordination (meeting the load), ability to provide emergency and backup support, power system stability, and two-way power flow
	Turning the system on and off	Power system coordination (meeting the load), ability to provide emergency and backup support, and power system stability
	Voltage support	Power system stability
	Frequency support	Power system stability
Inverter/PCS	Coordination of power and control functions for two-way power flow, communication from internal to external components	Cyber escalation can manage both the flow and the charge protections in the BMS, stability, and safety
Energy Management System (EMS)	Coordination of batteries in a site	Coordinated cyber impact (connection to other cyber components within one BESS)
Communications system	Connection of field system to operations center or other field systems	Cyber escalation (connection to other cyber components outside the single BESS)
BMS	Battery health monitoring and control	Escalating damage to components
	Fire prevention	Fires, equipment damage
	Temperature control	Runaway fires, equipment damage

Safety Instrumented System (SIS)	Life safety	Electrocution, harm to personnel

The BESS functionality's various critical aspects include communications ability (comms), charge and discharge control, and safety for equipment functions. The comms feature facilitates communication within the BESS, enabling control over the charge rate and limits as well as the ability to turn the system on or off fully or trip it completely. Additionally, the comms feature allows for incremental generation or discharge within predefined limits. Safety measures are paramount to prevent equipment damage and avert potential risks of escalating damage or harm to personnel, such as electrocution. Moreover, the cybersecurity impact potential of the BESS extends to its connection with other cybersecurity components within a single system. For example, the escalating cybersecurity impact potential involves connections to external cybersecurity components, including site, fleet, or utility networks, amplifying the scope of potential risks and implications.

Using the CIE approach, the authors determined a total score for each component regarding its impact of misoperation across cyber and physical domains. They also assigned a priority level to the consequence of the function marked in Table 2 and then used this prioritization identify the most critical components based on the types of solutions that can be applied to secure them in the short- and long-term. The results are shown in Figure 10. This represents a technical assessment of the capabilities of these devices and their potential impact on the wider network.

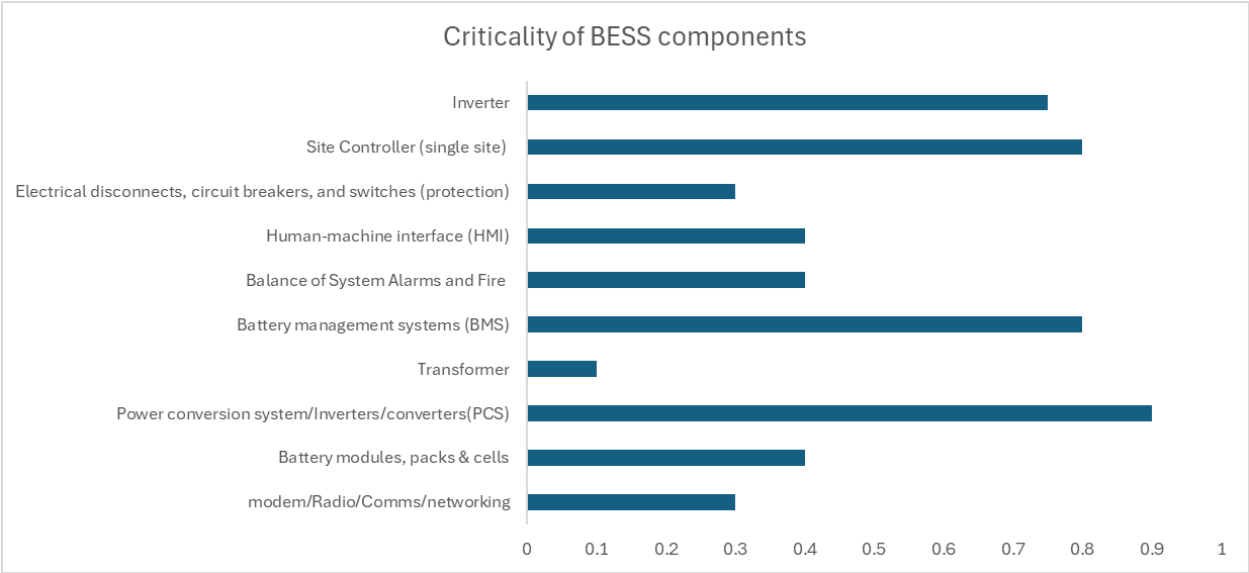

Figure 10: Criticality of BESS components.

Analysis of function, consequence, and cybersecurity capability concludes that PCS, BMS, and inverters should be prioritized at the BESS level, and site controllers should be prioritized at the fleet level (Table 2). The PCS is the critical digital technology that allows the BESS to perform both charging and discharging, enabling a two-way flow of energy. The BMS, while critical to BESS health and safety, can be isolated from a communications standpoint, but the PCS, by nature of its function to decide when to charge and discharge, must communicate with higher-level systems. The combined exposure and criticality of the device leads to its high criticality score (Table 3). The analysis presented in Table 4, is designed to be repeated for other architectures and scenarios and may change with functions presented in specific systems.

Table 3: Categorization of the components in the system and their capability.

	Comms	Charge /dis Control	On/ OFF	Gen – incremental	Equipment Safety	Life Safety	Cyber Access Potential to Impact Other Functions in BESS	Cyber Access Potential Mass Control/ Orchestration
Device (Single Site)								
Battery modules, packs, and cells			**X**			**X**		
PCS	**X**	**X**	**X**	**X**	**X**		**X**	**X**
Inverter	**X**	**X**	**X**	**X**				**X**
BMS	**X**	**X**	**X**		**X**		**X**	**X**
Environmental control system (heating, ventilation and air-conditioning system)								
Fire suppression system or fire control system		**X**	**X**			**X**		
Transformer			**X**					
HMI		**X**				**X**	**X**	
Electrical disconnects, circuit breakers, and switches (protection)		**X**	**X**		**X**	**X**	**X**	
Communications networking switches and cables	**X**						**X**	
Modem	**X**						**X**	**X**
Site BESS Controller (single site)/EMS			**X**	**X**	**X**			
Mass Control Items								
DERMS/Mass Control (utility)		**X**	**X**	**X**				**X**
Fleet Control (manufacturer/integrator/aggregator)			**X**	**X**			**X**	**X**
Cloud	**X**	**X**					**X**	**X**

2. Grid-Scale and Utility-Scale Operational Consequence

Multiple organizations commonly maintain communications with the BESS site26 creating attack exposure where these organizations could be used as a point of entry to connect to the BESS or could be secondary targets as adversaries use BESS communications infrastructure to pivot into new networks. Additionally, utilities have been the primary owners of BESS installations. However, there is a noticeable shift towards third-party ownership, primarily driven by financiers seeking investment opportunities in energy infrastructure.

Another factor is the rapid interconnectivity and cost reduction, which remain dominant goals in BESS deployment. While these objectives are crucial for scalability and economic viability, there is a risk of overlooking cybersecurity concerns in favor of achieving efficiency targets. Some entities are employing inventive interconnecting methods to avoid cumbersome generator registration processes. Notably, in Tesla's EV model, service control is retained by the OEM.27 This emphasizes the significance of OEMs in dictating service provisions and potentially exerting control over essential functionalities in BESS modes of operation such as Volt/VAR management service.

All these factors, as a use case, when combined with instances of BESS used in a large ISO with high penetration of resources, solidify the consequence analysis. The first step is to determine the criteria (i.e., factors) by which the consequence is assessed. This is put into the decision matrix shown in Table 4, which is used to rank the consequences. Note that reputational damage and environmental damage are not a part of the original Consequence Driven Cyber Informed Engineering (CCE) table and have been added for the CIE BESS analysis. Each consequence is weighted, the impact is ranked, and then the consequence is scored using the CCE methodology.[28] The onus is on the user to define the criteria that underpin their analysis, but using the matrix structure allows for calculating a rating for grid services selected. Additional factors are considered to account for environmental and reputational damage, which in BESS can be significant factors.

Table 4: Consequence analysis criteria. (based on CCE)

Criteria	None	Low	Medium	High
Area/Load Impact	Inconsequential	Loss of failure to service firm load of less than 300 MW (or) load supply loss of minimum state of charge (MSC) or 2,000 MW, whichever is lower.	Loss of failure to service firm load between 301 and 1,500 MW (or) load supply loss of between 2,000 MW (or MSC, whichever is lower) and 3,000 MW.	Loss of failure to service firm load greater than 1,500 MW or load supply loss of greater than 3,000 MW.
Duration	Inconsequential	Return of all service in less than one day (inability to serve firm load) or supply outage for less than one week.	Return of all service 1–5 days (inability to serve firm load) or supply outage for one week to one month.	Return of all service > five days (inability to serve firm load) or supply outage >one month.
Safety	Inconsequential	Risk onsite.	Definite safety risk offsite.	Loss of life potential.
Asset Owner/System Integrity	Inconsequential	Can restore with confidence in integrity.	Owner has knowledge but no resources (money,	Asset owner can restore but has no

			time, personnel) to restore.	confidence in integrity.
Cost	Inconsequential	Significant but recoverable.	Multiple years to financially recover.	Trigger of liquidity crisis or potential bankruptcy.
Reputational damage	Inconsequential	—	—	Customer loss of faith in utility.
Environmental damage	Inconsequential	—	—	Environmental damage.
Breadth	Inconsequential	Impact to single unit nearby through attack.	Impact to distribution operations through attack.	Impact to critical BESS operations through networked attack.

The use of consequence criteria and the ability to rate that criterion provides the organization with the option to indicate the extent of impact in which to represent their concerns. Once a rating within the bounds established in this set of criteria is supplied, the matrix paints a picture of organizational concerns. This overview indicates where the criteria rated highest represents the greatest concerns and irreparable consequences should the system fail or mis-operate. If any of the criteria in this system reaches above a certain threshold, defined by the organization, the system failure is represented as unacceptable, and further analysis is warranted such as in step four. It is the realization of these consequences that sets the basis for CIE Principle 1: Consequence-Focused Design.

During the analysis of BESS functions, mitigations can be prioritized around the system functions. For example, a BESS providing backup power to a hospital may have additional prioritized solutions. Using this method, supply chain concern can also be categorized, such as by the most critical locations being at risk by FEOC-owned systems. See Figure 11 below for solution prioritizations within consequential functions.

Figure 11: Example of ranking consequential functions using CIE and CCE for BESS in a system for prioritization of solutions.

4.3.4. Step 4: System Analysis

For those consequences deemed unacceptable, the user in this step documents the path from the functional thread to the arrival of the unacceptable consequence destination. Each available functional thread in the system architecture is analyzed on its own merits. From each enabling function involved in the functional thread, elements and linkages are made to connect those to the consequential element to demonstrate the interdependency between the function and the unacceptable consequence.

It is in this system analysis that the collaboration between engineering and cybersecurity personnel is warranted. From an engineer's perspective, the path from an enabling function and its causal analysis that produces the unacceptable consequence is explored. For example, if this data setpoint was adjusted in a certain manner, it would produce a specific system behavior. Then, if an adjustment of this other component and its setpoint produces this behavior, the two in tandem could constitute the unacceptable consequence. This engineering causal analysis represents a set of logic that traces how a functional thread could be altered to incur the unacceptable consequence.

Frequently, an engineer performs this type of analysis by thinking through failure mode analysis, which leads to incorporating safety mitigation techniques and technologies. The alteration in this analysis is the realization, due to digitization, that the very technologies and techniques engineers rely on for safety are at risk of cyber manipulation. So, it is important that engineers understand the causal thread from enabling functions to unacceptable consequences coming to fruition, and special consideration is warranted if the manipulation of a protective device is part of that causal analysis. These key moments become important for the following step, Mitigation Selection, especially. This causal analysis informs the identification of engineering control mitigations that contribute to the reduction in the impact of compromising the related enabling functions in the functional thread.

From a cybersecurity perspective, the path from an enabling function and its misuse analysis produces unacceptable consequences. For example, in combination with the engineering analysis demonstrating key setpoints, if an adversary performed this attack technique and achieved a foothold on a component and then performed this technique to achieve a foothold on the component that allowed them to alter said setpoint, this could lead to unacceptable consequences. At this point in the analysis, the cybersecurity professional assumes that the techniques and tactics used by an adversary are achievable regardless of complexity or cost, which might change the type of threat the adversary is likely to pose. This misuse analysis informs the identification of cybersecurity control mitigations that contribute to the reduction in the probability of compromising the related enabling functions in the functional thread.

This dual analysis forces users to confront the effect of manipulations and the possible vulnerabilities and security risks inherent in these system functions. Step four serves to bring to the surface the interplay of people, processes, and technologies within the functional thread and document the steps to realizing unacceptable consequence(s). For an example of this complete analysis on a BESS reference architecture, see Figure 12.

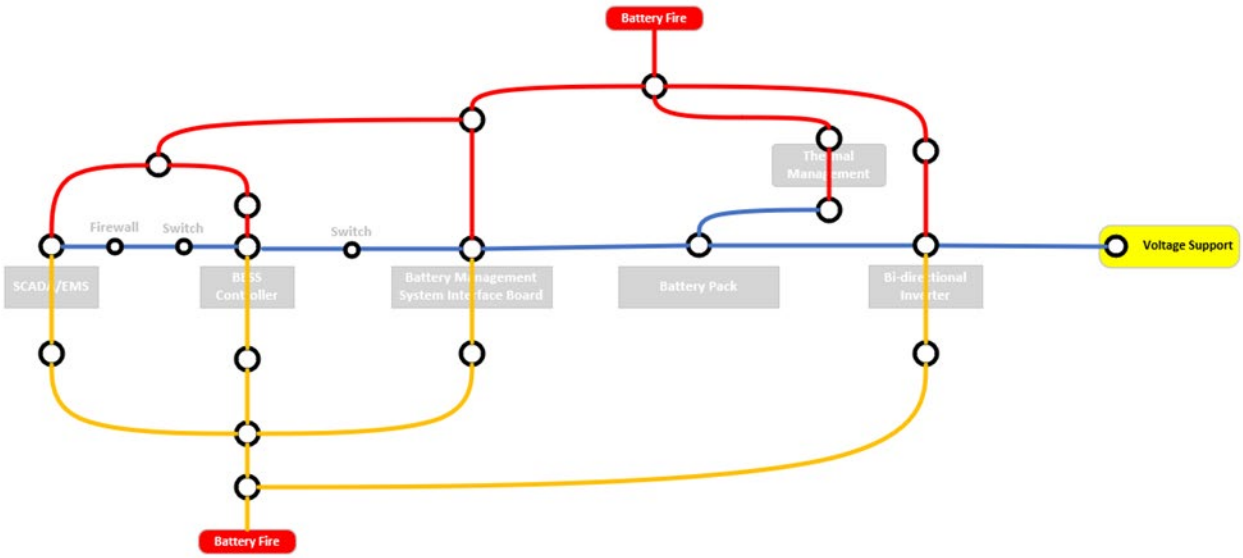

Figure 12: Function Consequence Analysis.

4.3.5. Step 5: Mitigations

In the final step, the user employs the step four analysis from function thread to unacceptable consequence to determine the location and type of mitigation to reduce or eliminate the impact of a given consequence. It is this combination of mitigations that gets at the heart of Principle 5 – Layered Defenses, and the types of mitigations emphasize CIE Principle 2 – Engineered Controls, CIE Principle 3 – Secure Information Architecture, CIE Principle 4 – Design Simplification, CIE Principle 6 – Active Defense, CIE Principle 9 – Cyber-Secure Supply Chain, CIE Principle 10 – Planned Resilience, and Principle 11 – Engineering Information Control.

Using the analysis paths defined allows CIE mitigation placements that target the causal effects to reduce or stop the causal propagation of the impact. CIE mitigations must be placed in relation to the causal effect because it is an engineering solution that regulates the physics of the underlying system processes. Likewise, these cybersecurity mitigations are related to the misuse effect. This is because the placement of cybersecurity controls reduces the probability that misuse occurs within the system configuration.

The combination of both cybersecurity controls against misuse possibilities and engineering controls that reduce impacts present a strong defensive posture for the functional thread(s) and its relationship to the unacceptable consequence(s). Since the placement of the mitigations provides a contextual relationship to the functional thread, the user can see the reference architecture components in which these mitigations are applied. Therefore, once a functional thread is accomplished and saved, the mitigations identified can be placed on their respective components or subsystem on the reference architecture. For an example of the mitigation indication on the reference architecture, see Figure 13.

In step five, the collection of available mitigations is selected and applied using the methodology above. While enhancements for non-domestic systems are considered, protection should be built-in through knowledge of the challenge and incorporating this methodology. However, not all solutions are relevant or applicable. Method users should first consider evaluating their consequences and pick a set of mitigation solutions that reduces the greatest number of consequences and the highest priority threats, while working to create a defensible, secure solution that matches the organization’s risk acceptance threshold.

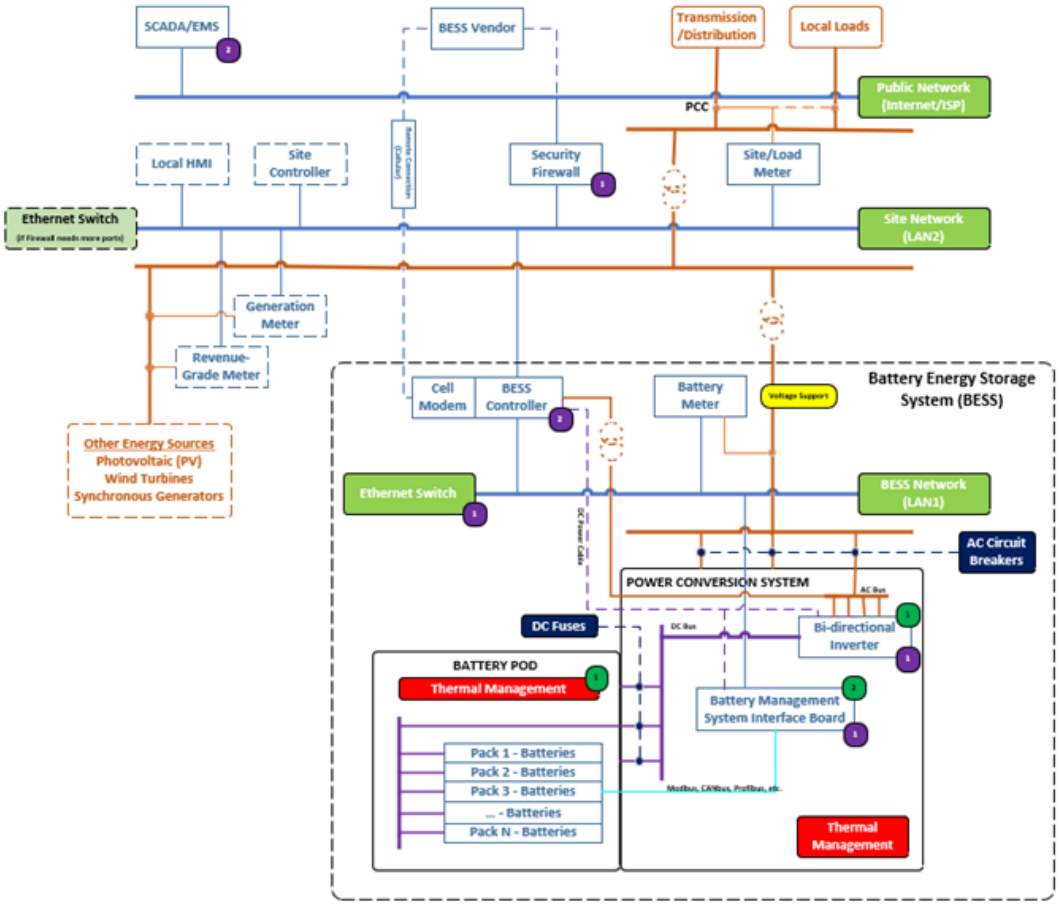

Figure 13: Mitigation Architecture.

A comprehensive list of CIE and Cybersecurity controls is available from the INL CIE program. The discussion of this methodology is intended as a starting point for evaluating BESS implementations. CIE Principle 5 – Layered Defenses and CIE Principle 7 – Interdependency Evaluation recommends that a protection scheme include both cybersecurity and CIE controls be present in the defense of the critical functions of a system.

4.4. Strategic and Continuous Assessment

The final part of the CIE analysis methodology is the recognition of a continuous assessment process. When new information is shared (a vulnerability or change in ownership of a company), the same methodology should be revisited and reapplied to evaluate the effectiveness of current and new controls. This is not designed to be static but a continuous evaluation.

To make the process circular in nature through continuous improvement, the underlying reference architecture is expected to be adjusted. For instance, CIE Principle 4 – Design Simplification emphasizes the point that if the technology or feature can be removed outright, it eliminates the possibility of manipulation at that point in the analysis and reduces the attack surface. As an example, Figure 14 below shows the removal of the cell modem so that the only uplink to the BESS vendor is through the security firewall component that is part of the communication subsystem.

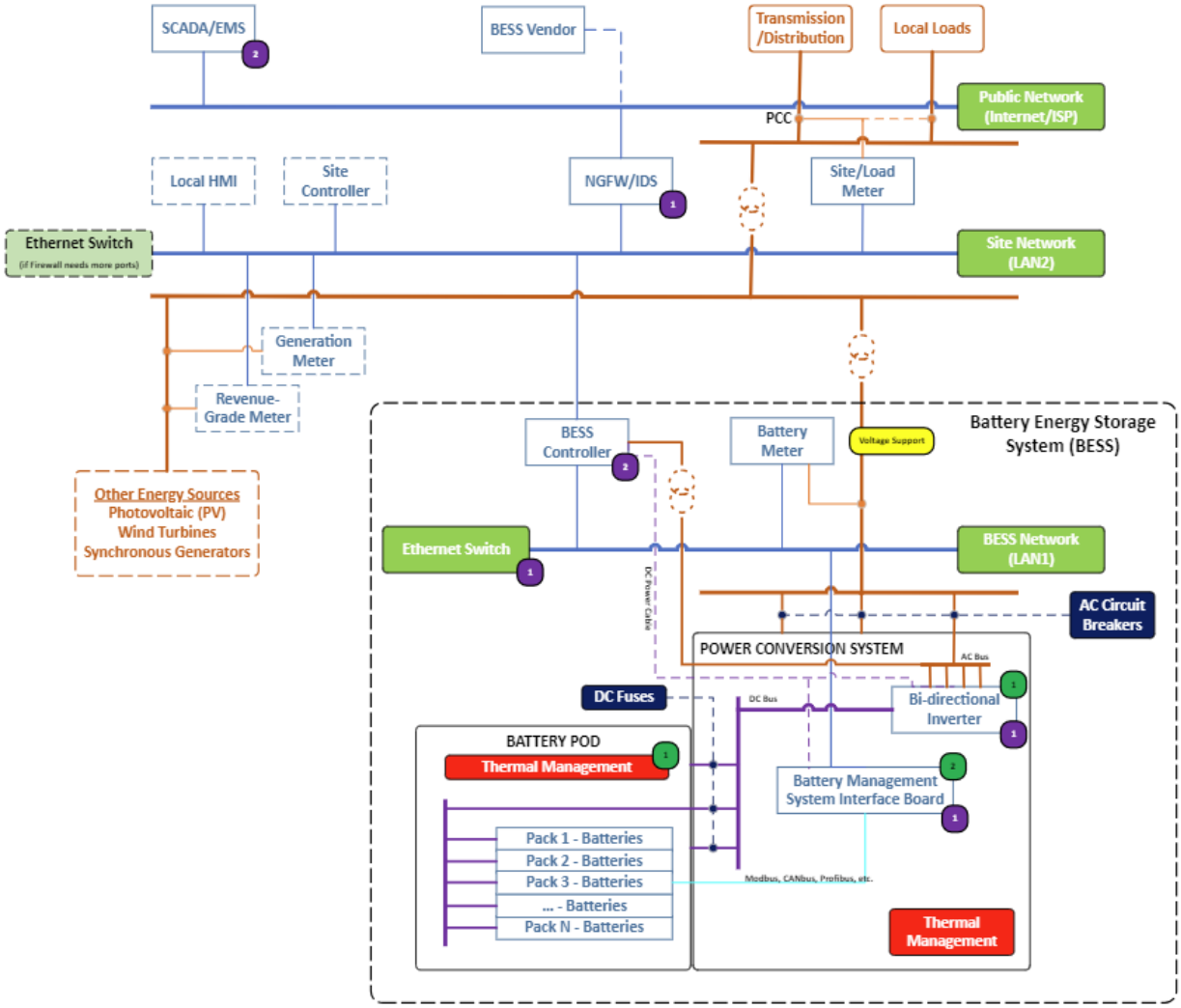

Figure 14: Updated Reference Architecture.

The remaining report sections demonstrate the CIE analysis methodology and its application through a case study where an inverter-based resource experienced a misoperation event. For brevity, assumptions about the reference architecture will be made and identified when used.

5. CASE STUDY

5.1. NERC Report Summary on IBR Misoperation Event in 2023

In 2023, a significant misoperation event involving IBRs occurred within the Western Electricity Coordinating Council (WECC). The events highlighted several critical issues related to the performance and reliability of IBRs, which have direct implications for BESS as well.[29] The events were triggered by a combination of a grid disturbance due to a subsequent equipment failure in a major substation. The misoperation involved the failure of control systems in several large-scale IBRs. Specifically, there were errors in the control algorithms that led to incorrect power output adjustments and communication failures between IBR units and the central grid management system. IBR misoperation events can cause frequency fluctuations and necessitate emergency interventions to stabilize the system(s). Often, the primary causes of misoperation are design flaws in the control algorithms and inadequate testing of IBR integration under extreme or abnormal conditions.

The capabilities and limitations of IBRs are evident, particularly in their response time to disturbances and reliability under stress. Similar issues can affect BESS, which includes smart inverter(s), particularly in areas of concern such as control systems and integration with existing grid infrastructure. Potential impacts of BESS misoperation include failure to provide grid services, power outages, reduced grid stability, and increased operational costs due to emergency interventions. Additionally, the increasing deployment of microprocessor-based components into those control algorithms provides the possibility that an adversary can introduce the necessary alterations to cause misoperation of the IBR, which includes BESS installations.

Given these findings, it is crucial that BESS installations be strategically deployed in locations where they can provide the most benefit, such as areas prone to grid disturbances or with high renewable energy penetration, but that these BESS installations include CIE in its system lifecycle. The principled application of CIE contributes to the thorough testing of BESS under various operational and adversary scenarios, robust design standards for control systems, and enhanced monitoring systems to detect and mitigate potential issues and failures early.

5.1.1. Outline of Event

In the battery event in California, the California Independent System Operator (CAISO) identified significant instances on March 9, 2022, and April 6, 2022, noting reductions in power outputs across multiple BESS and solar PV facilities. These events met the criteria for Category 1a and 1i events, respectively, per the NERC Event Analysis Program, based on total MW losses and the number of facilities experiencing an outage. Following these occurrences, NERC and WECC collaborated to develop a disturbance report, focusing specifically on BESS due to their exclusive involvement in the disturbances. CAISO independently gathered information from affected entities and conducted follow-up calls to aid root cause analysis. The report, prepared by NERC and WECC in collaboration with CAISO, aims to share key findings and recommendations with the industry.[30]

On March 9, 2022, a generator bus fault occurred at a natural gas-fired, simple-cycle facility in Riverside County, California. This fault led to a C-phase-to-ground fault on the 220 kV system, resulting in the disconnection of natural gas generators carrying 694 MW. Additionally, IBRs from various facilities were unexpectedly reduced by 408 MW, with 124 MW attributed to BESS. The fault resulted in a total loss of 1,102 MW of generation, causing the system frequency to drop to 59.916 Hz. CAISO and the Balancing Authority raised regulating unit output to assist in frequency recovery, with normal frequency restored within three minutes.

On April 6, 2022, a B-phase-to-ground fault occurred at a new BESS plant undergoing testing. This fault led to an unexpected reduction of 498 MW from multiple IBRs, causing the system frequency to fall from around 60.014 Hz to 59.924 Hz. Recovery efforts by the CAISO Balancing Authority and Area Control Center normalized frequency within one and a half minutes. Both events occurred in the Southern California area within the CAISO footprint, with multiple BESS and solar PV facilities identified as exhibiting unreliable performance. All affected facilities are located within or near the Southern California area. The main causes of the BESS trip are summarized as follows:

- Inverter instantaneous AC overcurrent
- Inverter instantaneous AC overvoltage tripping
- Inverter DC voltage unbalance tripping
- Inverter unbalanced AC current tripping
- Inverter DC bus overvoltage.

Full transparency of this event detailed that none of the facilities involved in the battery event met CAISO's requirement of 10 milliseconds (ms) data recording resolution. Additionally, none of these

facilities had inverter-level oscillography data available due to the absence of required fast logging. CAISO reported that these deficiencies have since been rectified. Furthermore, while one facility had legacy inverters utilizing momentary cessation, grid operators of other affected facilities miscoded inverter tripping lasting tens of seconds as momentary cessation. It is important to note that momentary cessation is a controlled behavior during specific grid conditions and differs significantly from inadvertent inverter tripping and subsequent reconnection after a short time.

5.2. CIE Analysis of Event

A couple of key points are of interest from a CIE perspective from the use case. The first is the following statement, “The misoperation involved the failure of control systems in several large-scale IBRs. Specifically, there were errors in the control algorithms that led to incorrect power output adjustments and communication failures between IBR units and the central grid management system.” Control algorithms are the key items in a process because this is both the destination of monitoring information and often the source of command information. It is this focal point that, when configured digitally, which is often the case in modern process automation, provides, at minimum, a key opportunity for an adversary to manipulate.

The second significant point in the more detailed outline is the listing of the main causes of the BESS trips. The listing of trip conditions is interesting in multiple ways: first, the use of over- and under-voltage and over- and under-current tripping is a normal protection equipment function, and that technology is available. Second, this protection equipment is becoming increasingly digitized, which brings in cybersecurity implications that should be considered as part of a CIE Analysis and emphasized by Principle 8 – Digital Asset Awareness. Therefore, while protection equipment is key to reducing or eliminating the probability of equipment failure from an adverse condition, the increasing digitization warrants an additional analysis so that it can include cyber-informed reasoning in connection with the safety-informed reasoning that includes that equipment in a BESS design.

Another key point in the more detailed outline is this statement, “Grid operators of other affected facilities miscoded inverter tripping lasting tens of seconds as momentary cessation. It is important to note that momentary cessation is a controlled behavior during specific grid conditions and differs significantly from inadvertent inverter tripping and subsequent reconnection after a short time.” Furthermore, because the miscoded inverter tripping produced the appearance of momentary cessation, there is the interesting interplay of misoperation being interpreted as normal response actions. There is a timing component here from an engineering standpoint that represents an opportunity for engineering controls to protect this controller behavior of momentary cessation and prevent this crossover between misoperation and normal recovery actions. CIE at its heart is a quest to best handle cyber impacts, and in this case the digital technologies increase the opportunity to recreate the impacts explored in the use case with digital manipulation. The following analysis walks through the CIE analysis methodology above and seeks to identify opportunities made available by the CIE principles.

For step one, the reference architecture will reuse the depiction used in the previous section (Figure 15). While it is understood this may not be exactly accurate, it clearly demonstrates the normal subsystems available in a BESS installation. It is assumed this adequately represents the BESS system for demonstration purposes.

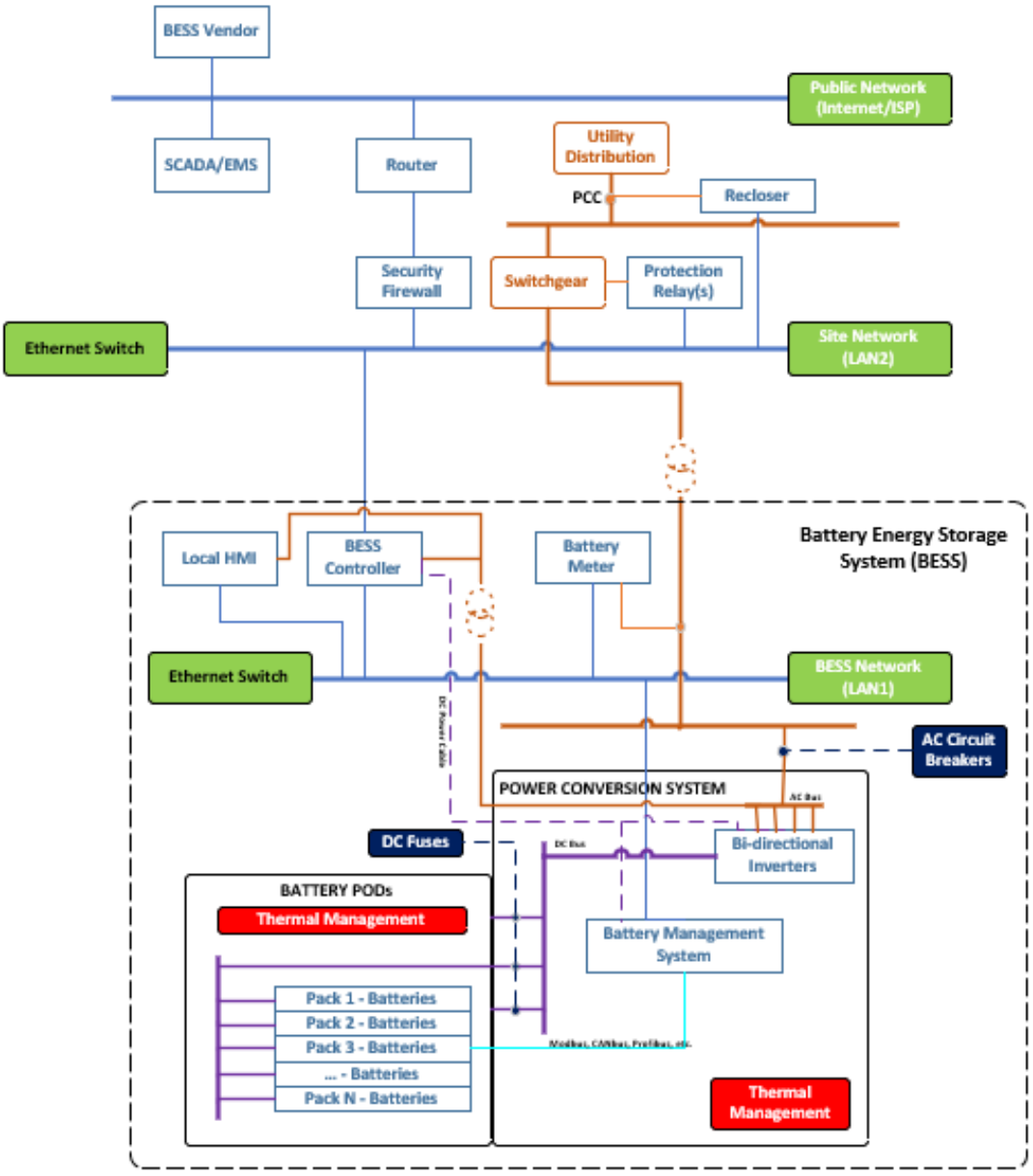

Figure 15: Use Case Reference Architecture.

This architecture currently provides awareness of notable interdependencies as part consideration of CIE Principle 7 – Interdependency Evaluation. The mechanism for this interdependency is the network connections between the communication subsystem (network switches, firewall, router) and the other subsystems (EMS, BMS, controller, etc.). Furthermore, a special consideration is the fact that the EMS and the rest of the BESS system share a communication path across the public network. From the power delivery side, an awareness of the interdependencies is also recognized by the connections that allow power flow between the battery packs and the other subsystems (PCS, electrical protections, etc.).

In step two, when thinking about the grid service and for this use case, the analysis will focus on frequency support. The assumption around this selection for this discussion is the emphasis on frequency deviations in the provided use case details. Often, BESS systems provide a collection of grid services, such as backup power, voltage support, etc., but for brevity, we will assume only frequency support as the critical function provided by this BESS architecture. The boundary interface for this service will be the

point of common coupling between the BESS installation and the utility distribution grid. Furthermore, the delivery of this service is facilitated by the entire BESS installation, as indicated by the yellow highlighted zone in Figure 16 below.

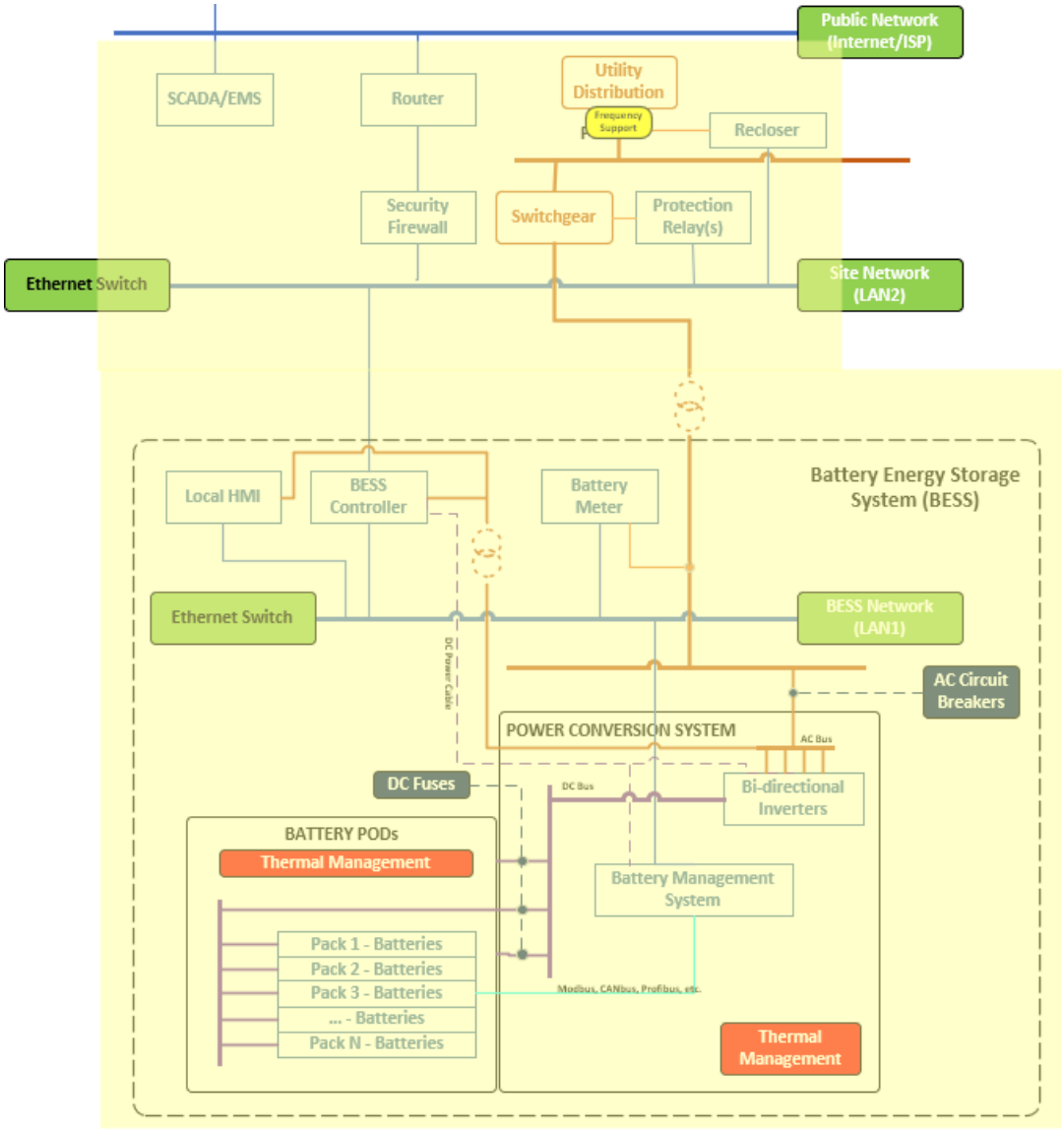

Figure 16: Area of Effect for Frequency Support Service.

Therefore, when thinking about the enabling functions that participate, ensuring the delivery of frequency support and the protection of equipment that supports this frequency support is the key to identifying opportunities for consequence analysis (steps three and four) and mitigations (step five). The following functional thread, in Figure 17 below, walks through the steps. As mentioned previously, describe this functional thread, especially how digital technology is facilitating the delivery of the grid service and protecting the equipment supporting that delivery, which represents the heart of CIE Principle 8 – Digital Asset Awareness.

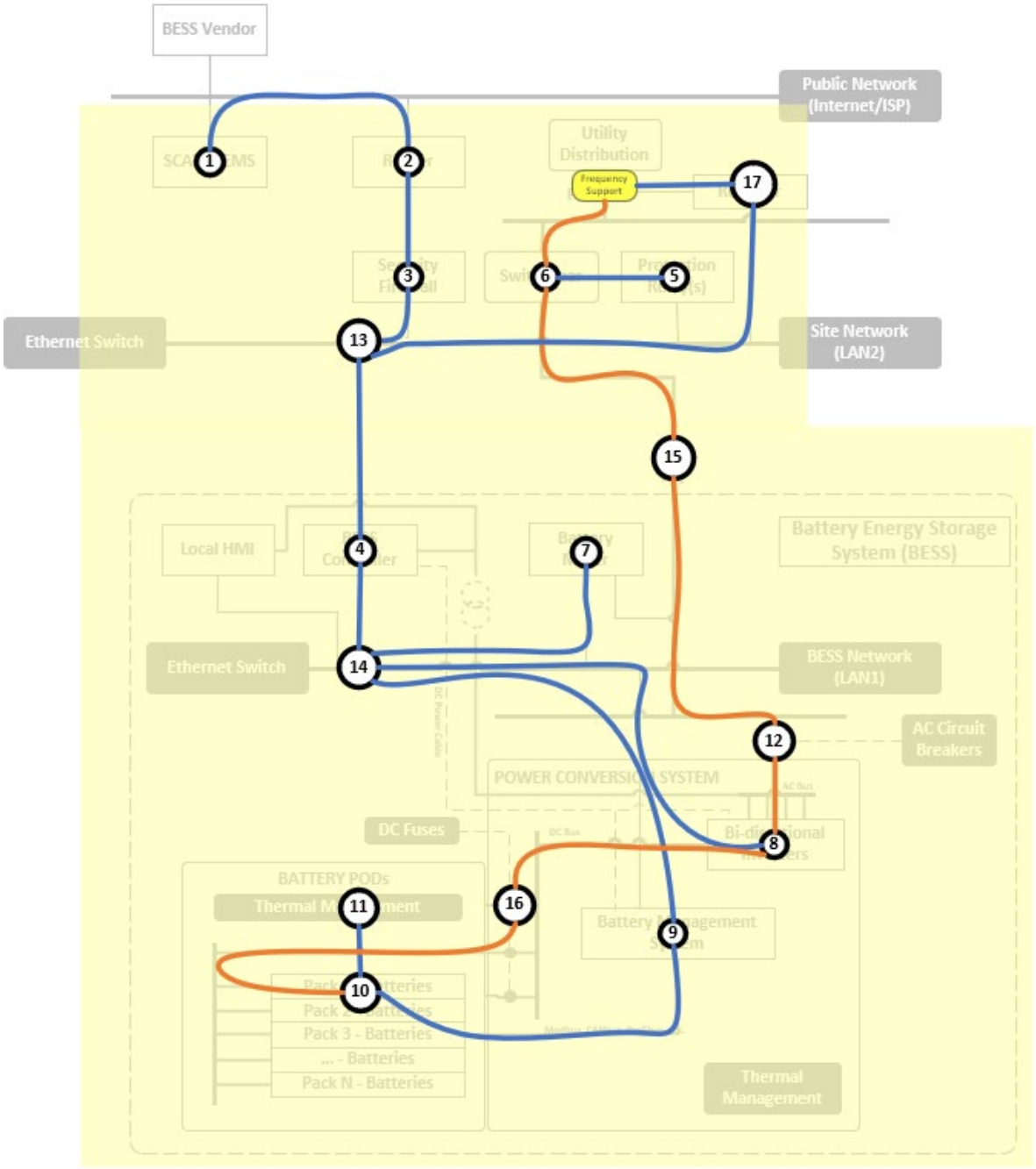

Figure 17: Frequency Support Functional Thread example.

Table 5: Enabling Function example descriptions.

ID	Component	Function
1.	EMS SCADA Service	Provides any adjustments for setpoint, scaling, and range values to the BESS controller.
2.	Router	Provides the Packet Routing from the BESS location to the EMS SCADA service location via the public internet
3.	Security Firewall	Provides the Network Access Policy from the Public Network to the local BESS site network.
4.	BESS Controller	Primary location for the frequency setpoints, power setpoints, delta setpoints, and other key information used to maintain the frequency support mode of operation. Commands the total System Power Input and Output. This is determined by the target power from the power mode and the power delta provided by the frequency support mode of operation. For instance, if frequency drops below the low frequency setpoint, the BESS increases its power output (or reduces charge input) at a rate configured by the delta setpoints, and vice versa, if the frequency rises above the high frequency setpoint, the BESS decreases its power output (or increases charge input) likewise.
5.	Protection Relay(s)	Provides the under- and over- voltage and current measurements and trip points measurements and commands to switchgear.
6.	Switchgear	Provides the circuit breakers to disrupt or allow power flow.
7.	Battery Meter	Measures the power output of the BESS system.
8.	Inverter (PCS)	Provides the power transformation between AC and DC, as well as provides measurement of power at its terminals.
9.	BMS	Provides the analysis and management for battery cells and battery packs and the commands to output/input power out and into the battery packs.
10.	Battery Packs with Battery Cells	Provides the measurements of cell voltage, cell temperature readings.
11.	TMS	Provides the commands and control of the temperature of the battery packs/cells, and environment in the BESS installation. If fire protection is installed, then fire detection and fire suppression.
12.	AC Circuit Breakers	Provides overcurrent protection to the conductors between the device and the Inverter per any local code requirements.
13.	Network Switch #1	Provides the Local Area Network (LAN) communication for the BESS Site network that connects the BESS Controller to any various site level metering, controllers, or other services, and the firewall. Dependent on size of site locations/site services.

14.	Network Switch #2	Provides the local area network (LAN) communication for the BESS system components within the BESS installation such as the BESS Controller to BMS(s), TMS(s), Inverter(s), and Battery meter(s). Dependent on size of installation.
15.	Transformer	Provides the voltage transformation from BESS location levels to utility grid levels.
16.	Fuses	Provides overvoltage and/or overcurrent electrical protection to Battery Packs on DC Bus.
17.	Recloser	Provides transient fault detection and response between the Utility grid and the BESS site location.

The presentation of enabling functions is still abstract for brevity, whereas a more thorough engineering-level depiction would specify exact tag names, understanding of process curves, and other key details that increase the quality of understanding of how each component performs its duties (Table 5). Regardless, as these enabling functions are enumerated, the opportunities for various manipulation points become more evident. The specific points, especially the data points that are communicated, become the basis for CIE Principle 3 – Secure Information Architecture analysis.

When thinking about the next step and providing that consequence analysis, the use case provides context for the level of impact that was achieved with the normal failure produced from the phase-to-ground faults and their effect on frequency regulation, highlighted in red text. Using those specifics from the use case and the criteria provided in the CIE analysis methodology above produces the following depiction in Table 6. Additionally, considering the impact if it was replicated by cyber manipulation (highlighted in green), there is a clear change in the criteria ratings, highlighted in green text.

Table 6: Consequence analysis criteria for the use case. [CCE][31]

Criteria	None	Low	Medium	High
Area/Load Impact	Inconsequential	Loss of failure to service firm load of less than 300 MW (or) load supply loss of MSC or 2,000 MW, whichever is lower.	Loss of failure to service firm load between 301 and 1,500 MW (or) load supply loss of between 2,000 MW (or MSC, whichever is lower) and 3,000 MW.	Loss of failure to service firm load greater than 1,500 MW or load supply loss of greater than 3,000 MW.
Duration	Inconsequential	Return of all service in less than one day (inability to serve firm load) or supply outage for less than one week	Return of all service 1–5 days (inability to serve firm load) or supply outage for one week to one month	Return of all service > five days (inability to serve firm load) or supply outage >one month
Safety	Inconsequential	Risk onsite	Definite safety risk offsite	loss of life potential

Asset Owner/System Integrity	Inconsequential	Can restore with confidence in integrity	Owner has knowledge but no resources (money, time, personnel) to restore	Asset owner can restore but has no confidence in integrity
Cost	Inconsequential	Significant but recoverable	Multiple years to recover financially	Trigger of liquidity crisis/potential bankruptcy
Reputational damage	Inconsequential	—	—	Customer loss of faith in utility
Environmental damage	Inconsequential	—	—	Environmental damage
Breadth	Inconsequential	Impact to single unit nearby through attack	Impact to distribution operations through attack	Impact to critical BESS operations through networked attack

The ability of cyber manipulation to increase the consequence of impact is notable because when considering cyber manipulation, the ability of the utility to perform recovery actions or the possibility of equipment damage is fundamentally different, because the manipulation makes ownership of the recovery strained or the loss of protective measures available (if the protection measures are digital assets). This growth in the impact risk (duration, system integrity, and breadth) warrants a level of investment in performing targeted mitigations so that the risk of impact returns to normal operations. It would be at this stage that the organization decides if a consequence is acceptable or unacceptable. It is the assumption of this analysis that the growth in impact is unacceptable and necessitates continued analysis.

Extracting the functional thread into a focused view leads to the next step, where a system analysis is performed from both the engineering and cybersecurity professional perspectives. See Figure 18 below for this extracted functional thread.

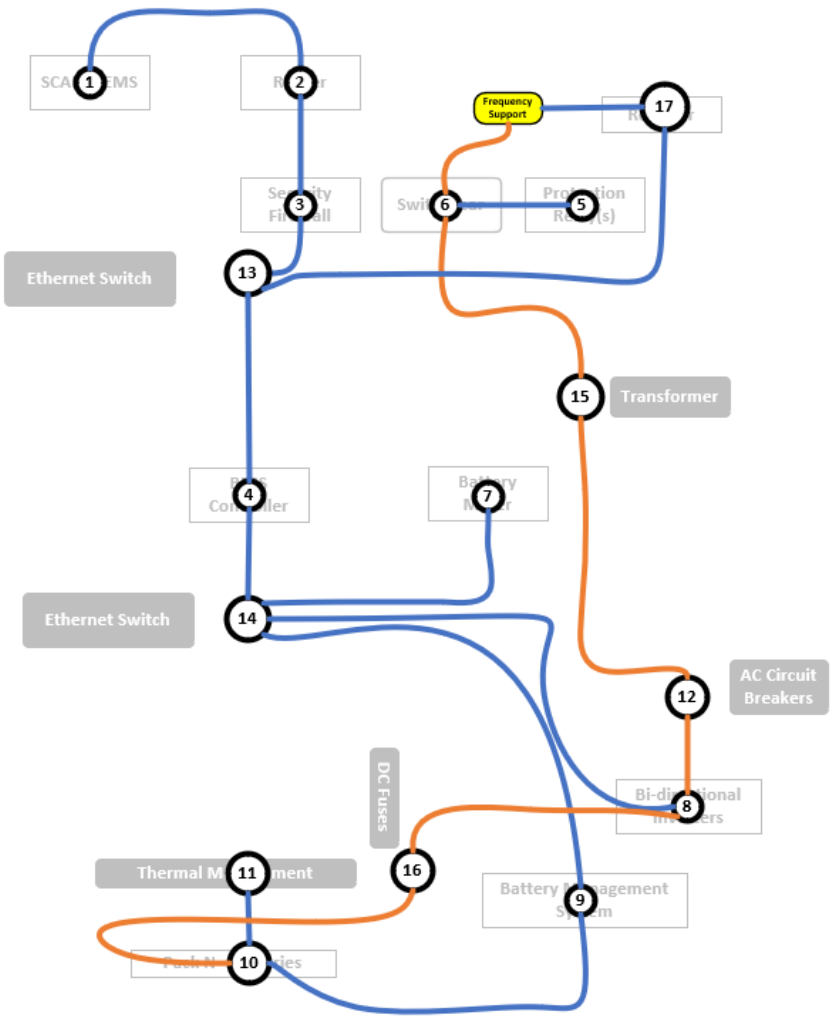

Figure 18: Simplified Frequency Support Functional thread example.

From the engineering perspective, the setpoints and deltas that inform the frequency support mode of operation are critical command settings delivered from the EMS or SCADA to or initialized in the BESS controller. Furthermore, the inverter and battery meter provide feedback for the current power, voltage, and frequency measurements. From a causal analysis, the engineer interrogates the implications of command mis- and mal-operation and receives information to determine the opportunity for manipulation. For instance, if the delta setpoints were adjusted to inform the BESS system of how quickly to discharge or charge, this could contribute to a rapid discharge or charge of the system. Rapid discharge or charge operations often underpin the opportunity for abusing the thermal characteristics of the battery.

This, in combination with adjustments to the setpoints or heating commands of the thermal management system, could increase the likelihood of BESS impacts. Finally, the adjustment of the setpoints could easily cause the BESS system to shut down in a denial of service (DoS) fashion due to the frequency limits being placed outside of normal operations. Depending on the size of the BESS installation, this could be detrimental to local grid operations, whereas in this case, the loss of the BESS is recoverable by the bulk energy system. This small example of engineering causal analysis produces opportunities for the identification and implementation of CIE-engineered controls (CIE Principle 2) and other key CIE principal integration.

From a cybersecurity perspective and knowing that, the communication of command and sensor information is provided by a set of network paths and the digital functions that exist in components at all levels of the BESS system (see nodes with blue interconnections). From a threat and attack vector perspective, an adversary achieving access to the EMS solution or the networks within the BESS installation provides different opportunities. For instance, from the EMS service an adversary can pivot to the BESS controller, which provides several opportunities for compromise (i.e., uploading new firmware, updates, command issuance, etc.). In another tactic, an adversary living on the internal network within the BESS system between the BESS controller and underlying system components, such as the BMS, inverter, or TMS, provides similar manipulation opportunities at these lower layers. This is especially concerning when considering the supply chain of FEOC components or the security of FEOC-approved personnel working on components in these lower layers. This misuse analysis of what cyber professionals focus on provides clear identification of cybersecurity controls, such as network segmentation, access control, firmware validation, etc. Key traditional digital cybersecurity controls also validate and protect from setpoint adjustments include, but is not limited to, encrypted communications, next generation firewall (NGFW) capabilities, intrusion detection system (IDS), allowlist and denylisting, etc. Cybersecurity control frameworks such as the National Institute Standards and Technology (NIST) 800-82 (overlaying NIST 800-53)[32], IEEE 1547.3[33], ISA/IEC 62443[34], and others provide a wealth of understanding for the types and applications of these cybersecurity controls.

Considering engineering, causal analysis in advance propels the user into the CIE principles and available control mitigations that can be considered from the engineering perspective. These types of controls have the unique opportunity to reduce or eliminate the impact of cybersecurity compromise, and when implemented in combination with the cybersecurity controls identified from the misuse analysis, represent the enhanced cybersecurity control scheme that best addresses the overall BESS security. The remaining sections of this paper provide definitions and an example of CIE principle controls relating to this use case analysis.

5.2.1. Principle 1: Consequence-Focused Design

Principle 1, Consequence-Focused Design, is covered by the consequence analysis performed in Section 5.1. Awareness of the potential consequences, enabling functions for key components, and functional threads gives the context to engineers to apply mitigations focused on reducing the impact of likelihood of consequences through the remaining principles.

Key questions and examples for this section are omitted as they are covered in detail in the previous section.

5.2.2. Principle 2: Develop Engineering Controls Around the Site

As highlighted above, Consequence-focused Design (Principle 1) delves into the numerous possible threats to a system's integrity and operational status that must be protected as a priority from cyber and physical events. Principle 2, engineered controls, follows this consequence prioritization to ensure those systems are adequately safeguarded against threats by adopting and sustaining the necessary engineering defenses. Just as safety considerations serve as the groundwork for systems, engineered controls represent a security-focused analog (and a combination of safety and security should be considered). These controls consist of well-defined and systematically maintained control measures that complement traditional cybersecurity (i.e., digital) and safety controls.

The goal is to identify and adjust the engineering process controls design at the outset of system development to prevent or minimize cybersecurity threats. This approach reduces reliance on subsequent additions of IT and OT security measures during the actual implementation phase. When controls and processes are effectively coordinated, they can either eliminate or substantially diminish the damage an event may inflict. Like safety considerations, CIE controls shift protective measures to the preliminary conceptual and design stages. This adjustment allows for applying conventional safety hierarchy of

controls into cybersecurity applications. Even slight design modifications, such as removing an unnecessary wireless feature, can prevent certain cyber-attack methods that might be otherwise hard or expensive to defend against.

One of the primary advantages of setting cybersecurity criteria from the start is the integration of several engineering risk management practices like defense-in-depth and fail-safe modes. The concepts and requirements phases offer a chance to recognize external influences, digital infrastructure interactions with the system, and the stakeholders involved. Early inclusion of engineered control considerations can reduce the system's digital exposure, lessen the dependency on digital systems, or offer a less complex alternative. Moreover, well-planned controls can decrease the need for adjustments as the system or its environment evolves throughout its lifecycle. As the system progresses from design to operation, continuous engineered controls provide ongoing protection against significant cybersecurity-triggered events by safeguarding the assumptions and mitigations initially made in the risk assessment.

Digital systems are subject to rapid changes. The key questions listed in this section are designed to pinpoint controls that might alter the originally identified risks.

Key Engineering Control and Mitigation Considerations:

- What fundamental physical principles or energy forms (e.g., electricity, pressure, temperature, and potential energy) are essential to this system?
    - What types of engineered systems (e.g., IT, OT, electrical, mechanical pneumatic, hydraulic, thermal, and chemical) are anticipated or necessary to achieve the Concept of Operations (CONOPs) objectives?[35]
    - Which engineering controls are applicable to these different engineered systems?
- Is remote activation feasible for these controls?
- How is access control managed for each control point?
- Are controls designed to be active by default, or do they require manual initiation or maintenance?
- Are engineered controls specified in contractual agreements?
- Which controls are integrated into the product, and which are external?

Specific Questions for BESS in Utility Operations:

- Does the fire suppression system employ analog mechanisms?
- Does the HVAC thermal management system on the battery rely on digital signaling?
- For alternate storage systems (e.g., secondary generation like propane):
    - Is it accessible via an analog or relay-logic transfer switch?
    - Can it compensate for reduced BESS capacity?
- List current protections on the BESS (specify if digital configuration is involved):
    - Overcurrent
    - Overvoltage
    - Undervoltage
    - Over/under frequency
    - Other protections

- Does the BESS include a battery protection circuit for cells?
    - Is this circuit dependent on digital technologies?
- Does the charge controller incorporate non-digital mechanisms to prevent overcharging?

Example of Specific Engineered Control for BESS in Utility Operations

Table 7 shows a sample migration score for BESS engineering controls in a CIE framework. The vendor or asset owner operator (AOO) column designates who is expected to have responsibility for implementing that mitigation.

Table 7: Sample Mitigation, Score for Engineering Controls for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Install a circuit element that events when a rate of change limit is achieved for discharge or charge. This event is used in the control logic of the inverter to regulate the output voltage, frequency, and waveform of the AC power to match the grid's requirements and maintain grid stability.	High	$$	Moderate	AOO

5.2.3. Principle 3: Secure Information Architecture

Principle 3 involves developing a robust data protection strategy for identified critical data flows, following the principles of consequence-focused design outlined in Principle 1. This strategy aims to focus on highly sensitive information and the systems housing it, bolstering control, security, and surveillance over these assets. It is crucial to recognize that each system may handle data critical to vital operations, necessitating protection against unauthorized exposure and, more critically, against malicious or accidental alterations. Early in the process, project teams can identify data elements closely tied to potentially severe outcomes. Key considerations include data element origin and modification points, protective measures, and the feasibility of implementing data verification processes through analog checks or benchmarking against existing data.

As the design progresses and foundational network and data service architectures are defined, engineers can implement precise digital controls and delineate specific zones and segments. For example, segregating applications with high risk or significant consequences from the primary network infrastructure.

Key Questions to Consider:

- How is trust established and periodically revalidated for users and systems?
- Who is responsible for initiating, maintaining, and reconfirming trust in users and systems?
- What is the frequency of revalidation for trust?
- Which unnoticed data elements could critically impact system functionality?

- Considering people, processes, technology, identified consequences, and essential functions, what assumptions exist about information exchange among individuals, technology, and process components?
- What adverse outcomes could occur if these assumptions are not met?
- What information exchanges are vital for process operations?
- What possible actions result from these information exchanges?
- Which information exchanges or data transformations are most critical, considering potential outcomes?
- How does authorization or trust influence these information exchanges?
- Which information transfers are crucial for driving process actions related to predetermined consequences, involving interactions solely between technology and process components?
- How can monitoring these exchanges or enabling data validation opportunities enhance resilience, reliability, or security to prevent failures or tampering with severe consequences?

Additional Considerations:

- How are network connections between segments of the overall design established?
- How do different subsystems interact?
- How will the system interface with the external environment beyond its boundaries?
- What information is exchanged, and for what purpose?
- What assumptions are made about the recipients of this information, and what levels of confidentiality, integrity, and availability are required?
- How do external entities utilize data from the system, and what measures ensure its suitability?
- How does the system process incoming external data, and how is its validity verified?
- Are the resources adequate to meet communication needs, including security, capacity, and speed?

Example of Specific Secure Information Architecture for BESS in Utility Operations:

Data Management with Battery Vendors:

- Develop a plan specifying critical data requirements for battery vendors.
    - Outline what information can be shared with different entities.
    - Share the minimal necessary information with non-domestic vendors.

Controller Design and Network Segmentation:

- Limit non-essential information and communications architecture in controller design specifications.
- Validate the read or write access required for key setpoint between the EMS and battery control system,
- Implement network segmentation, utilizing DMZs to separate operational networks for devices, control centers, and substations, especially for non-domestic environments.

Operational Model and Cloud Readiness:

- Develop an operational model prioritizing minimal consequences for devices with lower trust levels.
- Conduct assessments for cloud readiness, data residency compliance, and considerations for private and public cloud deployments.

Table 8 shows a sample migration score for secure information architecture.

Table 8: Sample Mitigation, Score for Secure Information Architecture for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Implement network monitoring that focuses on the commands and setpoints directly related to the frequency support mode of operation (informed by engineering) between the EMS and BESS Controller and the BESS controller with the inverter.	High	$	Medium	AOO

5.2.4. Principle 4: Design Simplification

During the process of design simplification, engineers must identify those components not strictly necessary for their system to function and determine which of these components could have significant negative impacts if misused. They are tasked with evaluating how to pare down their system to the essential elements that deliver critical operations and ensure robustness. Design simplification involves streamlining the system, component, or design architecture from the start to eliminate unnecessary complexities that could have severe repercussions despite their limited value. This preemptive simplification lowers the chances of the digital functionalities being misused, whether intentionally or accidentally. Part of this streamlining involves minimizing unused or unnoticed capabilities in digital systems, which, though often overlooked or turned off by users, can be exploited by malicious actors.

Systems acquired through purchase may come with an array of features that exceed the necessary operational requirements. While these additional features can be set up to be invisible to legitimate users, they remain accessible to potential attackers and may be abused during various stages, from implementation to maintenance. These superfluous features could result in dire outcomes if used by malicious entities or uninformed operators. Therefore, engineers should assess the possibility of their complete removal of features that are not indispensable. If full removal is not feasible, consideration should be given to how alerts might be set up for the use of these functions or how the system might reject unwanted commands before they are carried out.

While design simplification can enhance cybersecurity, it must be carefully weighed against other factors, such as business requirements, operational efficiency, and safety considerations, during the design process. Indiscriminate feature elimination can accidentally cut out vital functions; some might not seem crucial because they are used rarely, yet they are important in specific contexts. Consequently, simplification demands a thorough comprehension of the system's demands, its structure, and its operational protocols. With this knowledge base, simplification can be consistently applied throughout the product's life cycle—from development to testing to operation. It is essential to verify that nonessential features have been excised correctly, ensuring the retention of all vital functions.

Example of Specific Design Simplification for BESS in Utility Operations:

Device Feature Optimization:

- Prioritize essential device features.
- Evaluate alternative alarms for critical items using reliable sensors.
- Implement features gradually with thorough equipment reviews.
- Streamline components for critical functions.

Table 9 shows a sample mitigation for design specifications within the CIE framework.

Table 9: Sample Mitigation, Score for Design Simplification for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Remove the capability for BESS controllers to communicate with Vendors or other authorized third parties via a cell modem so that it must communicate through a next generation firewall (NGFW) or another industrial secure remote access solution. (Increased visibility) -or- Remove the allowance for the BESS controller to command the TMS system and allow TMS to make localized stand-alone decisions only for temperature control.	Moderate	$	Easy	AOO

5.2.5. Principle 5: Layered Defense

The most effective defense against critical consequences involves a combination of physically based analog mitigations, protective measures for key system elements, detection of adverse operating or security conditions, and capabilities for response and remediation. In resilient layered defenses, engineers collaborate with operational cybersecurity teams to strategically assemble these defenses, aiming to mitigate the most severe impacts of prioritized consequences. They ensure that each defensive capability and service is finely tuned based on identified risks, thereby minimizing potential impacts.

Example of Resilient Layered Defense for BESS in Utility Operations:

BESS placement and configuration:

- BESS will be situated at the edge of an environment with multiple layers of imperfect perimeter protection and detection, featuring several necessary interfaces that span the threat perimeter.
- BESS components offer extensive features and configuration options, some of which may not be utilized by the utility. The design team seeks guidance on how to detect the activation of unused features.

As detailed in Figure 19, the components of a security architecture include:

- Detection
- Analysis
- Decision support/visualization
- Mitigation
- Sharing

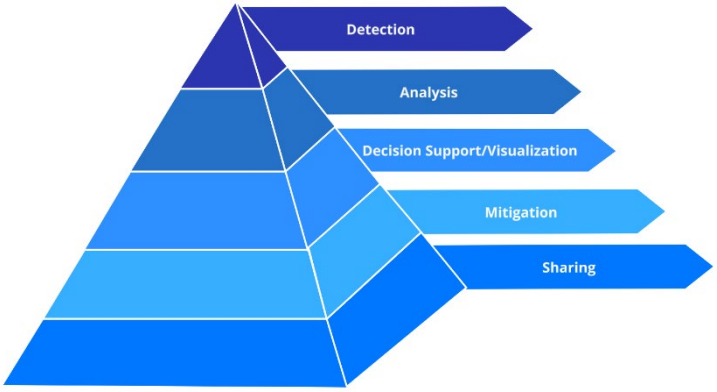

Figure 19: Security Architecture Pyramid.

Table 10 details a sample mitigation for a resilient layered defense.

Table 10: Sample Mitigation, Score for Resilient Layered Defense for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Ensure critical enabling functions have at a minimum of two independent defensive mechanisms (i.e., an engineered control(s) and a digital control(s).	High	$$	Moderate	AOO

5.2.6. Principle 6: Active Defense

Planning for active defense should commence from the conceptual design phase of a system and continue throughout its lifecycle until retirement. During the design phase, teams should strategize defensive actions for critical events. This process involves thorough discussions among system designers, operators, and cybersecurity experts to analyze potential adverse consequences, their pathways (kill chain), and manifestations within the system. From these discussions, system states and anomalies that could serve as early indicators of predefined consequences should be identified. Detailed plans should then be drafted outlining specific roles and responsibilities across all relevant stakeholders. Active defense strategies often necessitate collaboration across diverse roles associated with the system. Once plans are finalized, regular practice drills should be conducted to ensure readiness and periodic assessments should be performed to evaluate the effectiveness of the approach. This ongoing process helps in identifying emerging threats, indicators, and opportunities for enhanced defensive measures.

Example of Active Defense for BESS in Utility Operations:

Risk Assessment and Mitigation:

- Evaluate the kill chain to understand the sequence leading to adverse consequences and define actions upon detecting indicators.
- For non-domestic BESS, establish indicators for potential supply chain attacks and dormant behaviors.

Table 11 details a sample mitigation for active defense.

Table 11: Sample Mitigation, Score for Active Defense for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Establish and train operations staff—including operations personnel, engineering teams, maintenance staff, and internal and external security personnel—to promptly execute predefined procedures in response to precursor events such as abnormal process parameter fluctuations, equipment malfunctions, or unusual system behavior. These procedures may include isolating affected systems, implementing temporary operational changes, or activating active defense measures.	Moderate	$	Moderate	AOO

5.2.7. Principle 7: Interdependency Evaluation

All systems exhibit interdependencies, both direct and indirect. While teams routinely assess risks posed by physical interdependencies in standard systems engineering processes, they often overlook how a cyber-attack or digital failure in an interconnected system could impact the system currently under design. When evaluating interdependencies from a cyber-informed perspective, it is crucial to review previously identified physical interdependency risks while considering whether a cyber-attack could exacerbate or intensify certain consequences more than a physically driven event. Are there functions within the interdependent system that operators typically cannot access yet could potentially cause adverse effects on our system if activated? Where might interdependent systems trigger command logic within the system under design? How might automation between these systems lead to cascading effects? Similarly, where might the system under design unexpectedly influence interconnected systems?

Example of Interdependency Evaluation for BESS in Utility Operations:

Communication Infrastructure:

- This system necessitates communication links with adequate bandwidth and low latency to multiple locations.
- Some physical locations currently lack continuous network connectivity.
- Certain logical locations, currently external to the utility, may not be in use today but will be essential for accessing new value streams in the future.

Vendor Support Requirements:

- Vendor support is essential for significant changes and adjustments to the microgrid, both as a system and its individual components.
- Some vendors may require or prefer a continuous connection to the system for routine troubleshooting and calibration during its initial operation.
- Many vendors are expected to mandate interactive remote access as a warranty condition for their components.

Table 12 details a sample mitigation for interdependency evaluation.

Table 12: Sample Mitigation, Score for Interdependency Evaluation for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Identify backup sources for critical inputs to ensure continuity of operations in case of disruptions and establish protocols for rapid switching between the primary and alternative sources.	High	$	Moderate	AOO

5.2.8. Principle 8: Digital Asset Awareness

The digitization of energy infrastructure offers significant advantages, enabling faster and more automated operations than previously possible. However, digital assets and functions present unique vulnerabilities and modes of fragility compared to their analog counterparts. Beyond susceptibility to attacks, these assets can behave differently from analog systems, necessitating careful consideration of cybersecurity measures. Digital asset awareness starts during the design phase by recognizing that any digital device essentially functions as a general-purpose computer with specific command logic layered on top. This architecture can be exploited by attackers or affected by logic failures, potentially causing the device to ignore inputs, alter command logic, or execute commands unexpectedly. Early consideration of these risks allows for the implementation of robust controls that are not solely reliant on digital defenses.

During operations, digital devices require specific maintenance practices such as regular patching, upgrades, and the logging and exporting of commands and system data. It is crucial to maintain a comprehensive inventory of devices by hardware model, software version, patch level, location, update history, and operational function. Exporting and retaining logs for forensic purposes and maintaining a gold disk configuration of the latest software and logic ensure a clear understanding of system status, ongoing operations, maintenance requirements, and identified vulnerabilities. This approach also guarantees the ability to restore or replace systems as necessary.

Example of Digital Asset Awareness for BESS in Utility Operations:

- The BESS project will include new servers, endpoints, and supporting networking switchgear.
    - Some of the communications between endpoints are new, and the team has not thought through all the desired functions that communications complexity could cause.
- Some existing systems may need to be changed and upgraded (configuration and physical).

    - Some of these changes will involve trading out analog systems for digital ones.
- The BESS will bring some new operations and will interface with existing distribution automation and fleet operations.
    - This will allow some BESS to continue to provide uninterrupted service through different outage scenarios.
    - It would also allow an adversary to use those same built-in capabilities to make a switching sequence that would be undesired, dangerous, or damage equipment by repeatedly closing into faults. This could cause larger outages or worse.

Table 13 details sample mitigation for digital asset awareness.

Table 13: Sample Mitigation, Score for Digital Asset Awareness for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Documentation about the system should include the following elements reliant on digital devices: critical monitoring and control functions, operations requiring precise data acquisition and analysis, and maintenance tasks that are facilitated or enhanced by digital systems.	High	$	Easy	AOO

5.2.9. Principle 9: Cyber-Secure Supply Chain Controls

During the early design phases, engineers can establish core security features and assumptions that all suppliers must adhere to when providing components or services for the system. These guidelines may specify required features for digital systems, restrictions on their acquisition, and protocols for verifying and signing updates. They also encompass vendor practices for onsite and remote maintenance, as well as requirements for sharing information on cyber incidents, vulnerabilities, bills of materials, and vendor development processes. Each control contributes to the overall security of the supply chain.

These requirements should be discussed with stakeholders responsible for their enforcement, including procurement, cybersecurity, and system operators. For each control, considerations should include verification methods, frequency, and responsible parties (e.g., procurement, cybersecurity, operators). These processes must be integrated into system development and operation requirements, with multiple verifications scheduled for controls susceptible to change over time. While these engineering controls align with the organization's purchasing and cybersecurity processes, they are designed to address potential catastrophic system consequences and may exceed general due diligence practices.

Example of Secure Supply Chain for BESS in Utility Operations:

Vendor Selection and Management:

- Consider potential vendors who are new to our organization and potentially nondomestic.
- Implement rigorous supply chain vetting practices before final selection.
- Minimize vendor dependency on maintaining a mix of house-created code and integrated software/hardware components.

Support and Access Management:

- Specify in contracts to restrict the vendor's attempt to require onsite and remote support post-installation. Ensure this is clearly outlined and provide training for domestic solution providers.
- Manage and validate the removal of remote access for external parties.

Comprehensive Procurement and Risk Management:

- Ensure procurement requirements and service contract terms comprehensively cover warranty terms and assess inherent risks, particularly associated with limited system access.

Table 14 details a sample mitigation for a secure supply chain in terms of the CIE framework.

Table 14: Sample Mitigation, Score for Secure Supply Chain for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
The organization has established criteria for identifying critical products and services, ensuring enhanced procurement scrutiny (e.g., vendor certification or qualifications, receipt inspection, etc.) for these items.	High	$	Easy	AOO

5.2.10. Principle 10: Planned Resilience

Resilience entails planning for various failure modes of a system, especially those associated with previously identified undesired consequences. Understanding these failure modes involves preparing to operate under reduced levels of performance or reliability. Diminished operating modes can be integrated into operational expectations for well-understood modes of operation. Each diminished operating mode should include plans detailing its triggers, operational procedures, and necessary adjustments to staff, systems, safety protocols, performance criteria, and other system conditions. Once integrated into the overall system operating modes, regular training, exercises, and performance assessments in these diminished modes are essential.

These resilient diminished operating modes should encompass scenarios such as digital failures or cyber-attacks. Critical systems should also address operations during anticipated cyber-attacks affecting system components, instances where data validity is uncertain, unreliable critical automation logic, or disruptions in core network connections or support services. Executing these modes typically involves collaboration between the operations team and cybersecurity counterparts, ensuring clarity on respective roles and responsibilities. Furthermore, considering these operating modes may necessitate system design adjustments to enable limited manual operation options during periods when digital systems are non-operational or deemed untrustworthy.

Planned resilience considerations should also encompass strategies for restoring untrusted systems to full functionality within the system's operational context. This includes defining operational steps required to regain trust and assessing the feasibility of restoring trust based on system or component functionalities.

Example of Planned Resilience for BESS in Utility Operations:

Operational Continuity of the BESS System:

- The BESS system must operate continuously, 24/7, indefinitely, and adapt to all environmental and operational conditions, including unforeseen ones.
- From the prioritized consequence list, are there specific adverse environmental or operational conditions for which diminished operating modes can be developed?
- Consider developing diminished operating modes with limited communication or restricted critical function support.

Table 15 details a sample mitigation for planned resilience in terms of the CIE framework.

Table 15: Sample Mitigation, Score for Planned Resilience for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Develop tailored incident response strategies for cyber threats, outlining procedures to adapt, recover, and restore critical system functions. Especially with the integration of CIE-engineered controls (Principle 2)	High	$$	Moderate	AOO

5.2.11. Principle 11: Engineering Information Control

From the initial design of a system to its retirement, a vast amount of information is generated. This includes details on system design, components, operational skills, performance, and maintenance procedures. This information, in adversarial hands, can inform on system weaknesses, existing component vulnerabilities, and even human targets to aid in planning their attack. Such information can be released during procurement processes, often shared via public release, to ensure an open and fair competitive process. Such information can be inadvertently released during procurement processes, often shared publicly to ensure fair competition. Job listings seeking specific technical skills may also inadvertently disclose system features or vulnerabilities. Additionally, news articles or success stories about a system's operational debut might include photos or details that are valuable to adversaries.

During the system design process, the engineering team should identify critical information that would be valuable to an adversary using a prioritized list of potential consequences. They can then develop administrative processes to protect this information, including:

- Determining who can access the information
- Preventing inadvertent duplication and sharing
- Removing access when necessary
- Reviewing and approving information releases
- Ensuring team members understand the sensitivity of the information they handle

Given that engineering systems can remain active for decades, it is essential to protect even the earliest design information throughout the system's life cycle.

Example of Engineering Information Control for BESS in Utility Operations:

Information Release During Procurement:

- The team must provide significant electrical, controls, and other sensitive design information to vendors during procurement.
- Vendors may involve subcontractors as part of their solutions team.
- The team seeks advice on incorporating information protection criteria into non-disclosure agreements (NDAs) during procurement to ensure that sensitive information remains under their control and is not copied or stored by vendors and subcontractors.

Publicity and Media Releases for the New Microgrid:

- Significant publicity and media coverage will accompany the completion of the new microgrid.
- Selected vendors will want to publicize their involvement and the scope of the project.
- Upon project completion, vendors will likely share details about the system and its benefits with future customers, as seen in similar case studies on their websites.
- The team's organization will also want to inform ratepayers about the benefits of the automation investment through news articles, both locally and on their website.
- How can the team ensure these information releases are controlled and that vendors do not disclose more information than appropriate?

Hiring Temporary Employees for the Upgrade:

- The team will likely hire temporary employees for the upgrade, some of whom may transition to permanent roles in the operations team.
- These employees will need specific technical skills, some of which are sensitive.
- Once temporary employees are released after the BESS implementation, it is crucial to ensure they do not retain copies of system information.

Request for Insights:

- What are the best practices for protecting our engineering information?

Table 16 details a sample mitigation for engineering information control in terms of the CIE framework.

Table 16: Sample Mitigation, Score for Engineering Information Control for BESS in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Establish mandatory reporting requirements for sensitive information and implement controls to prevent accidental or unnecessary disclosure. Conduct regular audits to ensure compliance with reporting protocols.	High	$	Easy	AOO

5.2.12. Principle 12: Organizational Culture

Shared beliefs, perspectives, and values about cybersecurity determine how a group will prioritize investments and actions to improve its realization. There is not a desire to invest in people, processes, and technology to provide cybersecurity for a culture that does not value risk management, viewed as an unnecessary expense, low risk or impact, or an impediment to productivity. An engineering design team, cognizant of the consequences of digital failure or cyber-attack on a system under design, has a fundamental responsibility to aid stakeholders. This includes those who are accountable and responsible

or who have consulted or informed regarding the system so they may understand the need for cybersecurity and how each stakeholder's role can affect, both positively and negatively, the overall security of the system. Proactive measures include removing workarounds and discussing the changes made because of the potential vendor threat. Additionally, communication with leadership surrounding the additional requirements in place for FEOC battery systems is necessary.

Example of Cybersecurity Culture for BESS in Utility Operations:

Behavioral Changes for the Upgrade:

- This upgrade will necessitate different behaviors from leaders, managers, and workers across various roles, including procurement, human resources (HR), IT, and plant operations teams.
- An all-hands meeting will be conducted to inform the team about the overall approach to engineering security, although this overview may not suffice.
- It is essential to identify and promote positive individual behaviors and organizational choices related to the microgrid project and its infrastructure.
- How can the team ensure new hires receive the same level of acculturation?

Secure-by-Design Approach:

- Leadership accepts a Secure-by-Design approach but may reconsider if delays or additional expenses are perceived to be caused by this approach.
- How can the team help leadership understand and appreciate the long-term value of cybersecurity?

Table 17 details a sample mitigation for organizational culture in terms of the CIE framework.

Table 17: Sample mitigation score for BESS organizational culture in CIE Framework.

Mitigation	Score	Cost	Difficulty	Vendor or AOO
Implement reward systems and recognition programs to reinforce behaviors and choices that promote security outcomes, fostering a culture of proactive risk management and compliance.	High	$$	Easy	AOO

6. SUMMARY AND CONCLUSIONS

In summary, this report presents a detailed roadmap for enhancing BESS and integrated system cybersecurity using the cyber-informed engineering methodology. This process is intended to address

battery supply chain risks and the complex interplay between energy security and sustainable energy transition within the U.S. The key findings can be encapsulated as follows:

1. **Cybersecurity Integration**: Adopting CIE methodologies is essential for embedding engineering considerations for cybersecurity in the battery systems lifecycle from design through operation.
2. **Consequence-Based Prioritization:** Using a modular consequence-based assessment framework to prioritize supply chain components can influence strategic manufacturing and security decisions.
3. **Recommendations for Resilience:** Targeting immediate and long-term mitigation strategies to address supply chain vulnerabilities through a set of strategic initiatives is proposed. These initiatives were evaluated against their cost implications and potential to enhance security.

These recommendations are informed by technical analysis and aim to guide strategic decision-making in strengthening the resilience and security of the battery supply chain. Future efforts should continue to integrate and refine these findings, leveraging CIE principles to analyze the BESS to adapt to changing conditions and emerging threats. For a much larger collection of possible CIE control mitigations, please contact the Idaho National Laboratory's CIE group by emailing cie@inl.gov.

Page intentionally left blank

7. REFERENCES

[1] U.S. Energy Information Administration, "Energy Storage for Electricity Generation," Aug. 28, 2023. [Online]. Available: https://www.eia.gov/energyexplained/electricity/energy-storage-for-electricity-generation.php. [Accessed: Dec. 16, 2024].

[2] U.S. DOE Office of Manufacturing and Energy Supply Chains, "Interpretation of Foreign Entity of Concern," U.S. Department of Energy, May 6, 2024. [Online]. Available: https://www.energy.gov/articles/doe-releases-final-interpretive-guidance-definition-foreign-entity-concern. [Accessed: Dec. 16, 2024].

[3] Martina, Michael. 2024. "Exclusive: Duke Energy to Remove Chinese Battery Giant CATL from Marine Corps Base." *Reuters.* February 9. https://www.reuters.com/business/energy/duke-energy-remove-chinese-battery-giant-catl-marine-corps-base-2024-02-09/. [Accessed: Dec. 16, 2024].

[4]International Energy Agency. 2024. "Batteries and Secure Energy Transitions: Executive Summary." *IEA,* Paris. https://www.iea.org/reports/batteries-and-secure-energy-transitions/executive-summary. [Accessed: Dec. 13, 2024].

[5] White & Case LLP, "New Details on Section 30D Clean Vehicle Tax Credits: Foreign Entity of Concern Restrictions," Aug. 17, 2023. [Online]. Available: https://www.whitecase.com/insight-alert/new-details-section-30d-clean-vehicle-tax-credits-foreign-entity-concern-restrictions. [Accessed: Dec. 16, 2024].

[6] H.R. 2670, 118th Congress, 2023. [Online]. Available: https://www.congress.gov/bill/118th-congress/house-bill/2670. [Accessed: Dec. 16, 2024].

[7] Jenkinson, O. 2023. "Russian 'spy ship' filmed by Danish crew amid wind farm sabotage fears." *WindPower Monthly*. April 19, 2023. https://www.windpowermonthly.com/article/1820151/russian-spy-ship-filmed-danish-crew-amid-wind-farm-sabotage-fears. [Accessed: Dec. 16, 2024].

[8] Center for Strategic and International Studies. 2023. "Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario." *CSIS.* August 11, 2023. https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario. [Accessed: Dec. 16, 2024].

[9] Petkauskas, Vilius. 2022. "Deutsche Windtechnik hit with a cyberattack, a third on Germany's wind energy sector." *Cybernews.* April 27. https://cybernews.com/news/deutsche-windtechnik-hit-with-a-cyberattack-a-third-on-germanys-wind-energy-sector/. [Accessed: Dec. 16, 2024].

[10] Misbrener, K. 2023. "UL and NREL Release New Solar Inverter Cybersecurity Standard." *Solar Power World.* April 18. https://www.solarpowerworldonline.com/2023/04/ul-and-nrel-release-new-solar-inverter-cybersecurity-standard/. [Accessed: Dec. 16, 2024].

[11] IEEE Standards Association. 2023. *IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems.* December 11. https://standards.ieee.org/ieee/1547.3/10173/. [Accessed: Dec. 16, 2024].

[12] North American Electric Reliability Corporation (NERC). 2024. *NERC Launches IBR Registration Initiative Resources to Highlight Progress and Keep Stakeholders Informed.* February 29. https://www.nerc.com/news/Pages/NERC-Launches-IBR-Registration-Initiative-Resources-to-Highlight-Progress-and-Keep-Stakeholders-Informed.aspx. [Accessed: Dec. 16, 2024].

[13] U.S. DOE Office of Cybersecurity, Energy Security, and Emergency Response. Upcoming. "Battery Energy Storage Systems Report." 2025.

[14] The White House. 2024. "A Guidebook to the Bipartisan Infrastructure Law." Last updated January, 2024. https://whitehouse.gov/build/guidebook/. [Accessed: Dec. 16, 2024].

[15] Greening the Grid. n.d. *Grid services and value-stacking. U.S. Agency for International Development.* https://greeningthegrid.org/energy-storage-toolkit/topics-resources/grid-services-and-value-stacking. [Accessed: Dec. 16, 2024].

[16] U.S. DOE Office of Energy Efficiency and Renewable Energy. N.d. "Solar Cybersecurity Basics." *U.S. Department of Energy*. Accessed December 13, 2024. https://www.energy.gov/eere/solar/solar-cybersecurity-basics. [Accessed: Dec. 16, 2024].

[17] Goel, S. and R. Sharma. 2017. "Performance evaluation of stand alone grid connected and hybrid renewable energy systems for rural application: A comparative review", *Renewable Sustain. Energy Rev.*, vol. 78, pp. 1378-1389. [Accessed: Dec. 16, 2024].

[18] Nadeau, J. 2024. "Third-party breaches top global energy companies." *Security Intelligence.* February 6, 2024. https://securityintelligence.com/articles/third-party-breaches-top-global-energy-companies/. [Accessed: Dec. 16, 2024].

[19] Fazzini, K. 2018. "Chinese spy chips are found in hardware used by Apple, Amazon, Bloomberg says; Apple, AWS say no way." *CNBC.* October 4, 2018. https://www.cnbc.com/2018/10/04/chinese-spy-chips-are-said-to-be-found-in-hardware-used-by-apple-amazon-apple-denies-the-bloomberg-businessweek-report.html. [Accessed: Dec. 16, 2024].

[20] Military News. 2012. "Proof that Military Chips from China are Infected." *Military Advantage.* May 30, 2012. https://www.military.com/defensetech/2012/05/30/smoking-gun-proof-that-military-chips-from-china-are-infected. [Accessed: Dec. 16, 2024].

[21] Lyngaas, S. 2019. "Utah renewables company was hit by rare cyberattack in March." Cyber Scoop. October 31. https://cyberscoop.com/spower-power-grid-cyberattack-foia. [Accessed: Dec. 16, 2024].

[22] Sobczak, B. 2019. "First-of-a-kind U.S. grid cyberattack hit wind, solar." Energy Wire. October 31. https://subscriber.politicopro.com/article/eenews/1061421301. [Accessed: Dec. 16, 2024].

[23] SektorCERT. 2023. "The Attack against Danish Critical Infrastructure. TLP-CLEAR." 2023. https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf. [Accessed: Dec. 16, 2024].

[24] Idaho National Laboratory, "CIEBAT," GitHub, 2023. [Online]. Available: https://github.com/idaholab/CIEBAT. [Accessed: 16-Jan-2025].

[25] Idaho National Laboratory, "CSDET Technical Assistance and Training," INL, 2023. [Online]. Available: https://inl.gov/csdet-technical-assistance-and-training/. [Accessed: 16-Jan-2025].

[26] Weaver, G., M. Culler, and E. Stewart. 2024. Organizational Influence on Supply Chain for Digital Energy Infrastructure: Business Models, and Policy Landscape." 2024 IEEE Trust Privacy and Security Conference. Washington, DC, United States. October 28-30, 2024. [Accessed: Dec. 16, 2024].

[27] Tesla, Inc. n.d. Tesla Owners Manual. Accessed April 24, 2024. https://www.tesla.com/ownersmanual. [Accessed: Dec. 16, 2024].

[28] Idaho National Laboratory, "CCE Phase 1-4 Reference Document," INL, July 2023. [Online]. Available: https://inl.gov/content/uploads/2023/07/CCE-Phase-1-4-Reference-Document.pdf. [Accessed: Dec. 17, 2024].

[29] North American Electric Reliability Corporation. 2023. *2023 State of Reliability Technical Assessment (NERC).* June. https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2023_Technical_Assessment.pdf. [Accessed: Dec. 16, 2024].

[30] North American Electric Reliability Corporation (NERC). 2023. *2022 California Battery Energy Storage System Disturbances.* September. https://www.nerc.com/comm/RSTC/Documents/NERC_BESS_Disturbance_Report_2023.pdf. [Accessed: Dec. 16, 2024].

[31] Idaho National Laboratory, "CCE Phase 1-4 Reference Document," INL, July 2023. [Online]. Available: https://inl.gov/content/uploads/2023/07/CCE-Phase-1-4-Reference-Document.pdf. [Accessed: Dec. 17, 2024].

[32] NIST, "Guide to Industrial Control Systems (ICS) Security," Initial Public Draft, NIST Special Publication 800-82 Revision 3, Aug. 2022. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/82/r3/ipd. [Accessed: Dec. 16, 2024].

[33] IEEE Standard 1547.3-2007, "IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems," Apr. 2007. [Online]. Available: https://standards.ieee.org/ieee/1547.3/10173/. [Accessed: Dec. 16, 2024].

[34] International Society of Automation (ISA), "ISA/IEC 62443 Series of Standards," [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed: Dec. 16, 2024].

[35] U.S. Department of Justice. n.d. *The Objective of the CONOPS.* https://www.justice.gov/archive/jmd/irm/lifecycle/appendixc9.htm. [Accessed: Dec. 16, 2024].