DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express 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. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

Cyber-Informed Engineering

CIE Analysis Process for Engineered Systems

September 19, 2025

Authors:

Ben Lampe
Idaho National Laboratory

Andrew Ohrt
West Yost Associates

Jeremy Smith
West Yost Associates

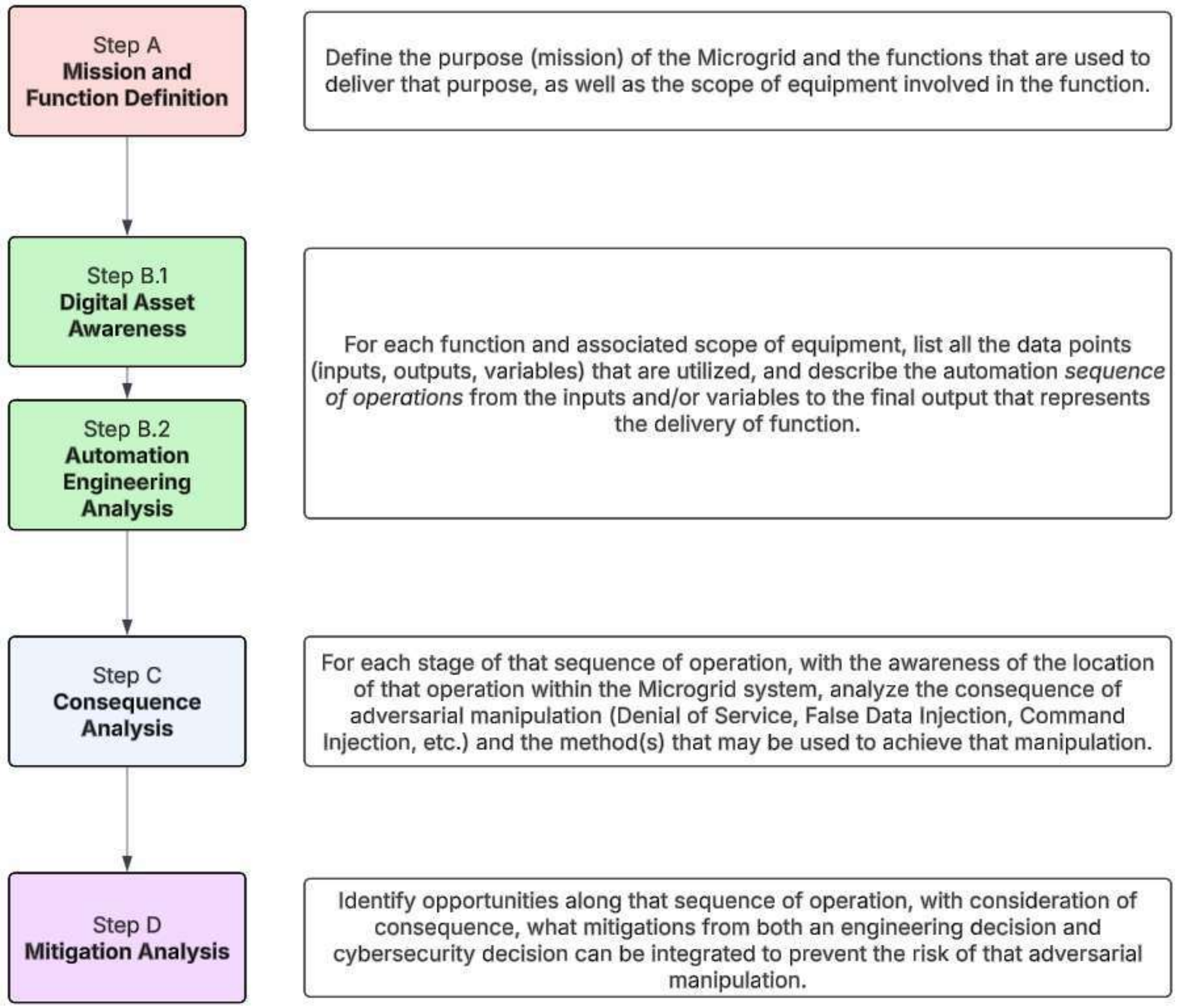
Cyber-Informed Engineering (CIE) Program activities are sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) and performed by Idaho National Laboratory and the National Renewable Energy Laboratory.

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, trademark, 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.

Contents

Process



Step A **Mission and Function Definition**

Define the purpose (mission) of the Microgrid and the functions that are used to deliver that purpose, as well as the scope of equipment involved in the function.

Step B.1 **Digital Asset Awareness**

Step B.2 **Automation Engineering Analysis**

For each function and associated scope of equipment, list all the data points (inputs, outputs, variables) that are utilized, and describe the automation *sequence of operations* from the inputs and/or variables to the final output that represents the delivery of function.

Step C **Consequence Analysis**

For each stage of that sequence of operation, with the awareness of the location of that operation within the Microgrid system, analyze the consequence of adversarial manipulation (Denial of Service, False Data Injection, Command Injection, etc.) and the method(s) that may be used to achieve that manipulation.

Step D **Mitigation Analysis**

Identify opportunities along that sequence of operation, with consideration of consequence, what mitigations from both an engineering decision and cybersecurity decision can be integrated to prevent the risk of that adversarial manipulation.

This process describes how to integrate the CIE principles into an engineered system that is being conceptualized or a system that is already deployed to achieve a cyber-informed decision. For new systems that are being conceptualized this produces new functional security requirements that will guide the official design or design implementations to guide the actual building and commissioning activities. For already existing systems that are assessed for digital risk, this produces new opportunities to retrofit the current implementation to mitigate newly realized digital risk from newly identified vulnerabilities or new upgrades added to the system. This process is the basis of current CIE Analysis tools: CIE Microgrid Analysis Tool (CIEMAT)[1] and CIE Battery Analysis Tool (CIEBAT).[2]

To capture the results of this analysis, you can use excel (see CIEMAT/CIEBAT) or a control narrative-style word document. For a larger organizational-centric workflow to address organizational practices and active defense as an organization for these engineered systems, please refer to this resource: Integrating CIE into Enterprise Risk Management[3].

For each step in this process, the use of identified CIE Questions draws out the expected contents. The next section breaks out each Step into an expanded definition and examples.

Document System and Components for Application to Integrated Design

Owners and application engineering teams require documentation to protect functions. To apply CIE principles, owners and engineers use documentation of the following components and functions from original equipment manufacturers (OEM) and package systems:

- Mechanical and electrical systems that provide, support, or protect functions. Though typically part of most manufacturer O&M documents, any modifications or optional configurations should be described so the owner can evaluate the impact to their mission.

- Programmable components should be cataloged along with all interfaces, update method, and options for protection and recovery. If documentation of programmable components includes information from the subassembly manufacturer, all options or modifications implemented should be described. This includes back-up copies deployed programming.

- Networkable components must be cataloged, even if an interface or media is not utilized or physically disabled. If documentation of network components includes information from the subassembly manufacturer, all options or modifications implemented should be described. This must include back-up copies deployed programming.

[1] Idaholab, “Idaholab/CIEMAT: Cyber-Informed Engineering (CIE) Tool for Microgrid Resilience,” GitHub, https://github.com/idaholab/CIEMAT.
[2] Idaholab, “Idaholab/CIEBAT: Cyber-Informed Engineering (CIE) Tool for Battery Energy Storage System Analysis,” GitHub, https://github.com/idaholab/CIEBAT.
[3] Andrew Ohrt et al., “Integrating Cyber-Informed Engineering into Enterprise Risk Management,” (Technical Report) | OSTI.GOV, September 30, 2024, https://www.osti.gov/biblio/2480935.

Using the documentation of mechanical, electrical, programmable, and network components owner/engineer stakeholders apply Steps A through D of the CIE analysis process as follows:

1. **Mission and Function Definition (Step A)**
    - Define the overall purpose (mission) of the Microgrid.
    - Identify the functions and scope of equipment that the microgrid supports and that support the microgrid.
2. **Digital Asset & Automation Analysis (Step B)**
    - **B.1 Digital Asset Awareness:** List all data points (inputs, outputs, variables) for each function and equipment. This includes data points *external* to the microgrid.
    - **B.2 Automation Engineering Analysis:** Describe the automation sequence of microgrid, including inputs/variables with *external systems*.
3. **Consequence Analysis (Step C)**
    - For each step in the sequence, analyze the consequences of potential adversarial manipulation of the microgrid to external system and owner critical functions.
    - Identify how such manipulations could be achieved, including vectors to and from owner equipment separate from microgrid components.
4. **Mitigation Analysis (Step D)**
    - Identify opportunities to mitigate risks, considering both engineering and cybersecurity options that may be external to microgrid components.
    - Integrate measures that prevent or limit adversarial manipulation weighing desired features against acceptable level of risk to critical functions beyond the microgrid.

Application of this process defines the system's (i.e., microgrid, battery energy storage system, etc.) purpose, maps its digital assets and automation flows, analyzes potential cyberattack consequences, produces engineering controls, and develops cybersecurity mitigations.

A detailed description and example analysis of Steps A through D is provided below. This includes:

- Example output of each step, specific to a microgrid application
- CIE questions to facilitate analysis
- Considerations from the owner/engineer perspective

For the owner/engineer application of microgrid technology, the considerations will refer to *Figure 2 – Microgrid Network Schematic* which describes a facilities' networkable and programable components. The variable frequency drives (VFD) and associated motors are shown to represent typical loads. The controls and network architecture depicted has already been optimized based CIE principles.

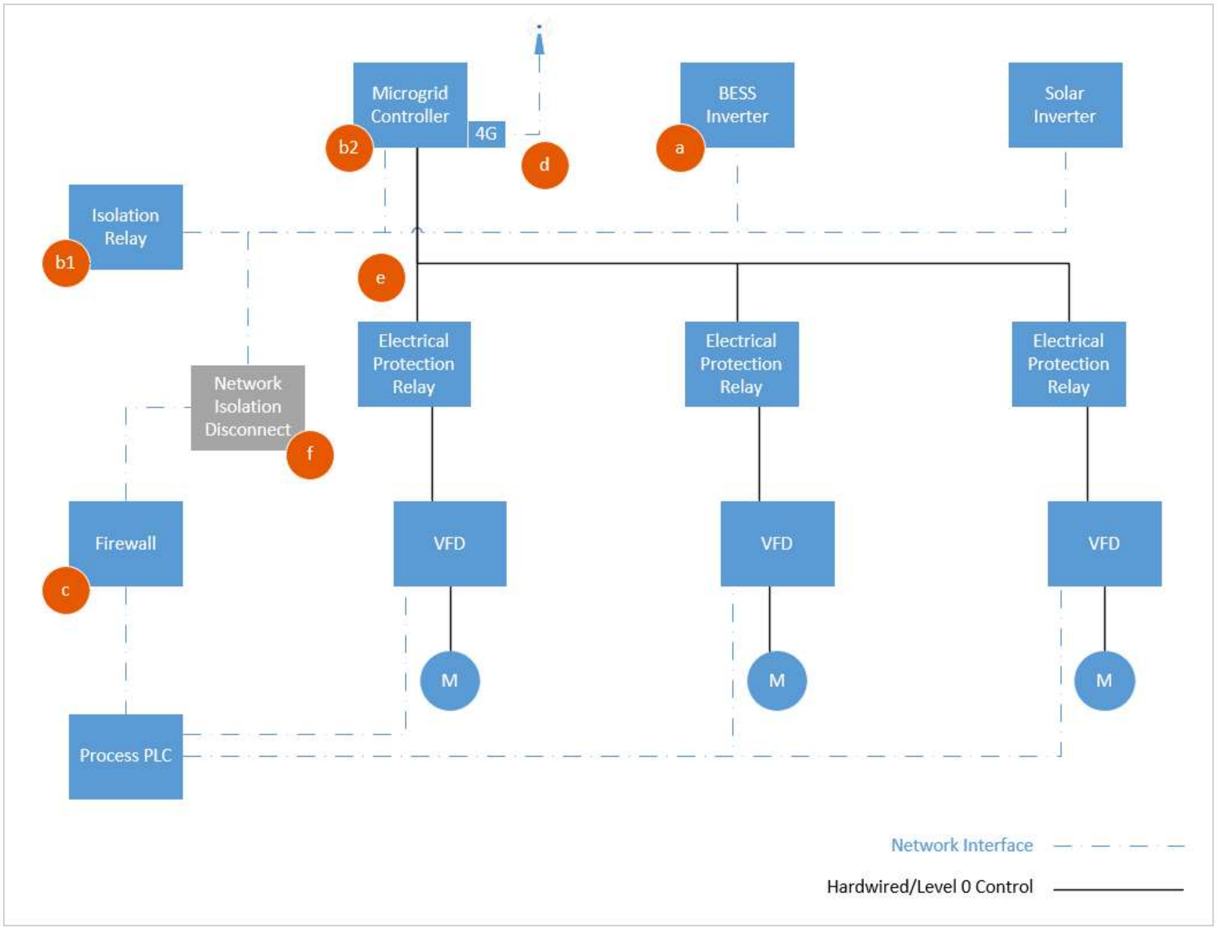

Microgrid Controller
4G
BESS Inverter
Solar Inverter
b2
d
a
Isolation Relay
b1
e
Electrical Protection Relay
Electrical Protection Relay
Electrical Protection Relay
Network Isolation Disconnect
f
Firewall
c
VFD
VFD
VFD
M
M
M
Process PLC
Network Interface
Hardwired/Level 0 Control

Figure 2 – Microgrid Network Schematic

Step A Mission and Function Definition

Define the Purpose *of the Engineered System*

The purpose of the Engineered System defines the mission that the engineered system is intended to fulfill. This purpose justifies the construction and specific location of the Engineered System. For example, in a Microgrid system, typical purposes include voltage and frequency regulation for grid stability, peak shaving, load following, spinning reserve for economic dispatching, provision of backup power, formation of island grids, and black starting during power loss events.

Example Answer: The purpose of this Microgrid is to provide backup power delivery during utility (grid) power outages for a residential subdivision.

Define the Functions *that are used to deliver that purpose*

A function refers to a set of actions executed to achieve the purpose of the Engineered System. It serves as the initial level of decomposition from the overall purpose into specific areas of activity. For example, in the context of Microgrid control systems, performance functions describe key decisions that are orchestrated to facilitate the purpose and include items such as controlling the transition between grid-connected and island modes, dispatching energy, and managing loads within the Microgrid's power delivery area. Other functions in the Microgrid control systems have a supporting nature (i.e., safety, etc.) and often are used across many other function types. Examples of supporting functions may include items such as thermal management, and energy management. Other function types may be described by an organization, but all function descriptions are expected to be further decomposed into a set of automation steps (a.k.a., Sequence of Operation) that will describe how they are orchestrated within the scope of equipment.

CIE QUESTIONS:

1. What are the mission-critical functions this system is required to perform?

Example: Three performance functions and two supporting functions used by the Microgrid to provide backup power are in scope of this analysis: The three performance functions are Planned Seamless Islanding, Unplanned Seamless Islanding, and Managing Loads, and the two supporting functions are thermal management and state of charge management.

NOTE: NEMA US 80056-2024[4] provides key examples of Microgrid performance functions that support the overall purpose of this engineered system's location. This resource includes insights into Key Performance Indicators (KPIs) and requirements for each function.

OWNER/ENGINEER (IMPLEMENTERS) APPLICATION CONSIDERATIONS:

1. Can the functions be ranked as primary, second, or tertiary based on their benefit or risk?

Example: The performance function of Unplanned Seamless Islanding may be more critical than Planned Seamless Islanding. In this scenario, avoiding equipment restart on transition to/from utility power is more important than power costs. Applying these priorities, the microgrid specification and configuration should focus on inverter sizing (Figure 2, Part-a) and real time performance. Maintaining continuous operations provides the primary basis

[4] "Microgrid Controller Performance," NEMA, https://www.nema.org/standards/view/microgrid-controller-performance.

for sizing of onsite power generation and storage. Cost mitigations such as time-of-use (TOU) would be secondary.

Define the Scope of Equipment *involved in the function*

The scope of equipment refers to the collection of equipment that contributes to the successful execution of the function under analysis. All functions may share the same scope of equipment, or a single function may involve a distinct set of equipment compared to other functions. The depth of the scope under consideration is determined by the analysis team. Greater depth provides more comprehensive insights but also requires additional analysis time.

CIE QUESTIONS:

1. What parts of the design contains digital components or subcomponents?
2. What areas of the system design are most linked to high impact consequences?

Example: The operation of Unplanned Seamless Islanding involves the Battery Meter, the Battery Controller, Battery Management System, Battery Packs, Battery Cells within those Packs, and the Smart Inverter.

OWNER/ENGINEER APPLICATION CONSIDERATIONS:

1. What components outside the microgrid support these primary functions?
2. How do the system components and facility components interface for these functions? Does the system specification and configuration align to these functions?

Example: Focusing on the Unplanned Seamless Islanding priority, does the microgrid rely on a facility, system, or component to accomplish power transfer? This could include coordination with a power meter, relay, generation source, or facility control system (PLC, software, or network). Based on Figure 2, Part b1 and Figure 2, Part b2, the microgrid controller and dedicated isolation relay accomplish the islanding function separate from the process equipment or PLC.

Step B Digital Asset Awareness and Automation Engineering Analysis

Define the Information Model *for each function and scope of equipment considered for analysis, list the data points that are used*.

Data points are the inputs, internal variables (such as setpoints or calculation results), and outputs used to deliver the function under consideration. Each data point exists in one or more pieces of equipment. When data points are communicated between equipment, they are outputs in the source equipment and inputs in the destination equipment. If a data point undergoes no operations (i.e., calculations, logical checks, etc.) in a piece of equipment, it can be considered both an internal variable and a communicated output or input (a.k.a., pass-through data). For example, a setpoint in a Distributed Energy Resource Management System (DERMS) human-machine interface (HMI), which is then communicated directly to a Battery Controller, would be an input, stored as an internal variable, and subsequently communicated as an output to the Battery Controller.

Similar to the scope of equipment, the depth of data point identification affects the analysis depth and time required. At a minimum, allow engineers to prioritize the most import data points in the function under consideration to keep scope limited as applicable. Adequate depth is necessary for thorough analysis preparation. Examples of data point identification include Point Schedules in Building Automation projects and Tag Lists in other automation projects.

CIE QUESTIONS:

1. What fundamental physics or energy sources, such as voltage, pressure, heat, and potential energy, will be involved in this system? (This informs the types of data points often maintained in a system to monitor and control these physics/sources.)
2. For each of the process steps, what are the core inputs, outputs, mechanisms (people, tools, systems) and controls (safety standards, regulations, requirements)?
3. How are digital assets used to meet system requirements?

Example: A list of data points used in this function and scope of equipment.

Name	Description	Units	Equipment
Total Charge Power	*Maximum Charge Power*	*W*	*Battery Controller, BMS*
Battery Temperature	*Active Battery Module Temperature*	*Celsius*	*BMS, Battery Module*
Max Battery Temperature Setpoint	*Temperature Setpoint Threshold*	*Celsius*	*BMS, Battery Module*
…	*…*	*…*	*…*

OWNER/ENGINEER APPLICATION CONSIDERATIONS:

1. Beside the primary functions (Step A considerations), what components outside the system support functions that provide secondary or tertiary benefits?

2. How do the system components and facility components interface for these other

functions?

Example: Planned Seamless Islanding relies on more interfaces to facility equipment to provide a broad range of benefits. The microgrid provides solar generation and battery condition to the facility control system. The facility control system provides information critical loads, loads available for load shedding, and status of backup generators.

Describe the Sequence of Operation *for that function*.

The Sequence of Operation outlines the step-by-step process and logic required to perform the actions that define the function under consideration. This sequence specifies the order of operations, conditions for transitioning between operations, and interactions between the different data points used in specific operations. Each of these characteristics describes the delivery of the function. The Sequence of Operation provides awareness of where in the scope of equipment a given operation occurs. Furthermore, a description for each operation provides sufficient context to understand the sequence's functionality and enables stakeholders to begin identifying potential risks, consequences, and mitigation opportunities.

When documenting these Sequences of Operation, it is essential to balance the depth of detail provided. While a comprehensive understanding of each step is valuable, the primary objective is to offer a clear description rather than exhaustive logical proof of the sequence. This approach ensures that the focus remains on setting up the discussion for consequence and mitigation analysis in subsequent steps. Delving too deeply into logical intricacies can be counterproductive and time-consuming, as it may obscure the broader picture and delay the analysis process. Therefore, maintaining a balance between depth and clarity is crucial. This balance ensures that the Sequence of Operation remains a practical tool for guiding further analysis and decision-making, rather than becoming an overly complex and cumbersome depiction.

CIE QUESTIONS:

1. How do the various subsystems communicate with each other?
2. What are the expected system states?
3. How are components linked to others? What network interdependencies exist and how/where are they clearly mapped?
4. How are digital assets used to meet system requirements?
5. How is the system designed to perform each of its critical functions?

Example: The following statements represent a sequence of operation within a Battery Energy Storage System example.

The Temperature sensor senses the value for ‘Battery Temperature’ in the Battery Module communicates ‘Battery Temperature’ to the BMS as a 4-20mA raw electrical signal.

BMS receives the value ‘Battery Temperature’ and stores the value in its memory for use in the following calculation: If ‘Battery Temperature’ is greater than ‘Max Battery Temperature Setpoint’, then communicate a ‘Disconnect Battery Module’ command to Battery Module as a raw 12VDC relay signal. BMS communicates a new ‘Total Power Charge’ value to the Battery Controller with a network connection via the local ethernet switch.

The local ethernet switch switches the traffic between the BMS, Battery Controller, and local Human Machine Interface (HMI) for the Battery System. Additionally, the local ethernet switch provides an uplink to the Site network switch.

Battery Module receives the ‘Disconnect’ signal and actuates the contactor connecting the Battery Module to the DC Bus. The string of Battery Cells within that Module are removed from the overall potential power delivery.

OWNER/ENGINEER APPLICATION CONSIDERATIONS:

1. How do the system and facility control system coordinate to accomplish a the function (e.g., Planned Seamless Islanding transfer in a Microgrid)?

Example: The microgrid indicates sufficient solar generation and battery condition to accommodate a time-of-use based transfer.

After transfer to islanding, a battery train encounters a fault. Although the island is maintained, the is insufficient capacity for the duration of the time-of-use period. indicates a state of change or health issue.

In Figure 2, Part c, the firewall provides for secure communications between the microgrid and process network.

Step C Consequence Analysis

Analyze the Consequence of Adversarial Manipulation *for each stage of the Sequence of Operation*

Analyzing the consequence of adversarial manipulation involves systematically evaluating each stage of the Sequence of Operation to identify and assess the causal effect of data point manipulation that could be exploited by a malicious actor. This type of manipulation can take various forms, including denial of service (DoS), which disrupts the communication of data points to prevent the data from reaching the next step; false data injection, which introduces incorrect data values as inputs, causing an erroneous outcome from the step; command injection, which alters outputs from a step so that the next step receives and executes unintended equipment states; and corrupted calculations or operations themselves, which compromises the integrity of calculations or operations, leading to incorrect transformations of data points despite accurate inputted data points.

This analysis is engineering-centric and involves an examination of how these manipulations could impact the output of the overall function or specific steps of the Sequence of Operation. For each step or set of steps of the Sequence of Operation, engineers identify the potential consequences of such adversarial actions. This includes assessing the impact on system performance, determining if the manipulation could lead to safety impacts, such as endangering human lives, evaluating the loss of reliability in the equipment such as unrecoverable equipment damage resulting from a battery fire or other catastrophic failures or prolonged outages and the inability to restore normal operations promptly.

By tagging consequence analysis descriptions that lead to unacceptable impacts, such as life safety risks or severe equipment damage, this analysis helps prioritize mitigation opportunities not previously considered through the normal process of engineering. The goal is to ensure that the system remains resilient against adversarial manipulation, maintaining both safety and operational performance and reliability.

It is important to note that the level of effort required for performing this analysis can be substantial. Therefore, it is essential to consider what is reasonable and practical within the constraints of available resources and time. A balanced approach should be taken to ensure thoroughness without becoming overly exhaustive. The use of quick descriptions demonstrating engineering analysis often contains sufficient detail for future mitigation analysis on only the critical areas where the impact of adversarial manipulation would be most detrimental.

CIE QUESTIONS:

1. What are the consequences that could result from a failure or unexpected operation of the system's critical functions?
2. What impacts could there be to mission delivery, safety, security, the environment, equipment and property, financials, or corporate reputation?
3. What are the limits of acceptable degradation for these parameters and sequences?
4. What deviations from expected system states and anomalies might be initial indicators of consequence?
5. How might loss or instability in this equipment or the connectivity between system elements/parameters lead to consequence?
6. How would a failure of this equipment affect the service?
7. What potential cascading failures may need to be accounted for?

Example: For the sequence step at the BMS that does the comparison between 'Battery Temperature' and 'Max Battery Temperature Setpoint', if an adversary moves the setpoint below common operating temperatures, it would cause increased disconnections of the Battery Module(s), prevent the battery system from having sufficient 'Total Power Charge' if the battery system needs to supply backup power. Operational Impact and loss of service. If an adversary moves the setpoint substantially higher than normal, the battery system if heating up due to other adversarial action or during high-stress seasons, like middle of summer, could degrade the quality of the battery cells, leading to loss of performance and life of the battery itself. Also prevents the battery from disconnecting which contributes to an increased risk of thermal runaway and unrecoverable equipment damage.

OWNER/ENGINEER APPLICATION CONSIDERATIONS:

1. Does the facility control system or its integration to the system increase or decrease the risk of negative consequences?

Example: Additional integration with the facility control system is required to enable supporting features including coordination of Planned Seamless Islanding transfers.

This additional integration with facility systems could allow the adversarial manipulation to coordinate the timing the exploits with other sensitive facility operations, including load shedding or equipment rotations.

Analyze the Method(s) of Compromise *that may be used to achieve that manipulation (OPTIONAL)*

Analyzing the methods that may be used to achieve adversarial manipulation involves identifying and evaluating the techniques and tactics that malicious actors could employ to compromise the system. This part of the analysis is cybersecurity-centric and focuses on understanding how specific attacks could be executed to disrupt the step(s) in the Sequence of Operation at a given equipment. For instance, supplying faulty firmware can lead to faulty operation logic or command injection, where the manipulated firmware causes the sequence step to execute incorrect data point outputs. Similarly, a network denial of service (DoS) attack can disrupt the data point communication between sequence steps.

By mapping out these methods, the analysis provides a view of the potential attack vectors and their implications. Sensitivity to detail should be applied to the steps where engineering has mapped consequential impacts. Ensuring that this analysis is aligned with the engineering-mapped consequential impacts helps prioritize efforts on the most critical steps in the Sequence of Operation.

Just like with the engineering analysis, it is important to note that the level of effort required for performing this analysis can be large. Therefore, it is essential to consider what is reasonable and practical within the constraints of available resources and time. A balanced approach should be taken to ensure thoroughness without becoming overly exhaustive. The use of quick descriptions describing adversarial tactics and techniques often contains sufficient detail for future mitigation analysis.

CIE QUESTIONS:

1. What would a cyber attack on this equipment require? What systems/equipment would an adversary need to access to create the specific effect?
2. How might an adversary need to traverse systems and subsystems in order to get access to this equipment?
3. What precursor events could occur leading up to consequence? How might adverse consequences manifest within this equipment, as conceptualized?
4. How might loss or instability in this equipment or the connectivity to other equipment lead to consequence?

Example: Cybersecurity Analysis: Adversary uses credential harvesting to gain a footprint on local battery network. Presence on the local network allows the adversary to reconfigure through an update routine on the BMS system to update the logic used by the BMS. The logic used contains the comparison calculation to allow the BMS to command when modules need to be connected or disconnected to maintain battery cell performance.

OWNER/ENGINEER APPLICATION CONSIDERATIONS:

1. Does the facility control system or its integration to the system increase or soften the attack surface?

Example: Additional integration with the facility control system required coordinate or trigger Planned Seamless Islanding transfers could include additional networked connections and programmable devices.

Without compromising the facility control system, a man-in-the-middle approach could be facilitated by sending or requesting invalid data from the microgrid or its components.

One potential vector for this attack is an external, foreign connection from the microgrid controller vendor at Figure 2, Part d.

Step D Mitigation Analysis

Identify Mitigation Opportunities *along each stage in the sequence of operation for an engineering and/or cybersecurity mitigation*

Identifying opportunities for engineering and cybersecurity mitigations involves pinpointing the specific steps within the Sequence of Operations where countermeasures can be applied to prevent or minimize the likelihood and impact of adversarial manipulation. This process focuses on those steps that have a relationship to unacceptable impacts, such as life safety risks or unrecoverable equipment damage.

Engineering mitigations, or engineered controls, include physical changes to the overall system and/or logical modifications to reduce the impact of adversarial action. Examples of engineering control opportunities are provided in the Mitigations tab found in CIEMAT[5]. Cybersecurity mitigations, or security controls, include implementing authentication and authorization mechanisms, employing encryption to protect data integrity and confidentiality during transmission, and deploying intrusion detection systems to identify and respond to suspicious activities, to reduce the exposure of the equipment to adversarial action.

By analyzing the steps in the Sequence of Operation, engineers and cybersecurity professionals can develop a list of mitigation opportunities that address cyber threats. To reduce the level of effort, this analysis should at a minimum prioritize steps where the impact of manipulation would be most detrimental.

CIE QUESTIONS:

1. Are analog or physical protections engineered into the system (where possible)? How dependent are the system's engineered controls on digital technologies?
2. What are the minimum functional capabilities needed? In concept, is there anything that is likely to be implemented via digital means that is not explicitly needed?
3. What specific controls (digital and otherwise) can ensure that the most critical data is available, valid, and secure?

   For each key data element, where must monitoring be in place to identify deviations from desired data states or settings? Is active monitoring

[5] Idaholab, "Idaholab/CIEMAT: The Cyber-Informed Engineering Microgrid Analysis Tool (CIEMAT) Can Inform Engineering and Traditional Cybersecurity Mitigations to Make Microgrid Site Installation More Resilient to Cyber Attack and Its Impact.," GitHub, https://github.com/idaholab/CIEMAT.

necessary, or is logging combined with a periodic manual review process sufficient? What data elements should be exposed for external monitoring to reveal potential process anomalies, provide process validation, and to validate security?

Example: Failure by the BMS to disconnect the module when needed for thermal protection could use an engineering control that provides a thermal detection mechanism, like a thermostat on or near the battery module, whose detection limit is +5-10 degrees higher than the 'Max Battery Temperature Setpoint'. When this thermostat triggers, it relays local control power within the cabinet to signal the contactor and disconnects the battery module. From a cybersecurity control perspective, eliminating the uplink from the local network switch to site network switch so that no direct physical path exists prevents remote management of the BMS directly. Or if required, ensure BMS has strong access control mechanisms like strong password complexity or multi-factor authentication.

OWNER/ENGINEER APPLICATION CONSIDERATIONS:

1. Are the risks associated with additional system integration to the facility control system acceptable?
2. Do supporting functions add possible negative consequences that could be controlled or mitigated, focusing only on enabling performance functions?

Example: Unplanned Seamless Islanding transfers can be accomplished without networked integration required by Planned Seamless Islanding transfers.

An owner may elect to only implement functions that can be supported with hardwired I/O and operator SOPs that can take the microgrid offline without special equipment or staff.

The owner/engineer associated with Figure 2 elected for additional supporting functions that relied on network integration. Therefore, the following mitigations were included:

- *Hardwired rather than network-controlled relays (Figure 2, Part e) to limit attack propagation from the microgrid*
- *An operator accessible network disconnect (Figure 2, Part f) to support an SOP to isolate and disable microgrid and operate only from utility power in the event of a compromise*

Turn Opportunities into Decisions

Translating mitigation opportunities into design and operational decisions involves taking the identified mitigation opportunities for both engineering and cybersecurity mitigations and formalizing them into actionable, concrete design requirements, specifications, or operational plans (i.e., SOPs, IR planning, etc.). Current safety equipment and cybersecurity best practices are expected in any existing engineered design, but these newly identified engineered control mitigation opportunities represent new decisions that enhance the system's security and resiliency beyond the information protection provided by traditional cybersecurity schemes. This is especially true if safety equipment is considered susceptible to adversarial manipulation due to its digital operations. These decisions can be articulated in two ways: new design requirements/specifications for future projects or actions to retrofit existing installations, contingent on budget constraints and risk acceptance.

CIE QUESTIONS:

1. What processes are in place to ensure system operators are aware of triggers to temporarily change operations in response to a perceived threat? What stakeholders should be notified if there is an active defensive threat or weakness to this system?
2. Do system requirements include a manual operation mode for any system that otherwise is controlled by an automated information system?
3. For services critical to the functionality of the system under design, what additional contract requirements, beyond the normal baseline, should be defined for security, performance, and verification relating to the desired services? What specific quality and security requirements apply to vendors/suppliers/service providers for critical system components and services?
4. Does the system's incident response plan contain a specific resilience focus and is there controls to ensure a fail-safe behavior?
5. What training, education, and practice will individuals and teams need to operate, maintain, secure, and defend the system throughout its lifecycle?

Example: Updates to the BESS design specification require the battery solution to include the out-of-band thermostat to be included in the contactor design between the Battery Module(s) and DC bus and temperature setpoint of thermostat must be set at a temperature 10 degrees higher than configured MAX temperature setpoint contained within the BMS system. Contracted Maintenance staff will also be trained and required to include inspection of thermostat setpoint as part of their seasonal cabinet inspections to ensure the setpoint is appropriate for the season and current BMS setpoint.

Conclusion

Completing this analysis and mitigation determination results in identifying a more holistic cybersecurity control scheme that provides functional assurance which is a higher order outcome than traditional cybersecurity security goals of information assurance. Providing functional assurance for the Engineered System's automation and control systems are only successful when the information contained within the Engineered System process is protected to reduce the exposure to cyber threats and any outcomes to adversarial actions are reduced or eliminated so that functions remain performant, safe, and reliable, which is the goal for any organization.

SAMPLE OWNER/ENGINEER ANALYSIS RESULT:

The following is an example that a typical owner/engineer may reach following the CIE analysis process steps:

> *Step A. Mission and Function Definition: The primary microgrid purpose is to supplement or replace the use of a gas-powered back-up generators. Additionally, the battery energy storage system, BESS, provides supplemental electrical power outside of utility electrical outages for peak power reduction.*
>
> *Step B.1 Digital Asset Awareness: The evaluation showed that BESS and inverters associated with solar power have digital components that cannot be fully integrated or monitored to manufacturer requirements.*
>
> *Step B.2 Automation Engineering Analysis: The microgrid should be disabled when the core function, to provide backup power, cannot be verified. The sequence of operations for the microgrid is to sense the incoming utility power, make sure it meets the required quality standards, and then if it deviates from those parameters, the battery storage system and solar together should supplement power or island to support continuous operation of process equipment. Controlled shutdown and planned islanding transfers are preferred over multiple interruptions of process operations.*
>
> *Step C. Consequence Analysis: Comparing normal process operations with planned and unplanned islanding identified several potential vulnerabilities. These vulnerabilities and resulting consequences are more severe when the microgrid is fully integrated to the process network. It is not possible to adequately interrogate or protect functions of the microgrid, BESS, or inverter due to the vendor system architecture (requires custom solutions). Therefore, these components represent potential gaps to be exploited by an adversary.*
>
> *Step D. Mitigation Analysis: The worst acceptable consequence of an attack would be losing the microgrid function and BESS capacity. This would result in the process relying solely on utility power. In this scenario, the process would fail or experience multiple interruptions (transfers) if gas-powered generators are retained.*

Cyber-Informed Engineering