INL/EXP-24-80783-Revision-0

Cyber-Informed Engineering Workbook: Substations

September 2024

Virginia L Wright, Benjamin Ruhlig Lampe

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/EXP-24-80783-Revision-0

Cyber-Informed Engineering Workbook: Substations

Virginia L Wright, Benjamin Ruhlig Lampe

September 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Cyber-Informed Engineering

Cyber-Informed Engineering Workbook: Substations

CIE Hands-On Training

August 20, 2024

Authors:

Virginia Wright
CIE Program Manager

Benjamin Lampe
CIE Researcher

Idaho National Laboratory

Contents

Acronyms

CIE	Cyber-Informed Engineering
INL	Idaho National Laboratory
IT	Information Technology
OT	Operational Technology

References

1. U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response*. Cyber-Informed Engineering Implementation Guide*. Version 1.0, August 7, 2023. https://www.osti.gov/biblio/1995796.

Figures

1. Workbook Purpose

This workbook presents a case study of a hypothetical project to support discussion and application of the principles for Cyber-Informed Engineering throughout the workshop. Though this scenario draws from a selection of real-world case studies, it is fictional.

Workshop participants are encouraged to use the workbook to capture insights and lessons learned.

2. Cyber-Informed Engineering Summary

Cyber-Informed Engineering (CIE)[1] offers an opportunity to "engineer out" some cyber risk across the entire system lifecycle, starting from the earliest possible phases of conceptual design and requirements development and system design—the most optimal times to introduce mitigations against cyber risk. CIE is an emerging method to integrate cybersecurity risk considerations into the conception, design, development, and operation of any physical system that has digital connectivity, monitoring, or control. CIE uses design decisions and engineering controls to mitigate or even eliminate avenues for cyber-enabled attacks or reduce the consequences when an attack occurs.

In the same way that engineers design systems for safety, engineers informed by CIE use similar methods to prevent or lessen the impact of a cyber-attack. CIE also allows the engineers to advise the approaches used by specialized Information Technology (IT) and Operational Technology (OT) cybersecurity experts to align cybersecurity mitigations to the most critical consequences identified by the engineers. Working together, both parties actively implement engineered and cybersecurity solutions to address the highest-risk consequences in their systems, ensuring robust protection for their devices and infrastructure.

This workshop summarizes the principles for Cyber-Informed Engineering, provided with the principle's initiating question in Figure 1.

[1] U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. *Cyber-Informed Engineering Implementation Guide*. Version 1.0, August 7, 2023. https://www.osti.gov/biblio/1995796.

	PRINCIPLE	KEY QUESTION
1	**Consequence-Focused Design**	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
2	**Engineered Controls**	How do I select and implement controls to reduce avenues for attack or the damage that could result?
3	**Secure Information Architecture**	How do I prevent undesired manipulation of important data?
4	**Design Simplification**	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
5	**Layered Defenses**	How do I create the best compilation of system defenses?
6	**Active Defense**	How do I proactively prepare to defend my system from any threat?
7	**Interdependency Evaluation**	How do I understand where my system can impact others or be impacted by others?
8	**Digital Asset Awareness**	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
9	**Cyber-Secure Supply Chain Controls**	How do I ensure my providers deliver the security the system needs?
10	**Planned Resilience**	How do I turn “what ifs” into “even ifs”?
11	**Engineering Information Control**	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
12	**Organizational Culture**	How do I ensure that everyone’s behavior and decisions align with our security goals?

Figure 1 - CIE Principles and Key Questions

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

Key Question

How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?

Principle Overview

Consequence-focused design is the first principle considered within a Cyber-Informed Engineering project. It results in insights that feed the remainder of the principles. **Consequence-focused design** begins with an analysis of the business purpose and its primary mission, the critical functions of the business, the interconnection of those functions to the system under consideration, and finally, the critical functions of the system itself. The team identifies the most consequential impacts, sometimes referred to as the high-consequence events (HCEs), that could result from disruption of the critical functions, especially those where the disruption of a system function could result in a mission-impacting consequence. The team develops a list of HCE's and prioritizes the most impactful. In the initial review, the team need not evaluate the potential or likelihood of these impacts being induced via digital failure or cyber-attack. Once HCE's are identified, the team can begin to explore how those effects could be realized via adversary attack or digital failure.

PRINCIPLE 2: ENGINEERED CONTROLS

Key Question

How do I select and implement controls to reduce avenues for attack or the damage that could result?

Principle Overview

For the most critical consequences and impacts determined in **Consequence-focused design**, we have an opportunity to think about the specific controls we'd like to have in place to prevent them. Eventually, we'll talk about the collection in terms of **Layered Defenses**, but at first, we can:

- Think about what kinds of controls we can have in place to prevent a consequence or mitigate its impact.
- Determine which controls are provided as a part of products and services we are using and which ones we might want to design in.
- Determine whether we can identify both physical controls and digital controls for a given consequence and the relative costs and benefits of each.
- Determine whether our controls prevent an attack, lower the impact of the attack, or serve to provide alarms or warnings of adverse situations.

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

Key Question

How do I prevent undesired manipulation of important data?

Principle Overview

Each system contains data linked to mission-critical consequences and impacts which should be protected from outsider view and, more importantly, adversary or failure-induced alteration. For each identified data element or stream, a **Secure Information Architecture** can be designed, guided by the consequences and impacts identified earlier, to segregate the most important data and the systems which contain it to provide more control, protection, and monitoring of those systems and that data.

We can start early in system design to identify those data elements most tied to a potential critical consequence, where they originate and are altered through the process, how they should be protected, and whether it is possible to design a data verification mechanism using the process, analog controls, or historic inputs.

Once our design is mature and the underlying network and data service architecture is under design, more fine-grained digital controls, and create specific zones and segmentation plans can be created.

PRINCIPLE 4: DESIGN SIMPLIFICATION

Key Question

How do I determine what features of my system are not absolutely necessary to achieve the critical functions?

Principle Overview

Systems formed through acquisition often have more features than are explicitly needed to perform required functions. Though these features can be configured not to be available to authorized system users, they are available to adversaries who gain access. These features can potentially lead to catastrophic impacts if used by malicious adversaries.

In **Design Simplification**, we consider which features of the system are not absolutely necessary and of those, which could lead to impactful adverse consequences if misused. We consider how to reduce the system to the minimum elements needed to provide mission-critical functions and necessary resilience. For each of the non-essential features, we consider whether we can completely remove them. When that is not possible, we collaborate with cybersecurity specialists to determine how to implement alarms and alerts when those functions are leveraged, or whether we can capture undesired commands at a network segmentation boundary before they are executed.

PRINCIPLE 5: LAYERED DEFENSES

Key Question

How do I create the best compilation of system defenses?

Principle Overview

The best defensive capability for critical consequences is formed by an assemblage of controls, including physics-based analog mitigations, capabilities to protect key system elements, capabilities to detect adverse operating or security conditions, and capabilities to aid in response and remediation. In **Resilient Layered Defenses**, engineers, and their operational cybersecurity support team work together to, for the most critical consequences identified, arrange the best compilation of those defenses to avert the worst impacts from the prioritized consequences. The engineers and operational cybersecurity team work together to ensure that each of the defensive capabilities and services is tuned based on the identified consequences and how the worst impacts of those consequences can be avoided.

PRINCIPLE 6: ACTIVE DEFENSE

Key Question

How do I proactively prepare to defend my system from any threat?

Principle Overview

Planning for **Active Defense** can begin as soon as a conceptual design for a system exists and it continues through the system's retirement. At the design phase, teams can begin to plan how defensive actions should be carried out for the most consequential events. This activity is aided by ensuring that the system designers, operators, and cybersecurity support team discuss the adverse consequences identified and how such events could occur, especially, at the appropriate level of detail for system maturity, the process, or kill chain of how the adverse consequence would manifest within the system. From this discussion, system states and anomalies which might be initial indicators of one of the identified consequences can be identified. Next, plans can be developed for actions to be taken upon detection of an identified indicator. Plans should include points of contact for specific roles and responsibilities across the spectrum of functions associated with the system, since **Active Defense** of the system may require support from a broad set of roles, and they may not all be aware of each other. Once plans are in place, systems should be created to ensure that these plans are regularly practiced, and that the overall approach is regularly assessed to identify emerging consequences, indicators, and opportunities for more advanced defensive approaches.

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

Key Question

How do I understand where my system can impact others or be impacted by others?

Principle Overview

All systems have interdependencies, both direct and indirect. While teams regularly consider the risks posed by physical interdependencies in the normal systems engineering processes, they rarely consider how a cyber-attack or digital failure of an interdependent system may affect the system under design.

When evaluating interdependencies from a cyber-informed perspective, evaluate the physical interdependency risks already considered, but judge whether a cyber-attack might make a given consequence more possible or might have the potential to make it more intense than a physically-driven event. Are there functions in the interdependent system not normally accessible to operators which might cause untoward effects on our system if activated? Where might interdependent systems activate command logic on the system under design? Where might automation between the two systems cause cascading effects? In the same vein, where might the system under design be able to affect the interdependent systems in unexpected ways.

PRINCIPLE 8: DIGITAL ASSET AWARENESS

Key Question

How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?

Principle Overview

The digitization of our energy infrastructure allows incredible benefits, providing speed and automation of operations not previously possible. However, digital assets and digitized functions have different weaknesses and frailty modes than their analog counterparts. Far beyond simply vulnerabilities to attack, these assets can function or be made to function in ways that their analog counterparts would not, and consideration of these risks is important to ensuring that the defensive measures for a system are cyber informed.

Digital Asset Awareness begins in design, by considering that any digital device is, at its core, a general-purpose computer with specific command logic for its function layered on top. An attacker, or more rarely, a logic failure can subvert this logic and cause the device to ignore input, change values in command logic, or even execute commands or automated logic unexpectedly. The consequences considered earlier in the process can highlight specific impacts we want to mitigate in design, hopefully with controls that are not solely digital in nature.

Secondly, in operations, digital devices require different forms of maintenance, including patching and upgrades and the export of logs and commands stored on the system. To ensure that such systems are maintained in accordance with the function of our system, we must track the devices installed by hardware model, software version, patch version, location, last update, last export, system function, etc. We should also export logs and, if possible, retain them for

forensic needs, along with a “gold disk” configuration of the latest software and logic, if needed. This ensures that we understand where the systems are within our processes, what is occurring on them, how they are maintained, and any emerging risks which have been identified as vulnerabilities. It also ensures that we can restore or replace them if needed.

PRINCIPLE 9: CYBER-SECURE SUPPLY CHAIN CONTROLS

Key Question

How do I ensure my providers deliver the security the system needs?

Principle Overview

Even at the early design phases, engineers can begin to establish the core security features and assumptions which should be implemented by every supplier bringing components or services into the system. These may include guidelines about required features in digital systems, limits on where such systems can be acquired, and how updates must be verified and signed. They may include practices for vendor behavior when providing onsite or remote maintenance. They may include requirements for sharing information about cyber incidents, vulnerabilities, bills of materials, and vendor development processes. Each of these controls contributes to the overall supply chain security of the system. These requirements should be discussed with the roles who may have a responsibility for ensuring them, including procurement, cybersecurity, and system operators.

For each control or feature, the team should consider how it will be verified, when it can be verified and how often, and who can perform the verification (procurement, cybersecurity, operators, etc.). These processes should be built into requirements for development and operations of the system, and verification should occur more than once for controls which could change or erode over time. The controls devised by the engineering team should be complimentary to those leveraged by the organization’s purchasing and cybersecurity processes, but because they are drawn from potential catastrophic system consequences, they may well exceed the general due diligence performed by the organization.

PRINCIPLE 10: PLANNED RESILIENCE

Key Question

How do I turn “what ifs” into “even ifs”?

Principle Overview

You can imagine the general operating mode of a system, with all functions available and working as expected; however, resilience requires that we imagine and plan for different kinds of failure modes of a system, ideally including those linked to the set of prioritized undesired consequences created earlier. We must understand these failure modes, including how to operate through them, albeit at a lower level of performance or reliability. Ideally, a set of diminished operating modes can be created which, though not ideal, can be built into expectations for well-understood modes of operation. Within each diminished operating mode,

plans can be made for what would cause that mode, how that mode would function, and the changes to staff, systems, safety guidelines, performance, or other system conditions when it is assumed. Once part of our overall set of system operating modes, it is reasonable to train, exercise, and assess our performance in each of these diminished modes on a regular basis.

These resilient diminished operating modes should include modes assumed because of a digital failure or cyber-attack. For any critical system, diminished operating modes should include operations during an expected cyber-attack involving one or several of those systems, operating when the team is uncertain of the validity of the data emerging from the system, where critical automation logic is not dependable, or where core network connections or support services are not available. It is likely that exercising these modes will require the operations team to pair with cybersecurity counterparts and understand the roles and responsibilities each will perform. Considering these operating modes may also require that the team consider altering the system design to allow limited manual operations options when digital systems are not operating or trusted. Note that a capability may be restored to diminished operation via use of an alternate mechanism or supply source.

Considerations for **planned resilience** should also include how untrusted systems can be restored to full function within the system context, including what operational steps will be required to ensure future trust, or whether that is possible given the function of the system or component.

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL

Key Question

How do I manage knowledge about my system? How do I keep it out of the wrong hands?

Principle Overview

From the first conception of a system until its retirement, immense amounts of information are created about how the system is designed, the elements and components within it, the skills required to operate it, its performance, procedures for maintenance and operations, and more. This information, in the wrong hands, can aid an adversary to understand system weaknesses, existing component vulnerabilities, and even human targets to aid in planning their attack. This information can be released during procurement processes, often shared via public release to ensure an open and fair competitive process. It can be released in job listings, where specific technical criteria are used to find good employment candidates but may also tip an adversary to system features or vulnerabilities. It can be shared in news articles or success stories about the system's entry to operations, where even a system photograph may release information helpful to an adversary.

During the system design process, the engineering team can begin to identify, using the prioritized list of consequences developed earlier, the specific information which would be of most value to an adversary to enact an undesired consequence. They can develop administrative processes for protecting the information, determining who can possess it, how to prevent inadvertent duplication and sharing, how to remove access, how to review and approve information release, how to ensure team members understand the sensitivity of the information

they have access to, and how to protect it, etc. Because engineering systems are in active use, sometimes for decades, it is crucial that even the earliest information about the system design be protected throughout the lifecycle of the system.

PRINCIPLE 12: ORGANIZATIONAL CULTURE

Key Question

How do I ensure that everyone's behavior and decisions align with our security goals?

Principle Overview

Shared beliefs, perspectives, and values about cybersecurity determine how a group will prioritize investments and actions to improve its realization. For a culture which does not value cybersecurity, whether they see it as an unnecessary expense, a low risk or impact, or an impediment to productivity, there will not be a desire to invest in people, processes, and technology to provide cybersecurity. An engineering design team, cognizant of the consequences of digital failure or cyber-attack on a system under design, has a core responsibility to aid the entire set of stakeholders who are accountable, responsible, consulted, or informed about the system to understand the need for cybersecurity and how each stakeholder's role can affect, both positively and negatively, the overall security of the system.

To build a culture of cybersecurity around the system design process, engineering design teams can emulate best practices for building a safety culture. These include having regular discussions about how and why cybersecurity is incorporated into the system, recognizing and celebrating good decisions and right actions of team members, and treating failures as opportunities for learning and improvement. Because team members external to the design process may not recognize how their job role can contribute to or diminish the cybersecurity of the overall system, it is important for the design team to personalize conversations to the individual. As discussed earlier under **supply chain controls**, these discussions should extend to everyone involved with the system, even a subcontractor or external service provider. Each person interacting with the system should understand the importance of ensuring its security and how their role contributes to that function.

3. Workshop Activity Overview

The scenario presented in this workbook is designed to provide a hands-on experience applying CIE principles in a fictional project. It is designed to elicit rich discussion about the principles among workshop participants. Feel free to ask questions of the moderators throughout the exercise.

There are likely to be key facts about the scenario that have been omitted or may be unclear. Participants are encouraged to make any needed assumptions about the project to enable application of the CIE principles.

3.1. Workshop Activity Background

At the Central Power and Light (CPL),a project team has been tasked with the design of a substation to support a 1000 MW data center. This initiative marks an opportunity to rethink traditional substation designs from the company's historical projects, which have primarily catered to industrial clients with demands ranging from 100 to 250 MW.

The client, a leading data center company, has approached CPL prompting the utility to consider a design process that goes beyond mere scaling of existing substation designs. The final goal is to deliver a substation that not only meets the very large load but is also designed with the foresight to support one of the various ownership options, any data center's future growth, and securing any technological evolutions. The goal of the team is to create an infrastructure that excels in reliability, efficiency, scalability, security, and resilience.

One of the key challenges lies in the proposed shared ownership model, wherein the data center company seeks a level of control over the substation—a scenario that potentially introduces a complex layer of shared management, requiring careful planning and a clear demarcation of operational responsibilities. Current options considered are: 1) the customer wants to own the substation and CPL owns a switching station, 2) CPL owns the whole substation, and the customer owns the feeds into the data center, or 3) CPL has some transmission-oriented banks where some of the banks in the substation are owned by the customer.

Further complicating the design is the possible integration of behind-the-meter generation. The data center's interest in sustainable energy solutions and autonomy in power generation necessitates a substation that can accommodate and manage possible parallel generation systems. If parallel generation is not available, then at a minimum backup power generation is expected. The team is expected to ensure that such an arrangement is not only viable but also secure, given the sensitive nature and types of expected important tenets of the data center's operations.

The projected implementation for the substation by the CPL team must anticipate the data center's projected expansion. The data center is expected to install a 500MW amount of load during each phase up to the expected 1000 MW total and expects the substation to grow in tandem with the client's needs without the necessity for extensive redesign or downtime.

Additionally, the project timeline enforces the need to diversify vendor relationships. The data center's aggressive timeline and the sheer scale of the substation have led to the exploration of equipment from nontraditional vendors from CPL's perspective. The team is charged with ensuring these components meet CPL and industry standards and can integrate.

The Data Center Customer has identified that the substations' resilience to cyber attacks is of great interest to them. They are a constant target of cyber threat actors and have regular reporting of their key suppliers being targeted in order to affect their operations. They believe that their power provider and the direct facilities supplying the data center will be key targets for direct and indirect cyber attack. Though they have backup power support within their facility, it will only address a short-term outage of power. They are depending upon the services within the substation to provide reliable power and reduce any outage event to only less than a couple of hours. These power capabilities must be resilient to cyber-attack.

3.2. Workshop Activity Details

The workshop activity for the CPL project team is centered around the design of a new substation to meet the unique requirements of a 1000 MW data center.

The Data Center company has approached CPL with a need that extends beyond the utility's traditional scope, pushing the envelope in terms of power delivery and infrastructure resilience. CPL is experienced at building infrastructure that meets NERC Reliability Standards, but in this case recognize that this substation will be classified as a CIP low impact facility and the NERC CIP Reliability Standards requirements for Low-Impact facilities do not provide sufficient security benefit for either the customer or the utility.

Another key part of the workshop will involve discussion around Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), and Quality Control (QC) procedures, particularly for equipment sourced from beyond the preferred suppliers' list.

The overarching goal in this activity is to understand the consequences involved in modern substations and challenge the applicability of existing company standards to the reduce or eliminating the impacts of these consequences in modern substations especially when scaling to such a substantial size. Participants will explore whether the utility's current standards suffice or if Cyber-Informed Engineering can illuminate areas within these standards that may require adaptation or enhancement, especially at this scale.

The workshop's process is intended mimic the customer substation development journey:

1. The initial engagement by marketing or economic development teams to address the data center's site and load projections, as detailed in the background section. For this workshop, it is assumed customer provided requirements (MVA, kV, power factor, location, month-year start delivery) has been captured.
2. The engineering phase where project specifics are determined (focus on this workshop activity).

The workshop will not be limited to cyber standards, which are minimal due to the general expectation of standardization in substation layout. Instead, it will encompass all aspects of the substation's design, acknowledging that cyber-induced consequences, such as physical or

kinetic events could reveal design vulnerabilities not previously considered. The intent is to examine components of the design to ensure the creation of a solution that is as resilient as possible.

Finally, the workshop is tasked with a review of the project's scope, re-thinking the boundaries of traditional company design standards, and exploring the necessary changes to meet the demands and consequences of a large-scale load as with this data center. Participants are expected to leave with a clear understanding of the challenges it presents, and the innovative enhancements CIE generates when meeting the data center's needs while maintaining the standards of reliability, security, and resilience.

3.3. Workshop Activity Scope

In this workshop, our focus is to simulate a collaborative discussion where workshop attendees function as the engineering staff at CPL. The instructors assume the role of CIE consultants, guiding the engineering team staff (workshop participants). Together, we aim to assist the utility staff in achieving their goal of substation design in response to the large data center load customer project.

This exercise will guide staff through a series of decision-making processes under the banner of the CIE principles to determine the operational and design practices that align with the utility's modernization goals. The outcome will be a plan confirming top/prioritized consequences, any key design decisions, integration of digital technologies with an appropriate CIE-informed mitigation strategy, and operational protocols for managing this substation with planned resilience.

The workshop will delve into CIE Principles, exploring their practical application and effectiveness in the context of the utilities' substation in response to a large load customer project. Participants will collaborate to further understand the implications of providing a cybersecurity protection scheme on an Operational Technology system that pulls from both traditional cybersecurity characteristics and engineering controls. It is our goal in this exercise to understand how both cybersecurity professionals and engineers can complement each other in a project's outcome.

4. Workshop Activity Analysis using CIE Principles

Work with your assigned team to consider and discuss how each principle applies to this fictional project. As a team, determine your feedback to the Utility engineering team on their implementation of CIE and be prepared to brief your answers out in the room.

The Utility staff team has provided some input for consideration under each principle but is open to your recommendations outside of those inputs.

4.1. CUSTOMER REQUIREMENTS

The following customer requirements were delivered by the initial marketing and economic development teams:

- 1200 MVA
- 230 kV
- > 0.95 lagging power factor
- Easily accessible for maintenance, secure and safe from potential hazards, and close proximity to data center location

4.2. SYSTEM DEFINITION

What components are involved in a substation? Which ones are the key components?

What do the design standards require for these components?

4.3. CRITICAL FUNCTIONS

What are the mission-critical functions this system is required to perform? (Principle 1)

What areas of the system design are linked to these critical functions? (Principle 1)

4.4. DIGITAL ASSET EVALUATION

What parts of the design will contain digital components or subcomponents? (Principle 8)

What network connectivity links each element of the high-level design? How do the various subsystems communicate with each other? (Principle 3)

How are digital assets used to meet mission-critical functions? (Principle 8)

4.5. CONSEQUENCE DEFINITION

What are the consequences that could result from a failure or unexpected operation of the system's critical functions? What impacts could there be to mission delivery, safety, security, the environment, equipment and property, financials, or corporate reputation? (Principle 1)

Are there adverse operating modes that are prone to high-impact consequences? What circumstances require or cause these modes? (Principle 1)

4.6. CONSEQUENCE ANALYSIS

Which digital features in a system have the potential to cause critical consequences from unexpected operation or attack, and how can those features be identified during development, procurement, and integration? (Principle 8)

How might loss or instability in a subsystem or the connectivity between system elements lead to high-impact consequences? (Principle 1)

How might loss or instability in a subsystem or the connectivity between system elements lead to high-impact consequences? (Principle 1)

How would a failure (frailty or attack/exploit) of each component affect the overall system? (Principle 1)

For each of the system's critical consequences, what would a cyber attack on that consequence require? What systems would an adversary need to access to create the specific effect? How might an adversary need to traverse systems and subsystems in order to get access to the critical systems and components? (Principle 5)

What precursor events could occur leading up to identified high-consequence events? How might adverse consequences manifest within this system, as conceptualized? (Principle 6)

What deviations from expected system states and anomalies might be initial indicators of one of the identified consequences? (Principle 6)

What potential cascading failures may need to be accounted for? (Principle 7)

What are the limits of acceptable degradation for the system's critical functions? (Principle 10)

4.7. MITIGATIONS

Are analog or physical protections engineered into the system (where possible) for each high-consequence event identified? (Principle 2) How dependent are the system's engineered controls on digital technologies? (Principle 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? (Principle 4)

What specific controls (digital and otherwise) can ensure that the most critical data is available, valid, and secure? (Principle 3)

For each key data element, where must monitoring be in place to identify deviations from desired data states or settings? Is active monitoring 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? (Principle 3)

What enterprise IT defensive layers will this system benefit from, e.g., enterprise firewalls, IT network monitoring, etc.? (Principle 5)

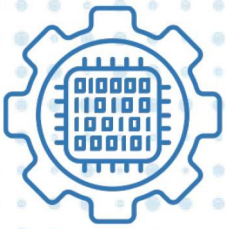
What processes are in place to ensure system operators are aware of triggers to temporarily change operations in response to a perceived threat? What stakeholders should be notified if there is an active defensive threat or weakness to this system? (Principle 6)

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? (Principle 9)

Do system requirements include a manual operation mode for any system that otherwise is controlled by an automated information system? (Principle 10)

Does the system's incident response plan contain a specific resilience focus and is there controls to ensure a fail-safe behavior? (Principle 10)

What training, education, and practice will individuals and teams need to operate, maintain, secure, and defend the system throughout its lifecycle? (Principle 12)



Cyber-Informed Engineering

Idaho National Laboratory