Cyber-Informed Engineering

Cyber-Informed Engineering Workbook

CIE Hands-On Training

May 29, 2024

Authors:

Virginia Wright
CIE Program Manager

Benjamin Lampe
CIE Researcher

Contents

Acronyms

CIE	Cyber-Informed Engineering
ICS	Industrial Control System
INL	Idaho National Laboratory
IT	Information Technology
OT	Operational Technology
P&ID	Piping and Instrumentation Diagram
SCADA	Supervisory Control and Data Acquisition
SMWU	Small Municipal Water Utility
VPN	Virtual Private Network
VFD	Variable Frequency Drive

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 **Error! Reference source not found.**.

[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

3. Exercise 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. Exercise Background

The Small Municipal Water Utility (SMWU) operates a regional water distribution system, central to which, is an array of booster pump stations. These stations are strategically positioned to overcome hydraulic challenges, such as maintaining adequate water pressure across the changes in topography and over long distribution distances. Ensuring that this water is delivered to all service areas within the correct pressure parameters is critical for customer use and satisfaction. It is also a required element for the system compliance with the industry codes and regulations.

In addition, to maintain the water quality, the regional water distribution system has installed a chemical injection system at each booster station location. These systems are calibrated to inject the correct dosages of chemicals to keep the water within the narrow chemical composition margins as dictated by health and safety standards.

The scale of the SMWU's operations is modest, which presents unique challenges. With a constrained budget, the utility must optimize a small workforce to cover all operational aspects, from routine maintenance to emergency repairs. Staff members are cross trained to perform an array of tasks, which is a necessity given the limited personnel resources.

A significant limitation for the SMWU is the absence of advanced remote monitoring and management systems. This means that the utility's personnel must physically visit each booster station for inspections, troubleshooting, and maintenance. These site visits are time-intensive, especially considering the geographic layout of the service area, which can require staff to travel for 1-2 hours to reach remote stations. This lack of remote capabilities not only affects the rapid response times for addressing issues but also impacts the overall operational efficiency and increases wear and tear on company vehicles.

The following Figure 2 provides a representative view of one of the SMWU's booster pump stations. This technical illustration is intended to showcase the mechanical and structural components that the utility's staff manage on a regular basis. It highlights the type of equipment and infrastructure that are essential for the continuous operation of the water distribution system and serves as a visual aid to illustrate the operational environment of the SMWU.

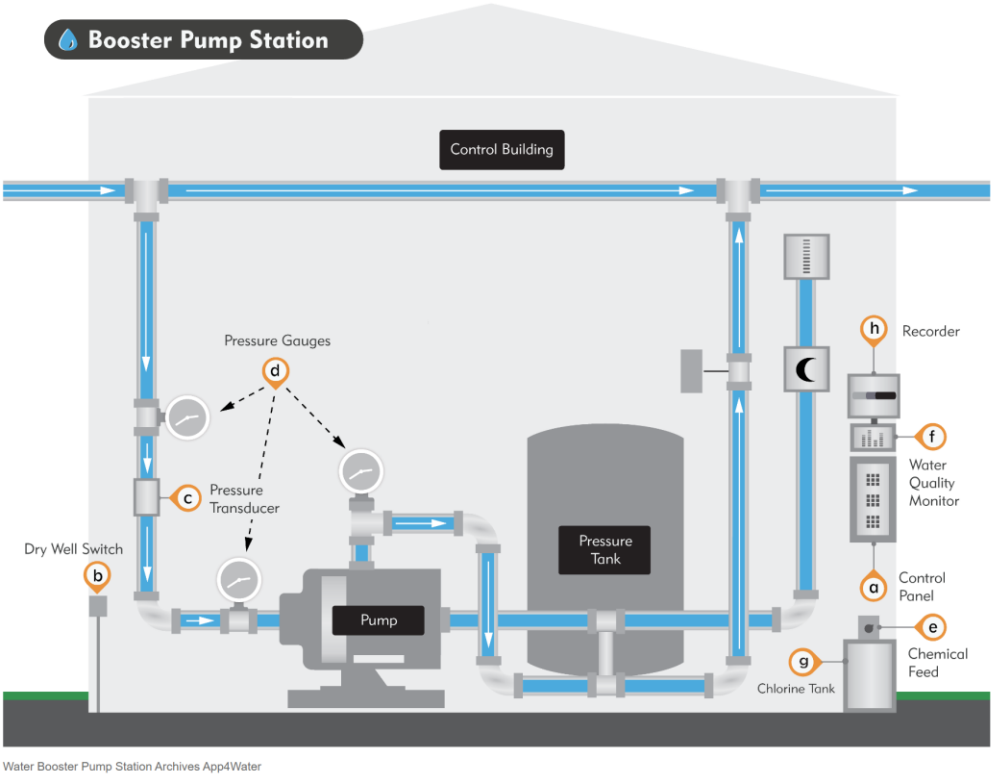


Figure 2 - Booster Pump Station

Adapted from: https://www.app4water.com/product-category/applications/booster-pump-station/

3.2. Exercise Details

This SMWU has recently secured a rural grant which has presented the municipality with the opportunity to modernize its regional water distribution system. Management, having attended a recent water industry conference, held discussions with consultants in this space to understand what some cutting-edge water management technologies are. Through these discussions, it became evident that implementing a cloud-based control system with supervisory control and data acquisition (SCADA) capabilities would be instrumental in optimizing the operations of their water distribution network.

Recognizing that such a technological upgrade aligns perfectly with their strategic vision and the grant, the municipality has pursued the adoption of cloud-based software to enable remote control over their pumping stations. This advancement marks a departure from the traditional operational model—relying on manual oversight by a small team—to a more efficient and centralized approach, where fewer personnel are required for on-site station management. By leveraging this modern technology, the municipality anticipates a shift in focus from spending excessive time and resources on site visits to enhancing the overall management and efficiency of their water distribution system. The excitement surrounding this shift is apparent as it represents a key step towards more sustainable and proactive operational management.

Upon selecting a vendor with expertise in cloud solutions for the water sector, the municipality was introduced to a suitable software solution. However, recognizing their team's lack of

experience with cloud technology and heightened awareness of cybersecurity threats, as evidenced by recent news of attacks in other sectors, they sought to deepen their understanding of the potential risks involved.

In a consultative conversation with their engineering partner, the municipality inquired about the cybersecurity implications of moving their operations to the cloud. The response was twofold: first, there was an emphasis on the importance of assessing the cyber maturity of the chosen vendor to ensure they are well-equipped to handle security concerns. Second, the conversation turned to the concept of Cyber Informed Engineering (CIE). By applying CIE principles to the existing system design, the municipality could mitigate the impact of cyber-attacks, even in the event of a failure of vendor security and maintain greater control over the security of their operations.

With an open attitude toward these considerations, the municipality has initiated this engagement to explore these cybersecurity measures further, marking the beginning of their journey toward a modernized, cloud-enabled water distribution system.

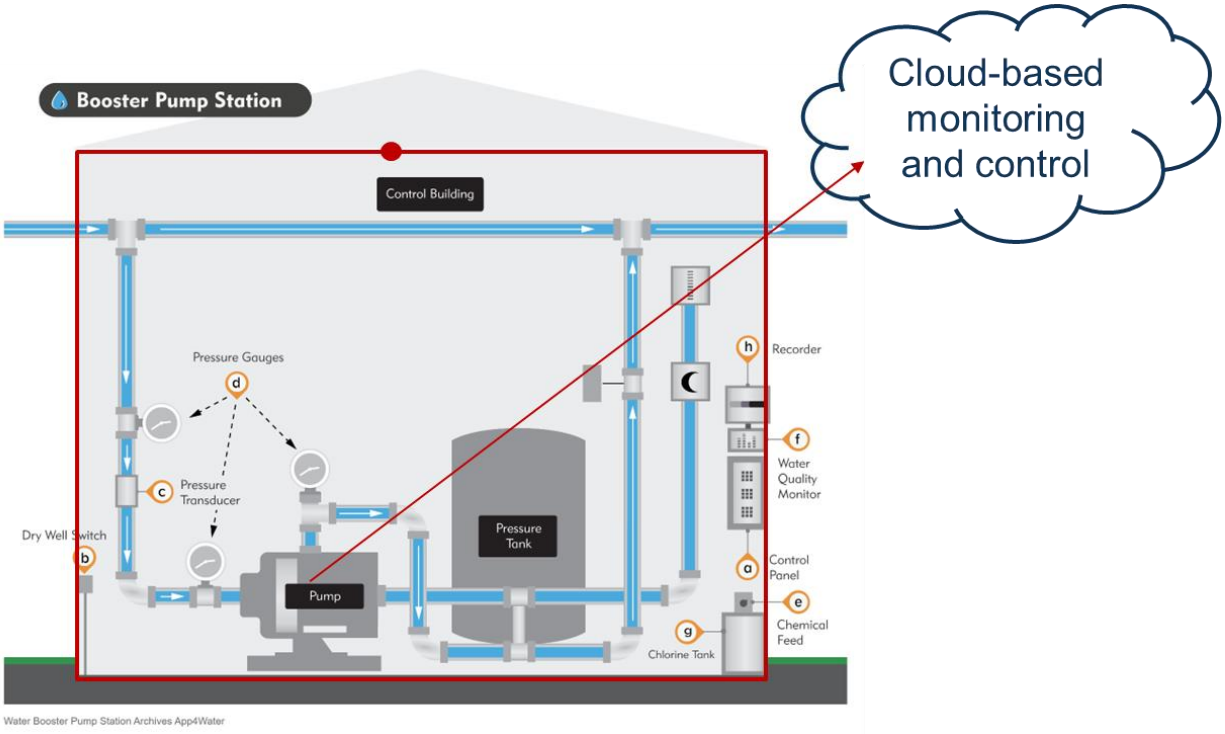


Figure 3 - Cloud-Enabled Booster Pump Station

Adapted from: https://www.app4water.com/product-category/applications/booster-pump-station/

3.3. Exercise Scope

In this workshop, our focus is to simulate a collaborative discussion where workshop attendees function as the engineering partner to the Small Municipal Water Utility (SMWU). The instructors assume the role of Cyber-Informed Engineering (CIE) consultants, guiding the engineering partner (workshop participants). Together, we aim to assist the SMWU in achieving their goal of implementing a cloud-enabled Supervisory Control and Data Acquisition (SCADA) system for their water distribution network.

For the purposes of this exercise, we will work under the assumption that the cloud-enabled SCADA solution proposed for SMWU incorporates several baseline cybersecurity features. These features are in alignment with industry best practices for a robust SCADA system and include, but are not limited to, role-based access control mechanisms to ensure that system access is granted based on user roles and responsibilities, logging mechanisms, and a comprehensive password policy to enhance security protocols. Additionally, we assume the deployment of a Virtual Private Network (VPN) that connects the cloud-based SCADA service to the security firewall routers. These routers are to be installed at each booster station site within the various subregions of the SMWU's operational area. The use of VPNs is intended to create a secure communication tunnel between the cloud service and the physical infrastructure of the booster station(s), thereby safeguarding data transmission against unauthorized access and other network transportation concerns.

The workshop will delve into CIE Principles, exploring their practical application and effectiveness in the context of the SMWU's transition to a cloud-based system. 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 the shared venture to protect the SMWU's water distribution network as it moves towards a more technologically advanced, cloud-enabled operational modes.

4. Exercise 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 SMWU team on their implementation of CIE and be prepared to brief your answers out in the room.

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

4.1. 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.

INPUTS FROM THE SMWU

- Our staff are familiar with manual operations of a booster pump station, and even with an automated system, will retain that familiarity.
- Any consequence that results in limited downtime (less than a day) is acceptable; however, damage to equipment needed for operation of the system is not.
- Due to our limited budgets, we are particularly sensitive to failures that require equipment replacement or having many spare parts.
- Currently our water quality system is only locally controlled and fully analog, but future funding could result in multiple automation capabilities.

EXERCISE TASK

Identify up to FIVE possible high consequence events for the SMWU water system and document them here.

1.	
2.	
3.	
4.	
5.	

Share the high consequence events with your team and determine which of them should be considered the worst-case consequence. Document this worst-case consequence event here, provide a justification of why it is considered the worst case, and use it as the basis for the subsequent exercises.

Worst Case Consequence Event	**Justification**

4.2. 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:

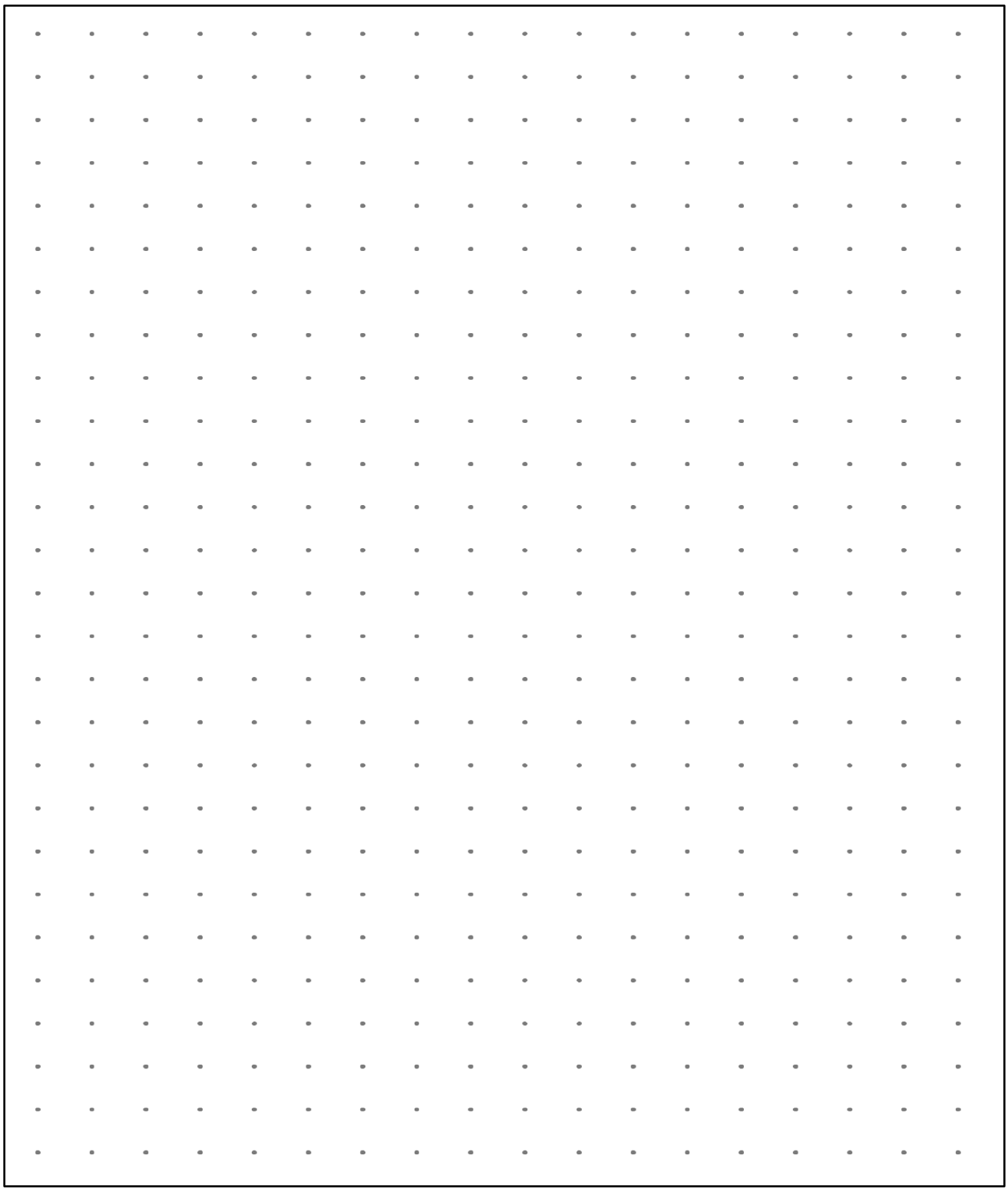
- Think about what kinds of controls we can have in place to prevent a consequence or mitigate its impact.
- Determine which controls are provided as a part of products and services we are using and which ones we might want to design in.
- Determine whether we can identify both physical controls and 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.

INPUTS FROM THE SMWU

- Our ideal control would be:
    - Deterministic (governed by physics)
    - Not networked / digital
    - Visible, possible to validate non-digitally
    - Complimentary with existing protections
- We are sensitive to the cost and maintenance of any engineering control since the control will be applied to all booster stations.

EXERCISE TASK

Draw or document an engineering control below that mitigates the worst-case consequence identified in Principle 4.1. Describe how it mitigates the worst-case consequence.



4.3. 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.

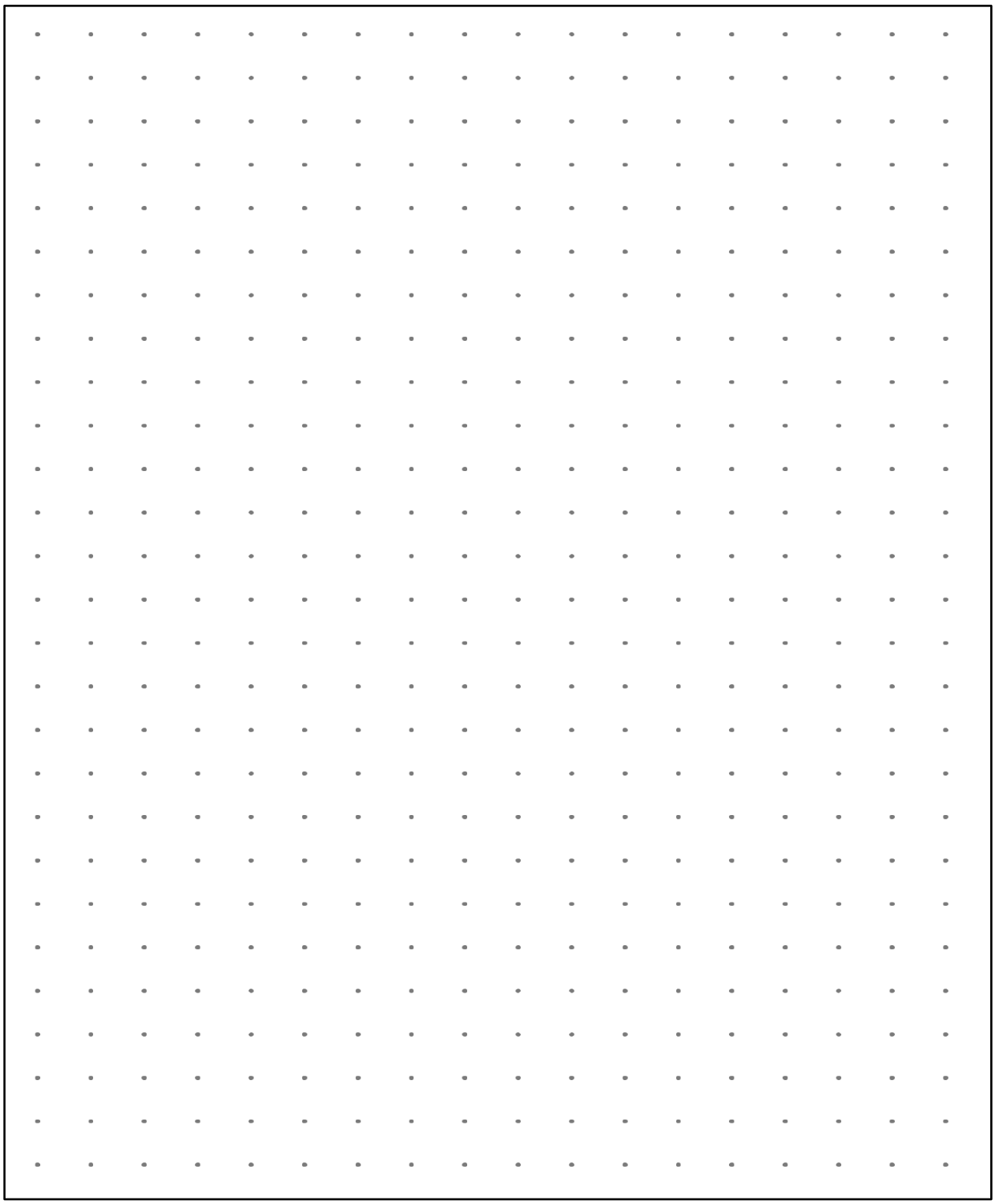
Once our design is mature and the underlying network and data service architecture is under design, more fine-grained digital controls, and create specific zones and segmentation plans can be created.

INPUTS FROM THE SMWU

- Network entry point linked to cloud vendor has standard security package.
- SMWU will monitor and log traffic on this interface according to standard practice.
    - Logging for the tool interfaces with the organizational logging system.
- We understand from the vendor that traffic in and out of the solution is encrypted between the cloud provider and the site network boundary. See **Appendix C** for a diagram of the solution provided by our vendor.
- We use Modbus as our protocol of communication in the system, and so with this upgrade we expect to be using the ModbusTCP payload.
- Where could manipulation of data lead to Engineering or Operational Impacts? These could include:
    - Loss of Protection
    - Loss of Safety
    - Loss of Productivity and Revenue
    - Damage to Property
- How should the potential for these specific operational impacts inform the cybersecurity strategy?

EXERCISE TASK

From the equipment that facilitates the worst-case consequence, identify the data elements involved in that process and the systems that originate, use, change, or validate that data:



4.4. 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.

INPUTS FROM THE SMWU

- When we first deployed this booster station, the pump was tested with a variable frequency drive. We noticed during our run time that maintaining a fixed pressure did not require any variation in running the pump, it seemed to follow an on-off behavior even with the variable frequency drive.
    - SMWU wonders if a variable frequency drive (VFD) would provide valuable features or whether this set of features is more than needed.
- The cloud ICS system has the ability to activate and control pumps and can be applied to the chemical injection system.
    - Given SMWU's familiarity with manual operation, the team wonders if the design should be simplified to only the automation of the pumps at the beginning.

EXERCISE TASK

Considering the worst-case consequence from Principle 1, and the equipment used in relation to that consequence, Principle 3, identify any functions discussed in the example that may not be absolutely necessary. Consider the benefit vs. risk of those features.

Function / Feature	Benefits	Risks

4.5. 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.

INPUTS FROM THE SMWU

- Areas of defensive options we understand are:
    - physical access considerations,
    - process considerations,
    - people considerations, and
    - digital considerations.
- We wonder how many layers of protection provide best benefit with least cost/overhead?
- How can cybersecurity prioritize defenses according to the consequences identified by engineering?
- How can engineering and cybersecurity work with vendors to detect and prevent the identified consequences from happening?
- How many layers of protection can we assemble?
- How can we inform cybersecurity requirements?

EXERCISE TASK

Consider the equipment used to facilitate the worst-case consequence event identified earlier, identify and document the layered controls (digital and engineered) that are used to mitigate the event:

Digital Controls	**Engineered Controls**

4.6. 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.

INPUTS FROM THE SMWU

- At the moment, none of our procedures take a potential cyber-attack on pump controls into consideration.
- How would we defend against that action?
- How do we expect our vendor to participate in our system defense? Do we need additional contracts? Have we established that they can perform to our expectations?
- How will engineering and cyber work together during the defense?
- Have we documented and practiced our defense?
- What are some minimal overhead actions we can perform to exercise our defenses?

EXERCISE TASK

Identify the roles involved in active defense and the responsibilities of each of those roles, considering each of the **Layered Defenses** identified.

Role Involved in Active Defense	**Responsibilities and Action(s)**

How would you exercise these roles and responsibilities?

4.7. 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.

INPUTS FROM THE SMWU

- We have built up a good reputation amongst our community. We don't want to risk that reputation through a vendor failure.
- We have added a new interdependency – the cloud service and software. Beyond specific cyber-attack, how might instability in this service affect our operations?
    - What happens if the service goes down?
- What is our ongoing plan to ensure that our vendor and their sub-vendors understand the criticality of their service for SMWU operations?

EXERCISE TASK

Document what "other" systems this system relies on and what effect a loss of the "other" systems may have on this system. Give special attention to your worst-case consequence.

"Other" System	**Effect on this System**

Document what effect on the "other" systems, including SMWU customers, the loss of functionality of this system may have. Give special attention to your worst-case consequence.

Which function of this system is lost?	**Effect on "Other" System**

4.8. 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.

INPUTS FROM THE SMWU

- We have talked to the vendor about extending the product to allow remote control of the chlorinator. We are used to operating it manually.
    - How will the use of digital technology change engineering risk?
    - Is the dispensed amount hardwired or adjustable?
    - How do we know that the product was actually dispensed?
- We are curious how much of our system is not digitally vulnerable versus non-digitally vulnerable.

EXERCISE TASK

Consider the system components that could be part of a worst-case consequence identified previously and document the digital functions in that system, and the effect if those functions are compromised.

System Components	Common Digital Functions	Effect of Compromise

4.9. 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.

INPUTS FROM THE SMWU

- Pumps are our biggest lead time for supply chain, followed up by the water quality system components.
- We examined the components used by the vendor and the security culture of the cloud company, and both were very mature. However, there are still some questions we need to ask.
    - How is the system patched? How are patches delivered? Can the asset owner accept or reject a patch?
    - Does the software vendor or cloud provider ever allow access to our system to their vendors or maintainers?
    - How are 3rd-party support providers, including the call-in support, qualified and vetted?

EXERCISE TASK

Provide insights you would like procurement agents to know when procuring the system from the supplier (i.e. items to watch out for, priorities to enforce), and insights you would like integrators to know when implementing the system at SMWU.

Purchasing

System Component or Feature	Procurement Insights

Integrators

System Component or Feature	Integrator Insights

4.10. 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.

INPUTS FROM THE SMWU

- SMWU is certain that they can maintain their capability to perform manual operations and sees that as a primary **planned resilience** tactic.
- They will need to initiate an alternate contracting mechanism (and receive emergency budget) if manual operations are needed for more than two weeks.
- What if an attacker turned all of the pumps on or off? What if the application stopped working? How should we think about our limited staffing in resilience planning?
- What if the application vendor reported an adversary attack? What fallbacks exist in our system or processes?
- What if the cloud vendor had ransomware?

EXERCISE TASK

Consider your worst-case consequence, document what an initial diminished operating mode may look like, including its effect and how long can that be sustained before it becomes untenable. Then indicate the actions (i.e. action plan) that would lead the system back to normal operating mode.

Initial Diminished Operating Mode	**Effects of Diminished Mode**
At what point does the Diminished Operating Mode become untenable for the organization?	
Action Plan to return to Normal Operating Mode	

4.11. 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.

INPUTS FROM THE SMWU

- SMWU is REQUIRED to share information about municipal technology investments with the public and this grant will publish SMWU's summary proposal on the internet.
    - How much information about this upgrade must be shared?
    - What should be kept out of the record?

EXERCISE TASK

Considering the worst-case consequence and the equipment involved, identify any engineering information deserving information control protections. For example, make and model of specific equipment involved, software applications used, or material suppliers.

If any of the identified information was given to an adversary through some means, such as social media, job posting, etc., how might it be used to compromise the equipment/system and lead to the worst-case consequence?

4.12. 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.

INPUTS FROM THE SMWU

- Our organization all voted in favor of the cloud vendor (i.e., finance/accounting, IT, and Cybersecurity) and the vendor's demonstration about cybersecurity best practices they have implemented, but our engineering mindset still had questions about its impact to process concerns. Our openness to discuss this has led to multiple ideas about how to protect and operate this system.
- How do we build an inclusive cybersecurity culture?
    - How do we involve this new vendor in our culture
- Who else in our culture should we involve closely?
    - How can we promote the right security goals for our system?

EXERCISE TASK

Consider and document how each of the roles below are involved with defensive controls of this system. Identify how the culture should reinforce their responsibilities.

Operations Team	**Cybersecurity Team**
Safety Team	**Management Team**
Legal/Procurement/HR Teams	**Engineering Team**

Appendix A: Piping and Instrumentation Diagram (P&ID)

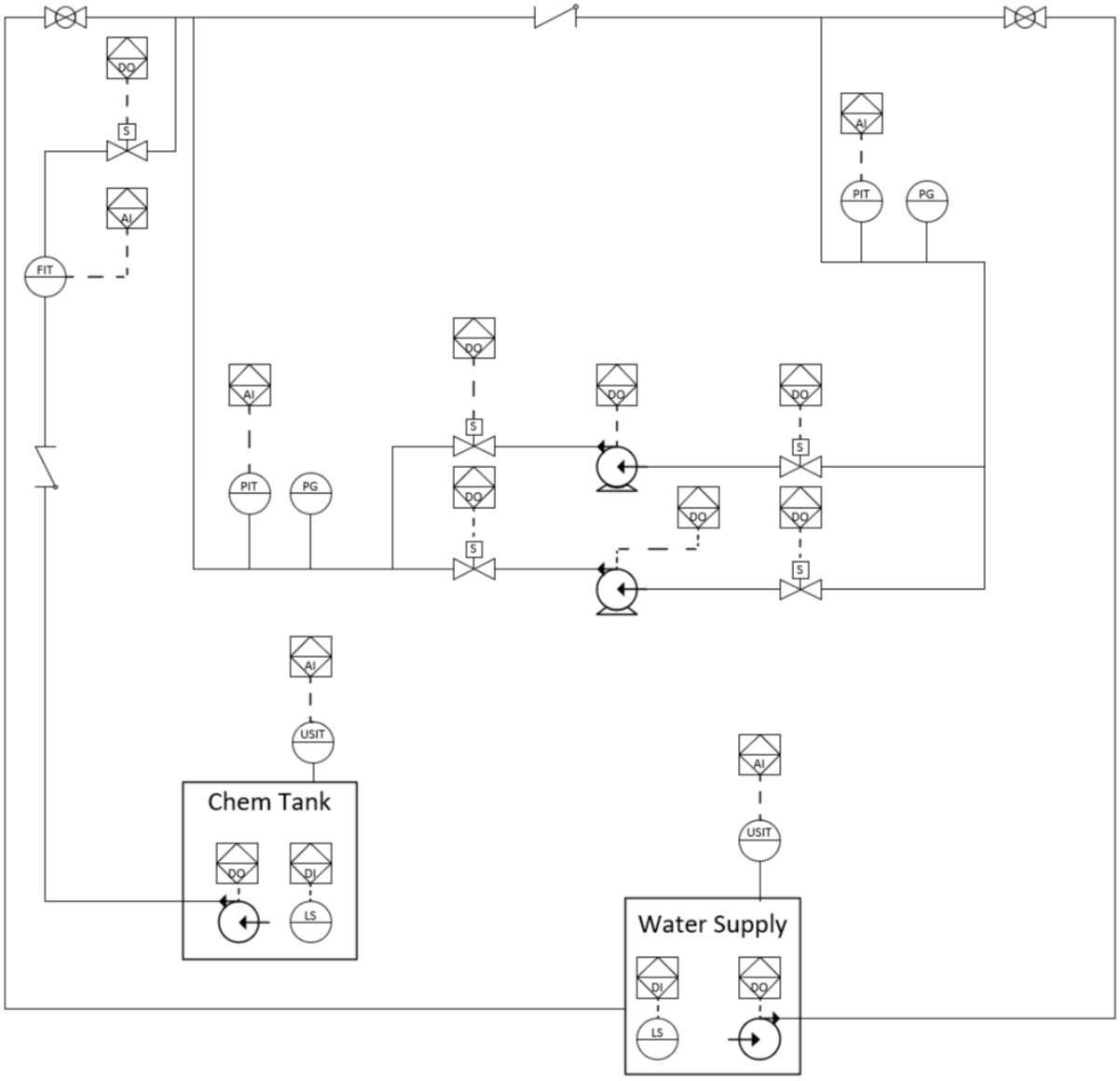


Figure 4 - Booter Pump P&ID Diagram

Appendix B: SCADA Network Diagram

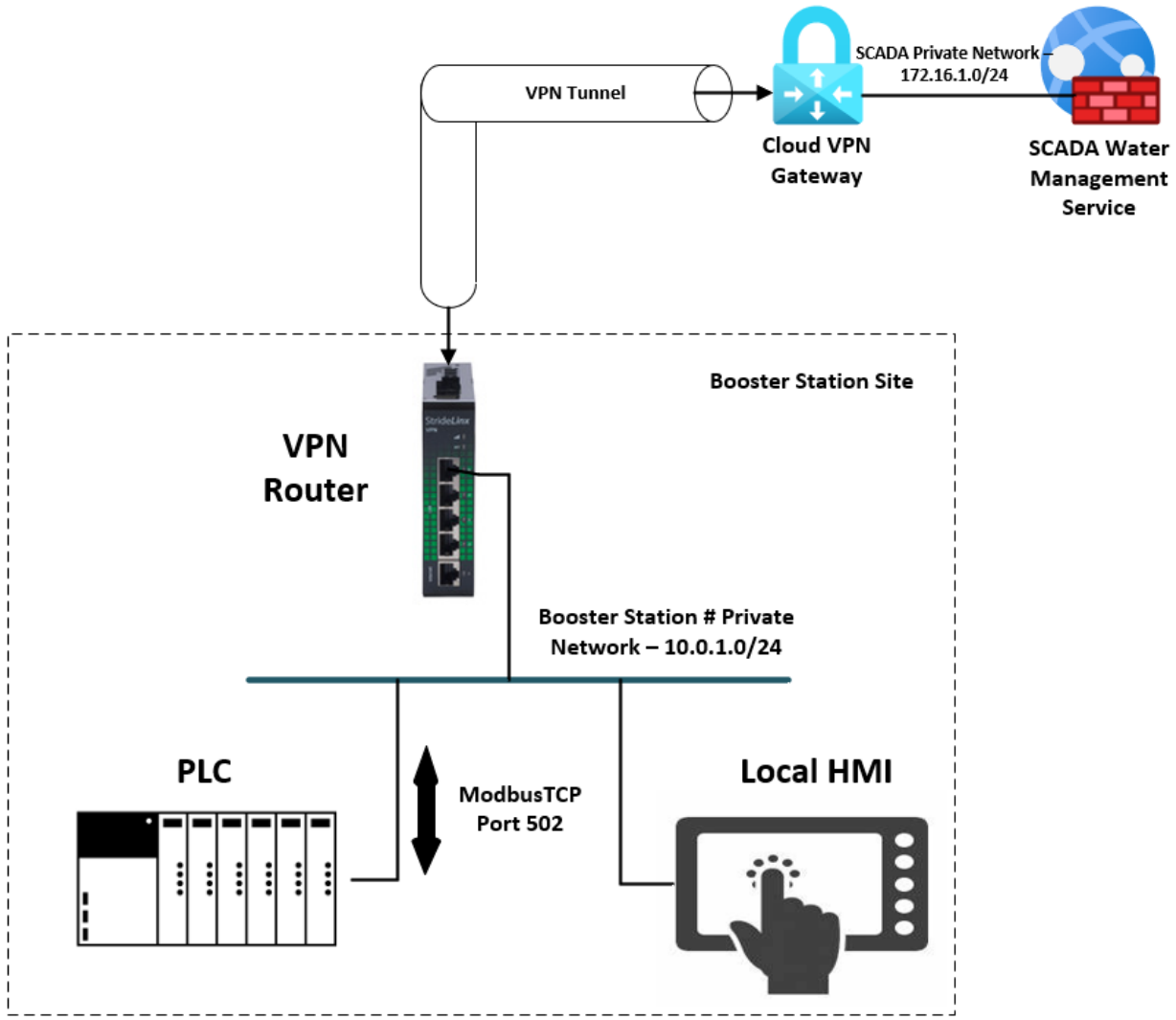


Figure 5 - SCADA Network Diagram

NOTES:

Cyber-Informed Engineering

Idaho National Laboratory