U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

INL/RPT-23-74072

Cyber-Informed Engineering
Implementation Guide

Version 1.0

AUGUST 7, 2023

CIE Implementation Guide Quick Facts

PURPOSE

Describes the principles of Cyber-Informed Engineering (CIE) and outlines questions that engineering teams should consider during each phase of a system's lifecycle to effectively employ these principles.

PRIMARY USER

System or design engineers and technicians for critical energy infrastructure installations.

WHY TARGET ENGINEERS?

CIE extends "secure-by-design" concepts beyond the digital realm to include the engineering of cyber-physical systems. CIE introduces cybersecurity considerations at the earliest stages of system design, long before the incorporation of software and security controls. It calls on engineers to identify engineering controls and design choices that could eliminate attack vectors for cyber actors or minimize the damage they could inflict.

This approach creates new opportunities for *engineering teams*—and not just cybersecurity teams—to secure the system *using the physics and mechanics of engineering controls*—not just digital monitoring and controls.

NOTE ON THE MATURATION OF CIE

Since the term Cyber-Informed Engineering entered the literature in 2017, subsequent research and policy publications have progressively refined and solidified CIE principles, in service of better answering the question: "What is Cyber-Informed Engineering and what does it mean to do CIE?"

This Implementation Guide continues down that path by describing the CIE principles in significant detail for the first time. The guide represents the thought leadership of more than 115 contributors (see Appendix A) from a multi-disciplinary CIE Community of Practice, led by researchers at the Idaho National Laboratory (INL) and National Renewable Energy Laboratory (NREL).

The authors expect and welcome robust feedback from the stakeholder community and plan to conduct a revision cycle of this Implementation Guide over the next year. Contact CIE@inl.gov to offer input.

Contents

DISCLAIMER

Prepared for the U.S. Department of Energy (DOE), Office of Cybersecurity, Energy Security, and Emergency Response (CESER) by Idaho National Laboratory, operated by Battelle Energy Alliance LLC, under DOE Idaho Operations Office Contract DE-AC07-05ID14517, and by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy LLC, under Contract No. DE-AC36-08GO28308.

PART A

Overview and Orientation

PART A

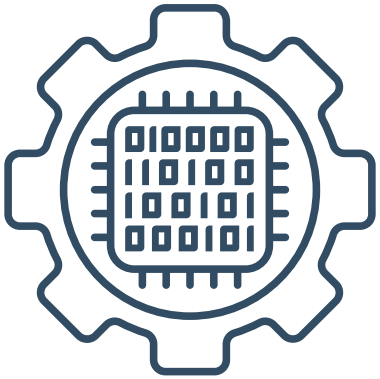
Purpose of the CIE Implementation Guide

This Implementation Guide describes the principles of Cyber-Informed Engineering (CIE) and outlines questions that engineering teams should consider during each phase of a system's lifecycle to effectively employ these principles. It describes **what** it means to engineer systems in a cyber-informed way, rather than offering a comprehensive, step-by-step process or procedure for CIE implementation. This guide complements—but does not replace—the application of cybersecurity standards or practices currently in place within an organization.

Engineers and technicians that design critical energy infrastructure installations can use this Implementation Guide to integrate the 12 principles of CIE into each phase of the engineering lifecycle, from concept to retirement. The guide is aimed at system or design engineers, rather than software engineers or operational cybersecurity practitioners. That is because the engineers who design, build, operate, and maintain the physical infrastructure are best positioned to leverage a system's engineering design to diminish the severity of cyber attacks or digital technology failures.

CIE expands cybersecurity decisions into the engineering space, not by asking engineers to become cyber experts, but by calling on engineers to apply engineering tools and make engineering decisions that improve cybersecurity outcomes. CIE examines the engineering consequences that a sophisticated cyber attacker could achieve, and drives engineering changes that may provide deterministic mitigations to limit or eliminate those consequences.

CIE and "Secure-by-Design" Concepts



CIE extends "secure-by-design" concepts beyond information technology (IT) and software engineering to include the engineering of cyber-physical systems. Secure-by-design approaches typically describe a shift in focus for software developers from finding and patching vulnerabilities to eliminating the design flaws in the software architecture that enable those vulnerabilities. CIE extends this concept beyond software design, introducing cybersecurity considerations that engineers can address at the earliest stages of system engineering, long before the incorporation of software and security controls.

Traditionally, engineering design teams have not recognized the opportunity to create cybersecurity improvements in systems through initial design and engineering decisions. These opportunities, if missed, are often costly or even impossible to implement later in the development process, potentially leaving in place cyber risks that security teams must endlessly manage and monitor. Enabling cybersecurity considerations at the beginning of the system lifecycle not only avoids this outcome, but creates new opportunities to secure the system using physics and mechanics, not just digital monitoring and controls.

Additionally, this practice allows the engineering team—which is ultimately responsible for identifying and mitigating functional and security risks for the system—to better tailor digital system protections according to the overall system risk and to consider impacts of digital failure or cyber attack into the overall system development process.

Ultimately, the use of Cyber-Informed Engineering to address cyber-physical risks will be recognized as part of the overall "standard of care" for engineering design. While these concepts can be most fruitful when considering the design of a new system, they are useful to consider even for a currently existing system to raise the engineering-based protections that system employs for digital failure or cybersecurity risk.

Proactive Collaboration Required to Effectively Use the Guide

System or design engineers applying the CIE principles will require proactive collaboration with other engineering disciplines, as well as IT and cybersecurity specialists and other business units. Effectively answering the questions laid out in the guide requires a multi-stakeholder approach to systems and engineering design, where security, risk management, and other business function leaders team up with engineers early in system design. This enables a shift in systems engineering that will create a culture of cybersecurity aligned with the existing industry safety culture.

CIE Background

The National Cybersecurity Strategy of 2023[1] called for a large-scale shift to secure-by-design approaches for the digital ecosystem that underpins U.S. critical infrastructure systems. For energy infrastructure in particular, it explicitly recommends implementing the Congressionally-directed National CIE Strategy[2] to proactively build in cybersecurity. This Implementation Guide takes a crucial step to do just that—providing guidance for engineers to incorporate CIE throughout the design and engineering process, and meeting a key National CIE Strategy recommendation.

The National CIE Strategy was developed by an executive task force, assembled by the U.S. Department of Energy (DOE)'s Office of Cybersecurity, Energy Security, and Emergency Response (CESER), that included energy sector asset owners and operators, vendors and manufacturers, standards organizations, research and academic institutions, National Laboratories, and government agencies. It outlines strategic recommendations across

1 The White House, *National Cybersecurity Strategy*, March 2023.

2 U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response, *National Cyber-Informed Engineering Strategy*, June 2022.

five pillars of action, including raising awareness of CIE, building CIE into engineering education and accreditation, developing a body of knowledge and resources for CIE, and implementing CIE in both existing systems and future infrastructure designs.

Since the strategy's publication in June 2022, the CIE initiative has continued to grow and evolve, with multiple efforts under way to implement key strategy recommendations. Bolstering these efforts is the CIE Community of Practice, which has formed with more than 200 practitioners to help translate CIE concepts into technical requirements and drive the development of a robust CIE body of knowledge and resources—including this Implementation Guide. See Appendix A for a list of contributors and see Appendix D for additional CIE resources.

Cyber-Informed Engineering Principles

CIE is an engineering approach that integrates cybersecurity considerations into the conception, design, build, and operation of any physical system that has digital connectivity, sensors, monitoring, or control. Rather than add cybersecurity controls after the design is complete, CIE offers the opportunity to use engineering to eliminate or mitigate avenues for cyber attack—starting from the earliest stage of design and continuing throughout the system's lifecycle.

Today, engineers and industrial control system (ICS) technicians build energy systems with specific goals for safety, reliability, and functionality. While systems engineering includes considerable safety and failure mode analysis, cybersecurity risks are often not specifically addressed—particularly the risks of intentional cyber compromise, exploitation, and misuse.

Simply put, traditional engineering risk management approaches rarely address the risks of directed, purposeful system manipulation or disruption performed by an intelligent and capable cyber adversary. Instead, cyber risk management is conducted by cybersecurity teams, who are called in only after system components are selected to harden the integration of those components. This process delays the introduction of cybersecurity mitigations until late in the engineering lifecycle, providing inadequate and more costly protection for the nation's energy infrastructure.

CIE aims to shift the way the nation's engineers, ICS technicians, manufacturers, and operators approach security in energy systems design. **This approach offers new opportunities to "engineer out" cyber risk—that is, to use early design decisions and engineering controls to reduce, mitigate, and even eliminate the consequences of a cyber attack.**

Figure 1. CIE Principles

	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?

Researchers first began to define a CIE approach in 2017, identifying a set of principles to consider when solving an engineering problem.[3] In the intervening years, those principles have been refined and revised, and this Implementation Guide offers the most current and granular identification of CIE principles to date. The principles identified here are not exhaustive but do serve as important elements within an ICS engineering risk-management process.

This Implementation Guide provides a deep discussion of each principle, and the questions and considerations an engineering team must address to embody the principle in their resulting system. Those questions and considerations are presented for each phase in the system lifecycle.

3 Robert Anderson, Jacob Benjamin, Virginia Wright, Luis Quinones, and Jonathan Paz, *Cyber-Informed Engineering*, U.S. Department of Energy Office of Nuclear Energy and Idaho National Laboratory, March 2017.

Systems Engineering Lifecycle Model for CIE

As a project progresses from initial concept, through design and ultimately implementation, the design team has different opportunities to identify, implement, and verify cyber protections and mitigations appropriate for the system. This Implementation Guide presents each CIE principle for each phase of the engineering lifecycle. By considering CIE through a systems-engineering perspective, rather than as principles alone, practitioners can understand how the application of CIE changes through a project's lifecycle. This approach encourages more thorough up-front work for requirements, design, and stakeholder coordination.

This guide offers considerations to practically apply CIE principles at each lifecycle phase. The team considered several systems engineering models to use as a basis for this Implementation Guide, but they found that many models were either too granular or too industry- or system-specific to adopt directly (see Appendix B for a discussion of the models considered).

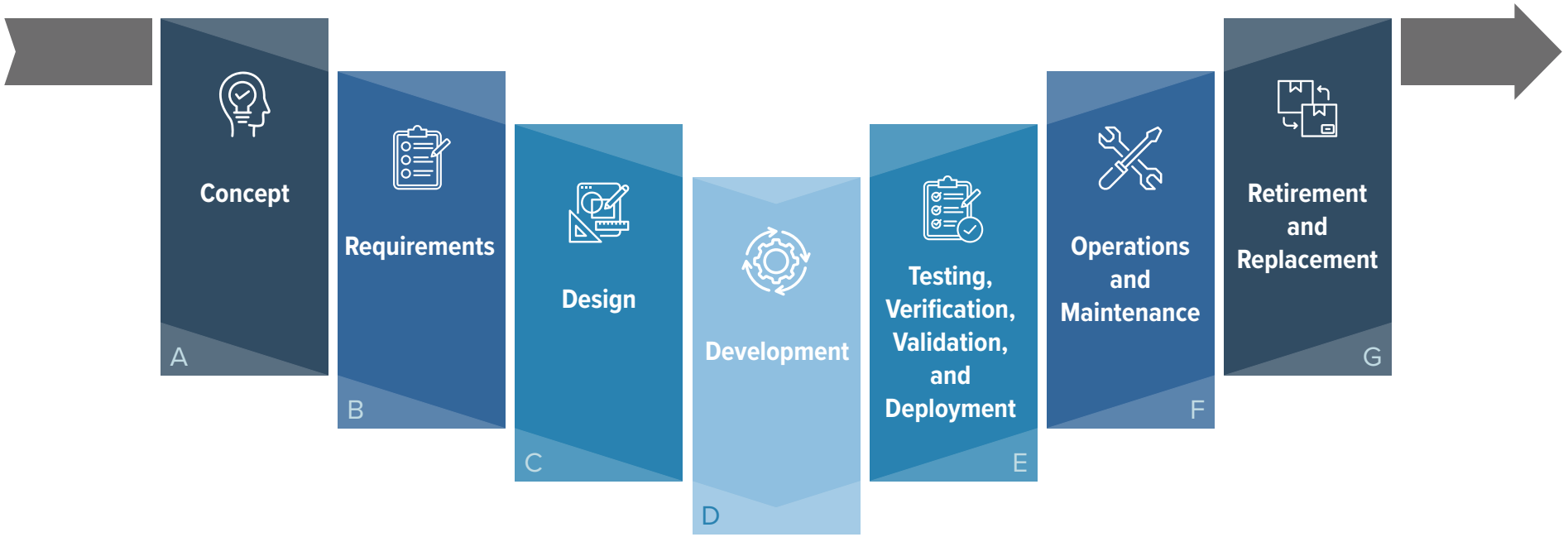
This guide uses an engineering lifecycle model that simplifies the lifecycle into seven core systems engineering phases, with three controlling processes that occur across all phases (project management, risk management, and change/configuration management).

This model offers several benefits:

- Simple enough to identify discrete CIE considerations at each phase
- Focused broadly on systems engineering, rather than specifically on software engineering
- Can be flexibly adapted to a variety of common engineering lifecycle models

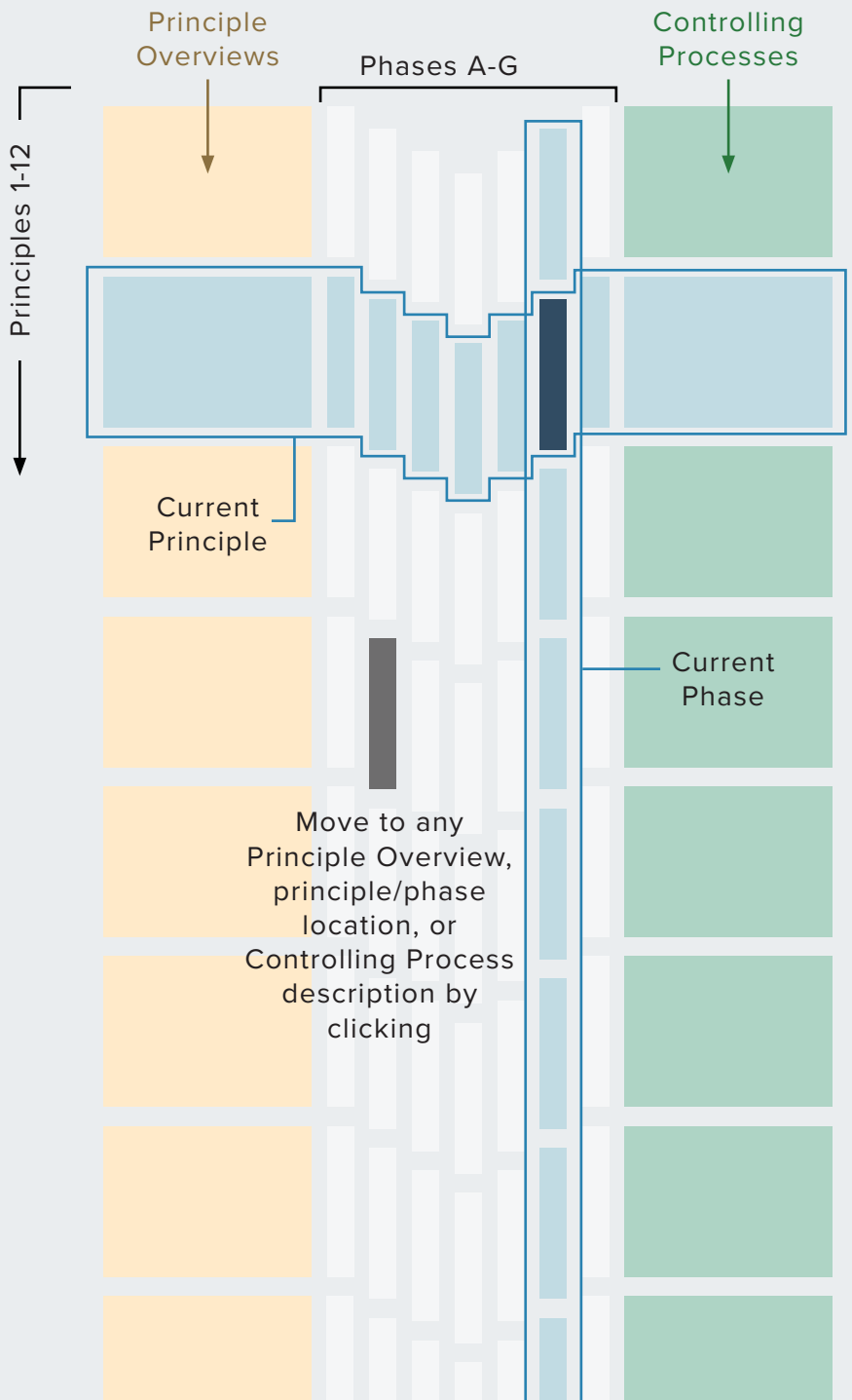
Engineers should be able to align each phase in this Implementation Guide with one or more phases in their own preferred systems engineering model and apply the guidance at each relevant phase.

Figure 2. CIE Systems Engineering Lifecycle Model



PART B

Implementing CIE Principles in Each Phase of the Systems Engineering Lifecycle



How to Use the Implementation Guide

Navigating the Implementation Guide

Part B of the Implementation Guide includes a section on each of the 12 CIE principles that describes the questions to consider at each phase of the engineering lifecycle model. The guide is chronologically ordered by principle, with subsections for the lifecycle phases. However, readers can navigate through the document either by principle or by engineering lifecycle phase using the navigation tools on the left side of the page. Engineers interested in viewing considerations for a specific phase of the engineering lifecycle can click vertically through that phase in the navigation, rather than scrolling chronologically.

How to Apply the Implementation Guide to a System or Project

The Implementation Guide is intended to be used as both an educational guide and reference material for engineers. Engineers are recommended to:

1. Read the overall guide and think through the questions posed.
2. Consider who within the organization can provide the necessary input to answer those questions, and how gathering those insights might change the approach to system design.
3. Review the Case Study in Appendix C to understand how these questions can be applied to a real-world project and the implications of CIE considerations.
4. Revisit the questions in the guide and identify how to incorporate some or all into the design and development lifecycle.

Note on Guide Terminology

This guide does not serve as an introduction to project management, systems engineering, computer programming, operating systems, industrial control systems, or cybersecurity. Readers are assumed to be familiar with the basics of these disciplines and the terminology used therein. Where sector-specific terminology is used, references to definitions are provided.

PRINCIPLE 1

Consequence-Focused Design

1

KEY QUESTION

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

Principle Description

Apply CIE strategies first and foremost to the most critical functions the system performs. Typically these are functions that, if manipulated or subverted, could result in unacceptable or catastrophic consequences for the organization, including undesired impacts to security, safety, quality, the environment, availability or effectiveness of products or services, system integrity, and public image. Use a structured and thorough process to identify areas where digital technology is used within these functions.

Consider where an unprotected action or failure of the function that leverages digital technology might lead to a high-consequence event. These could include unauthorized system actions, invalid data that would drive an automated action, or interdiction of a digitally governed control. Examine the controls that exist to minimize impacts of misuse or failure and whether those controls are implemented via digital technology, physical mechanisms, or a combination of both.

This list of high-impact consequences underpins the work engineers will perform throughout the system design lifecycle and the actions to be taken and their priority within each CIE principle. For each element identified in the work above, engineers will consider engineered controls (see Principle 2: Engineered Controls), that could either remove the possibility for the unprotected action or mitigate its consequences. These changes complement traditional cybersecurity protections to increase the overall resilience of the system to undesired digital events that could result in catastrophic consequences.

Consequence-Focused Design Considerations at Each Lifecycle Phase

Because the Consequence-Focused Design principle provides key inputs for other principles, it should be the first principle considered at the beginning of the lifecycle phase. Consequence-Focused Design functions as a foundational principle that, once assessed, is used as the basis of consideration for all other principles. At a high level, early considerations may focus on identifying negative business consequences such as delivery failure, equipment damage, or impacts to safety, that may apply to the system generally, before linking consequences to specific design elements to engineered mitigations. Systems with a high potential for accidents, misuse, or sabotage resulting in catastrophic consequences will require a stronger emphasis on consequence-focused design.

Specific elements considered in the Consequence-Focused Design principle will shift as the principle is applied across time and system maturity. It is important to note that the trajectory of industry and technology changes may affect consequence assessment throughout a system's lifecycle. Consequence is a moving target that should be regularly re-assessed even if the considered system is not changing.[4]

4 This idea aligns with ISA/IEC 62443 "Assess, Design & Implement, Operate & Maintain" 62443-3-2, which focuses on regular risk assessment for the System under Consideration (SuC). While the system may not have changed, the patches, updates, added users, third-party admin access to firewalls and switches, and organizational culture do often change, creating previously unconsidered consequences. The reassessment should also have externally vetted peer review to avoid internal company bias.

PRINCIPLE 1 PHASE A

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. Though some of the questions posed for this principle are similar to those asked in an overall risk assessment, the questions are intended to surface the potential for digital technology subversion or failure to manifest undesired consequences and to dispel assumptions that digital technology will only behave in desired or expected ways.

The Consequence-Focused Design principle can be applied to the concept phase by considering the following questions:

1 What is the purpose of this organization? What critical functions does the organization perform?

2 What is the purpose of this system?

a How does the system support the purpose of the organization?

b What system processes exist to ensure the success of this purpose?

c What system processes, if they fail or operate unexpectedly, will cause that purpose to fail?

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

a How does the system connect to the critical functions of the organization?

b What needs does the system address and how does it meet those needs?

c Which specific aspects of the concept of operations (CONOPS) enable these critical functions?

4 What are the consequences that could result from a failure or unexpected operation of the system's critical functions?

a What impacts could there be to mission delivery, safety, security, the environment, equipment and property, financials, or corporate reputation?

b What happens if multiple consequences happen concurrently in time?

EXAMPLE: A vibration monitoring system fails to detect an overworn bearing in a turbine generator. As a result, the equipment is damaged and must be replaced, causing a long outage and production loss.

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN
CONCEPT PHASE (continued)

5 What business areas may be uniquely impacted by system failure or unexpected operation?

a Which parts of the business would be affected by each consequence?

b Which resulting consequences could be categorized as "acceptable" and could be managed within organizational risk management processes?

c Which consequences (physical or otherwise) are "unacceptable" and must be mitigated? Document these distinct consequences.

EXAMPLE: Loss of control or disruption of a large power transformer within the bulk electric system (BES) could affect the transmission capacity of a regional electric power grid. Depending on the location, downstream effects could impact large population centers, national security sites, or the Eastern/Western Interconnects of the BES.

6 What regional or environmental consequences may result from system failure or unexpected operation?

a What entities would be affected for each consequence? Consider connected communities, infrastructure, and environments.

b What changes to the original design are needed to account for failure mechanisms that may vary from region to region?

7 What crucial assumptions have been made in the CONOPS that the system works as expected?

a What violations of those assumptions may result in high-impact consequences?

8 Where might routine system operations diverge from the expected CONOPS?

a At each instance where that might happen, what are the impacts?

9 Are there adverse operating modes that are prone to high-impact consequences?

a What circumstances require or cause these modes?

b In adverse operational conditions, how might system states evolve before the ultimate consequence occurs?

10 What staffing roles in the system have the most potential to interact with high-consequence events? What training or other supports will they need to perform those roles effectively?

a Where might a role gain access to functionality that was not anticipated and for which the requisite support or training is not in place?

b What are the impacts if an adversary gained access to this role and the requisite functions?

PRINCIPLE 1 PHASE B

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Consequence-Focused Design principle can be applied to the requirements phase by considering the following questions:

1 **Are the consequences associated with each requirement traceable via documentation? For each requirement:**

- a How could this requirement be violated (including by failure or misuse of digital systems)?
- b What, specifically, would happen if this requirement were violated?
- c What specific parts of the system would be affected if this requirement were violated?

EXAMPLE: A material must be raised to a certain temperature before entering another part of the system. A temperature probe ensures this requirement is met. What would happen if the temperature probe was compromised?

2 **What requirements should be added to design and procurement specifications for systems and services in order to address potential high-impact consequences?**

3 **What requirements can be put in place to validate that the system is not entering consequence-prone operational states during commissioning testing, while in operation and when maintenance and upgrades are being performed?**

- a How can engineers enact requirements to lower potential impacts from consequence-prone operational states?

PRINCIPLE 1 PHASE C

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

DESIGN PHASE

The design phase includes elements of project architecture design, systems decomposition, and component-level design. The Consequence-Focused Design principle can be applied to the design phase by considering the following questions:

1 What areas of the system design are most linked to high impact consequences?

- a How can awareness of these linkages be leveraged to strengthen the system's overall design?

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

- a What consequence might be triggered and how would that event occur?

3 What parts of the design will contain digital components or subcomponents?

- a Where might the specific design of each component allow the potential for high-impact consequences that were not envisioned before?
- b How would a failure (frailty or attack/exploit) of each component affect the overall system?
- c How can system-level design account for additional consequences introduced by this component? What fail-safes[5] relative to this component should be built into the system-level design?
- d How can component-level design address additional consequences this component may introduce?
- e How else should component-level consequences be documented and managed?

4 What are the critical components and subcomponents in the system design?

- a What are the consequences of failure or misuse of each critical component?
- b What are the lead times for repair or replacement of each critical component?
- c How does this affect the system requirements?

EXAMPLE: In an electric transmission system, the transformer is a critical component with potential high-impact consequences, including the failure to deliver power. Misuse of digital features in a transformer could result in consequences from unscheduled outages to equipment damage and may have additional downstream effects. Repairs could require outages to last from hours to several days.

Lead times on replacements of transformers can be 60-70 weeks or more. Transformers are often built to specific requirements and are often not interchangeable.

5 See "fail safe" entry in: National Institute of Standards and Technology Computer Security Resource Center, "Glossary."

PRINCIPLE 1 PHASE D

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Consequence-Focused Design principle can be applied to the development phase by considering the following questions:

1 What specific consequence mitigations depend on the software/hardware/facility/process element under development and construction?

a Can this component's design and development address the consequences it introduces?

b Are there other areas of the system where capability development is needed to mitigate consequences induced by this component?

c Which, if any, features of this component serve as digital controls that prevent an identified high-priority consequence?

2 How will the component's consequence mitigation capability be verified?

PRINCIPLE 1 PHASE E

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Consequence-Focused Design principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1 Do verification and validation test cases encompass all envisioned undesired consequences?

a Do the implemented mitigations work as expected? Have mitigations that do not work exactly as expected been documented?

b Are the proposed mitigations still adequate for the potential consequences? Are there potentially more effective mitigations that should be considered?

c Some mitigations may require the full system or system of systems level testing to verify and validate. Has that requirement been documented and reflected in system test cases?

2 Did/could the integration of subsystems and components create the potential for new undesired consequences?

PRINCIPLE 1 PHASE F

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

OPERATIONS AND MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Consequence-Focused Design principle can be applied to the operations and maintenance phase by considering the following questions:

1 **What high impact consequences could be initiated by a failure to perform maintenance correctly or at the right interval?**

- a What training and support is needed to lower the potential or the impact of this occurrence?

EXAMPLE: Deferred maintenance on large water mains that degrade over time is a good example of this. As their condition deteriorates, the potential increases for an over-pressure event to cause catastrophic damage.

2 **What preventative maintenance tasks must be performed on what interval to ensure consequence mitigations continue to function as designed AND as intended?**

- a Would the under-performance of maintenance make undesired consequences more likely or impactful?
- b Are the impacts of deferring or under-performing maintenance effectively documented?

3 **What anticipated changes, modifications, or upgrades could alter the consequences of system failure, misuse, or compromise?**

- a How does this impact system operations? What is the process to reassess consequences before the change is implemented?
- b What are the consequences of code updates?

PRINCIPLE 1 PHASE G

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

RETIREMENT AND REPLACEMENT PHASE

The Consequence-Focused Design principle can be applied to the retirement and replacement phase by considering the following questions:

1 **What must be retrieved, archived, recovered, destroyed or disabled before releasing components from the system to their eventual disposition?**

- a What consequences could result from system components or data being acquired by a capable and motivated adversary?
- b Which system components or data could be leveraged to realize these identified consequences?

2 **Are there post-retirement requirements for any kind of operational readiness for the retired system?**

- a What high-impact consequences are related to those requirements, and what new mitigations are needed to ensure that the new requirements can be met?

3 **What in the planned retirement and replacement activities might put unexpected strain on the overall system protections and resilience?**

- a How could this lead to high-impact consequences?

4 **Are there previously unidentified or undocumented consequences this system protects the organization from?**

- a Is this documented in the system retirement plan?

5 **How will consequences associated with the replacement system be the same or differ from the retired system?**

- a What does the replacement team need to know about the list and priority of consequences associated with the system being replaced?

PRINCIPLE 1 PHASE ALL

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Consequence-Focused Design principle can inform these controlling processes by considering the following questions:

Project Management

1. How will the project plan adjust to necessary changes that result as consequences are considered?
2. How should schedules and workflows account for high-consequence events?
3. What is the process for gaining resources to adapt a design to a specific undesired digitally enabled consequence? Who makes those resources available?
4. What are the technical metrics to be used to determine the consequence of events? How can the right set of metrics be identified to compare the consequence of different events?

Change/Configuration Management

1. Do project processes allow for continual reassessment of consequence paths as mitigations and redesigns are performed?
2. How can downstream implications from changes to mitigate undesired consequences be avoided?

Risk Management

1. What is the practice for avoidance, acceptance, transfer, or reduction of potential digitally induced consequences?
2. How are costs of identified consequences estimated? How are mitigation costs estimated? How is the return on investment of mitigation estimated?
3. Does the method of requirements gathering across the project process adequately identify what could go wrong at any point and consider what would be required to make that consequence occur?
   a. Has consequence analysis been conducted with a diverse team of subject matter experts (SMEs) that will elicit consequences from multiple perspectives?
4. Which stakeholders are responsible for the potential harms for identified consequences? How are they included in mitigation decisions?
5. Have all high-impact, digitally induced consequences been identified as either a business risk and/or a risk to the community or nation? Have the interdependencies that each consequence would exercises been identified?
   a. Which consequences affecting the community are within the organization's scope to mitigate? Which are not?

PRINCIPLE 2

Engineered Controls

2

KEY QUESTION

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

Principle Description

Identify engineering design changes to process controls early in system design to eliminate or mitigate cyber risk, thereby reducing the need to bolt on additive IT security controls during implementation. Taken together, coordinated controls and processes are used to eliminate or significantly reduce the consequences that a cyber attacker could achieve. This requires integrating cyber experts and expertise into system design, engineering, and operations.

Engineered Controls Considerations at Each Lifecycle Phase

Whereas Principle 1: Consequence-Focused Design explores the wide range of potential challenges to a system's integrity, Principle 2: Engineered Controls seeks to implement and maintain the necessary protections of those systems against those identified challenges. Engineered controls form a security-related counterpart to the safety basis for systems, establishing a well-documented and maintained strategy of complementary and graded protective measures.

Historically, cybersecurity teams apply most security controls after the design and development phases are complete, protecting against the vulnerabilities that arose during the earlier phases. Following the parallel of safety basis, cyber-informed engineered controls bring this consideration forward to the early conceptual and design phases. This provides the opportunity to leverage the traditional safety Hierarchy of Controls.[6] Small design changes, such as the elimination of an unneeded wireless interface, can eliminate the possibility of certain attack vectors that may otherwise be difficult or costly to secure against.

One of the biggest benefits of establishing cybersecurity requirements early is the ability to incorporate many engineering risk management best practices, such as defense-in-depth and safe failure modes. The concept and requirements phases provide an opportunity to identify the external influences, the digital infrastructure that may interact with a system, and the involved stakeholders. Including engineered control considerations early can minimize the digital footprint of a system, avoid the sole reliance on digital systems, or substitute a dependency for a more easily managed alternative. Further, well-engineered controls can minimize the changes needed as the system or system environment changes over its lifecycle. As the system matures through design into operation, CIE controls continue to protect against the identified high-consequence cyber-initiated events by protecting the risk assessment assumptions and mitigations.

Digital systems can evolve rapidly. The key questions outlined within this section can identify controls that may potentially change the risks as initially identified.

6 The Hierarchy of Controls has five levels of action, in preferred order based on effectiveness: elimination, substitution, engineering controls, administrative controls, and personal protective equipment (PPE). See Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, "Hierarchy of Controls," last updated January 2023.

PRINCIPLE 2 PHASE A

PRINCIPLE 2: ENGINEERED CONTROLS

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Engineered Controls principle can be applied to the concept phase by considering the following questions:

1 How can the team prepare to identify and perform risk reduction through the Hierarchy of Controls to mitigate cyber-initiated high-impact consequences?

a What opportunities exist? Are there aligned practices that provide these elements that should be considered?

b How can the team plan to ensure these processes do not create unintended consequences during system operation or as a result of mis-operation?

2 What fundamental physics or energy sources, such as voltage, pressure, heat, and potential energy, will be involved in this system?

a What types of engineered systems are expected/required to enable the operations set forth in the CONOPS (e.g., IT, operational technology [OT], electrical, mechanical pneumatic, mechanical hydraulic, thermal, chemical)?

b What engineering controls are relevant to these specific engineered systems?

3 What stakeholders or personnel will use the identified engineered controls?

a Are the engineered controls aligned with required processes for operation, maintenance, and record-keeping?

b Which SMEs or personnel should be included in focused discussion?

c How are the designers working with system users to ensure that the suggested mitigations are maintained and will perform as expected throughout the operation lifecycle of the system and any operational dependencies they may create?

4 Which stakeholders do the identified engineered controls protect?

a Who could be impacted by the digitally induced high-impact consequences that these controls will mitigate, keeping in mind the interdependencies the consequences would exercise?

5 What key functional controls of the system will be dependent on digital technologies?

a What identified consequence does this control aim to prevent? What risk will this dependency introduce?

b How can teams mitigate these risks?

6 What are the system's regional and sector-specific cybersecurity regulatory requirements or security directives?

a Will this system be deployed across multiple regulatory domains?

7 How can cybersecurity assumptions and requirements be incorporated into the definition of needs for regional/external and business architecture?

a How much confidence does the team have in the security and resilience of existing architecture?

b Are there established best practices for each of the risk reduction methods of the Hierarchy of Controls that should be considered?

8 How will engineered controls impact existing (or normally used) safety controls?

a Do engineered controls need to be modified to accommodate different physical, regional, or environmental nuances?

b Do the engineered controls need to be modified to accommodate unique business needs?

9 Where might an alternate concept or the elimination of a low-priority need provide an opportunity to eliminate an undesired digitally induced consequence?

PRINCIPLE 2 PHASE B

PRINCIPLE 2: ENGINEERED CONTROLS

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Engineered Controls principle can be applied to the requirements phase by considering the following questions:

1. **Do requirements include cybersecurity and resilience needs?**

2. **How can requirements incorporate specific controls aligned with the Hierarchy of Controls for each identified high-impact consequence?**
   - a Are there aligned practices that provide these elements that should be considered?
   - b What requirements exist that are met by including digital controls? Can these requirements be satisfied through other engineered solutions instead?
   - c What are the potential conflicts between requirements and cybersecurity best practices, and how can they be mitigated?

3. **Are derived requirements associated with each mitigation or control documented?**
   - a Are the controls manual, hardwired, or digital?
   - b Can the controls be actuated remotely?
   - c What is the nature of the access control for each activation?
   - d Are the controls on by default or do they need activation or maintenance?

4. **Are analog or physical protections engineered into the system (where possible) for each high-consequence event identified?**
   - a Do the identified requirements incentivize this approach?
   - b Are there opportunities to leverage non-digital controls to reduce risk/dependencies for key functions of the system and subsystem?

PRINCIPLE 2 PHASE C

PRINCIPLE 2: ENGINEERED CONTROLS

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Engineered Controls principle can be applied to the design phase by considering the following questions:

1 **How dependent are the system's engineered controls on digital technologies?**

- a Can failure modes be eliminated or mitigated by adding mechanical, non-digital, or non-networked equipment (e.g., pressure relief valves, thermal fuses on electrical systems)?
- b What risks does each dependency introduce?
- c How can those risks be mitigated?
- d Is there an opportunity to leverage non-digital controls?

2 **Can controls be coordinated appropriately between systems? Are there dependencies or conflicts?**

3 **Is there a process to reevaluate and/or modify the controls strategy as the system design matures?**

4 **Are the mitigations included in the system design effective in the adverse operating modes identified for the system?**

- a How might abnormal and adverse operating modes impact planned mitigations?

PRINCIPLE 2 PHASE D

PRINCIPLE 2: ENGINEERED CONTROLS

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Engineered Controls principle can be applied to the development phase by considering the following questions:

1 **What fail-safe mode is used to select the materials used for fabrication?**

2 **Are the appropriate stakeholders and experts engaged throughout the development process to identify opportunities for risk reduction and identify potential failure modes not yet accounted for?**

PRINCIPLE 2 PHASE E

PRINCIPLE 2: ENGINEERED CONTROLS

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Engineered Controls principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1. **Do engineered controls need to be tested, verified, validated, and deployed in a specific order to achieve their intended purpose, given any dependencies?**
2. **Does the integrated quality control plan incorporate testing for digital failure, misuse, and abuse of engineered controls?**
3. **How will the team verify that the mitigations are present as specified?**
   a. What tests will be conducted during Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT)?
4. **How will the team validate that the mitigations put in place work as expected?**
   a. How is sequence testing phased to validate the engineered controls and the layered defenses?
   b. What specific test results would prove that mitigations accomplished what they set out to do?
   c. What validation mechanisms can the team use?
5. **Has each digital feature that serves as a control for undesired consequences been tested? What assumptions about failure or adversary control are implicit in the tests?**
6. **How can tests be designed to validate system-level consequence mitigations without harming the system being tested?**
   a. Can mitigations be sufficiently tested without breaking the system?
   b. Can outputs of mitigation testing be generalized to an operational scale?
   c. What assumptions or constraints are required for the mitigation to be effective? Have these been documented?

PRINCIPLE 2 PHASE F

PRINCIPLE 2: ENGINEERED CONTROLS

OPERATIONS AND MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Engineered Controls principle can be applied to the operations and maintenance phase by considering the following questions:

1 How are controls reassessed and monitored for changes impacting their effectiveness?

- a How can teams ensure alignment with the Hierarchy of Controls?
- b How is the potential for gradual weakening of controls through evolving operations accounted for?
- c How does the team identify and remedy ineffective implementation or administrative workarounds that may invalidate controls?

2 As new features or system patches are introduced, how is the team repeating the cycle of evaluating risk, developing controls, and documenting?

- a How can this cycle frame thinking about planned resilience, active defense, and layered defenses?

PRINCIPLE 2 PHASE G

PRINCIPLE 2: ENGINEERED CONTROLS

RETIREMENT AND REPLACEMENT PHASE

The Engineered Controls principle can be applied to the retirement and replacement phase by considering the following questions:

1 **How are the assumptions and bases for the engineered controls protected as the system evolves?**

- a Where might a system replacement violate prior assumptions of protections?
- b What does the team need to know?

2 **Of the controls put in place, which might not be available for the replacement team?**

- a What recommendations for design team on alternate controls could provide the same protections?

3 **Which best practices capture the replacement features of the outgoing system, process, and/or components?**

4 **What external factors or considerations could impact the retirement or replacement of implemented controls?**

- a What is the response to a component's vendor end-of-service support?
- b Will replacement parts reliably be available over the lifecycle of the system?

PRINCIPLE 2 PHASE ALL

PRINCIPLE 2: ENGINEERED CONTROLS

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Engineered Controls principle can inform these controlling processes by considering the following questions:

Project Management

1. Are contracts written to encompass engineered controls?

Risk Management

1. What past and present designs or modifications to systems, processes, or components have interdependencies or conflicts with other systems, processes, or components?
2. Is the necessary data from periodic reviews, maintenance, and trend analysis available to the stakeholders of each system or function?
3. Are the roles and responsibilities for high-consequence engineered controls well-documented and understood?
4. How do each of the opportunities of the Hierarchy of Controls allow us to accept, transfer, avoid or reduce potential undesired digitally induced consequences?
    a. How are these processes being documented?
    b. What metrics can be used to prove reduction or elimination of high-consequence CIE impacts?
    c. What downstream impacts exist for implementing this control (e.g., additional cost, maintenance)?
5. What metrics can be used to prove elimination of high-consequence CIE impacts?

Change/Configuration Management

1. What downstream impacts may result from changing engineered controls?
2. How will the team ensure continued safety, security, and resilience during change or configuration that impacts engineering control functions?

PRINCIPLE 3

Secure Information Architecture

KEY QUESTION

How do I prevent undesired manipulation of important data?

Principle Description

Recognize that each system has the potential to contain data linked to critical functions that should be protected from outsider view and, more importantly, from adversarial or failure-induced alteration. For each identified data stream, design a secure information architecture, guided by the consequences and impacts identified in Principle 1: Consequence-Focused Design. This will segregate the most important data and the systems that contain it to provide more control, protection, and monitoring of those systems and that data. Some mechanisms used include network segmentation, data segregation, data replication, and role-based access.

Secure Information Architecture Considerations at Each Lifecycle Phase

A project team can start early in system design to identify those data elements most tied to a potential critical consequence. Important considerations include where data elements 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 comparison to previously collected data elements.

Once the design is more mature and the underlying network and data service architecture are understood, engineers can create fine-grained digital controls along with specific zone and segmentation concepts.

PRINCIPLE 3 PHASE A

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Secure Information Architecture principle can be applied to the concept phase by considering the following questions:

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

- a How will the system communicate outside of the facility/system boundaries?
- b What is being communicated and for what purpose?
- c What assumptions are made about who receives those communications, and what kinds of confidentiality, integrity, and availability are needed?
- d How are external communications partners using this system's data? What must be done to ensure it is fit for purpose?
- e How does the system use incoming external data? How is it validated?
- f Are there resources to support communications requirements, including security, capacity, and speed?

2 How would the loss or manipulation of an external communications channel, or the data within it, affect the system?

- a Is each communication channel continuous or does it operate only as needed?
- b If an adversary had control of each communications channel, what consequences could result? (See Principle 8: Digital Asset Awareness for additional relevant considerations.)

3 What are the key data elements involved in the process that the system will execute?

4 For each of the process steps, what are the core inputs, outputs, mechanisms (people, tools, systems) and controls (safety standards, regulations, requirements)?[7]

- a Where is data originated, transformed, or finalized?
- b Where might there be an opportunity to verify or validate the outputs of one process step that are the key inputs to another?

7 U.S. Department of Commerce, National Institute of Standards and Technology (NIST), "Integration Definition for Function Modeling (Idef0)," December 1993.

5 **What otherwise unconsidered data elements are tied to critical consequences for the system?**

6 **Considering people, processes and technology and the consequences and critical functions identified earlier:**

a What assumptions are made regarding exchanges of information (e.g., between people and technology, process elements and people, technology and process, technology and technology) and the needs of the process?

- What consequences might occur if these assumptions were violated?
- Where might digital technology failure or cyber attack enable one of these consequences?

b What exchanges of information must happen for processes to function?

- Where do potential process actions flow from these exchanges?
- Which are the most important exchanges of information or data transformations, given potential consequences?
- How does authorization or trust factor into these exchanges of information?
- Which data exchanges drive process actions tied to identified consequences and involve data exchanges only between technology and process elements?
  - » Where might monitoring these flows or offering opportunities for validation of data provide resiliency, reliability, or necessary security to prevent a failure or manipulation from driving a critical consequence?

7 **Considering possible process anomalies, which additional data elements involved in the process would be useful to diagnose the extent or cause of the anomaly?**

a To what extent are these data elements independent of each other, either physically or digitally?

b Can physically and digitally independent data elements serve to diagnose the extent or cause of each considered anomaly?

8 **What are consequences of a loss of view and/or a loss of control (or confidence in those communications) to each architectural zone and/or conduit?**[8]

a How could this loss affect the process, depending on the data within the zones or conduits?

8 For definitions of denial of view, loss of view, loss of control, and denial of service, see MITRE, ATT&CK for ICS, "ICS Techniques," v13.1.

PRINCIPLE 3 PHASE B

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Secure Information Architecture principle can be applied to the requirements phase by considering the following questions:

1. **How is trust in users and systems established and revalidated?**
   - a Who is responsible for establishing, maintaining, and validating trust in users and systems?
   - b On what frequency should this revalidation occur?
2. **How long should each key data element in the process be stored on the device or system closest to where it is used in the process?**
3. **What data elements at which stages must be retained beyond the instantaneous process?**
   - a For how long?
   - b What are the view and retrieval requirements?
4. **For each key data element, where must monitoring be in place to identify deviations from desired data states or settings?**
   - a Is active monitoring necessary, or is logging combined with a periodic manual review process sufficient?
5. **What data elements must be replicated on multiple systems as part of the process function?**
6. **What are the institutional standard requirements for protecting the expected types of data within the system?**
   - a Where should those requirements be tailored to adapt to the consequences and impacts for the system or process?
7. **What data elements should be exposed for external monitoring to reveal potential process anomalies, provide process validation, and to validate security?**
8. **Are there requirements that control system communications, frequency of communications, expected throughput, protocols, and data exchanged?**
   - a How do requirements drive communication links that can withstand high-impact consequences from compromise or failure of communications?
   - b What assumptions are built into those requirements? How should that affect the design?

PRINCIPLE 3 PHASE C

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Secure Information Architecture principle can be applied to the design phase by considering the following questions:

1 **What techniques will be used to validate process data in creation, transformation, and finalization?**

2 **How will monitoring be used to validate data in the process?**

- a What techniques will be used to monitor that data?
  - What data and data collection mechanism will be used to collect out-of-band data for validation?
- b Where will digital monitoring techniques be used and where will analog be used?

3 **What engineering-based protection and verification could ensure that critical data has not been manipulated?**

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

5 **What are the consequences of loss of functionality or failures that occur in each architectural segment, zone, or conduit?**

- a How should identified consequences drive the design of security zones and boundaries?
- b Do any of the security zones or boundaries make necessary functions more difficult?
- c Do any of the security zones or boundaries add potential risk to operations?

6 **Is there any operating mode, including those outside of the norm, that might subvert the designed security protections?**

- a Can compensating controls built into the system protect data in adverse or exceptional operating modes?

7 **How will the presence of security controls and validations, particularly at process boundaries, prevent some of the potential consequences from taking place?**

8 **How will data be exposed for monitoring?**

- a How will exposed data be protected?
- b Are there any additional consequences that should be considered if that data is obtained by attackers or changed?

PRINCIPLE 3 PHASE D

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Secure Information Architecture principle can be applied to the development phase by considering the following question:

1 **How does the team responsible for developing security zones and boundaries receive information about the function, critical data, and consequences of the engineered system?**

PRINCIPLE 3 PHASE E

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Secure Information Architecture principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1. **How can testing of data controls and validations ensure that controls are functional from a security perspective and that they work as envisioned?**
2. **How can testing include the adverse operating modes already considered?**

PRINCIPLE 3 PHASE F

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

OPERATIONS AND MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Secure Information Architecture principle can be applied to the operations and maintenance phase by considering the following questions:

1. **How will data no longer needed for system functions be purged? When does that happen?**
   - a What processes and standards can ensure that purged data is securely deleted or destroyed and cannot be recovered?

2. **What aspects of security architecture, including maintenance of security zones and boundaries, are dependent upon human action?**
   - a What training, monitoring and other human performance reinforcement is necessary to ensure that humans involved in operations, maintenance, changes, and upgrades perform their roles as expected?
   - b Who is responsible for developing and maintaining a training plan?

3. **Are there any unanticipated adverse or extraordinary operating modes that have the potential to violate security controls or validation mechanisms placed on the data?**
   - a How can the information architecture evolve to protect data in those instances?

PRINCIPLE 3 PHASE G

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

RETIREMENT AND REPLACEMENT PHASE

The Secure Information Architecture principle can be applied to the retirement and replacement phase by considering the following questions:

1. **As the system moves towards retirement and replacement, what additional data needs to be archived?**
   a. What data will be purged?
2. **Are there any controls or validation mechanisms that a downstream system is depending on that may not function in the same way when the system is retired and replaced?**
3. **What system infrastructure is retained for use in other systems, and what are the security implications of this requirement to these other systems?**
4. **What requirements and design elements for controlling and protecting data should be implemented in the replacement system?**

PRINCIPLE 3 PHASE ALL

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Secure Information Architecture principle can inform these controlling processes by considering the following questions:

Project Management

1 What project management controls ensure that decisions involving secure information architecture are made collaboratively between engineering teams (who are aware of critical elements of operational processes), cybersecurity teams, and information management teams (who are responsible for creating the system architectures for creating, storing, transporting, maintaining, archiving, and purging data)?

Risk Management

1 How are risks associated with undesired manipulation of data identified, tracked, and resolved?

- **a** Who is responsible for tracking and resolving risks to data security?
- **b** Does this involve consultation with relevant officers from IT, engineering, and control system operational components to address consequences of unauthorized data manipulation?

Change/Configuration Management

1 How is change and configuration management arranged to govern decisions and changes that may affect the secure information architecture?

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 Description

Simplify the system, component, or architecture design and limit high-consequence, low-value complexity within digital functions at the outset. This reduces the opportunity for intentional or unintentional misuse of digital functionality. Design simplification includes reducing latent capabilities in digital systems that operators may disable or may not even be aware of, but which attackers could leverage.

Secure Information Architecture Considerations at Each Lifecycle Phase

Systems formed through acquisition often have more features than are explicitly needed to perform required functions. Though these features can be configured to be unavailable to authorized system users, they are accessible to adversaries and can be misused during system implementation, operation, and maintenance. These features can potentially lead to catastrophic impacts if used by malicious adversaries or unknowing operators.

In design simplification, engineers consider which features of their system are not absolutely necessary and, of those, which could lead to impactful adverse consequences if misused. Engineers must evaluate ways to reduce their system to the minimum elements needed to provide mission-critical functions and necessary resilience.

For each of the non-essential features, consider whether they can be removed entirely. When that is not possible, consider how alarms and alerts could be configured for when those functions are used, or whether undesired commands can be blocked before they are executed.

Design simplification holds great potential for improving cybersecurity, but must be balanced against all other business, operational, and safety drivers within the design process. Arbitrary removal of features can result in inadvertent removal of critical features, including some that may be only needed in infrequent scenarios (and are therefore not immediately recognizable as critical). For this reason, design simplification requires a detailed understanding of the system, including its requirements, architecture, and operations. Once this understanding is achieved, it will inform simplification efforts in each stage of the project lifecycle including development, testing, and operation. Verification must be done to ensure that unnecessary features have been removed, while all critical features remain.

PRINCIPLE 4 PHASE A

PRINCIPLE 4: DESIGN SIMPLIFICATION

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Design Simplification principle can be applied to the concept phase by considering the following questions:

1 What are the minimum functional capabilities needed?

- a In concept, is there anything that is likely to be implemented via digital means that is not explicitly needed?
- b Are there any conceptual features that have the potential to be low-value during normal operations but may result in, or contribute to, a high-consequence event if compromised?
- c Are any functional concepts redundant with other features and do not add measurable value to the overall system concept?

2 How might the regulatory environment limit or influence opportunities for design simplification?

- a Do regulations require the inclusion of certain functions or digital components?
- b If these functions or components increase complexity without adding value, is there any option to substitute or negotiate an alternative?

3 What factors shaped similar existing system designs? How have those factors evolved over time?

- a What alternative simplified design concepts exist, and how can their impact on overall cyber risk be evaluated?

4 Are there certain capabilities that are needed only at certain points of the lifecycle or during certain operating modes? If so, can the active use/exposure of these capabilities be tailored or modified?

- a How do capability requirements change during emergency operations, commissioning, startup operations, steady-state operations, shutdown, and decommissioning?

PRINCIPLE 4 PHASE B

PRINCIPLE 4: DESIGN SIMPLIFICATION

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Design Simplification principle can be applied to the requirements phase by considering the following questions:

1 Can a different, simpler device that contains fewer features meet the defined system requirements?

a Instead of installing a separate digital device, can another digital device be dual-purposed elsewhere in the system to meet these requirements?

b Are there alternate, non-digital means to satisfy a given requirement?

2 Where might design simplification affect or conflict with other stakeholders and requirements?

a Are there tradeoffs that should be evaluated for a given design simplification (e.g., loss of redundant control, reduced reliability, reduced operator visibility)?

b How should tradeoffs and conflicting requirements be adjudicated? Can the identified critical functions and consequences inform adjudication?

3 Are all system requirements traceable to the necessary functions identified in the CONOPS?

a How is “complexity creep” managed as requirements grow?

b What system requirements are driving the inclusion of digital devices in the system? Are there alternate, non-digital means to satisfy a given requirement?

PRINCIPLE 4 PHASE C

PRINCIPLE 4: DESIGN SIMPLIFICATION

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Design Simplification principle can be applied to the design phase by considering the following questions:

1 **Are each of the digital design elements traceable to a specific project requirement or critical operation/process?**

- a Are there any design elements that can be eliminated or simplified at this stage that are not necessary to satisfy any requirements or enable critical operations/processes?

2 **What simplification techniques and procedures can the owner/operator adopt to simplify design?**

- a Does the system have tested and accepted design templates that can be deployed?
- b Are there engineering standards that might constrain design options without sacrificing critical functionality?
- c Can an independent review of the design be organized to focus on simplification?

3 **Is the simplification analysis of the components and features of the systems well-documented and available?**

- a Have simplification processes been applied to the system previously, and can those processes be reapplied?
- b Have tradeoffs of simplification measures been documented?
- c Have simplification processes been applied to other similar systems, and can those processes be reviewed for applicability?

PRINCIPLE 4 PHASE D

PRINCIPLE 4: DESIGN SIMPLIFICATION

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Design Simplification principle can be applied to the development phase by considering the following question:

1 **Assuming the design has been successfully simplified, how can the team ensure complexity is not re-introduced during development?**

PRINCIPLE 4 PHASE E

PRINCIPLE 4: DESIGN SIMPLIFICATION

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Design Simplification principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1. **How are simplified designs verified to have eliminated unneeded features?**
2. **How are simplified designs validated to meet functional requirements?**
   a. Can a traceability matrix be created to verify functional requirements are met?
3. **How are simplified designs validated to confirm actual reduction of complexity and risk as analyzed?**
   a. Can an independent review of the design gather fresh perspectives on design effectiveness, simplicity, tradeoffs, and risk?

PRINCIPLE 4 PHASE F

PRINCIPLE 4: DESIGN SIMPLIFICATION

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Design Simplification principle can be applied to the operations and maintenance phase by considering the following questions:

1 **What support is included in system design to enable operations and maintenance (e.g., engineering workstations, remote access for third-party entities, human-machine interfaces [HMIs], operator laptop connections)?**

- a Can any of these be eliminated without compromising operations and maintenance effectiveness?

2 **What is the process for identifying and remediating complexity on already-implemented systems?**

- a What are the methods, such as reverse engineering or forensics, for identifying critical components and functions?
- b What additional methods need to be applied when an already implemented system does not match its own design documents (due to undocumented evolution, feature creep, etc.)?

3 **How is the original analysis for design simplification decisions preserved and used to inform system evolution?**

- a What is the design review and simplification process for evaluating potential additional features?
- b As new, desirable features are identified during operation, how can they be verified as “critical” and how can design simplification be applied to these features as they are implemented?

PRINCIPLE 4 PHASE G

PRINCIPLE 4: DESIGN SIMPLIFICATION

RETIREMENT AND REPLACEMENT PHASE

The Design Simplification principle can be applied to the retirement and replacement phase by considering the following questions:

1 During the retirement and replacement process, is there a process to evaluate if further design simplification can be made on the replacement system?

a Are there now more tailored components available that have eliminated unneeded features?

b Are there now components more conformant to standards that would enhance security and reliability?

c Are there other concessions for legacy hardware or software that are no longer present in the system or system interfaces?

d Is there a process to audit and identify unneeded features on retiring components?

PRINCIPLE 4 PHASE ALL

PRINCIPLE 4: DESIGN SIMPLIFICATION

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Design Simplification principle can inform these controlling processes by considering the following questions:

Project Management

1 How can the systems engineering management plan support simplification?
   - **a** What guidelines should the systems engineering plan have for simplifying digital aspects of design?
   - **b** What measures should be used for establishing "simplicity?"
     - How should simplicity measures account for the possibility of unverified/unverifiable trust?
     - Who can make these decisions and how are they made?
   - **c** At which stage(s) is this analysis performed?
   - **d** How can project management tools and processes support simplification?
   - **e** Where can the relative importance of simplification and security be weighed against other factors (e.g., cost, features)?
   - **f** Where might options for design simplification affect other stakeholders or interdependencies? How should that be adjudicated, documented, and tracked?
   - **g** What lessons learned from component design simplification can be incorporated in the system design simplification?

Risk Management

1 How can risk management tools and processes support simplification?
   - **a** How is the overall change in risk measured and compared between different design simplification choices?
   - **b** Have components already in their most simplified form been analyzed for residual risk?
   - **c** Are there areas of unverified trust that require additional layered defenses?

2 How will risk be tracked and managed as design modifications are made or proposed to simplify the system?

Change/Configuration Management

1 How can change management tools and processes support simplification?
   - **a** Do project processes allow for reassessment of design features and capabilities for further simplification and risk reduction throughout the system lifecycle?
   - **b** How are assumptions and analyses related to design simplification considerations documented and preserved?

PRINCIPLE 5

Layered Defenses

5

KEY QUESTION

How do I create the best compilation of system defenses?

Principle Description

Assume compromise and employ a defense-in-depth strategy, reducing the opportunity for a single failure to impact critical functions or create cascading failures. This includes building in diversity, redundancy, and system hardening for adequate defense and predictable degradation during a cyber incident.

Layered Defense Considerations at Each Lifecycle Phase

The best defensive capability for critical consequences is formed by an assemblage of controls, including physically 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. For each critical consequence identified, engineers and their operational cybersecurity support team work together to arrange the best compilation of defenses to avert the worst impacts from the prioritized consequences. This team works 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 5 PHASE A

PRINCIPLE 5: LAYERED DEFENSES

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Layered Defenses principle can be applied to the concept phase by considering the following questions:

1 For each of the system's critical consequences, what would a cyber attack on that consequence require?

- a What systems would an adversary need to access to create the specific effect?
- b How might an adversary need to traverse systems and subsystems in order to get access to the critical systems and components?[9]

2 What defensive mechanisms exist within the organization for systems like this one?

- a How do they provide physical or cyber protections?
- b Which are recommended by the cybersecurity team for systems like this one?
- c What resources are associated with their use?
- d How might these defenses be incorporated to build layered defenses?

3 How will the controls developed for Principle 2: Engineered Controls add to the layered defenses?

- a What additional layers are needed for each control to detect anomalies in the protection that the control provides?

4 What enterprise IT defensive layers will this system benefit from, e.g., enterprise firewalls, IT network monitoring, etc.?

- a Where might it increase the protective benefit to discuss the specific consequences prioritized for this system with the protection service owners?

5 Are the layered defenses identified for this system fully independent of each other and the system?

- a How might dependencies and interdependencies between the defenses, or between the defenses and the systems required for their execution, affect the potential for critical consequences?
- b Are there any common points of failure? How can they be mitigated?
- c What redundant system components and resources are needed to enable fully independent protection layers?

9 The MITRE ATT&CK Enterprise and ATT&CK ICS frameworks may provide helpful insight into how an attack might occur.

PRINCIPLE 5 PHASE B

PRINCIPLE 5: LAYERED DEFENSES

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Layered Defenses principle can be applied to the requirements phase by considering the following questions:

1 What are the key system requirements that drive decisions on layered defenses?

- a From which stakeholders should key system requirements be gathered to make layered defense decisions?
- b What are the subsystem requirements for layered defenses?
- c Are there any operational, environmental, or regulatory requirements that may drive specific defense mechanisms or requirements for how defense mechanisms work?

2 Do any of the system's functional requirements drive additional requirements for system defenses?

- a How do changes in system requirements affect layered defenses?

3 How are redundant defenses isolated such that failure of one has no effect on others?

- a What critical functions require redundant controls?
- b Could complete loss of any one redundant control affect others?
- c Are there single points of failure that could impact multiple redundant controls?

4 What are the critical system safety requirements for layered defense (e.g., the minimum and maximum ranges of temperature, flow, level, and pressure for the proper sizing of vessels, piping, valves, and instrumentation)?

5 What are the key aspects of the project architecture where layered defenses can be incorporated?

- a Are requirements for layered defense in line with the design principles and the CONOPS?
- b Are there any conflicts with requirements for other dependent systems or subsystems?
- c How could the execution of defensive systems negatively impact the system's performance? What requirements should control that?

PRINCIPLE 5 PHASE C

PRINCIPLE 5: LAYERED DEFENSES

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Layered Defenses principle can be applied to the design phase by considering the following questions:

1 What are the key elements of system design where layered defenses should be implemented?

- a What are the key system and subsystem interactions where layered defenses can be incorporated to avoid cascading failures?
- b What are the key system components where layered defenses can be implemented?
- c Where are the points within the system design where it is difficult to incorporate layered defenses? What can be done to address that?

2 What component-level security features will be considered as part of an overall defense-in-depth approach?

- a How does the design ensure layered defenses are effective for both cyber and physical system components?

3 Are layered defenses correlated to the reliability of the system and/or consequence magnitude?

- a Which critical functions are highest priority for the creation of layered defenses?
- b How are increased protections designed for systems with higher probability of attack? What additional protections are provided?
- c How are increased protections designed for systems with high-consequence outcomes? What additional protections are provided?

4 How can the mean time to detect an anomaly be shortened for critical functions and systems?

- a Are there automated monitoring tools that should be included in the design?
- b How are alerts managed? Does the design of the system provide a path for the right people to see and respond to the alerts quickly enough?
- c Are there specific conditions that should be considered abnormal for the system and that should be considered when planning system monitoring?

PRINCIPLE 5 PHASE D

PRINCIPLE 5: LAYERED DEFENSES

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Layered Defenses principle can be applied to the development phase by considering the following questions:

1 **How is the developer informed about the requirements for layered defenses for the elements under construction?**

2 **How do we ensure that layered defenses persist through system integration?**

- a Do subcomponent layered defenses complement each other?
- b Are there any layered defenses that contradict each other when integrated?

PRINCIPLE 5 PHASE E

PRINCIPLE 5: LAYERED DEFENSES

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Layered Defenses principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1. **Examine failure scenarios for individual components. How can layered defenses mitigate the impact of those failure modes?**
2. **How can the deployment of layered defenses be verified?**
   a. What metrics can be used to track or verify performance?
3. **How do we ensure the effectiveness of layered defenses for components and systems?**
   a. What kind of tests and verification approaches are needed for system-level assurances?
4. **How can tests be designed to validate the effectiveness of layered defenses without harming the system being tested?**
   a. Can layered defenses be sufficiently tested without breaking the system?
   b. Can outputs of testing be generalized to an operational scale?
5. **What constraints are required for the layered defenses to be effective? Have these been documented?**

PRINCIPLE 5 PHASE F

PRINCIPLE 5: LAYERED DEFENSES

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Layered Defenses principle can be applied to the operations and maintenance phase by considering the following questions:

1 What are the fundamental operational needs during commissioning, startup operations, steady state, emergency operations, shutdown, and decommissioning?

- a What layered defenses can enable primary operational needs during various operating conditions or states?
- b What are the automated operations during commissioning, startup operations, steady state, emergency operations, shutdown, and decommissioning?

2 What preventative maintenance tasks must be performed, and at what interval, to ensure layered defenses continue to function as intended?

- a Are the impacts of skipping or under-performing maintenance effectively documented?
- b What preventative maintenance tasks are needed for layered defenses to be continuously effective throughout different stages of system operation? How are they documented?
- c How does vulnerability patching impact the effectiveness of layered defenses?

3 How might external factors change the system's layered defenses over time?

- a How can the team ensure that layered defenses are still appropriate after system upgrades, configuration changes, and changes in critical consequences?

4 How will system upgrades impact the effectiveness of layered defenses?

- a What upgrades need to be made to layered defenses to adjust to the impacts of system changes?

PRINCIPLE 5 PHASE G

PRINCIPLE 5: LAYERED DEFENSES

RETIREMENT AND REPLACEMENT PHASE

The Layered Defenses principle can be applied to the retirement and replacement phase by considering the following questions:

1 **How can we ensure that defenses are still appropriate considering changes or degradation in defense mechanisms?**

2 **How can we ensure that necessary layered defenses are preserved during retirement and replacement?**

- a Are there improvements that can be made based on lessons learned from the outgoing system?
- b Does the new system introduce additional risk that requires new or expanded layered defenses?
- c Is the layered defense function still appropriate or necessary in the replacement system?
- d What changes need to be made in layered defenses to allow for secure system retirement or replacement?

3 **What layered defenses need to be operational to ensure continued, secure operations during retirement and replacement processes?**

- a What are the residual risks from keeping or removing aspects of layered defense during retirement and replacement?

PRINCIPLE 5 PHASE ALL

PRINCIPLE 5: LAYERED DEFENSES

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Layered Defenses principle can inform these controlling processes by considering the following questions:

Project Management

1. What resources are needed to deploy and maintain layered defenses across the system lifecycle?
   - a. What costs are associated with implementing layered defense?
   - b. Does the layered defense architecture justify the project cost?
2. Are single failures identified in this system occurring in other systems?
   - a. Can they be resolved with the same or similar layered defense?
3. Who are the key stakeholders that need to be engaged for approving the implementation of layered defenses?

Risk Management

1. What new risks could be introduced by this strategy?
   - a. How can these new risks be avoided, transferred, or mitigated?

Change/Configuration Management

1. How can changes to the system and business processes affect layered defenses?
2. Do project processes allow for continual reassessment of layered defenses as mitigations and redesigns are performed?
3. What compliance and regulatory requirements need to be addressed to implement layered defenses?

PRINCIPLE 6

Active Defense

KEY QUESTION

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

Principle Description

Employ real-time active capabilities and preplanned contingency actions to deter, detect, and delay cyber threat activity, enabling critical functions to continue operating resiliently until the threat has been neutralized and normal functionality is recovered.

Active Defense Considerations at Each Lifecycle Phase

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 begin to plan how defensive actions should be carried out in response to the most consequential events. System designers, operators, and the cybersecurity support team should understand the identified adverse consequences and how they could be realized, considering the system maturity, physical process, and kill chain.

From these plans, these teams compile a list of all anomalies, system conditions, and contextual circumstances that could bring about these consequences. Preplanned actions and triggers for their implementation should include specific roles and responsibilities across the spectrum of roles associated with the system, since active defense of the system may require support from a broad set of roles. Once defense plans are made, all teams should practice them regularly. They then incorporate feedback from both practice and real-world employment to continually improve the active capabilities and preplanned actions.

PRINCIPLE 6 PHASE A

PRINCIPLE 6: ACTIVE DEFENSE

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Active Defense principle can be applied to the concept phase by considering the following questions:

1 What precursor events could occur leading up to identified high-consequence events?

- a How might adverse consequences manifest within this system, as conceptualized?
- b How are operations staff expected to respond to these precursor events?
- c What will trigger temporary operational changes in response to a perceived threat? What conditions will indicate that it is appropriate to revert to normal posture?

2 Which stakeholders could support active defense measures during an active threat?

- a Who interacts with the system from outside the organization? Who would be involved internally (within the business unit)?
- b What is their role in deterring, detecting, and delaying threat activity or supporting critical functions' resilience?

3 How are potentially at-risk functions identified in normal and abnormal operating conditions?

- a How can we reduce the normal attack surface of critical functions while maintaining adequate functionality?
- b Are there alternative ways to perform the critical functions of this system?

4 How do functional needs influence possible active defense measures?

- a How can active defense mechanisms be developed and deployed to still meet core system needs, such as reliability or cost of operations?
- b How does the CONOPS limit and constrain temporary active defense plans?

5 What attacker and defender strategies and models are needed for active defense?

- a What assumptions have been made about defender and attacker capabilities?
- b What modeling assumptions could lead to inaccuracies?

PRINCIPLE 6 PHASE B

PRINCIPLE 6: ACTIVE DEFENSE

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Active Defense principle can be applied to the requirements phase by considering the following questions:

1 **What are the expected system states?**

- a What deviations from expected system states and anomalies might be initial indicators of one of the identified consequences?

2 **How can assets be segmented and critical functions isolated?**

- a What assets host and support critical functions?
- b Do these assets have dependencies or interconnections that could interfere with segmentation?
- c Which critical functions are dependent on connected assets?

3 **How do we ensure that active defense activities are not overly disruptive to critical functions?**

- a What countermeasures and compensating controls can support active defense while maintaining critical functionality?
- b What requirements for resilience should be considered within active defense, including time to recover and desired system functionality upon recovery?

4 **How are assumptions about system defense documented in system requirements?**

PRINCIPLE 6 PHASE C

PRINCIPLE 6: ACTIVE DEFENSE

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Active Defense principle can be applied to the design phase by considering the following questions:

1 What data and information are required for active defense? How are they acquired?

- a Where can data acquisition points be designed into the project's architecture?
- b How will sensors deliver the appropriate data, based on the design, that will help operators to recognize indicators of identified consequences and trigger active defense states?

2 How and where are operational contingency plans in case of an attack documented?

3 Which stakeholders should review the complete design and recommend design alternatives?

- a Have system operators identified multiple active defense concepts and validated how those may affect operations?
- b Have cybersecurity staff recommended multiple active defense concepts to deter, detect, and delay threats and facilitate recovery?

PRINCIPLE 6 PHASE D

PRINCIPLE 6: ACTIVE DEFENSE

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Active Defense principle can be applied to the development phase by considering the following questions:

1 How are active defense components developed?

a What controls, specifically including those for acquisitions processes, are in place to ensure timely delivery of active defense components?

b How will developers integrate active defense components into the overall system? At what stage of the fabrication process are these components to be integrated?

PRINCIPLE 6 PHASE E

PRINCIPLE 6: ACTIVE DEFENSE

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Active Defense principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1. **Does active defense effectively isolate or remove threats without compromising critical functions?**
   - a. What types of testing can be conducted to verify the efficacy of active defenses without breaking the system?
2. **What methods can be used to validate that the system will support selected concepts of active defense?**
   - a. How will defensive concepts change if the system doesn't function as expected?
3. **What is required for active defense processes to be effective?**
   - a. How does the testing, verification, and validation process enumerate assumptions and constraints?
   - b. Have these been documented?
4. **Do outputs of active defense testing sufficiently generalize to full-scale operations?**
   - a. If not, what additional testing is needed and how will it be performed?

PRINCIPLE 6 PHASE F

PRINCIPLE 6: ACTIVE DEFENSE

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Active Defense principle can be applied to the operations and maintenance phase by considering the following questions:

1. **How are active defense features/tools tested and validated during system operations?**
   - a. Are features consistently tested following maintenance, changes, and upgrades?
   - b. What ongoing exercises should be performed to ensure that active defense stakeholders and tools continue to work as expected?
2. **How are ongoing defensive expectations documented?**
3. **What processes are in place to ensure system operators are aware of triggers to temporarily change operations in response to a perceived threat?**
   - a. Who has the documented responsibility and accountability to initiate preplanned active defense measures?
   - b. Who is responsible and accountable for terminating these measures once they are no longer appropriate?
4. **What stakeholders should be notified if there is an active defensive threat or weakness to this system?**
   - a. How might active defense implementation impact stakeholders, and how should they be notified of impact?
   - b. What stakeholders (both within the business unit and externally) should be involved in the execution of active defense strategies? What is their role in mitigating the issue or providing external resilience?
   - c. What is the documented, exercised cross-notification procedure between operations/engineering and security teams?

5 **How might system operators be impacted by deployment of dynamic systems to remove or isolate a threat?**

6 **How does defense posture change to meet technological changes and upgrades?**

a How do changes and upgrades to personnel and process alter the system's active defense posture?

b How do these changes and upgrades alter the system's active defense posture?

7 **Do processes for troubleshooting and diagnosis of process anomalies include the possibility of digital sabotage?**

a What would an operator look for to confirm or deny the possibility of digital sabotage?

PRINCIPLE 6 PHASE G

PRINCIPLE 6: ACTIVE DEFENSE

RETIREMENT AND REPLACEMENT PHASE

The Active Defense principle can be applied to the retirement and replacement phase by considering the following questions:

1 **What assumptions about active defense will continue to be true for a replacement system? What will change?**

- a How are success and failure observations and lessons learned from active defense over the retiring system's lifecycle documented?

2 **If there are post-retirement operational requirements for the system, how will those requirements affect the delivery of active defense?**

- a What data may be contained on retired systems?

PRINCIPLE 6 PHASE ALL

PRINCIPLE 6: ACTIVE DEFENSE

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Active Defense principle can inform these controlling processes by considering the following questions:

Project Management

1 What resources must be deployed to maintain dynamic elements across the system's lifecycle?
   - **a** How can resources be incorporated and justified in the resource and management plan, rather than adding them after the fact?

2 Does the systems engineering management plan drive the development of specific stakeholder-involved active defense planning for each consequential unmitigated risk in the system?
   - **a** How can the systems engineering process ensure that the right stakeholders are engaged in planning for defensive activities?
   - **b** Can dynamic elements employed here be utilized in other systems as well?

Risk Management

1 What new risks could active defense employment introduce?
   - **a** Does active defense effectively isolate or remove threats without compromising critical operations?

2 What are the downstream impacts of implementing active defenses?

3 What compromises to critical operations were identified as potential outcomes of isolating or removing a threat? Should these also be considered in other areas or systems?

Change/Configuration Management

1 How do regulatory changes alter the system's active defense posture?

PRINCIPLE 7

Interdependency Evaluation

7

KEY QUESTION

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

Principle Description

Integrate input from multiple disciplines (e.g., safety, quality, maintenance, chemical) and departments (e.g., operational, business) to understand how digital misuse could affect their area of operations. This ensures engineers can adequately plan for risks introduced by system interdependencies that may be outside of the engineer's traditional purview.

Interdependency Evaluation Considerations at Each Lifecycle Phase

All systems have interdependencies. A system is either required for, or dependent on, other systems to function normally. These interdependencies can be direct or indirect: a relationship can be strong and unambiguous, with no intermediate steps, or it can be the result of cascading impacts through other systems or entities. Risks posed by *physical* interdependencies are often considered in the normal systems engineering processes, but cyber attacks or digital failures of interdependent systems may have significant effects on not only the system under design but also on upstream and downstream systems in the dependency chain.

Interdependencies represent special challenges to cyber-informed design. Often, systems that are required for (or dependent on) the system under design are engineered and controlled by others with different interests and design strategies. A cyber-informed interdependency evaluation can broaden a physical interdependency risk assessment to consider, for example, whether a cyber attack might make a given consequence more possible or more harmful than a purely physical hazard or event would.

Perhaps there are functions in an upstream system invisible to the system's operators that might cause untoward effects on the system if activated. Perhaps an attack on an upstream system might activate command logic on the system under design. Where might automation between interdependent systems cause cascading effects? And is the system being designed with an understanding of the potential impacts of a cyber attack on downstream systems—and the corresponding consequences of those disruptions?

PRINCIPLE 7 PHASE A

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Interdependency Evaluation principle can be applied to the concept phase by considering the following questions:

1 What dependencies does the conceptual system have on other regional systems, infrastructures, and services?

- a What other organizations will interact with the dependent functions, and how will those cross-organizational relationships manage their interactions and shared risks throughout the system's lifecycle?
- b Who should be consulted to enumerate how each interdependent system supports the delivery of the conceptual system's critical functions?

2 What entities provide critical inputs to this system?

- a What procurement strategies can be adopted that take resilience against cyber attacks into account?
- b Are some of the system's planned service providers more reliable, less volatile, or better prepared to recover in the face of cyber threats?
- c If access to a critical input is lost, where else can the system get it, and/or how will the system continue to execute its critical functions without it?

3 What dependencies does the conceptual system have on other internal business systems or infrastructures?

- a Are there subsystems within the conceptual system that are specially or uniquely required for the overall conceptual system to operate, and how might those subsystems be exposed to cyber risk?

4 What inputs do the system's critical functions require that are not directly and completely controlled by its owners?

- a Can inputs beyond direct control be obtained from alternative sources in case of a disruption to a primary source?

5 Where are potential points of interconnection frailty within the conceptual design?

6 What interdependencies apply to system-level critical function delivery?

a What pertinent stakeholders are involved in system-level critical function delivery?

b What sources supply system needs (e.g., data, power, water)?

PRINCIPLE 7 PHASE B

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Interdependency Evaluation principle can be applied to the requirements phase by considering the following questions:

1 Can additional requirements help mitigate or manage the risk of already identified interdependencies?

a What alternative/backup sources exist for established dependencies?

b What requirements for the system (physical/manual or digital/automated) can be added to its design to manage the impact of disruptions upstream or downstream beyond the organization's control?

c What measures can protect against dependency failures for critical function delivery needs?

2 What system requirements, if any, depend on external systems, people, assets, or services?

3 What system requirements, if any, depend on other internal systems, people, assets, or services?

4 How are components linked to others?

a What network interdependencies exist and how/where are they clearly mapped?

b What potential cascading failures may need to be accounted for?

PRINCIPLE 7 PHASE C

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Interdependency Evaluation principle can be applied to the design phase by considering the following questions:

1 Are supply chains of components in the design well documented?

a How are opportunities for disruptions caused by supply chain shocks minimized?

b Have designers studied the relative likelihood of cybersecurity-related hazards to component supply among different design choices?

2 Can the digital devices in the design alert interdependent downstream systems of impending service or product interruptions?

a Can they do so promptly to minimize dependent systems' mean time to detect and recover from interruptions?

PRINCIPLE 7 PHASE D

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Interdependency Evaluation principle can be applied to the development phase by considering the following questions:

1. **How are the inclusion of components and the interdependencies between them documented during the development process?**
2. **Are tools and resources for fabrication and assembly of the system subject to supply shortages from companies or entities outside of the organization's control?**
3. **What upstream and downstream dependencies impact resources used to develop the system (e.g., personnel, computing hardware and software, fuels, and other physical supplies)?**
   a. Can identified development components be replaced with alternatives if dependent systems are compromised?

PRINCIPLE 7 PHASE E

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Interdependency Evaluation principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1. **How can the team incorporate interdependent subsystem resilience into testing protocols?**
   - a. Are there process pathways that are singular and linear, without alternatives, and thus entirely dependent on the routine function of upstream processes?
   - b. How might alternative process pathways be validated to mitigate cyber-related interruptions to primary process steps?
2. **What metrics (e.g., public safety, financial consequences, critical function disablements) can measure how failure of this system produces downstream impacts to dependent systems?**
3. **How will dependencies be detected and verified?**
   - a. Can the same methods be applied to special types of dependencies, such as circular dependencies (i.e., what this system produces is necessary for the supplier) or those that are associated with known vulnerabilities or threats (e.g., from an untrusted and/or foreign source or with a history of failures)?
4. **Is there a third-party integrator or package vendor of hardware/software/configurations that may provide assurance of supply chain resilience and trust?**
   - a. If one does exist, is it necessary or can interdependency resilience be ensured without it?
5. **Are any inputs to process elements singular (i.e., only one input used, whether other inputs are available or not)?**
   - a. What are the higher-order effects of a failure of that single input?
   - b. Has consequence analysis been performed for the failure of that single input for downstream dependent systems?
   - c. Will the addition of an alternate process element produce a reduction of risk that is worth the necessary correction to the process, and can a cost-benefit analysis be designed and performed to assess this?

PRINCIPLE 7 PHASE F

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Interdependency Evaluation principle can be applied to the operations and maintenance phase by considering the following questions:

1. **How are third-party task-critical assets controlled for operational and maintenance requirements?**
2. **How are third-party test, measurement, and diagnostic equipment controlled for operational and maintenance requirements?**
3. **Is the system required (as a third-party component) for the maintenance and operation of other systems inside or outside of the organization or entity?**
   a. If so, what are the consequences of its failure to downstream systems?
4. **How might changes in interdependent systems drive the need for additional controls, capabilities, or investments?**
   a. What processes will ensure awareness of changes that take place?
   b. Are agreements in place for suppliers to alert the organization (during steady-state or stressed operations of the system) if their systems have been compromised by a cyber attack? Are agreements in place for what their mitigation strategies might be?
   c. Are assurances, standard operating procedures, and alerts provided to those dependent systems in case of a cyber attack that disrupts system operation?

PRINCIPLE 7 PHASE G

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

RETIREMENT AND REPLACEMENT PHASE

The Interdependency Evaluation principle can be applied to the retirement and replacement phase by considering the following questions:

1 **What entities will be responsible for, or involved in, the retirement and disposal of the system and its components?**

   a What cybersecurity-related situations have those entities faced (or might they face) that would prevent or alter the plan for system disposal?

2 **Are there specific pathways for a cyber-related interruption as the system is retired?**

   a Will the cessation of services or functions provided by components of the system compromise its cyber resilience and impact its ability to deliver services to dependent systems during its shutdown?

3 **Have system interdependencies (either previously known, established, or discovered during operation) been documented and shared with those that are designing a replacement?**

PRINCIPLE 7 PHASE ALL

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Interdependency Evaluation principle can inform these controlling processes by considering the following questions:

Project Management

1. How will interdependencies to/from the system be systematically identified, recorded, mitigated, and managed?
2. Can a dependency profile, outlining high-level categories (rather than specific instances of the category) of interdependent systems, be created and documented?

Risk Management

1. At what phases of the systems engineering lifecycle will the organization ensure it has identified, recorded, mitigated, and managed system interdependencies?
2. Is there a specific allocation of management funding to develop strategies for handling the risk of interdependent systems' cyber exposure?

Change/Configuration Management

1. How does the change/configuration management process account for introduction of new dependencies, or elimination of existing dependencies?
2. How is the system under design receiving ongoing information about changes in systems it is dependent upon for critical functions?
3. How is the system under design providing information about changes to external systems dependent upon it?

PRINCIPLE 8

Digital Asset Awareness

KEY QUESTION

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

Principle Description

The digitization of critical infrastructure allows incredible benefits, providing speed and automation of operations not previously possible. However, digital assets and digitized functions have weaknesses and frailty modes that are different 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 could not, and consideration and mitigation of these risks is vital to ensuring that the defensive measures for a system are cyber-informed. While current cybersecurity practices emphasize identification, tracking, and regular updates of digital devices, there is less emphasis on ensuring that engineers understand how unexpected operation of digital devices can affect process performance.

Interdependency Evaluation Considerations at Each Lifecycle Phase

Digital asset awareness begins by considering that any digital device is, at its core, a general-purpose computer. This means that, given the right conditions, an attacker could subvert a device's logic and cause it to ignore input, change values in command logic, or even execute commands or automated logic unexpectedly. Once engineers have identified the unexpected digital asset operation risks of their system, they can mitigate them in design, ideally with controls that are not solely digital in nature. Designers and operators must fully understand the impact to the system of a compromised digital device and plan mitigations accordingly.

Another aspect of digital asset awareness is ensuring a comprehensive understanding of the device, the subcomponents within it, its intended functions and capabilities, and its configuration from design through its operational life. Digital devices require maintenance, including patching and upgrades, and must be tracked by a wide range of measures (e.g., hardware model, software version, patch version, location, last update, last export, system function). Logs should be exported and, if possible, retained for forensic needs, along with known good copies of the latest software, configurations, and process logic.

These steps provide ongoing insight into the state of the devices, processes running on them, their maintenance, and any emerging risks arising from their vulnerabilities. It also ensures that they can be restored or replaced if needed.

PRINCIPLE 8 PHASE A

PRINCIPLE 8: DIGITAL ASSET AWARENESS

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Digital Asset Awareness principle can be applied to the concept phase by considering the following questions:

1 Which elements of the conceptual system are likely to depend on digital devices?

a Which elements depend on large numbers of digital devices all operating securely?

b Which elements depend on a device that is integral to operations, monitoring, or maintenance of a critical function?

2 What need does the inclusion of digital assets fulfill?

a What requirements are met by the use of digital assets? Is the device needed for safety, functionality, quality, etc.?

b What requirements can only be fulfilled by digital assets?

3 Can the breadth of digital asset use be minimized to reduce risks to critical functions?

a If the device uses a digital asset, how could it lead to an unacceptable consequence? (See Principle 1: Consequence-Focused Design for discussion of consequences.)

b Is there an alternative to a digital asset that could be used to fulfill the operational requirement?

4 What operations and maintenance will digital assets in the conceptual design require?

a What systems are likely to have digital components that will need updates, verification, or other IT or cybersecurity operational attention?

b How might operations and maintenance activities associated with digital assets make undesired high-consequence events more likely or more impactful?

c What procedures should be developed to ensure that operations and maintenance activities do not exacerbate the possibility for high-consequence events?[10]

10 These questions should be revisited as functions in the system are identified to have digital components through the design and development phases.

PRINCIPLE 8 PHASE B

PRINCIPLE 8: DIGITAL ASSET AWARENESS

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Digital Asset Awareness principle can be applied to the requirements phase by considering the following questions:

1. **Which core system requirements are likely to require digital assets to meet?**
   - a. What additional requirements can constrain the impact of or reliance on digital assets while still meeting the core requirements of the system?
2. **What information is included in requirements about the functional specifications of digital assets, potential abuse/misuse scenarios, and requirements guiding abuse/misuse prevention?**
   - a. What does the system need to not do? How can that be ensured? Does prevention depend entirely on digital mitigations, or are there non-digital elements to the mechanisms for ensuring performance?
   - b. How do misuse/abuse assumptions and requirements flow down into subsystem requirements?
   - c. How do abuse/misuse scenarios change operators' thinking about subsystems and their requirements?
3. **How are digital assets used to meet system requirements?**
   - a. For assets directly delivering critical functions, how could unexpected performance drive a deviation from system requirements?
4. **What requirements exist to drive selection of specific digital technologies?**
   - a. How are the cybersecurity requirements for digital technology informed by the engineering functions of the system?
   - b. What quality is required for digital components and subcomponents?
   - c. Do requirements thresholds include open-source and third-party components?
5. **How will digital assets be tracked?**
   - a. What system or subsystem requirements must be included to ensure accurate and appropriate digital asset tracking?
   - b. What procurement package specifications must be drafted for third-party vendors to enable asset tracking?
6. **How do misuse/abuse assumptions that are tied to critical consequences flow down into component requirements?**
   - a. How do the misuse/abuse assumptions drive requirements for components and subcomponents?

PRINCIPLE 8 PHASE C

PRINCIPLE 8: DIGITAL ASSET AWARENESS

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Digital Asset Awareness principle can be applied to the design phase by considering the following questions:

1 How is the system designed to perform each of its critical functions?

- a Where are areas of the design where the performance of critical functions depend upon the functionality of digital assets?
- b What controls exist to prevent a critical impact from occurring in the case of an unexpected operation or attack of the digital asset? Where are those controls supplied by digital technology?
- c Where must non-digital controls or mitigations be added to the design to ensure performance of critical functions?

2 Which of the requirements will be implemented via digital means?

- a What consequences could the use, misuse, or failure of digitally-enabled functions allow that the requirements did not anticipate?
- b How can the design account for these potential consequences?
- c What fail-safes should be built into the design?

EXAMPLE: A digital temperature probe reports incorrect information due to an attack on the logic of the I/O device; however, a pressure-relief valve ensures that high-pressure steam can safely escape if this condition is not corrected.

3 Does the digital asset inventory adequately detail all commercial off-the shelf digital devices as they are specified in the design?

- a Do digital device inventory details account for their provider's resilience to supply shortages?

PRINCIPLE 8 PHASE D

PRINCIPLE 8: DIGITAL ASSET AWARENESS

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Digital Asset Awareness principle can be applied to the development phase by considering the following questions:

1. **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?**
   a. How will these risks be mitigated?
2. **How is the development team tracking all components used in the development process?**
   a. Who is evaluating the included components for software/hardware risk due to foreign ownership, control, or influence?
3. **What kind of asset/component tracking will developers and contributors use?**
4. **How is tracking of known-good images, configurations, and logic ensured?**
   a. How are decisions regarding this process documented (including rationale and results)?

PRINCIPLE 8 PHASE E

PRINCIPLE 8: DIGITAL ASSET AWARENESS

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Digital Asset Awareness principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1. **How will unit testing evaluate security?**
   - a. For devices whose primary function is security, how will unit tests evaluate their configurations and effectiveness?
   - b. For devices whose primary function is not security, how will unit tests evaluate their role in promoting security?
2. **How will system tests verify that the controls on features where abnormal operation or attack could lead to critical consequences work as expected?**
3. **How will the system tests ensure that delivered digital assets contain the expected hardware, software, and firmware?**
   - a. How will a system test validate the configuration?
   - b. How will a test document and address discrepancies?
   - c. What methods will verify that the components are entered into tracking systems?
   - d. What methods will verify that the integration of systems and subsystems does not violate assumptions and requirements regarding functional limits?
   - e. Does integration of components result in any new elements or tightly coupled sets of elements that need to be tracked?

4 **How will system tests verify that known-good images, configurations, and logic can be applied as needed?**

5 **How is the completeness and accuracy of the asset inventory validated, and how will tests validate its ability to be adjusted over time, as needed?**

6 **Does validation demonstrate that each component, subsystem, and system does what it is supposed to and only what it is supposed to?**

- a What features exist on the components, subsystems, and systems that will not be leveraged by the system?
- b How are they disabled and how can monitoring alert on use of the disabled functions?
- c Has validation included sufficient testing of expected abnormal conditions or inputs to validate the reliability of the system in adverse operating conditions?

EXAMPLE: Some utilities use wireless, VSAT, or microwave links as backup communications if a primary communication mode fails. However, these pathways are not always monitored and may be incorrectly assumed to be unavailable to an adversary when not in use.

7 **Do the digital components used meet the defined quality and security standards?**

- a What methods can be used to verify the quality of digital components?

PRINCIPLE 8 PHASE F

PRINCIPLE 8: DIGITAL ASSET AWARENESS

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Digital Asset Awareness principle can be applied to the operations and maintenance phase by considering the following questions:

1. **What tasks will operations and maintenance staff perform that require direct interface with digital assets?**
   - a How are the operations and maintenance staff who interface with digital assets continuously reevaluating the potential for those assets to operate in unexpected ways?
2. **What process or continuous audit exists to track the functions of digital assets and what has changed during operations?**
3. **What operations and maintenance activities affect asset tracking?**
   - a What processes ensure that changes to software, logic or configurations are tracked?
   - b What triggers are in place to ensure updates to records?
4. **What digital maintenance is required (e.g., upgrades, patching, making backups)?**
   - a What is the process to document and understand how digital maintenance, changes, and upgrades could impact the function and risk profile of the system?
5. **Is there an established process to ensure that applied packages from updates/patches are necessary and desired?**
   - a What processes can validate that the patch works as promised (and only as promised)?
   - b What potential changes might the patch make to the system's critical consequences?
   - c Where patching may be delayed or not performed, what impact could the vulnerability have on the system?
   - d Can implementing alternate controls limit impacts or detect exploitations of the vulnerability?

6 How will digital assets tied to critical consequences change over time?

a How are these changes and upgrades tracked?

7 Are there potential cascading effects tied to critical consequences that could be introduced by modifications to digital assets?

a How are changes evaluated to understand impacts to other systems?

8 What might drive the addition of new digital assets to the system?

a What process exists to ensure that new digital assets introduced to the system are tracked?
b Are the new digital assets truly necessary to support a core function of the system?
c How might the introduction of a new digital asset impact risks tied to critical consequences?
d How do newly introduced assets enter the asset tracking program?

PRINCIPLE 8 PHASE G

PRINCIPLE 8: DIGITAL ASSET AWARENESS

RETIREMENT AND REPLACEMENT PHASE

The Digital Asset Awareness principle can be applied to the retirement and replacement phase by considering the following questions:

1 What digital assets are being replaced or retired?

a What function did the digital asset fulfill?

b Do replacement digital assets introduce new risks that are not yet documented?

c Can assumptions about the retired system be applied to the replacement system?

d Does the removal of a retired asset leave a security gap? (In other words, was the asset fulfilling a security function that must now be performed by some other asset?)

2 What information or artifacts could remain on digital assets after their removal from the system?

a Would the release of those artifacts present a risk to the system?

3 What information or artifacts must be kept (e.g., logs, configurations, data, system images)?

PRINCIPLE 8 PHASE ALL

PRINCIPLE 8: DIGITAL ASSET AWARENESS

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Digital Asset Awareness principle can inform these controlling processes by considering the following questions:

Project Management

1. What is the systems engineering management plan for digital asset inventory logging and tracking throughout its entire lifecycle?
   - a. Where is it stored?
   - b. Who has access?
   - c. How is it managed?
   - d. What information is included?
   - e. What are the processes for ensuring it stays updated and accurate, and who is responsible for updating it?
2. How does the systems engineering plan ensure that systems engineers challenge traditional functional assumptions about digital assets?

Risk Management

1. How does the organization-wide risk register include cyber risks arising from digital assets?
2. How does the register monitor outside sources of information regarding risk of different assets?
   - a. Is there a process for updating the risk register when new vulnerabilities are discovered on deployed assets?

Change/Configuration Management

1. How will the project perform change management?
   - a. How will it track changes to devices and systems?
   - b. How will new devices and systems enter the asset tracking program?
2. Do changes to the assets or configurations trigger a review of the security posture of the new or updated devices and the systems or subsystems of which they are a part?
   - a. Are there processes in place for these reviews?
   - b. Are these processes approved, and are all involved parties aware of them?
3. Does procurement of new assets trigger new security efforts focused on requirements analysis, system design, and testing of the new assets?
4. Does retirement of assets trigger an analysis to determine the security functions played by the assets and how those functions will be performed going forward?

PRINCIPLE 9

Cyber-Secure Supply Chain Controls

KEY QUESTION

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

Principle Description

Use procurement language and contract requirements to ensure that vendors, integrators, and third-party contractors are aware of and work with the contracting organization to mitigate the critical consequences identified within the processes and systems their products and services will support. Require that they deliver products that provide engineering-based protections to mitigate the critical consequences of digital risk. Validate that the security posture of the organization, their products, and their performance is appropriate for the impact their services and products have on the contracting organization's critical functions. Leverage contract enforcement mechanisms throughout the life of the contract to assure performance against the contract.

Cyber-Secure Supply Chain Controls Considerations at Each Lifecycle Phase

Even at the early design phases, engineers can begin to document assumptions about and establish the core security features that 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 digitally 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 those who may have a responsibility for ensuring them, including engineering and delivery leads, as well as procurement, cybersecurity, and system operators.

For each critical control or feature associated with the procurement, the team should consider how the control will be verified, when it can be verified and how often, and who can perform the verification (e.g., procurement, cybersecurity, operators). The team must build these processes into the requirements for development and system operations, and verification should occur more than once for controls that 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 exceed the general due diligence performed by the organization.

PRINCIPLE 9 PHASE A

PRINCIPLE 9: CYBER-SECURE SUPPLY CHAIN CONTROLS

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Cyber-Secure Supply Chain Controls principle can be applied to the concept phase by considering the following questions:

1. **Given the critical functions of the project—for the relevant sector, subsector, organization, region, and application area—what are the key supply chain concerns with obtaining the products and services needed to make the project successful?**
   - a Are there regulations, guidelines, or best practices that should be consulted?
2. **Which products and services to be procured are critical to system functions or to mitigations of critical consequences?**
3. **How does the organization designate critical products and services and ensure added procurement attention?**
   - a What additional procurement requirements does the organization define based on the critical functions the product or service will support?
4. **What assumptions does the system concept make about the availability, quality, and security of the critical items or services in the supply chain?**
   - a How can the organization make those qualities explicit in requirements?
5. **As different concepts for the system are explored, which offer the least supply chain risk?**
   - a Which concepts have the potential to use technology the organization is familiar with and knows how to mitigate?
   - b Which concepts will use suppliers with a history of good performance within the organization's supply chain constraints?
   - c Which concepts leverage technology that is initially and continuously available within appropriate time frames for the system?

6 **What opportunities exist for interruption in delivery of critical components needed on a reoccurring basis?**

- a Can these interruptions be avoided by using alternate methods of delivery or by arranging for multiple alternate sources?
- b Could these interruptions be accomplished via digital means? How can these be prevented?

7 **How will the organization communicate with vendors and service providers of critical products and services about the critical functions their capabilities will support in the system?**

- a How will the organization communicate how their product or service under procurement supports those critical functions?
- b How will the organization communicate the high-impact consequences of unexpected operations or attacks?
- c How will the organization document the expected security functions of the product under procurement aligned with these functions and consequences?
- d How will the organization communicate the vendor's accountabilities in mitigating and preventing those events?

PRINCIPLE 9 PHASE B

PRINCIPLE 9: CYBER-SECURE SUPPLY CHAIN CONTROLS

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Cyber-Secure Supply Chain Controls principle can be applied to the requirements phase by considering the following questions:

1 **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?**

2 **For services and components that are critical to system function, what avenues of supply chain attack exist?**

- a What are the entry nodes (i.e., initiating attack node in the supply chain) and the defense/mitigation strategies upstream, midstream, and downstream the supply chain?
- b Which of these supply chain attacks can be mitigated, and how? Which can be detected?
- c Which new supply chain risks might occur as the project moves through the development lifecycle? Which might present only during operations and maintenance? Which might present at system retirement?

3 **For critical components and services for the system under development, how can the design team become aware of the vendor's suppliers who might add undue risk in the supply chain?**

4 **What specific quality and security requirements apply to vendors/suppliers/service providers for critical system components and services?**

- a Are suppliers held to standards that might conflict with system requirements?
- b Are suppliers held to standards that are not necessary given the function the service or component performs?
- c Are suppliers held to standards that cannot be complied with? If so, what other mitigations could be put in place?

EXAMPLE: The terms of a procurement contract require no open-source and no foreign equipment within a critical subsystem; however, the vendors under consideration cannot field a product that meets those requirements.

5 What provenance requirements apply to critical products in the supply chain?

a Are there restrictions to using, for example, open-source or foreign-manufactured products?

6 Is there a risk that the procurement of critical products and services might be sourced via undesired means (e.g., secondary market, untrusted supplier)?

a How should component procurement requirements be framed to ensure this does not happen?

7 How can organizational procurement requirements benefit the project's procurements?

a Is there a vendor certification program that eliminates foreign-sourced high-risk equipment?

b Are there organizationally approved vendors capable of delivering on a procurement that requires them to eliminate features or develop additional controls on demand?

8 Based on the importance of the vendor's product or service in the system under design, what incident and vulnerability disclosure mechanisms—for both the product or service under procurement and for the vendor themselves—should be included in the contract?

9 What forms of security testing and verification are needed, given the criticality of the product or service to the system under design?

a Where might the terms of service prohibit needed testing? How can this be fixed?

b How will the organization use third-party testing to verify and validate the product and the security of its subcomponents? How should this be specified in system requirements?

10 What kinds of information about product subcomponents and internals (e.g., hardware bills of materials [HBOMs] and software bills of materials [SBOMs],[11] subcomponent vendors, use of open source) will the organization require for critical system components? What kinds of enumeration are required for external services critical to the system?

a How can contract language incentivize this?

11 See "SBOM" entry in: National Institute of Standards and Technology Computer Security Resource Center, "Glossary."

PRINCIPLE 9 PHASE C

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Cyber-Secure Supply Chain Controls principle can be applied to the design phase by considering the following questions:

1 For each critical product or service to be procured to create the system, consider:

a What critical functions does the product or service support?

b How could unexpected operation, failure, or attack affect the product or service lead to an undesired catastrophic impact?

c What undesired features may exist in the product or service? How can those be limited within the contracting process?

2 Does the design include critical functions dependent on components with high supply chain risks?

a How might supply chain disruption impact the system design?

b What dependencies exist between critical functions and “at-risk” components?

c What mitigation mechanisms can reduce the design risk?

3 Should any potential engineering controls be reconsidered due to identified supply chain risks?

a For any critical components or subcomponents with high supply chain risk, could the component be eliminated?

b Is there an available substitution component with a lower supply chain risk?

c What additional contract terms would reduce the potential for risk?

d Is there a way to change the design to accommodate an insecure, insufficient, or delayed component?

PRINCIPLE 9 PHASE D

PRINCIPLE 9: CYBER-SECURE SUPPLY CHAIN CONTROLS

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Cyber-Secure Supply Chain Controls principle can be applied to the development phase by considering the following questions:

1. **If critical software (including open-source) or hardware providers change during the project, how would that change affect the project?**
   - a How would it affect the identified consequences? What additional contract or engineering controls should be considered?
   - b How does this apply to changes in a vendor's suppliers?
2. **What documentation requirements does the organization use during the development process?**
   - a Is the development team producing a bill of materials or otherwise documenting all elements going into the product?
   - b Is this information readily available to those who may need it in the future to understand impacts of vulnerabilities or operations and maintenance needs?
3. **During the development process, how is the organization tracking, receiving, and storing critical components within the system?**
   - a Is the security of those processes aligned with the criticality of the components? Is there a risk of supply chain issues within the development, construction, and delivery process?

PRINCIPLE 9 PHASE E

PRINCIPLE 9: CYBER-SECURE SUPPLY CHAIN CONTROLS

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Cyber-Secure Supply Chain Controls principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1 For critical components, what aspects of the product's functionality and security requirements are actively tested?

- a How are controls deemed critical to the function of the system tested, verified, and validated?
- b What consequence scenarios are leveraged to drive test procedures?
- c How are variances documented and addressed?

2 How is vendor compliance with supply chain requirements validated?

- a How can vendor-supplied information provide insight on a critical component's fitness for use and its supply chain?
- b What is the process to evaluate all hardware and software components to validate that all prioritized supply chain risks were effectively met?

3 Are there specific security requirements relevant to integration that should be specified for integrators?

- a What information about high-impact consequences related to items under test is provided to testers?
- b If services or components are added at integration, how are they evaluated for supply chain risk?

PRINCIPLE 9 PHASE F

PRINCIPLE 9: CYBER-SECURE SUPPLY CHAIN CONTROLS

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Cyber-Secure Supply Chain Controls principle can be applied to the operations and maintenance phase by considering the following questions:

1. **What critical digital systems rely on components/materials that are needed on a reoccurring basis?**
   - a What functions are dependent on regularity of this supply?
   - b What processes ensure these reoccurring needs are fulfilled reliably?
   - c What alternatives are available if the supply chain cannot provide the needed components or materials?
2. **What ongoing vendor contracts ensure critical functions associated with the system?**
   - a Are any critical services provided remotely?
   - b How is the ongoing security of the service and the service provider assessed and ensured?
3. **Do contractors or vendors have persistent, long-term connections to the organization's system?**
   - a What contractual terms manage those connections?
   - b Is it possible to put controls on those connections to be activated at the organization's discretion?
   - c How could these connections put critical functions of the system at risk?
4. **Are the vendors using cloud services that will have long-term persistent connections to the system?**
   - a Is it possible to prevent unauthorized control actions on those connections via non-digital means?
   - b How can the potential for this connection to affect critical functions be limited?
5. **Have all vendor contracts been evaluated for needed changes in support and responsiveness once the system is operational?**
6. **How do contracts for maintenance incorporate supply chain controls associated with the critical functions identified for the system?**

7 What are the risks that a component or subcomponent within the system will remain in use after its support contract expires?

a Are assessments for support contract expiration regularly performed?
b What impact could loss of support have on the patches and support received?
c Do critical functions of the system require vendor support? How will the loss of vendor support impact critical functions of the system?
d How many systems can be unsupported before a mandatory repair and replacement must be initiated?
e Are there additional support options the organization can pursue for critical components?
f Do these risks warrant any reconsideration around layered defenses?
g What risks does the lack of product support put on planned resilience?
h Are there replacement options?

8 How are third-party suppliers and vendors involved in the system's active defenses?

a How are they informed about critical consequences of the system associated with their support requirements?
b Do contracts drive the specific time frames and measures of response aligned with the system's active defenses? How is this exercised?

9 Is there an established process to ensure that applied packages from updates or patches are necessary and desired?

a How are provided patches assessed?
b How is the supply chain for provided patches validated? How is the accuracy of the signing authority ensured?
c How is the risk of patching assessed? How is it mitigated?
d Is there an opportunity for micro-patching or taking only desired updates?
e What processes can validate that the patch works as promised (and only as promised)? How are potential changes the patch may make to the system's critical consequences evaluated?
f Where patching may be delayed or not performed, what impact could vulnerabilities have on the system? Can alternate controls be implemented to limit impacts or detect exploitations of vulnerabilities?
g What are the implications if an update or patch is refused?
h How can the team evaluate the effectiveness of the patch against critical vulnerabilities?

PRINCIPLE 9 PHASE G

RETIREMENT AND REPLACEMENT PHASE

The Cyber-Secure Supply Chain Controls principle can be applied to the retirement and replacement phase by considering the following questions:

1 What supply chain controls are needed to source replacement critical systems/components?

a Does the replacement procurement process for critical systems, services, and components use the same due diligence as the original procurement process above? How are supply chain risks assessed for incoming replacement components?

b How does the team ensure that replacement components are reliable?

c What existing assumptions about the cyber security of the supply chain will apply to the replacement system? What assumptions are different?

2 How does the organization retire the system's critical legacy subcomponents? How does it select replacements?

a How could lack of replacement availability impact the system's design, and therefore the necessary supply chain controls?

3 How might the existing supply chain processes change with the transition to replacement systems/components?

a Will acquisition requirements change?

b Will the replacement system require compliance with new regulations?

PRINCIPLE 9 PHASE ALL

PRINCIPLE 9: CYBER-SECURITY SUPPLY CHAIN CONTROLS

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Cyber-Secure Supply Chain Controls principle can inform these controlling processes by considering the following questions:

Project Management

1. Do procurement planning and control documents include vendor requirements and contractual language derived from the potential for cyber risk that their products, services, and security performance pose to the system?
   - a. How is vendor-provided procurement language validated against project requirements?
   - b. Have integrators and third-party contractors provided contract requirement alternatives and validated procurement criteria against their own standards?
   - c. Is defined procurement language effective to promote compliance with design specifications and organizational processes/controls for cybersecurity?
2. What overall organizational policies govern the formation of security requirements for contracts and procurements?
   - a. How are those policies relevant to this project?
3. How will potential cost increases associated with higher supplier standards affect the success of the project?
4. Is the contracting office equipped with the right knowledge, processes, and resources to apply contract requirements as needed for the system?
   - a. If not, how can the project team ensure procurements happen according to requirements?
5. How is the project team ensuring that the procurement language incorporates all desired project controls for high-consequence system risk?
6. What lessons learned can be documented for project process improvement?
   - a. Were the contracting mechanisms effective for cyber-secure supply chain controls?
   - b. Were there supplier relationships that simply didn't work/had to be terminated?
   - c. How could contracting mechanisms be improved to support future supplier relationships?

Risk Management

1. What is the organizational tolerance for supply chain risk?
   - a. How is the system risk tolerance different from the organizational risk tolerance?
   - b. What are the key concern focus areas regarding the supply chain?
   - c. What organizational measures are in place to prevent, validate, and verify supply chain risk and risk mitigation strategies?
2. Which supply chain criteria are elevated to go/no-go requirements?

Change/Configuration Management

1. How can risks that arise from a system lifecycle outliving the supplier relationship be managed?
   - a. What is the standard process to follow once critical system components are out of warranty or out of support?
2. Is the plan for system lifecycle support documented? Will the vendor or asset owner manage the system throughout its lifecycle?

PRINCIPLE 10

Planned Resilience

10

KEY QUESTION

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

Principle Description

Expect that any digital component or system may be compromised at some point during its lifecycle, and plan for continued operation during and after a cyber attack that degrades digital controls.

Planned Resilience Considerations at Each Lifecycle Phase

Planned resilience anticipates how critical functions could fail due to a cyber incident and incorporates design or planning elements that create conditions for safe failure or continued operations under these circumstances. It is important to understand the system’s different failure modes, including how to operate through them, even if it is at a lower level of performance or reliability.

Engineers and designers should create a set of known diminished operating modes that, though not ideal, can be built into expectations for well-understood modes of operation. Within each diminished operating mode, engineers can make plans for what would cause that mode, how that mode would function, and what changes the mode would have on staff, systems, safety guidelines, performance, or other system conditions. Once these diminished conditions are part of the overall set of system operating modes, it is reasonable to train, exercise, and assess performance in each of the pre-defined 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. With these modes in place, the team may need to alter the system design to allow limited manual operations options when digital systems are not operating or trusted.

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 10 PHASE A

PRINCIPLE 10: PLANNED RESILIENCE

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Planned Resilience principle can be applied to the concept phase by considering the following questions:

1 What people, materials, and equipment are needed to withstand and recover from a catastrophic event?

a Where will these resources be needed?

b Will these resources be used to meet critical system operation objectives, including supporting the required time to recovery for critical functions, sustaining other critical system functions, and enabling graceful degradation?

c What is the right level of responsibility for different stakeholders?

2 What are the critical system functions for which resilience must be planned?

a Should specific resilience plans be made for any potential high-priority system or sub-system needs with a large digital dependency?

b What would digital resilience and diminished operating modes look like for the system?

3 What are the limits of acceptable degradation for the system's critical functions?

a How can the layered defenses developed for Principle 5: Layered Defenses help ensure that limits are not exceeded?

b Does this meet our documented goals for resilience of the critical function affected?

c What is the CONOPS for a system in a degraded state?

4 Can the system operate under abnormal operating conditions that could be created by alternative sources or inputs?

a What is the range of conditions that would allow continuity of operations, even if stressed?

b What conditions is the system expected to operate under (i.e., normal range), and what conditions might it be required to operate under (i.e., possible range)?

c Who would be responsible for various key roles and responsibilities in an abnormal operating condition?

5 Are there regional interdependencies with potential digital causes or modes that resiliency planning must be adapted for?

a Using the interdependency analysis (conducted during the concept phase of Principle 7: Interdependency Evaluation), what can be inferred about the impacts of those dependencies on system resilience at a regional level?

b Has interdependency analysis information been disseminated and discussed with the right parties to make it useful in resilience planning?

6 Are there external/regionally driven resilience considerations for the system?

a How reliable are the critical functionalities (power, communication, etc.) that the system would depend on?

b Have conceptual alternatives been identified to maintain system operation if those functionalities become unavailable?

c How is the reliability of the system impacted when upstream interdependent systems are in diminished operating modes?

d What resilience measures can help address these potential impacts?

7 What are the regional impacts of a resilience failure of the system?

a Has the organization had conversations with the key regional stakeholders that depend on the system?

b Based on these conversations, should any additional resilience needs be considered?

c Are there resilience resources that can or should be shared?

8 Has resilience been specifically considered as part of the concept of operations for the system?

a How can the concept of operations be optimized to deliver on both critical system functionality and planned resilience?

b Is operation in a degraded cyber or physical state acceptable as part of the concept of operations?

c If so, should there be a separate concept of operations for the system in a blue-sky state and in a degraded state?

9 What cyber incident response strategies will be utilized?

a Conceptually, how should the system respond, adapt, and recover from cyber incidents?

PRINCIPLE 10 PHASE B

PRINCIPLE 10: PLANNED RESILIENCE

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Planned Resilience principle can be applied to the requirements phase by considering the following questions:

1 What specific resilience requirements must be included?

a Has the minimum requirement for the system to be considered operational been defined in order to understand what successful system adaptation looks like?

b What are the specific resilience requirements associated with system and component recovery time; maximum product, productivity, or functionality loss; or the maximum amount of downtime that can be endured?

c What outputs—which may be controlled by others—does the system enable?

2 Do system requirements include a manual operation mode for any system that otherwise is controlled by an automated information system?

a Have dependencies on automated systems been completely removed from manual modes?

b What bypasses may exist in compromised systems and subsystems? What higher-consequence systems may need parallels on different technology or manual operations?

3 Should it be a requirement to isolate or bypass compromised subsystems and still have the system function?

a What would this look like, and is it described in sufficient detail in the requirements?

b In a degraded state, are there subsystems that should be required to be eliminated to simplify the attack surface or resilience environment?

4 How might enabling remote access for vendors or internal operations impact overall system resilience?

a If remote access is allowed, should additional controls such as increased monitoring and encryption be required?

b Do system requirements put adequate restrictions and protections in place for remote access to ensure system resilience even if remote access is compromised?

PRINCIPLE 10 PHASE C

PRINCIPLE 10: PLANNED RESILIENCE

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Planned Resilience principle can be applied to the design phase by considering the following questions:

1. **What are the critical features of components that serve key system functionalities?**
   a. How can they be optimized for planning resilience at component level?
2. **What is the fail-secure (similar to fail-safe) configuration for each component, and how does that affect the system's resilience posture?**
3. **What redundancy is present in system components?**
   a. Is there data that needs to come from multiple sources to ensure data availability and integrity?
   b. Are they "hot swappable" or must the system be shut down for repairs?
4. **How can the mean time to recover be minimized?**
   a. Are there ways to automate portions of the recovery?
   b. Have the backups been tested regularly to ensure they are not corrupt?
   c. Is the recovery process well defined and tested regularly?
   d. Does the recovery team have the right tools and resources?

PRINCIPLE 10 PHASE D

PRINCIPLE 10: PLANNED RESILIENCE

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Planned Resilience principle can be applied to the development phase by considering the following questions:

1 What does it mean to inject resilience into the software and hardware for each component?

a Is there a best practice configuration/setup guide for the component that could be followed that already considers resilience?

b Can resilience considerations be added as a specification for vendor procurement packages?

2 Is resilience being considered during the development process?

a Can system monitoring begin during the development process?

b Are team members encouraged to report lessons learned during the development process that might strengthen resilience?

PRINCIPLE 10 PHASE E

PRINCIPLE 10: PLANNED RESILIENCE

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Planned Resilience principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1 How will resiliency measures be validated to work as desired?

a What methods can be used to validate resilience measures with no adverse consequences?

b What types of data are needed to validate the resiliency measures?

c Can testers use random component shutdown to inform consequence evaluation and engineered controls to validate that resilience works as planned?

d How does this validation account for high-consequence feature sets?

2 What unit tests are needed for determining and testing a fail-secure state for components and the system as a whole?

3 What are the critical subsystem functionalities that need to be verified to provide for planned resilience of the overall system?

PRINCIPLE 10 PHASE F

PRINCIPLE 10: PLANNED RESILIENCE

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Planned Resilience principle can be applied to the operations and maintenance phase by considering the following questions:

1 Does the system's incident response plan contain a specific resilience focus?

- a Are plans for functional restoration adequately independent of exploitable digital controls?
- b Do roles clearly define who performs which tasks during an incident?
- c Are incident response plans and/or business continuity plans reviewed regularly to ensure they are kept up to date and remain effective?

2 What are the training requirements for resilience topics?

- a Are staff receiving the correct amount of resilience training that is applicable to their role?
- b When enabling functions have been outsourced, how does internal staff access this institutional knowledge in a timely manner when needed for troubleshooting/investigation, response, and recovery?
- c Are tabletops or other hands-on training and exercises performed regularly?

PRINCIPLE 10 PHASE G

PRINCIPLE 10: PLANNED RESILIENCE

RETIREMENT AND REPLACEMENT PHASE

The Planned Resilience principle can be applied to the retirement and replacement phase by considering the following questions:

1 **Have resilience lessons learned been properly documented and shared?**

2 **If a new system is to be commissioned before the retirement of the old system, are there potential resilience risks to either system during the transition?**

PRINCIPLE 10 PHASE ALL

PRINCIPLE 10: PLANNED RESILIENCE

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Planned Resilience principle can inform these controlling processes by considering the following questions:

Project Management

1. Is there a resilience plan for the system? Is there a template for creating them? Who owns the resilience plan?
2. Does the project management plan include the budget and time required to implement resilience measures and train staff on specific resilience principles?

Change/Configuration Management

1. Does the configuration management plan consider resilience goals?
   - **a** Do changes go through an adequate review to ensure the organization fully understands how that change affects the resilience of the system?
   - **b** If the system is required to stay operational, is there an environment where the change can be tested first?

Risk Management

1. Have risk assessments been performed at the appropriate times during the lifecycle of the system?
   - **a** Were confidentiality, integrity, and availability requirements considered during the risk assessments?
   - **b** Did an independent review team conduct an assessment to determine if the requirements were implemented correctly and truly mitigate the risk to the expected level?

PRINCIPLE 11

Engineering Information Control

11

KEY QUESTION

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

Principle Description

Protect sensitive engineering records (e.g., requirements, specifications, designs, configurations, testing) that, if released, may provide attackers critical information that places those systems at greater risk.

Engineering Information Control Considerations at Each Lifecycle Phase

Engineering information is a broad category of knowledge in various forms, including concepts, observations, specifications, procedures, logs, metadata, and more. This information can be stored and used in many different forms including on paper, in non-volatile storage, within systems, or by humans in the form of institutional knowledge. The sheer volume of information generated throughout the lifecycle of digital systems provides potential adversaries with an understanding of weakness, vulnerability, and capability not just of a single system, but also the facility or even sector. External and public-facing interfaces can provide a wealth of system knowledge through job postings, conference papers, procurement information, and news stories.

The protection of engineering information begins in the concept exploration phase by identifying what information could be misused, selecting a framework to securely contain and exchange information, and protecting the sensitive information collected on the environment in which a system will operate. As system engineering progresses, engineering information control must also consider not only the documentation surrounding a system, but also the availability, integrity, and confidentiality of the engineering data as it flows between digital systems, between internal stakeholders, and between external organizations such as customers, vendors, and regulators.

A robust information security posture identifies sensitive information and the systems that create it. This posture calls for protections during the use and transit of that data and ensures that the final destruction or archiving of sensitive information is carried out to minimize the resources and knowledge an adversary could use in an attack.

PRINCIPLE 11 PHASE A

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Engineering Information Control principle can be applied to the concept phase by considering the following questions:

1 How will sensitive information be identified as it is collected and created throughout the lifetime of the project?

a Who will determine what constitutes sensitive information about the system, and how will they make those decisions?

b Are there levels of data sensitivity, and if so, are there graded levels of protection?

c Could any of the information that the project will gather from the surrounding environment be used by an adversary to gain information not otherwise available?

d What stakeholders need to be involved to ensure potentially sensitive information and relevant context are correctly identified and protected?

2 What information must be shared externally and how will it be sanitized and protected?

a What information must be shared through mandatory reporting requirements, and what controls will protect against accidental or unnecessary disclosure?

b How can the impacts of external partners breaking information protection agreements be limited?

c Could an adversary reasonably derive sensitive system information from hiring and recruitment data?

3 What agreements and contractual obligations are needed to protect sharing sensitive information with partners and vendors?

a What potentially sensitive information can an outsider infer from the system needs or from a mandatory public bid solicitation process?

b How can that information stay controlled while still informing the design and development process?

c How will potentially sensitive design elements be protected?

d How should non-selected concepts or the rationale for design choices be protected?

e Could an adversary reasonably derive sensitive system information from similarities and standards in the sector?

4 How will sensitive information be protected during use, storage, and exchange between digital systems?

a Which elements of functionality described in the concept of operations have sensitivity?
b Can information be protected from detection?
c How is document revision handled and how could an adversary use the changes in different revisions to infer design outcomes?
d Projecting forward into requirements and design, how will the potential for sensitivity increase or change?

5 How will the needs of various internal stakeholders who will use sensitive information associated with the system be balanced?

a Are roles defined and privileges associated with access to data sets?
b What other system design efforts or existing elements of operations have sensitive information, and how is that information shared between relevant stakeholders?

6 Does a review of sensitive information illuminate additional consequences that should be protected against?

PRINCIPLE 11 PHASE B

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Engineering Information Control principle can be applied to the requirements phase by considering the following questions:

1 How do requirements ensure that all designed, constructed, operated, maintained, and retired elements of the system receive an analysis of potentially sensitive engineering information and adequate protections?

a What system requirements are sensitive?
b How can they be protected?
c How might sensitivities change over time?
d How can protection mechanisms be expressed as requirements?

2 How are engineering information controls passed to external stakeholders, such as subcontractors and distributors?

a Do contracts and other agreements control the sharing, retention, and disposal of technical details?

3 Do the requirements establish consistent and appropriate levels of system data protection through generation, utilization, and storage?

a How do sensitivities, based on the requirements above, trickle down to subsystems/components?
b What elements not considered sensitive at the overall requirements level might acquire or lose sensitivity when considered at the subsystem level?

PRINCIPLE 11 PHASE C

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Engineering Information Control principle can be applied to the design phase by considering the following questions:

1 What elements of design reflect the requirements for protection of engineering information?

a Are any tradeoffs necessary and if so, what elements allow us to make a discreet selection?

2 How is the sensitive information classification process re-engaged throughout the design process?

a Are there actions resulting from the design that create or generate the potential for sensitive engineering information not formerly defined in requirements?

PRINCIPLE 11 PHASE D

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Engineering Information Control principle can be applied to the development phase by considering the following questions:

1 How is sensitive engineering information that is produced or exposed through development protected?

a How will the team protect sensitive produced items (e.g., code) ?
b How will the team protect elements within produced items that are, themselves, sensitive?
c How will the team protect the sensitive facts or requirements that led to the production of items? What deployed configurations, logic, scripts, and process specifics should be safeguarded? How are these details that describe control/monitoring, data flow, process state, access control, and authentication measures within the assets protected?
d What potentially sensitive engineering data may be inadvertently created or maintained by logging, metadata, or other automated processes?
e What could an outsider infer about the system's hardware by knowing what software or licensing it is using and vice-versa?
f How is sensitive information protected from subcontractors who may not have been part of the design process, but are brought in to execute part of the system development?

2 How are contracts, procurement, and reporting documents written to enforce the established sensitivity requirements?

a Are partners providing the protection measures identified for engineering information either transacted as part of a procurement or within the systems being procured? How is this verified?
b What happens as a result of a failure or breach?
c How is the information in SBOMs/HBOMs and other mandatory disclosures adequately protected?

3 What features enabling development and troubleshooting could potentially reveal sensitive information?

a Are there service access features? Will they be accessible in the finished product?
b Are there debugging features in the selected hardware, firmware, or software?
c What hardware features being added or left off equipment could be used by an adversary to infer how that equipment will be used in the system?

4 Where might sensitivities not be under the organization's control or direction (e.g., supplier proprietary information), and what additional requirements and protection mechanisms will that information require?

PRINCIPLE 11 PHASE E

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Engineering Information Control principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1 What information is generated during testing, and how is it classified and protected?

- a What information about a system can be inferred from diagnostic tools, error codes, or logs?
- b What information from each phase of testing is preserved, and by whom?
- c How is design, development, and verification data from various partners archived and deleted?
- d What protections are in place for information revealed by component, system, and skid level testing or modeling results (such as detailed function and possibly thermodynamic, physical, or chemical properties)?

2 How are conflicts between preservation of data for future troubleshooting and training balanced against information security measures?

3 How are system information design protections verified and validated?

- a How is engineering information digitally protected while in use in the system, in transit on the network, and when resting in archives or backups?
- b Is the organization utilizing appropriate techniques and methods, such as penetration testing and open-source intelligence (OSINT) reconnaissance, to identify potentially exposed sensitive engineering information?

4 As development work concludes with specific contractors/vendors, what verification process will be used to ensure that they destroyed sensitive engineering information related to the project?

a During Site Acceptance Testing (SAT), what project contractors and providers must undergo final verification of deletion of sensitive engineering information?

b Is there any engineering information they need to keep?

c How is information storage and access control managed over time?

5 How is the production of system details residing with the integrator entity tracked, minimized, and controlled?

a What component-level control logic/configurations, communications (data flows and IP), and operational process details do system/subsystem integrators for the production environment have at deployment?

PRINCIPLE 11 PHASE F

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Engineering Information Control principle can be applied to the operations and maintenance phase by considering the following questions:

1 **What is the process to identify and respond to changes in engineering information sensitivity or control processes through the lifecycle of the system, including through operations, maintenance, changes, and upgrades?**

- a What potentially sensitive information could someone unintentionally share through operational occurrences?
- b What could an outsider observe or infer about systems through job postings, public tours, conferences, websites, or to external visitors?
- c What engineering information belonging to other organizations, such as vendors or contractors, is kept by the system owner or other service providers?
- d What procedures are in place to respond to inadvertently disclosed sensitive information?
- e How is information from a new system, change in process, or other disruption evaluated for sensitivity?

2 **How is vendor/contractor proprietary information destroyed or dispositioned once it is no longer needed?**

- a Do engineering information controls plan for vendor/contractor changes, mergers, and acquisitions?

3 **Do information security policies that overly constrain workflows "encourage" workarounds and bypasses?**

- a How can controls over workarounds and bypasses be enacted?

4 **How is the transfer and use of engineering information appropriately restricted to authenticated people and systems?**

a How are data ownership responsibilities and non-repudiation implemented?

b How are credentials and access granted to new users? How is access revoked when no longer needed?

c How is access to critical systems managed when under deadlines, under adverse operating conditions, during maintenance, and through unexpected problems?

d How is data destruction or revoked access verified?

5 **Are there procedures to destroy, disposition, or release for publication any information no longer considered sensitive? How are product and service providers informed?**

PRINCIPLE 11 PHASE G

RETIREMENT AND REPLACEMENT PHASE

The Engineering Information Control principle can be applied to the retirement and replacement phase by considering the following questions:

1 What are the regulatory and organizational data retention policies and how will they be enforced?

a Does record retention engage the risk management process?

b What record retention is important to the company and why?

c How is record retention and subsequent data destruction verified?

2 How can sensitive information be sanitized from outgoing systems while preserving institutional knowledge, lessons learned, or training information?

3 How is the security of the final destruction or storage of engineering information assured?

a Where might residual engineering information reside in databases or logs?

b What contractors or vendors must be contacted to arrange for final destruction or disposition of the information that they may still have?

c Has all proprietary contractor and vendor information relative to the system been appropriately disposed of or destroyed?

PRINCIPLE 11 PHASE ALL

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Engineering Information Control principle can inform these controlling processes by considering the following questions:

Project Management

1. How can the systems engineering management plan be designed and implemented as a tool to ensure sensitive engineering data is protected throughout the lifecycle of the project?
2. Does the management plan document what data should be protected, who should have access to what data, how sensitive data is to be protected, and what access controls will be used?
   - a. How often are these processes reviewed, and by whom?
3. What specific investments does the organization need to create secure data repositories for sensitive information in a cost-effective manner?
4. What information sharing methods will the organization use for sensitive engineering records?
   - a. Where are approved platforms, encryption requirements, etc. documented?
5. How is role-based access control (RBAC) utilized across the project to ensure sensitive data engineering records are only accessible to those who need it and who have the security training to keep it safe?
   - a. What roles across the team need access to what information? How is this documented and justified?
   - b. What are the boundaries for information exchange, and what are the approved processes or methods for exchanging information between each?
6. How does the organization track record retention length, number of copies, access distribution (i.e., how many roles/individuals can access certain data), etc.?

Risk Management

1. What risks are associated with the release of each engineering record?
   - a. How challenging would it be to mitigate each risk?
   - b. How does that challenge weigh against identified high-consequence outcomes associated with release of sensitive information?
   - c. Are there metrics to measure the criticality of a given engineering record?
2. Who is involved and who is responsible for assessing the impact of engineering information compromise versus the challenge to mitigate the risk?
3. What gaps or risks were identified pertaining to engineering information control that may need to be addressed elsewhere within the organization or in similarly structured projects?
4. What tools (e.g., redaction, controlled disclosure programs, employee awareness, data loss prevention tools, alternative records) are leveraged to identify, detect, and reduce risks associated with each release of potentially sensitive information?

Change/Configuration Management

1. Who decides who can establish, know, change, and destroy protected information?
2. How is the promotion of information from non-sensitive to sensitive handled? Who does cleanup?
3. How is the information on a system's installed updates, SBOMs, and other changes securely propagated to the stakeholders and systems?

PRINCIPLE 12

Organizational Culture

12

KEY QUESTION

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

Principle Description

Build cybersecurity into the organizational culture by leveraging a cross-functional and cross-disciplinary team to consider digital risks in system design and implementation. Adopt continuous cybersecurity training across the organization to collectively empower all staff to participate in cybersecurity.

Organizational Culture Considerations at Each Lifecycle Phase

Culture is the sum total of the organization's behaviors, practices, and choices that expose the organization's values and priorities. All organizations have a culture, even if it is not consciously recognized. Culture is an inherently human concept that influences almost everything that an organization does, to different degrees and in various ways, including those behaviors and choices that drive security outcomes. Because culture's patterns and trends aggregated over time create inertia, changing an organization's culture takes dedication over a relatively long period.

Cybersecurity has traditionally been approached as a post-hoc set of security measures imposed on organizational technologies and practices. These impositions are often perceived as inconveniences, even when acknowledged as necessary. Embedding security into the values and priorities of the organization and demonstrating that through behaviors and choices can move cybersecurity from an imposition to an inherent quality. This integration requires a holistic approach from senior leadership to managers and supervisors to front-line workers.

Shared beliefs, perspectives and values about cybersecurity determine how a group will help prioritize investments and actions to improve its realization. For a culture that 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 the people, processes, or 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 for, responsible for, consulted on, 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 in relation to 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.

PRINCIPLE 12 PHASE A

PRINCIPLE 12: ORGANIZATIONAL CULTURE

CONCEPT PHASE

The concept phase includes elements of environmental analysis, needs assessment, concept exploration, and development of a concept of operations. The Organizational Culture principle can be applied to the concept phase by considering the following questions:

1 What are the organization's stated and real priorities?

a What is senior leadership's intent and expectation for the purpose of the system?

b What are the interests of the senior leadership, of managers and supervisors, and of technicians and workers involved in creating and operating and maintaining the system?

c How do expectations transfer from the organization to supporting organizations (e.g., hardware vendors, consulting engineers)?

2 How does the organization determine the fundamental tradeoff between efficiency and security?

a How do prior experience and organizational culture shape the questions asked and the systems interrogated?

PRINCIPLE 12 PHASE B

PRINCIPLE 12: ORGANIZATIONAL CULTURE

REQUIREMENTS PHASE

The requirements phase includes elements of system requirements, subsystem requirements, project architecture, and recommendations for requirements gathering. The Organizational Culture principle can be applied to the requirements phase by considering the following questions:

1 What are the managerial, supervisory, and skilled worker behaviors that will drive success in meeting each requirement?

a What assumptions are made about the skill and experience of those who will operate, maintain, secure, and defend the system?

b What latent organizational strengths and weaknesses are interactive or correlated with system requirements?

2 How are error-likely circumstances identified throughout the lifecycle of the system?

a Where do error precursors (e.g., task demands, work environment, individual capabilities, human nature) exist in the concept of operations?

PRINCIPLE 12 PHASE C

PRINCIPLE 12: ORGANIZATIONAL CULTURE

DESIGN PHASE

The design phase includes elements of project architecture, systems decomposition, and component-level design. The Organizational Culture principle can be applied to the design phase by considering the following questions:

1. **How can individuals recognize complexity in design and avoid mistaking complexity for complicatedness?**

2. **How can engineers avoid resolving design issues and improving systems through means that add complexity?**

3. **How can systems be redesigned to be more tolerant of identified error-likely situations?**
   - a How can the team improve detection of plausible errors?
   - b How can the team improve the system's ability to "ride through" plausible errors and continue to function, even in a degraded state?
   - c How can the team improve recoverability from errors?

PRINCIPLE 12 PHASE D

PRINCIPLE 12: ORGANIZATIONAL CULTURE

DEVELOPMENT PHASE

The development phase includes elements of software and hardware creation and system fabrication and assembly. The Organizational Culture principle can be applied to the development phase by considering the following questions:

1 **What training, education, and practice will individuals and teams need to operate, maintain, secure, and defend the system throughout its lifecycle?**

2 **How can choices that accumulate technical debt be recognized and documented?**

PRINCIPLE 12 PHASE E

PRINCIPLE 12: ORGANIZATIONAL CULTURE

TESTING, VERIFICATION, VALIDATION, AND DEPLOYMENT PHASE

The testing, verification, validation, and deployment phase includes elements of unit testing and the integration and verification of the system and subsystems. The Organizational Culture principle can be applied to the testing, verification, validation, and deployment phase by considering the following questions:

1 What will incentivize individuals to speak up to report issues in people, process, and technology?

a Are sufficient staff involved with testing to perceive unexpected events and phenomena?

b Does the organizational culture encourage timely identification of problems without fear of reprisals for identifying organizational weaknesses?

PRINCIPLE 12 PHASE F

PRINCIPLE 12: ORGANIZATIONAL CULTURE

OPERATIONS & MAINTENANCE PHASE

The operations and maintenance phase includes elements of operations, maintenance, changes, and upgrades. The Organizational Culture principle can be applied to the operations and maintenance phase by considering the following questions:

1. **How is interpersonal and interorganizational trust maintained amongst operations, engineering, and security?**
2. **How do operators minimize and detect drift–the difference between work as performed and work as imagined?**
   a. Have any work practices deviant from the organization's security goals been inadvertently normalized and accepted?
3. **How will operators respond when they encounter abnormal situations or conditions?**
   a. What processes ensure that troubleshooting and diagnosis of process anomalies consider the possibility of digital sabotage?
4. **How is culpability determined for instances of "human error" to determine the root causes that need to be addressed to mitigate the risk of continued error?**
5. **What interventions can be employed (e.g., console error, counsel at-risk behavior, sanction recklessness) based only on the behaviors and choices and not on the outcomes realized?**
   a. What behaviors and choices support security outcomes, and how are those nurtured with positive reinforcement?
   b. What behaviors and choices harm security outcomes, and how are those changed with constructive coaching?

PRINCIPLE 12 PHASE G

PRINCIPLE 12: ORGANIZATIONAL CULTURE

RETIREMENT AND REPLACEMENT PHASE

The Organizational Culture principle can be applied to the retirement and replacement phase by considering the following questions:

1 **What facts and context about the system that reside in institutional memory are important to preserve for use in replacement or other systems?**

PRINCIPLE 12 PHASE ALL

PRINCIPLE 12: ORGANIZATIONAL CULTURE

CONTROLLING PROCESSES

Engineering teams leverage several controlling processes—such as project management, risk management, and change/configuration management—across the project lifecycle, spanning across the phases. The Organizational Culture principle can inform these controlling processes by considering the following questions:

Project Management

1 What organizational cultural assumptions and history influence managerial approaches to program and project management that affect or are affected by security?
   - **a** How are organizational assumptions about the effects of processes and behaviors influencing management of security projects and programs?
   - **b** To what extent does the organization perceive and comprehend the consequences of individual behaviors and choices?

2 How does the organization ensure that work is performed consistently with established standards and expectations?

3 What resources are needed to ensure the organization's culture positively influences the system's security performance?

Change/Configuration Management

1 How does the organization empower leaders at all levels to identify, prioritize, and eliminate latent organizational weaknesses?

2 Does the organization use data to understand where and why gaps between standards and performance exist?
   - **a** Are the methods valid and effective, producing the types of results the organization expects?

3 How does the organization use external information to identify needs to change internal systems?

4 How does the organization identify and prioritize strategic changes? How does it define and design the personnel and processes responsible for and engaged in effecting these changes? How does the organization control for disruptions in the established organizational culture resulting from the changes enacted?

5 How does the organization validate the accuracy and effectiveness of applied changes?

6 Are continuous improvement feedback loops based on kind, wicked, or fiendish environments[12]?

Risk Management

1 How do executives perceive and manage risks, and to what degree are they willing to increase risk in exchange for reduced costs?
   - **a** How are budget and timeline emphasized relative to security capability and performance?

2 How do executives establish and communicate clear performance expectations and goals for security?
   - **a** How confidently and completely can the organization define success?

3 How does the organization perceive and weigh internal versus external risks, and to what degree are these risks humanized or dehumanized?

4 To what degree is the organizational culture and the environmental culture critically analyzed to separate assumed influences from the effects of actual influencing forces?

5 How well do organizational choices, particularly at the senior leadership and board level, align with the organization's stated security goals?

12 For discussions of learning environments, see: Robin M. Hogarth, Tomás Lejarraga, and Emre Soyer, "The Two Settings of Kind and Wicked Learning Environments," Current Directions in Psychological Science, Vol. 24, No. 5 (October 2015), pp. 379-385; and Stuart Patience, "Learning environments: kind, wicked, and…fiendish?" Driverless Crocodile (January 31, 2021).

Appendix A: Guide Development and Contributors

Implementation Guide development was led by researchers at INL and NREL, with significant support from a multi-stakeholder development team that worked in concert with volunteer members of the CIE Community of Practice. Inputs to this guide were reviewed and informed by a broad set of stakeholders, including energy sector asset owners, manufacturers, engineering service providers, academic institutions, professional technical societies, research institutes, and government agencies.

IMPLEMENTATION GUIDE DEVELOPMENT TEAM:

Robert Anderson
Idaho National Laboratory

Victor Atkins
1898 & Co.

Marco Ayala
1898 & Co.

KatherineAnne Baker
Nexight Group

Lance Barnes
Idaho National Laboratory

Krystel Castillo
University of Texas at San Antonio

Samuel Chanoski
Idaho National Laboratory

Joel Cox
West Yost Associates

Robert Edsall
Idaho National Laboratory

Rob Foy
Nexight Group

Tim Gale
1898 & Co.

Jeff Gellner
Idaho National Laboratory

Rich Graham
1898 & Co.

Daniel Groves
West Yost Associates

Mary Rose Holtz
Idaho National Laboratory

Stephanie Johnson
U.S. Department of Energy

Jeremy Jones
Idaho National Laboratory

Lindsay Kishter
Nexight Group

Katya Le Blanc
Idaho National Laboratory

Sin Ming Loo
Boise State University

Richard Macwan
National Renewable Energy Laboratory

Joseph Mahanes
Idaho National Laboratory

Maurice Martin
National Renewable Energy Laboratory

Shane McFly
National Renewable Energy Laboratory

Timothy McJunkin
Idaho National Laboratory

Jakob Meng
Idaho National Laboratory

Matt Morris
1898 & Co.

Andrew Ohrt
West Yost Associates

Waylon Pattison
West Yost Associates

Jessica Robinson
Idaho National Laboratory

Daniel Rucinski
Idaho National Laboratory

Marc Sachs
Auburn University

Greg Shannon
Idaho National Laboratory

Jeremy Smith
West Yost Associates

Venkatesh Venkataramanan
National Renewable Energy Laboratory

Emily Waligoske
National Renewable Energy Laboratory

Justin Welch
Idaho National Laboratory

Gareth Williams
National Renewable Energy Laboratory

Zane Wilsterman
West Yost Associates

Virginia Wright
Idaho National Laboratory

ADDITIONAL CONTRIBUTORS

The development team additionally recognizes the contributions of several members of the CIE Community of Practice Implementation Working Group who helped develop and refine the questions and considerations within this Implementation Guide:

Irfan Ahmed
Virginia Commonwealth University

Tomomi Aoyama
Industrial Cybersecurity Center of Excellence, Omny

Wayne Austad
Idaho National Laboratory

Christopher Battisti
U.S. Army Corps of Engineers

Dawson Bell
Idaho Environmental Coalition

John Biasi
Burns & McDonnell

Andrew Bochman
Idaho National Laboratory

Joe Bush
U.S. Army Corps of Engineers

Konstantinos Chatziargyros
Stem Shipping

Craig Cocciola
TrainOnQ, LLC

Daniel Cole
University of Pittsburgh

James Cole
Idaho National Laboratory

Art Conklin
University of Houston

Heidi Cooke
ISA Global Cybersecurity Alliance

Jay Cribb
Southern Company

Megan Culler
Idaho National Laboratory

Joe Cummings
New York Power Authority

Daniel Diaz
Southern Company

Josh Duersch
College of Eastern Idaho

Sami Elmurr
Hunter Strategy

Ron Fabela
SynSaber

Jerome Farquharson
Burns & McDonnell

David Foose
Rockwell Automation

Andrew Ginter
Waterfall Security Solutions

Vergle Gipson
Idaho National Laboratory

Dan Goodlett
North American Electric Reliability Corporation

Larry Grate
Aleta Technologies

Deniz Gurkan
University of Houston

Charlie Hall
Frazer-Nash Consultancy

David Halla
Battelle

Ed Hicks
Forescout Technologies

Simha Himakuntala
Oak Ridge National Laboratory

Terry Holman
Battelle Memorial Institute

Susan Howard
M Baker International

Ryan Hoye
Black & Veatch

Ahmad Javaid
University of Toledo

Amanda Jones
West Yost Associates

Randall Joyce
Murray State University

Durgesh Kalya
Covestro LLC

William Keber
West Virginia National Guard

Steven Kunsman
Hitachi Energy

Mike Legatt
Resilient Grid

Justin Luebbert
National Rural Electric Cooperative Association

Rees Machtemes
Waterfall Security Solutions

Manuel Maestas
Idaho National Laboratory

Milos Manic
Virginia Commonwealth University

Glenn Merrell
Industrial Control Systems Security

Satyajayant Jay Misra
New Mexico State University

Robert Morgan
Southern Company

Susan Morris
Advanced Business Learning, Inc.

Jon Nelson
IEC

Matthew Nielsen
GE Research

Mark Permann
Idaho National Laboratory

Robert Renzulli
Pennsylvania Public Utility Commission

Raul Rodriguez
Dragos

Mark Roman
ManTech

Nicholas Seeley
Schweitzer Engineering Laboratories

Abhishek Sharda
Brown and Caldwell

Madeline Shunk
U.S. Army Corps of Engineers

Angela Sims-Ceja
Aurora Water

Tom Smertneck
Energy Aspects LLC, ISA District VP-Midwest North America

Charlie Souza
Syzygy Plasmonics

Shane Stailey
Idaho National Laboratory

Emma Stewart
Idaho National Laboratory

Frank Stieglitz
ISA Global Cybersecurity Alliance

Nesrine Taha
U.S. Army Corps of Engineers

Robert (Bob) Tarwater
Idaho National Laboratory

Eleanor Taylor
Idaho National Laboratory

Michael Thomas
Auburn University

Michael Thow
Electric Power Research Institute

Jesus Molina Torres
JMT

Stephen Trachian
Hitachi Energy

Tony Turner
Opswright

Nik Urlaub
MITRE

Laura Vaglia
U.S. Department of Defense, U.S. Army

Alex Waitkus
Southern Company

Jennifer Lyn Walker
Water ISAC

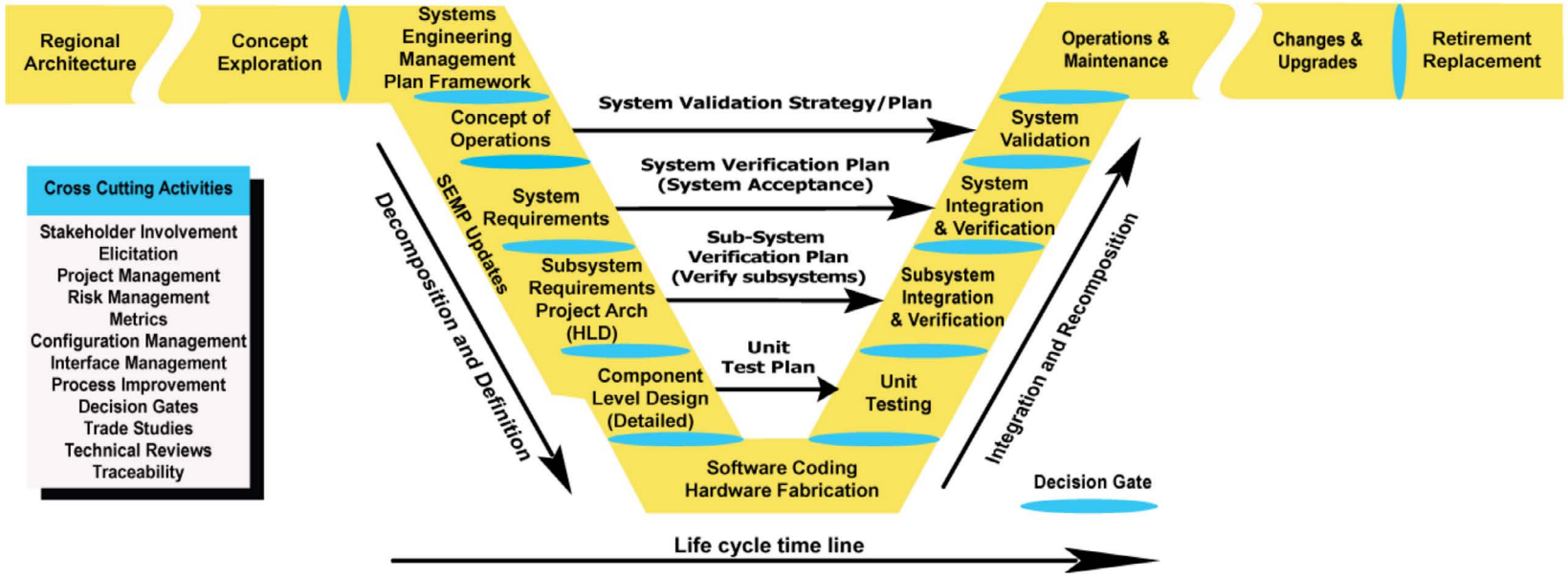
Ken Wang
U.S. Department of Defense

Michael Welch
Burns & McDonnell

Vince Zappula
BlastWave

Appendix B: Lifecycle Models Considered

Extensive literature review identified four lifecycle models for initial consideration, including the INCOSE project lifecycle model,[13] DOE project lifecycle model,[14] NIST Systems Security Engineering Framework,[15] and the U.S. Department of Transportation (DoT) Vee Technical Development.[16] Although each model provided unique benefits and perspectives, the DoT model was selected as the structure for primary mapping because of its significant level of detail around its phases. Further, the DoT model's terminology aligns most closely with that of industrial/energy infrastructure system design.



Source: DoT Systems Engineering Guidebook for Intelligent Transportation Systems

13 INCOSE, *Systems Engineering Handbook*, version 3.2.

14 U.S. Department of Energy, *Systems Engineering Methodology*, version 3 (September 2002).

15 National Institute of Standards and Technology, *Engineering Trustworthy Secure Systems*, NIST SP 800-160v1r1 (November 2022).

16 U.S. Department of Transportation Federal Highway Administration, California Division, "*Systems Engineering Guidebook for Intelligent Transportation Systems*," version 3.0 (November 2009).

Map of Implementation Guide Phase to DoT Phases

IMPLEMENTATION GUIDE PHASES	DoT Vee MODEL PHASES
Concept	• Regional Architecture (may require discussion of internal and external concept) • Needs Assessment and Concept Exploration • Concept of Operations
Requirements	• System Requirements • Subsystem Requirements and Project Architecture (Project Architecture straddles into Design) • Elicitation (cross-cutting)
Design	• Some of Project Architecture (see above) • Component Level Design (detailed)
Development	• Software Coding, Hardware, Fabrication
Testing, Verification, Validation, and Deployment	• Unit Testing • Subsystem Integration and Verification • System Integration and Verification • System Validation
Operations & Maintenance	• Operations and Maintenance • Changes and Upgrades
Retirement and Replacement	• Retirement and Replacement
Controlling Processes	• Systems Engineering Management Plan Framework • Elicitation (some may fit Requirements) • Decision Support/Trade Studies
Project Management	• Stakeholder Involvement • Project Management Practices • Metrics (some) • Project Process Improvement • Traceability (some)
Risk Management	• Risk Management Practices • Metrics (some) • Traceability (some)
Change/Configuration Management	• Configuration Management

The Implementation Guide development team initially chose this model for use in the Implementation Guide because it offers the following attributes:

- Includes a conceptual design phase (concept exploration and concept of operations), which is important for early inclusion and application of CIE principles.
- Includes clear, cross-cutting activities (creation and execution of validation, verification, and test plans) to which CIE principles and decisions/designs/requirements derived through the application of CIE principles can be included. Cross-cutting activities ensure that CIE-driven system requirements and designs are both included in the final system design and achieve their intended purpose.
- Includes a maintenance and operations lifecycle phase to ensure CIE principles are considered for the entire operational life of the system. This also helps ensure technicians have a role in the application of CIE.
- Includes a changes and upgrades phase so that CIE can be incorporated as designs, requirements, equipment, functions, etc. evolve over time.
- Includes a retirement/replacement/end of life phase.

While the DoT model provided a valuable framework upon which to unpack CIE's principles against the lifecycle of a project, the development team ultimately determined that the framework was too granular. After conducting an extensive mapping exercise across the entire DoT Vee and CIE's principles, the team identified core phases that apply synergistically to energy projects and have the flexibility to apply to other infrastructure that includes physical processes with digital control.

Appendix C: Engineering Case Study

Disclaimer

This scenario is fictional. Though it is pulled from actual events and experiences, the information below does not reflect any actual company or infrastructure.

C.1 Background – The Water and Wastewater Utility

The fictional water and wastewater utility discussed herein serves approximately 500,000 people and thousands of businesses with a service area of approximately 100 square miles. Over the nearly 100-year history of the organization, the utility has made investments in physical infrastructure currently valued at over $2 billion. Between 1990 and 2020, asset renewal and rehabilitation were generally deferred as a short-term cost savings measure. During this period, asset conditions declined, leading to service disruptions and unwanted attention from elected officials, the press, and customers. New utility management is now making substantial investments to provide reliable and resilient services to customers.

The utility has four primary facilities including:

- **Water Treatment Plant #1 (WTP #1)** – The critical function of WTP #1 is to provide high quality water. If the treatment plant is not able to provide high quality water, residents and businesses would be without clean water and a nearby regional power generation plant would not have water for steam generation and cooling. The supervisory control and data acquisition (SCADA) master system for all potable water facilities (WTP #2, pump station and remote wells) is located at WTP #1.
- **Water Treatment Plant #2 (WTP #2)** – The critical function of WTP #2 is to provide high quality water. If the treatment plant is not able to provide high quality water, nearby residents and businesses would be without clean water. This site has a SCADA node that relies on a data connection to servers located at WTP #1.
- **Water Pump Station** – The critical function of the pump station is to provide high quality water at a useful pressure. If the pump station is not able to provide water at a useful pressure, nearby residents and businesses could be without water. This could also impact the ability for the fire department to connect fire trucks and hoses to fire hydrants within the service zone to put out fires.
- **Wastewater Treatment Plant (WWTP)** – The critical functions of the WWTP are to

accept all wastewater from residences and businesses and treat the wastewater within regulations. If the WWTP is not able to accept all the wastewater, sewage will overflow on streets or at the WWTP. If the WWTP is not able to treat the wastewater within regulations, this can lead to property damage and illness. The SCADA master system for all wastewater facilities (WWTP and remote sewer lift stations) is located at the WWTP.

In addition, there are numerous smaller outlying facilities within the drinking water distribution system and wastewater collection system including:

- Remote groundwater well sites (potable water system)
- Remote tank sites (elevated) (potable water system)
- Wastewater lift stations (wastewater system)

Due to the burdens placed on the operations staff, the utility has established a temporary means of accessing the SCADA system that allows operators to remotely access the SCADA software systems from insecure locations.

Due to the deferred asset rehabilitation and renewal over several decades, utility management has become concerned with cyber-incidents that might result in physical consequences for the utility.

Engineering Department and Ongoing Investments

Due to increasing population and increasing regulatory pressures, the utility is making additional investments in new advanced water treatment processes at the existing facilities. The processes require automation to run successfully and optimally.

The utility has not developed and adopted engineering standards. They have previously been reliant on consultants to use their own standards.

Current use of Industrial Control System Technology

Two separate SCADA systems are used by the utility to monitor and control the water/wastewater (W/WW) facilities. One SCADA system is used to monitor and control the potable water facilities (water treatment plants, pump station, wells, elevated storage tanks). The other SCADA system is used to monitor and control the wastewater facilities (WWTP and remote wastewater lift stations). Standards for SCADA screens have not been implemented so each system uses different layouts, graphics, and colors. Different standards have been implemented for each new facility and at each new phase of construction.

Through various upgrade projects, the utility has transitioned away from hard-wired input/output (I/O) signals in favor of Ethernet communications with process control devices.

Each plant shares a similar general network topology—a star topology using multiple commercial-off-the-shelf vendor solutions including a mix of managed/unmanaged switches and proprietary communication devices (e.g., Allen Bradley ETAP). There is some network segmentation, and the site-to-site communications are using a combination of 900Mhz radios, microwave, and fiber optic lines. The control system technology, including network switching, WAN/LAN communications, firewall, and SCADA applications, are managed by operational technology staff. The virtualized server hardware and storage are managed by City IT.

Data is transmitted to a cloud-based service to provide regulatory reporting for users outside the SCADA environment. User access to the reporting function is managed within the cloud application. The Software-as-a-Service (SaaS) vendor uses Amazon AWS to host the application.

The utility has experienced intrusions into the IT and OT networks; however, no data or processes were compromised. The utility has not deployed a solution to actively monitor the environment. With the increasing number of documented insider threats to utilities, there is greater concern that the trust placed in the utility's people and systems is unverified and potentially—at some level of abstraction—unverifiable.

Project Delivery

The utility retains project managers to administer design and construction projects. Each design project is responsible for its own development standards, building on previous projects and references provided by design consultants. For each project scope, separate requirements, approach, and milestones are developed. This has led to a variety of project outcomes, equipment, and levels of detail in design documents.

CIE Program Launch

With the increased focus on investment to improve system wide security, reliability, and resilience, the utility is launching an internal program to integrate CIE principles into their engineering practices. The program creates internal processes to drive change, provide design and construction requirements, and assess existing facilities' risk.

The utility recently completed a SCADA Master Planning project to support the rollout of the CIE Program. The goal of the master plan was to identify the steps to improve the SCADA system and maintain a high level of reliability and security in the future. In addition to the standard technology evaluation and selection process, the planning process emphasized continuity of operations and resilience with and without automation.

These activities supported the inclusion of CIE as a foundational part of the utility's approach to engineering. The master plan led to the following:

- Design standards for electrical, SCADA, and networking
- Requirements for new project delivery workflow with CIE principles integrated into the engineering and review processes
- Organizational recommendations for CIE program management, including staffing needs with job descriptions and skillset requirements
- Prioritized project lists to assess and address existing site conditions
- Governance recommendations to maintain the SCADA system, supporting resources, and CIE reference documents

Specific examples of the application of and outcomes from the CIE initiative are described in detail in section 6 of this appendix.

C.2 CIE Team Roles and Responsibilities

Recognizing that no initiative would be successful without explicit ownership by team members, the utility developed a high-level roles and responsibilities matrix. Table 1 summarizes which organizational units are responsible for the application of each CIE principle, demonstrating the general breakdown of roles and responsibilities within the organization. Each organizational unit must consider each CIE principle through the engineering lifecycle, and may require additional support from other units. For example, IT Cybersecurity and Management may support OT Cybersecurity and Management with the application of Principle 3: Secure Information Architecture.

Table 1 - CIE Team Roles, Responsibilities and Associated Principles

ORGANIZATIONAL ROLES	PRINCIPLES	
Leadership	12	Organizational Culture
Operations	6	Active Defense
	7	Interdependency Evaluation
	10	Planned Resilience
Engineering	1	Consequence-Focused Design
	2	Engineered Controls
	4	Design Simplification
Procurement	9	Cyber-Secure Supply Chain Controls
OT Cybersecurity and Management	3	Secure Information Architecture
	5	Layered Defenses
	8	Digital Asset Awareness
Legal and Governmental Affairs	11	Engineering Information Control

C.3 Applying Cyber-Informed Engineering to the Water and Wastewater Utility

The utility begins with the CIE principles and associated definitions summarized in Table 2.

Table 2 - CIE Principles

	PRINCIPLE	DEFINITION
1	**Consequence-Focused Design**	Apply CIE strategies first and foremost to the most critical functions the system performs. Typically these are functions which, if manipulated or subverted, could result in unacceptable or catastrophic consequences for the organization.
2	**Engineered Controls**	Identify engineering design changes to process controls early in system design to eliminate or mitigate cyber risk, reducing the need to bolt on additive IT security controls during implementation.
3	**Secure Information Architecture**	For each identified data stream, a secure information architecture can be designed, guided by the consequences and impacts identified in consequence-focused design, 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.
4	**Design Simplification**	Simplify the system, component, or architecture design and limit high-consequence, low-value complexity within digital functions at the outset, reducing the opportunity for attackers to misuse digital functionality.
5	**Layered Defenses**	Assume compromise and employ a defense-in-depth strategy, reducing the opportunity for a single failure to impact critical functions or create cascading failures.
6	**Active Defense**	Employ dynamic elements in the design of systems that detect and defend against cyber threats, enabling the system to continue operating resiliently when an intruder is detected, and isolate or remove the threat without compromising critical operations.
7	**Interdependency Evaluation**	Integrate input from multiple disciplines and operational departments (e.g., safety, quality, maintenance, chemical) to understand how digital misuse could affect their area of operations.
8	**Digital Asset Awareness**	Maintain a complete and accurate digital asset inventory, enabling engineers to track hardware, firmware, and software over time, and actively analyze the vulnerabilities that may reside within them and facilitate evaluation of potential consequences arising from those vulnerabilities.
9	**Cyber-Secure Supply Chain Controls**	Use procurement language and contract requirements to ensure that vendors, integrators, and third-party contractors deliver products that meet design specifications and adhere to organizational processes and controls that support cybersecurity.
10	**Planned Resilience**	Expect that any digital component or system may be compromised at some point during its lifecycle, and plan for continued operation during and after a cyber-attack that degrades digital controls. Implement a zero-trust architecture to the greatest degree possible.
11	**Engineering Information Control**	Protect sensitive engineering records—including requirements, specifications, designs, configurations, testing, etc.—that if released may provide attackers critical information that places those systems at greater risk.
12	**Organizational Culture**	Build cybersecurity into the organizational culture by leveraging a cross functional and cross-disciplinary team to consider cyber-related concerns in the system design and implementation. Adopt continuous cybersecurity training across the organization to collectively empower all staff to participate in cybersecurity.

C.4 Engineering Lifecycle Phase Mapping

The guide provides engineering lifecycles phases common to some sectors and industries. The water/wastewater sector has a different model for engineering lifecycle phases. Both are shown in Table 3. Table 3 was developed to compare and align the two engineering approaches. This enables the application of CIE principles and associated questions within the appropriate phase for the utility.

Table 3 - Engineering Lifecycle Mapping

CIE IMPLEMENTATION GUIDE ENGINEERING LIFECYCLE PHASES					
Concept	Requirements	Design	Development	Testing, Verification, Validation, and Development	Operations and Maintenance

WATER/WASTEWATER SECTOR ENGINEERING LIFECYCLE PHASES				
Planning Concept	Preliminary Design Report	Detail Design	Construction and Commissioning	Operations and Maintenance

C.5 Applying CIE within the Utility

Utility operations and engineering projects are always ongoing. Because of this, the utility decided to identify how CIE would be applied from the beginning for engineering projects. This resulted in the following conclusions:

- Throughout the CIE process flow, organizational culture consistently includes cybersecurity in alignment with full implementation of CIE.
- CIE begins with Consequence-Focused Design. This is the first step in identifying critical functions and catastrophic consequences. Once the critical functions, supporting systems, assets, and staff are described and understood, potential consequences are identified, and engineered controls are identified and implemented to eliminate or mitigate the highest consequences.
- Once the highest consequences are addressed, the focus then shifts to securing the information architecture (Secure Information Architecture) to ensure the confidentiality,

availably, and integrity of data. As these principles are applied throughout the engineering lifecycle, Design simplification helps reduce the potential for vulnerabilities and associated risks that could potentially outweigh the benefits they bring to the system and organization.

- Even with the protections and mitigations from the prior principles, the utility establishes layered defenses. This helps prevent cascading failures if one element of the digital system becomes compromised. When assuming highly capable and well-resourced adversaries, active defense becomes critical for the operations staff to monitor the resilience of their systems. This principle supports operation when a threat is detected, and isolation or removal of the threat without compromising critical operations.
- Conducting an interdependency evaluation within the design process and regular updates through operations, maintenance, and retirement is necessary to maintain an up-to-date understanding of risk. The next step involves establishing digital asset awareness through compiling a complete and accurate digital asset inventory, enabling the evaluation and elimination of potential consequences arising from new vulnerabilities. This helps operations and supporting staff to address system or device-specific vulnerabilities as they are discovered, and better understand the full scope of capabilities (enabled or not) of the digital devices in the system.
- Planned resilience begins in the early engineering phases and is maintained and updated through the entire engineering lifecycle. Assuming that any digital component or system may be compromised and planning for continued operation during and after a cyber attack that degrades digital controls throughout the system is essential to the utility's maturing cybersecurity culture.
- Engineering information control protects sensitive engineering records that may facilitate a successful cyber attack. Preventing information from unauthorized release increases the difficulty for an attacker to successfully carry out their mission against the utility. Engineering information control and establishing cyber-secure supply chains help maintain secure and resilient operations. These must also be applied contractually and in practice for any consulting engineers, vendors, integrators, and contractors that support the utility.

C.6 CIE Control and Mitigation Examples

The narratives below provide a summary of the concerns and associated controls and/or mitigations each CIE principle helps the utility identify. Each example is focused on one specific CIE principle but frequently uses other principles in CIE to achieve a more secure and robust design. The matrices in section 7 below can be used to quickly identify which

CIE principles are relevant to each CIE control and mitigation example. For each CIE control and mitigation example, a select concept question from the Implementation Guide is included to illustrate how the question helped shape the utility's approach to CIE.

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?

1. Explicitly include cyber-enabled failure modes in design practices. While engineering processes previously used by the utility included the long-standing engineering practice of preventing failure scenarios, there was no discussion of cyber-enabled failure scenarios. Engineering processes now explicitly articulate and discuss cyber-enabled failure scenarios. This discussion begins with the utility's critical functions and the associated consequences to those critical functions being compromised are included in Table 4.

Table 4 - Critical Functions and Associated Consequences for the Drinking Water System

CRITICAL FUNCTION	ASSOCIATED CONSEQUENCES
1. Provide safe drinking water for consumption by residential, commercial, and industrial customers	1a. Distribution of unsafe drinking water – human health risks 1b. Insufficient drinking water 1c. Insufficient water for commercial and industrial operations
2. Provide water for firefighting	2a. Insufficient water for firefighting potentially allowing for the spread of fires in the service area
3. Provide cooling water for the electrical generating facility	3a. Disruption to the electrical generating processes and associated power supply to the region

The utility's systems, assets, and people are focused on achieving the mission and critical functions listed above. Through various assessments, the utility has identified uniquely critical assets including:

- Pumps
- Motors
- Variable frequency drives (VFDs)
- Water transmission and distribution mains

Cyber-enabled failure scenarios may be associated with each of these types of assets. The subsequent principles and associated examples were identified for implementation to control or mitigate cyber-enabled failure scenarios.

Supporting assumptions include:

- The adversary has logical and physical access.
- The adversary is knowledgeable of critical equipment, processes, and how to cause impact in the system.
- The adversary is well-resourced and capable.

Concept Question: What is the purpose of this system?

1. By considering the purpose of each system it can become easier to identify what the consequence would be for the overall plant.
    a. After mapping out each consequence for an impacted system it will clearly define which processes/assets/systems are critical and which are not.
    b. Establishing a focus on consequences will make the implementation of a resilient system easier.

Example: 1-1 When considering any changes to design and operation, each person should "engineer-out" cyber-enabled failure scenarios and the consequences of losing critical functions.

Principle 2: Engineered Controls

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

1. The use of hard-wired signals in combination with digital technologies will minimize the damage which could result from a cyber attack by allowing operators to monitor and operate key functions without the use of their SCADA system.
    a. Development of digital technologies implemented at utility facilities over the last decade has seen a significant increase in devices utilizing industrial internet of things (IIoT). One set of devices that uses data communications to monitor and even control motors are advanced motor management devices (AMMD) and variable frequency drives (VFDs). These devices have traditionally been used to provide overload protection for the motor. Now, these components that are routinely connected to the SCADA network have been provided with advanced motor protection monitoring and can even be used to monitor and control the process by adding remote I/O capability.
    b. Programmable logic controller (PLC) hardware has proven to be extremely robust with few hardware failures. This, combined with the flexibility of being able to make programming changes to logic, has led some designers to rely on the PLC to perform

all process logic and protection schemes. This occurs when the AMMD is connected to the SCADA system and all field sensor wires are connected directly to the PLC hardware or AMMD remote I/O, instead of hardwired to the motor starter. For water and wastewater (W/WW) facilities, this can introduce the risk that operators cannot perform critical functions such as losing control of a motor when the starter is in either REMOTE or LOCAL mode.

c. Problems can arise when the network becomes unavailable, or a PLC is compromised. When the network becomes unavailable, either due to cyber attack or failure, the data monitored by the module inputs are not available to the SCADA system. This can impact the process control if the PLC is used to activate an interlock, such as tank low level shutdown or pump discharge high pressure shutdown of a booster pump. Also, any output data points may become unresponsive. This is particularly an issue when PLC/controller logic is used to activate alarm conditions or start the pump. Another example could involve a bad actor disabling interlocks to cause asset damage or unsafe conditions to personnel.

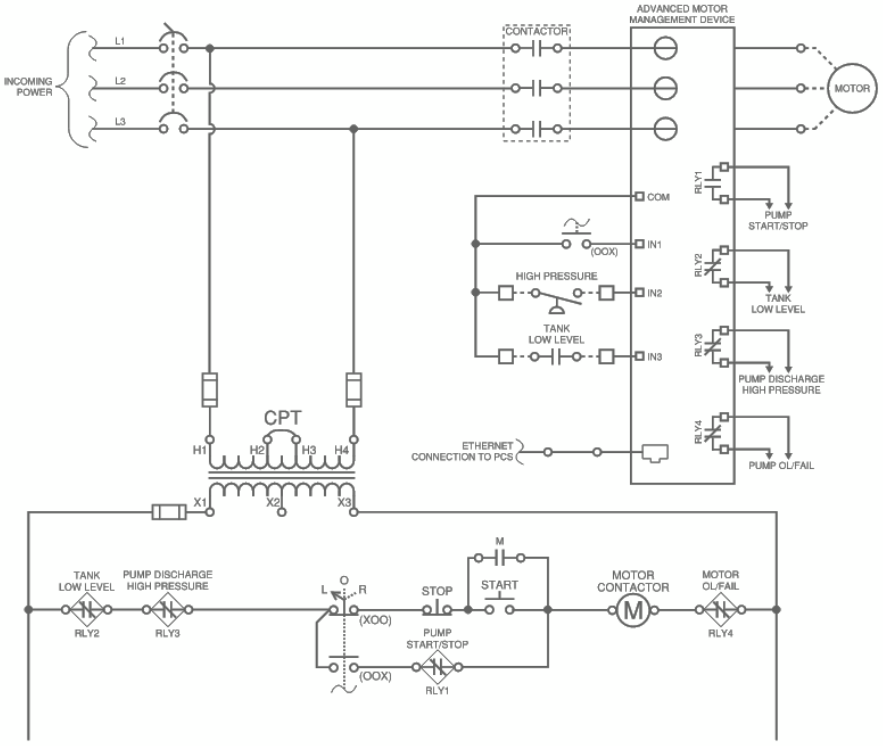
Concept Question: What key functional controls of my system are dependent on digital technologies?

1. The utility has multiple functional controls that are dependent on digital technologies, such as tank low level alarms and pump control. By identifying each of these signals and determining which are key for plant operation the utility can begin to apply the principles of CIE and seek methods for improving resilience.

   a. The utility is using these digital signals to allow a single operator to quickly operate the plant from a central location, minimizing the need for extra staff and allowing simultaneous monitoring of multiple functions across the plant. This control also allows operators to remotely access monitoring and control of certain plant operations.

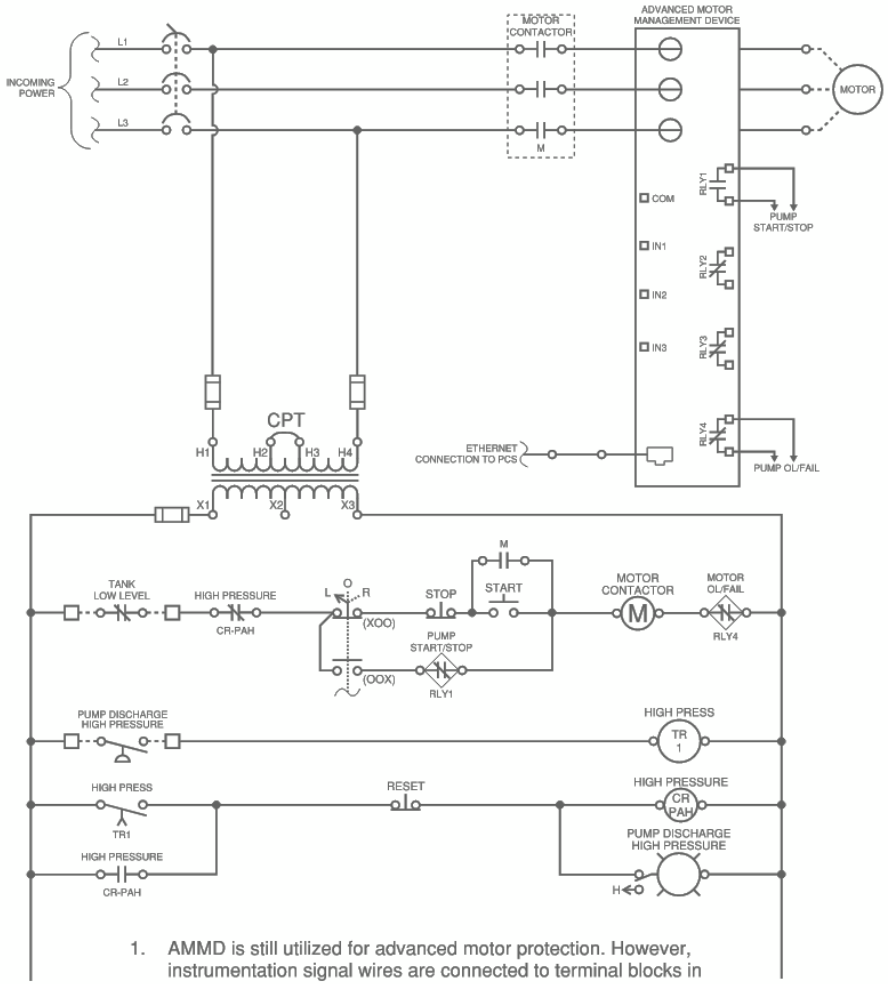
   b. This dependency on key digital signals introduces the risk of losing the ability control the plant in the event of a network loss due to malfunction or compromise. This could lead to damaged equipment, injured personnel, and risk to the public in the form of undrinkable water or environmental hazards from an overflow of wastewater.

Example: 2-1 Wire instrumentation signals directly to applicable motor starters to provide equipment and personnel protection for all modes of operation, even if the network or PLC have been compromised. Plan for all failure modes. Refer to Figure 1 for an example creating risk. Refer to Figure 2 for an example that minimizes avenues for attack. Brief descriptions of the differences between the designs presented in the schematics are included on the figures.



1. Simple motor control schematic that indicates all instrumentation signal wires connected directly to AMMD remote I/O.
2. Ethernet connection to PLC for monitoring of motor diagnostics and process data.
3. Relies on PLC to perform protection logic.

Figure 1. Example Schematic that Increases Avenues for Attack



1. AMMD is still utilized for advanced motor protection. However, instrumentation signal wires are connected to terminal blocks in the motor starter.
2. Ethernet connection to PLC for monitoring of motor diagnostics. Process data and motor signals are connected to PLC I/O.
3. Protection logic is done within the motor starter using control and timer relays.

Figure 2. Example Schematic that Minimizes Avenues for Attack

Principle 3: Secure Information Architecture

Key Question: How do I prevent undesired manipulation of important data?

1. Traffic control between the utility's devices and subnets was not clearly defined.
    a. If traffic control is not properly managed, there is minimal traffic visibility and flow control on the network. This leaves a blind spot for a bad actor to gain access to important data on the network.
2. The utility used the same profile for multiple operators who shared their password for the "Operator" profile.
    a. Allowing multiple users to share a profile limits the ability to determine who has authority and access to make changes and who does not. This can lead to an operator having insufficient access to do their job while another operator has too much access and can change the system without authorization.
3. Utility assets, both network and physical (e.g., VFDs, PLC, ETAPs), often present as avenues for attack where damage could result. If these assets are not secured with the proper controls, they present a vulnerability that could be leveraged by a bad actor.
4. Controls to minimize these avenues for attack consist of network segmentation and tools to monitor the network.

Concept Question: Will the system communicate external to the boundaries of the facility/system?

1. The utility has requirements for recording and reporting water quality data to outside governmental organizations. This information is sent from their SCADA network to the city's network and emailed to the required agencies.
    a. It is important to evaluate every communication pathway on a case-by-case basis, establishing the appropriate pathways and controls.

Example: 3-1 Network traffic should be handled by a highly available Next Generation Firewall (NGFW) appliance, policies and zones should be created to segment and control traffic.

Example: 3-2 Establish a Demilitarized Zone (DMZ) to separate SCADA network from The Cities network.

Principle 4: Design Simplification

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

1. The network architecture at The Utility was designed to use Ethernet Network Taps (ETAPS) which have limited security features. With only a digital presence on the network, a bad actor could send traffic to flood the ETAP or leverage vulnerabilities on the device since they do not fall into the typical cadence of patching. These two events could result in loss of remote control or a threat actor gaining control of the system.
    a. As this component is not absolutely necessary to the system, they can be replaced with managed industrial switches that provide enhanced monitoring capabilities, traffic control, and management interface access that can be segmented from control network. This may require extending copper/fiber from process panels to network distribution point.
2. The utility noted when troubleshooting issues within the PLC that several languages and difficult to understand routines were used throughout the program. This can significantly impede the utility's ability to pinpoint an attack.
    a. Standardizing a language and programming habits can improve troubleshooting time and aid in response and recovery from a successful cyber attack.

Concept Question: How do I determine what features of my digital system are not absolutely necessary?

1. Certain functions of the utility that were needed to monitor and control operations add complexity to the system.
    a. The utility should challenge any network device that is added to the control system to determine if it is necessary to accomplish the process control.
    b. For devices that are approved for implementation, the default settings should be disabled to the maximum extent possible.

Example: 4-1 Remove ETAPS and implement managed industrial switches for enhanced monitoring capabilities and traffic control.

Example: 4-2 Challenge all digital solutions to determine if the design can be simplified by removing or substituting something else for them.

Principle 5: Layered Defenses

Key Question: How do I create the best compilation of system defenses?

1. The utility was originally designed to use ETAPs, without a clear definition of traffic control between devices and subnets. This design provides minimal security features and allows for a single failure to impact critical functions.
    a. System hardening is essential to prevent cascading failures. Improvements include segmentation by process/device/zone, NGFWs using very granular policies, Zero Trust Architecture where possible, vulnerability management, early detection (i.e., tools to monitor, detect, and respond to anomalous traffic), and managed switches.

Concept Question: How will the controls developed for Principle 2: Engineered Controls add to our layered defenses? What additional layers are needed for each control to detect anomalies in the protection that the control provides?

1. By implementing engineering controls as discussed in Principle 2, the utility improved their Layered Defenses by having backup controls to their SCADA system. Additional layers can be added to further increase resilience.
    a. By implementing both physical and digital interlocks, the utility can prevent a bad actor from intentionally preforming actions remotely that would cause damage to the plant or injury to personnel such as closing a valve and starting a pump or filling a tank over its high setpoint.
        i. Digital interlocks help operators to avoid making mistakes that can cause damage to equipment, but a bad actor can manipulate these digital interlocks to prevent them from working properly. Having a physical interlock as a backup prevents remote override.
    b. As an added layer, defense warnings can be put in place that alert the operators if an interlock has been tested.
2. Automatic warnings can be put in place to inform operators that SCADA and physical readouts do not match.
    a. If a physical high-pressure switch were to set off an alarm warning the operator of high pressure, but a digital pressure transmitter shows pressure in the normal range, the SCADA system will send an instrument disagreement warning.
    b. The operator can then investigate if equipment has malfunctioned or if their digital system is being manipulated.
3. Performing regular training for operators on expectations and actions to take in the event of an instrument disagreement or tested interlock warnings will add another layer of defense to prevent damage to the plant or injury in personnel while also allowing them to recognize early warning signs of a compromised network.

Example: 5-1 Implement network segmentation, zero trust architecture, and up to date hardware to improve system hardening and prevent cascading failures.

Example: 5-2 Ensure both physical and digital interlocks are in place to prevent remote operation of equipment that could cause damage based on plant configuration.

Example: 5-3 Use warnings that inform operators of inadvertent testing of interlocks or when the physical and digital systems are in disagreement.

Example: 5-4 Train operators to recognize that inadvertent testing of interlocks and physical to digital disagreements could be early warning signs of a compromised network.

Principle 6: Active Defense

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

1. Currently, there is no OT network monitoring solution in place. If the utility is unable to determine if a device is infected in a timely manner, it could result in undesired consequences to the process(es).
    a. Implementation of a commercial off-the-shelf OT network monitoring solution to quickly identify infected device(s) enables to block/disconnect/isolate network connection/device(s). Additional operations and maintenance documentation for executing manual control of critical processes during a focused or sustained cyber attack can help to improve response and recovery.
    b. Training can help operations staff to understand the potential for a cyber-enabled failure mode, what indicators or system behaviors may indicate that an attack is imminent or underway. Operator's licensure does not include awareness of the potential for cyber-enabled failure modes. It does, however, provide extensive training for how to prevent and react to non-cyber-enabled failure modes.
    c. Employing dynamic elements in a system that actively detect and defend from cyber threats is key. Without the means to proactively prepare against cyber incidents, the utility will be left one step behind if a bad actor successfully caries out a cyber attack.

Concept Question: What events could occur leading up to identified high-consequence events?

1. Installing dynamic elements to actively monitor the system will give the utility extra time to respond to a cyber attack. Knowing what the early warning signs are and how to modify the network and system to minimize or prevent damage is an important next step.

a. Early warning signs may include assets restarting or unexplained changes in the process (pump stops).

b. After operators notice these warning signs, they should recognize that changes to controls and investigation may be necessary. This may include actions such as isolating areas of the network of greatest priority and/or concern.

Example: 6-1 Implement an OT network monitoring solution. Design network to support data collection by sensors. Employ Zero Trust Architecture where possible.

Example: 6-2 Generate documentation on how to detect early warning signs and how to block, disconnect, and isolate network connection(s)/device(s).

Principle 7: Interdependency Evaluation

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

1. The utility does not have avenues to encourage shared input from multiple disciplines of operation. Digital misuse and cyber threats will impact multiple systems and disciplines, so understanding these interdependencies is key to properly plan for cyber incidents and avoid cascading failures.

   a. Improvements include continuous inter-department training and exercises to build relationships between different disciplines, demonstrating the interdependence of the overall system.

   b. From a system-wide performance consideration, if either of the water treatment plants are operating below a minimum capacity, there is the possibility that the water system will experience low pressures or a lack of quality water into the system. This could negatively impact the regional power plant's ability to have water for steam or cooling. Vice versa, if the power plant is not able to reliably produce power for an extended period of time, the utility facilities will not be able to accomplish their critical functions.

Concept Question: What inputs do the critical functions require that are not directly and completely controlled by its owners?

1. The utility requires timely shipments of chemicals used to treat the water. They currently are dependent on one organization in the area to fulfill their contract.

   a. This dependency on a single outside source can create a single point of failure. To improve resilience and maintain operational status, alternative sources should be considered as backups to avoid having insufficient resources to safely treat the water.

b. All functions that are not directly controlled by its owners should have workarounds and/or backups to minimize the potential for consequences to be realized.

Example: 7-1 Implement continuous inter-departmental training to build relationships between different disciplines which will facilitate communication during emergency situations.

Example: 7-2 Ensure multiple sources are available for any dependency on outside inputs.

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?

1. The utility's current system does not have a digital asset awareness program or up-to-date digital asset inventory. Without a complete and up-to-date digital asset inventory, staff is unable to track hardware, firmware, and software over time, and actively analyze the vulnerabilities that may reside within them.
   a. Improvements include the implementation of a commercial off-the-shelf OT network monitoring solution that uses passive data collection to build an asset inventory, and interface with asset management system. Additionally, subscribing to vulnerability reporting services can help to monitor asset inventory risk.

Concept Question: What need does the inclusion of digital assets fulfill?

1. By tracking digital assets, the utility will be able to establish and maintain an accurate list of devices that are on the network and better understand the full suite of capabilities (enabled or not) that exist within the digital devices that make up the system.
   a. Unknown devices will be easier to identify, find, and block.
   b. Knowing when devices need to be patched to their most up-to-date version prevents the persistence of unpatched vulnerabilities in the system.
   c. Protections and monitoring can be put in place to alert operators if features of a device are enabled that are not intended, such as a device with the capability to broadcast its own Wi-Fi network suddenly doing so when that is not the intended normal operating mode.

Example: 8-1 Adopt a commercial off the shelf OT network monitoring solution that uses passive data collection to build an asset inventory.

Example: 8-2 Regularly update the software and firmware on all devices found in the inventory.

Example: 8-3 Build a device capability catalog that specifies both what a device is fully capable of and what features are actually intended to be enabled.

Principle 9: Cyber-Secure Supply Chain Controls

Key Question: How do I ensure providers deliver the security the system needs?

1. The utility currently has no cyber-secure supply chain controls in place. As such, the utility risks product deliveries that do not meet design specifications or adhere to organizational processes and controls that support cyber-secure engineering and operations.
    a. Improvements include security requirements in request for proposals (RFPs) and contracts, a Secure Software Lifecycle Development program in place where software is involved, tight controls on vendor access, hardware component purchases tightly controlled, approved vendors only, vendor vulnerability program and capabilities to address new "zero day" vulnerabilities, and vendor software bill of materials (SBOM)/ hardware bill of materials (HBOM) and associated reporting capabilities.

Concept Question: What assumptions does the concept of operations make about the availability, quality, and security of the critical items or services in the supply chain?

1. The utility has assumed that replacements for critical hardware and physical assets will remain widely available on the market and that the vendors will be focused on cyber-security when designing their product.
    a. This assumption should be tested to understand if the utility could continue to operate through replacement of critical pieces of equipment in the case of a supply chain breakdown.
    b. The utility can also inadvertently take on risk by trusting that all vendors share the same level of awareness about cybersecurity. Vendors handling the most critical information should have elevated contractual cybersecurity requirements.

Example: 9-1 Include security requirements in RFPs and contracts, develop a Secure Software Lifecycle Development program, and implement tight vendor controls.

Principle 10: Planned Resilience

Key Question: How do I turn "what ifs" into "even ifs"?

1. The utility is aware that bad actors may attempt to gain access to their network and have worked through scenarios to consider what they would do if an attack occurred. What they have not considered is how to maintain long term operation of the plant even if a cyber-attack were to cause long-term damage or disruption.
    a. It is not enough to just implement control to minimize attack avenues. For a system to be truly designed with the CIE principles, one must expect that any digital

component or system may be compromised at some point during its lifecycle, and plan for continued operation during and after a cyber attack.

   b. Resolutions such as hardwired controls for critical signals ensure that the system can function under manual operation, even when the PLC or network is compromised.

   c. If a PLC is compromised and troubleshooting or replacement is necessary, the utility must ensure they are able to respond and recover quickly and confidently. Developing programming standards can support response and recovery operations.

Concept Question: What people, materials, and equipment will be needed to withstand and recover from a catastrophic event?

1. Some backup equipment such as extra switches are stored in an accessible location on site at the utility, but only enough for occasional failure of a single device at a time.
   a. Having readily accessible backup equipment for critical processes is necessary to keep the plant operating in the event of a failure of a component but the backup inventory should include enough resources to recover quickly from a catastrophic event.
2. The utility has staff available to assist in recovery of a catastrophic event but will need to reach out to a third party for rebuilding the SCADA network.
   a. If the third party is not on contract to provide immediate response in the case of an emergency, it could take extra time to recover critical facilities.
3. The utility has some documentation on emergency response and recovery operations but lacks specific standards for network recovery after a catastrophic event.
   a. Having readily accessible response and recovery documentation in both digital and physical form will facilitate a quick recovery. Exercising staff knowledge, skills, and abilities to implement response and recovery operations are critical.

Example: 10-1 Verify the plant has the functionality to operate critical functions safely, long term, without the use of SCADA.

Example: 10-2 Ensure backup inventory is maintained to an acceptable level. Establish contractual agreements with third party consultants to lend immediate help in an emergency.

Example: 10-3 Develop written standards and procedures for recovery of network environments and train staff to expect that any digital component can become compromised and lose functionality.

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?

1. The city has a website where the minutes for board meetings can be found publicly. The utility has noted that during several meetings sensitive information has been brought up about plant operation and funding, such as specific versions and implementation of the SCADA network and the need for an upgrade to a modern version. The utility has also worked toward a model of complete transparency in their operations. As such, some sensitive information about their internal organization and procurement strategies is publicly available on their website.
    a. If sensitive information or engineering records (i.e., requirements, specifications, designs, configurations, and testing) gets into the hands of a malicious actor, the system could be placed at a greater risk of attack. Specific SCADA-related information about the utility was publicly available through procurement documents and standards posted on their website. Specific SCADA information such as the above should not be available through open-source intelligence sources. This data should be kept secure and only available on an as-needed basis through submittal of a request for information (RFI).
    b. As a public agency, the utility is required by state procurement law to publicize a great deal of information regarding any procurement decision. While the utility has some flexibility to protect sensitive information, they have assumed that more transparency of procurement practices is better. Thus, they have publicly released most of the information regarding the engineering of their systems. To prevent further release of sensitive information, staff responsible for CIE organizational principles educated the procurement staff on how engineering information needs to be protected. Now, detailed engineering information will not be posted publicly on the internet. In addition, any valid user of the information is now contractually required to be insured against unapproved information releases of the utility's information.

Concept Question: How will sensitive information be identified as it is collected and created throughout the lifetime of the project?

1. During the engineering lifecycle it is the responsibility of each staff member and external support personnel to adhere to engineering information controls. At each stage the information should be considered with a focus on consequence.
    a. Information such as contractors, organizational structure, and software details can all be used by threat actors to exploit vulnerabilities and more easily impersonate trusted individuals or companies.

b. This information should be documented as sensitive and an official warning citing federal exemptions from the Freedom of Information Act including America's Water Infrastructure Act of 2018 Section 2013(b), Amendment to Safe Drinking Water Act Section 1433 as well as state and local codes should be placed on the documentation.

c. Further information on protecting sensitive information within a water sector organization can be found in the Protecting the Water Sector's Critical Infrastructure Information: Analysis of State Laws by the American Water Works Association. Working with internal counsel and leadership to understand the controls available to the Utility allows for the unwanted release of information.

Example: 11-1 Identify sensitive information within the organization and verify each document has the appropriate warnings.

Example: 11-2 Ensure each staff member and outside consultants understand the need for confidentiality.

Example: 11-3 Minimize access to sensitive information and evaluate it on a case-by-case basis

Principle 12: Organizational Culture

Key Question: How do I ensure that everyone's behaviors and choices align with our security goals?

1. To maintain a truly cyber-secure system, it is important for the entire team to buy in. Implementing consistent cybersecurity training across the organization will collectively empower all staff to participate in cybersecurity practices across the engineering lifecycle. Cybersecurity isn't "just IT's" problem any longer.

   a. During table-top exercises, staff from other facilities are invited to join the exercises as observers and evaluators. This allows them to bring the lessons learned back to their facilities and colleagues. These tabletop exercises and associated training socialize the potential consequences of a cyber attack and the associated controls to prevent those consequences. For example, when the operations staff from WTP #2 observed a tabletop exercise emphasizing operations in the absence of automation they took the concepts back to their WTP. They didn't have any standard operating procedures for manual operations at several of their critical processes. The operators took the programs from the PLCs and determined the required actions to operate the processes in the absence of automation.

b. Awareness training and periodic updates emphasizing the importance of CIE is regularly done to update the following groups: Utility Leadership, Engineering, Operations and Maintenance, Risk Management. During each update, the staff responsible for implementing CIE across the organization provide updates on changes to the operating environment, new threats, incidents, and successful implementation of controls and mitigations. These conversations focus on the consequences mitigated and allow for the organization to update CIE implementation strategies.

Concept Question: How is the fundamental tradeoff between efficiency and security decided?

1. The utility has an ongoing internal debate on how to balance security and efficiency. One example is implementing remote access software to their SCADA network to allow for remote operation of the plant in an emergency. This flexibility increases their efficiency but at the cost of adding another attack vector that can be exploited.
   a. Operations staff are ultimately responsible for the day-to-day functioning of the system. Educating them on the risks and supporting them in the process of balancing efficiency and security that optimizes for resilience is critical. This could be accomplished through regular maintenance periods where the automation is unreliable and/or unavailable.
   b. Evaluating the tradeoffs may be more productive when a culture of cybersecurity exists.

Example: 12-1 Regularly conduct tabletop exercises with staff and discuss consequences of a cyber attack. Implement mandatory training for all staff on cyber security and implementing CIE principles.

Example: 12-2 Heavily scrutinize any function that lowers security in favor of efficiency.

C.7 Engineering Lifecycle Phase and CIE Principle Cross Reference Matrix

Table 5 and Table 6 organize the CIE controls and mitigations identified below according to either the related principles or the engineering lifecycle phase of implementation. In Table 5 each action, abbreviated from the description below, identifies a primary CIE Principle and secondary related principles. For example, the CIE control or mitigations associated primarily with Principle 3: Secure Information Architecture are also associated with Principle 1: Consequence-Focused Design and Principle 6: Active Defense.

Table 6 presents CIE controls and mitigations mapped to the engineering lifecycle phase that they are first associated with. The examples associated with Principle 6: Active Defense, are first associated with Testing, Verification, Validation, and Deployment (TVVD)/Construction and Commissioning.

Table 5 - CIE Examples by Principle

Primary Principle
Secondary Principle

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE	1 - Consequence-focused Design	2 - Engineered Controls	3 - Secure Information Architecture	4 - Design Simplification	5 - Layered Defense	6 - Active Defense	7 - Interdependency Evaluation	8 - Digital Asset Awareness	9 - Cyber-Secure Supply Chain Controls	10 - Planned Resilience	11 - Engineering Information Control	12 - Organizational Culture
Principle 1: Consequence-Focused Design	**1-1** When considering any changes to design and operation, each person should be considering and discussing cyber-enabled failure scenarios and the consequences of losing critical functions.	**P**									**S**		**S**
Principle 2: Engineering Controls	**2-1** Wire instrumentation signals directly to applicable cable motor starters to provide equipment and personnel protection for all modes of operation, even if the network or PLC have been compromised.	**S**	**P**		**S**								**S**
Principle 3: Secure Information Architecture	**3-1** Network traffic should be handled by a highly available Next Generation Firewall (NGFW) appliance, policies and zones should be created to segment and control traffic.	**S**		**P**		**S**	**S**						**S**
	3-2 Establish a Demilitarized Zone (DMZ) to separate SCADA network from The Cities network.	**S**		**P**		**S**					**S**		**S**

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE	Associated Principles											
		1	2	3	4	5	6	7	8	9	10	11	12
Principle 4: Design Simplification	**4-1** Remove ETAPS and implement managed industrial switches for enhanced monitoring capabilities and traffic control.	S		S	P		S						S
	4-2 Challenge all digital solutions to determine if the design can be simplified by removing them.	S	S		P						S		S
Principle 5: Layered Defenses	**5-1** Implement network segmentation, zero trust architecture, and up to date hardware to improve system hardening and prevent cascading failures.	S			S	P					S		S
	5-2 Ensure backup inventory is maintained to an acceptable level. Verify third party consultants have a contractual agreement to lend immediate help in an emergency.	S				P		S					S
	5-3 Develop written standards and procedures for recovery of network environments.	S				P					S		S
Principle 6: Active Defense	**6-1** Implement an OT network monitoring solution. Design network to support data collection by sensors. Employ Zero Trust Architecture where possible.	S		S			P						S
	6-2 Generate documentation on how to detect early warning signs and how to block, disconnect, and isolate network connection/device(s).	S					P						S
Principle 7: Interdependency Evaluation	**7-1** Implement continuous inter-departmental training to build relationships between different disciplines which will facilitate communication during emergency situations.	S						P			S		S
	7-2 Ensure multiple sources are available for any dependency on outside inputs.	S						P		S	S		S
Principle 8: Digital Asset Awareness	**8-1** Adopt a commercial off the shelf OT network monitoring solution that uses passive data collection to build an asset inventory.	S							P	S			S
	8-2 Regularly update the software and firmware on all devices found in the inventory	S		S					P				S
Principle 9: Cyber-Secure Supply Chain Controls	**9-1** Include security requirements in RFPs and contracts, develop a Secure Software Lifecycle Development program and implement tight vendor controls.	S								P	S		S

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE	Associated Principles											
		1	2	3	4	5	6	7	8	9	10	11	12
Principle 10: Planned Resilience	**10-1** Install hardwired controls for all critical systems.	S	S								P		S
	10-2 Generate documentation and train staff to expect that any digital component can become compromised and lose functionality and know how to operate in manual.	S									P		S
Principle 11: Engineering Information Control	**11-1** Identify sensitive information within the organization and verify each document has the appropriate warnings.	S									S	P	S
	11-2 Ensure each staff member and outside consultants understand the need for confidentiality.	S										P	S
	11-3 Minimize access to sensitive information and evaluate it on a case-by-case basis.	S										P	S
Principle 12: Organizational Culture	**12-1** Regularly conduct table top exercises with staff and discuss consequences of a cyber-attack.	S						S					P
	12-2 Implement mandatory training for all staff on cyber security and implementing CIE principles.	S						S			S		P

Table 6 - CIE Principles by Engineering Lifecycle Phase

First point in the Engineering Lifecycle that the example is considered

Continuation of the example through the Engineering Lifecycle

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE	CIE Engineering Lifecycle: Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance
		Water Sector Engineering Lifecycle: Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning		Operations and Maintenance
Principle 1: Consequence-Focused Design	**1-1** When considering any changes to design and operation, each person should be considering and discussing cyber-enabled failure scenarios and the consequences of losing critical functions.	■	■	■	■	■	■
Principle 2: Engineering Controls	**2-1** Wire instrumentation signal wires directly to applicable cable motor starters to provide equipment and personnel protection for all modes of operation, even if the network or PLC have been compromised.			■	■	■	■
Principle 3: Secure Information Architecture	**3-1** Network traffic should be handled by a highly available Next Generation Firewall (NGFW) appliance, policies and zones should be created to segment and control traffic.			■	■	■	■
	3-2 Establish a Demilitarized Zone (DMZ) to separate SCADA network from The Cities network.			■	■	■	■
Principle 4: Design Simplification	**4-1** Remove ETAPS and implement managed industrial switches for enhanced monitoring capabilities and traffic control.			■	■	■	■
	4-2 Challenge all digital solutions to determine if the design can be simplified by removing them.		■	■	■	■	■
Principle 5: Layered Defenses	**5-1** Implement network segmentation, zero trust architecture, and up to date hardware to improve system hardening and prevent cascading failures.			■	■	■	■
	5-2 Ensure backup inventory is maintained to an acceptable level. Verify third party consultants have a contractual agreement to lend immediate help in an emergency.				■	■	■
	5-3 Develop written standards and procedures for recovery of network environments.					■	■

First point in the Engineering Lifecycle that the example is considered

Continuation of the example through the Engineering Lifecycle

CIE Engineering Lifecycle

Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance

Water Sector Engineering Lifecycle

Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning	Operations and Maintenance

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE
Principle 6: Active Defense	**6-1** Implement an OT network monitoring solution. Design network to support data collection by sensors. Employ Zero Trust Architecture where possible.
	6-2 Generate documentation on how to detect early warning signs and how to block, disconnect, and isolate network connection/device(s).
Principle 7: Interdependency Evaluation	**7-1** Implement continuous inter-departmental training to build relationships between different disciplines which will facilitate communication during emergency situations.
	7-2 Ensure multiple sources are available for any dependency on outside inputs.
Principle 8: Digital Asset Awareness	**8-1** Adopt a commercial off the shelf OT network monitoring solution that uses passive data collection to build an asset inventory.
	8-2 Regularly update the software and firmware on all devices found in the inventory
Principle 9: Cyber-Secure Supply Chain Controls	**9-1** Include security requirements in RFPs and contracts, develop a Secure Software Lifecycle Development program and implement tight vendor controls.
Principle 10: Planned Resilience	**10-1** Install hardwired controls for all critical systems.
	10-2 Generate documentation and train staff to expect that any digital component can become compromised and lose functionality and know how to operate in manual.

First point in the Engineering Lifecycle that the example is considered

Continuation of the example through the Engineering Lifecycle

CIE Engineering Lifecycle

Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance

Water Sector Engineering Lifecycle

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE	Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning		Operations and Maintenance
Principle 11: Engineering Information Control	**11-1** Identify sensitive information within the organization and verify each document has the appropriate warnings.	■	■	■	■	■	■
	11-2 Ensure each staff member and outside consultants understand the need for confidentiality.	■	■	■	■	■	■
	11-3 Minimize access to sensitive information and evaluate it on a case-by-case basis.	■	■	■	■	■	■
Principle 12: Organizational Culture	**12-1** Regularly conduct table top exercises with staff and discuss consequences of a cyber-attack.					■	■
	12-2 Implement mandatory training for all staff on cyber security and implementing CIE principles.	■	■	■	■	■	■

Appendix D: CIE Background and Resources

March 2017: *Cyber-Informed Engineering* White Paper—Researchers at Idaho National Laboratory first began to define a CIE approach in 2017, identifying a set of principles to consider when solving an engineering problem. In the intervening years, those principles have been refined and revised in subsequent research efforts and publications. This Implementation Guide now offers the most current and granular identification of CIE principles to date.

June 2022: *National Cyber-Informed Engineering Strategy*—The National CIE Strategy was developed by a Congressionally-directed executive task force, assembled by the U.S. Department of Energy (DOE), that included energy sector asset owners and operators, vendors and manufacturers, standards organizations, research and academic institutions, National Laboratories, and government agencies. It outlines strategic recommendations across five pillars of action, including raising awareness of CIE, building CIE into engineering education and accreditation, developing a body of knowledge and resources for CIE, and implementing CIE in both existing systems and future infrastructure designs. This Implementation Guide directly addresses a recommendation in the Development pillar to develop an open-source library of CIE resources, including an implementation guide for the design and engineering process.

March 2023: *National Cybersecurity Strategy*—Objective 4.4 (Secure our Clean Energy Future) calls for the implementation of the National CIE Strategy.

July 2023: *National Cybersecurity Strategy Implementation Plan*—Initiative 4.4.3 directs DOE to build CIE training, tools, and support for CIE.

May 2023: *Using Cyber-Informed Engineering for Cyber Defense Workbook*—this workbook outlines how to implement CIE during a hypothetical system upgrade, including hands-on exercises. Developed in parallel with the Implementation Guide, it contains similar descriptions of the CIE principles that have been further refined in this Implementation Guide.

For more CIE articles, publications, webinars, and podcasts, visit: inl.gov/cie

Cyber-Informed Engineering
Implementation Guide

INL/RPT-23-74072

U.S. DEPARTMENT OF ENERGY
Office of
Cybersecurity, Energy Security, and Emergency Response