International Council on Systems Engineering
A better world through a systems approach

Welcome to the INCOSE Webinar Series

Wednesday, 19th June 2024 – Webinar 174

incose.org

Thank you to our 2024 Webinar Sponsors!

DASSAULT SYSTEMES

Platinum Partner

SPEC INNOVATIONS

Corporate Sponsor

Susan E. Ronning, P.E., PMP, ASEP

s.ronning@adcomm911.com
Susan.Ronning@incose.net

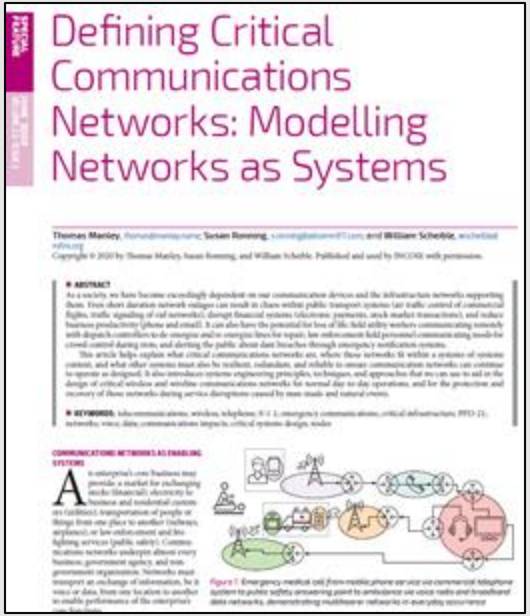
Owner & Principal Engineer, ADCOMM Engineering

- Founded in 1979; focused on Critical Communications Technologies for
  - Public Safety Agencies: Fire, Law, EMS
  - 9-1-1 and Critical Control Room Dispatch
  - Power/ Water Utilities and Transportation
- Vendor-neutral, independent consulting firm who advocates for our clients to ensure the right solution, using the right products and services at the right price.
- Combined team with 150+ years of Expertise
- Woman-, Minority-, and Veteran- Owned

ADCOMM
Engineering LLC
Bridging The Gap Between Operations & Technology®

INCOSE ICT Working Group

Chair, INCOSE ICT Working Group



Defining Critical Communications Networks: Modelling Networks as Systems

ict@incose.net

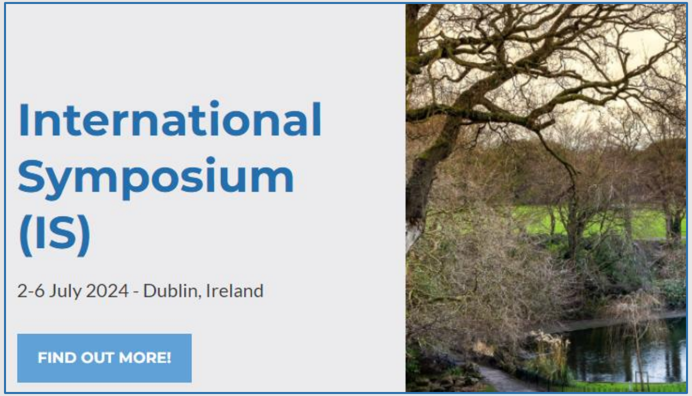
INCOSE Webinar 174:

Engineering-In Cyber through Systems Engineering

Presented by Virginia L. Wright

About the INCOSE Webinar Series

- Piloted in 2008
- A virtual offering aimed to provide relevant technical information and topics on systems engineering, on a regular basis and on an easy to access platform
- Held once a month (normally on the 3rd Wednesday)
- https://www.incose.org/events

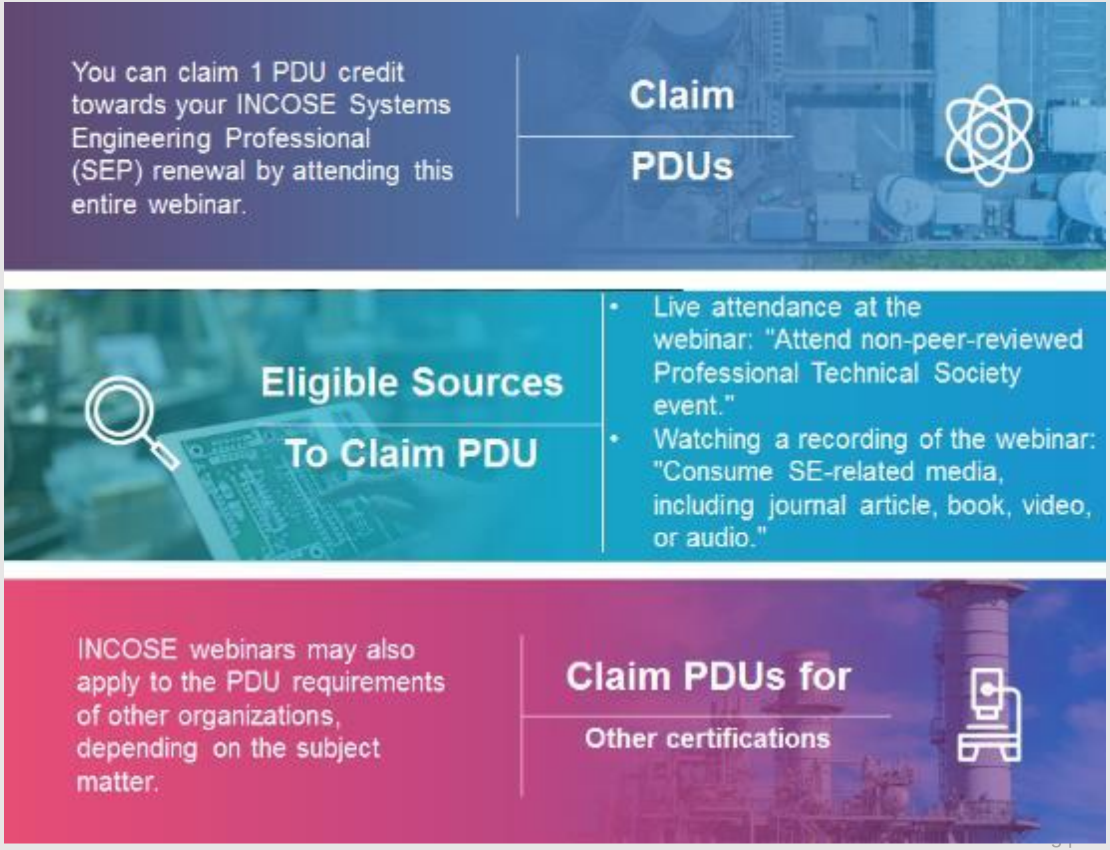


Questions? Comments? Suggestions?
Email us at webinars@incose.net!

Webinars & SEP PDU* Credits

More information can be found on [Renewing Certification (incose.org)]

*PDU – Professional Development Unit



Webinar Cadence

- **Welcome** (2-5 minutes)
- **Presentation** (40-45 minutes)
- Please use Q&A feature via Zoom to enter your questions
- **Q&A Session** (10 minutes)
- Questions will be selected and asked by the Host
- **Brief Closing** (2-5 minutes)

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

Cyber-Informed Engineering

National Cyber-Informed Engineering Strategy

from the U.S. Department of Energy

JUNE 2022

CESER Leadership

Puesh M. Kumar

Director

Puesh M. Kumar leads the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The office is focused on strengthening the security and resilience of the U.S. energy sector from cyber, physical, and climate-based risks and disruptions.

Puesh manages over 150 federal employees and numerous contractors who are engaged in National- and State-level policy development, executing technical assistance, conducting research, development, and demonstration (RD&D) projects, managing the U.S. Strategic Petroleum Reserve, and leading emergency response efforts in the U.S. energy sector. He represents the Department at National Security Council (NSC) meetings on cybersecurity and resilience, leads executive-level coordination with the private sector including the CEO-led Electricity Subsector Coordinating Council (ESCC) and senior executive-led Oil and Natural Gas

2024 INCOSE WESTERN STATES REGIONAL CONFERENCE

Cybersecurity by Design –
Applying Cyber Informed Engineering Principles and Practices

Susan Ronning, P.E., PMP, ASEP
Owner & Principal, ADCOMM Engineering LLC
Ben Amaba, PhD
Fellow, Industrial and Systems Engineering, Sonatype
Virginia "Ginger" Wright
Cyber-Informed Engineering Program Manager, Idaho National Lab
Col. Joseph Gilbert
Chief, Enterprise Services Division, U.S. Army

IWCE Connecting Critical Communications

#IWCE24

This Webinar is being recorded.

The full recording and slide deck will be made available to all INCOSE members and CAB Associates within 10-12 business days from original air date in the Professional Development Portal (PDP).

Questions? Comments? Suggestions? Email us at webinars@incose.net!

INCOSE Webinar 174:

Engineering-In Cyber through Systems Engineering

Presented by Virginia L. Wright

Hello.

Virginia Wright

CIE Program Manager,
Idaho National Laboratory

Ginger leads INL's implementation of the National Strategy for Cyber-Informed Engineering. She has led DOE-CESER's Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program, Software Bills of Material for the Energy Sector, critical infrastructure modeling and simulation, and nuclear cybersecurity. Ms. Wright has a Bachelor of Science in Information Systems/Operations Management from the University of North Carolina at Greensboro.

INL Background

- One in a network of 17 DOE national labs
- DOE's lead lab for nuclear energy
- A major center for National Security

6,122 Employees

524 Interns

$1.6 B Budget

235 Patents

INL Mission

Our mission is to discover, demonstrate and secure innovative nuclear energy solutions, other clean energy options and critical infrastructure.

INL Vision

INL will change the world's energy future and secure our critical infrastructure.

Research in the National Interest that **Maintains American Competitiveness & Security**

What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

-- *Cybersecurity and Infrastructure Security Agency (CISA)*

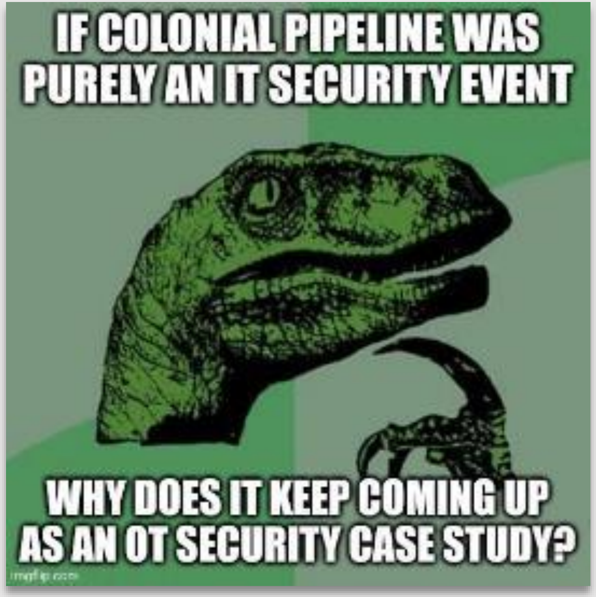
What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

-- *Cybersecurity and Infrastructure Security Agency (CISA)*

What's wrong with this picture?

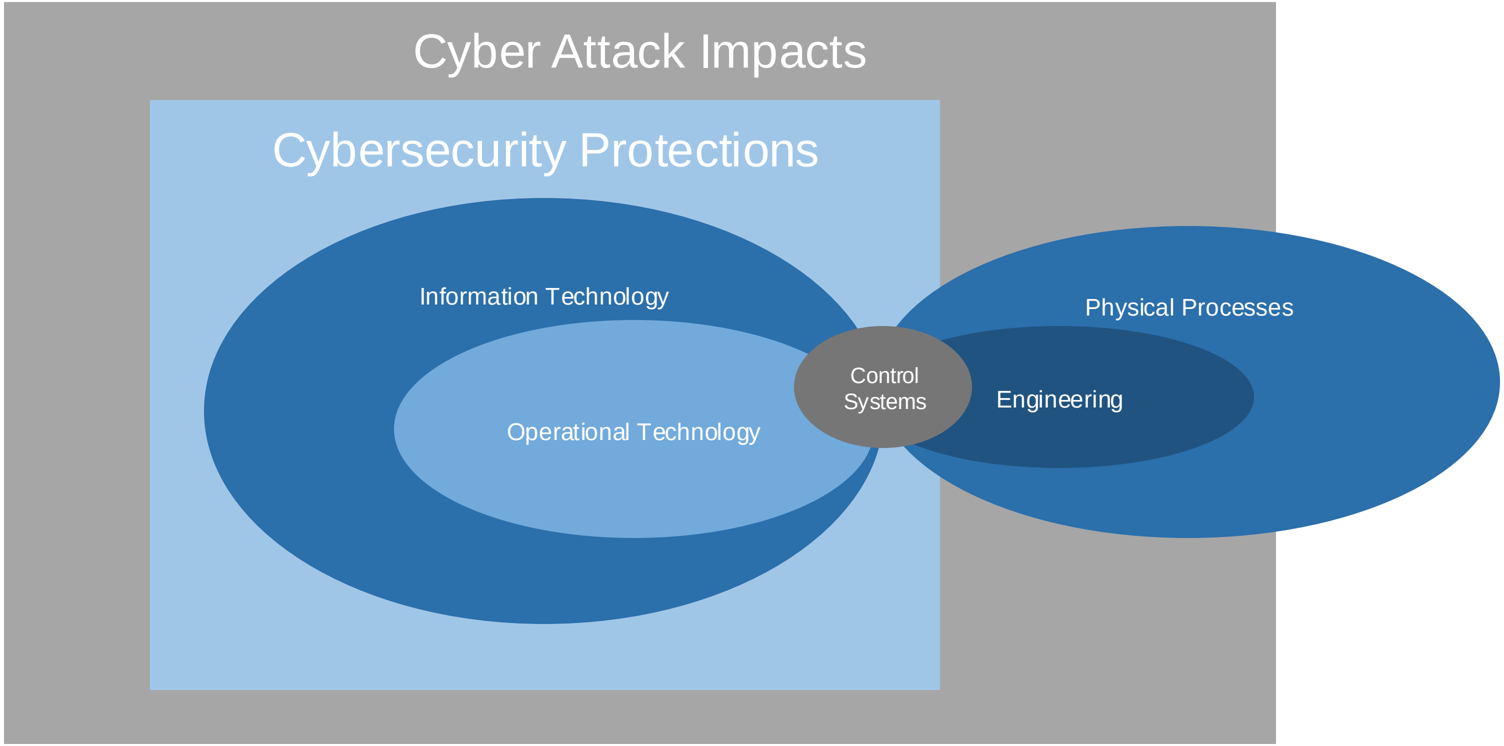
Cybersecurity is not just about data



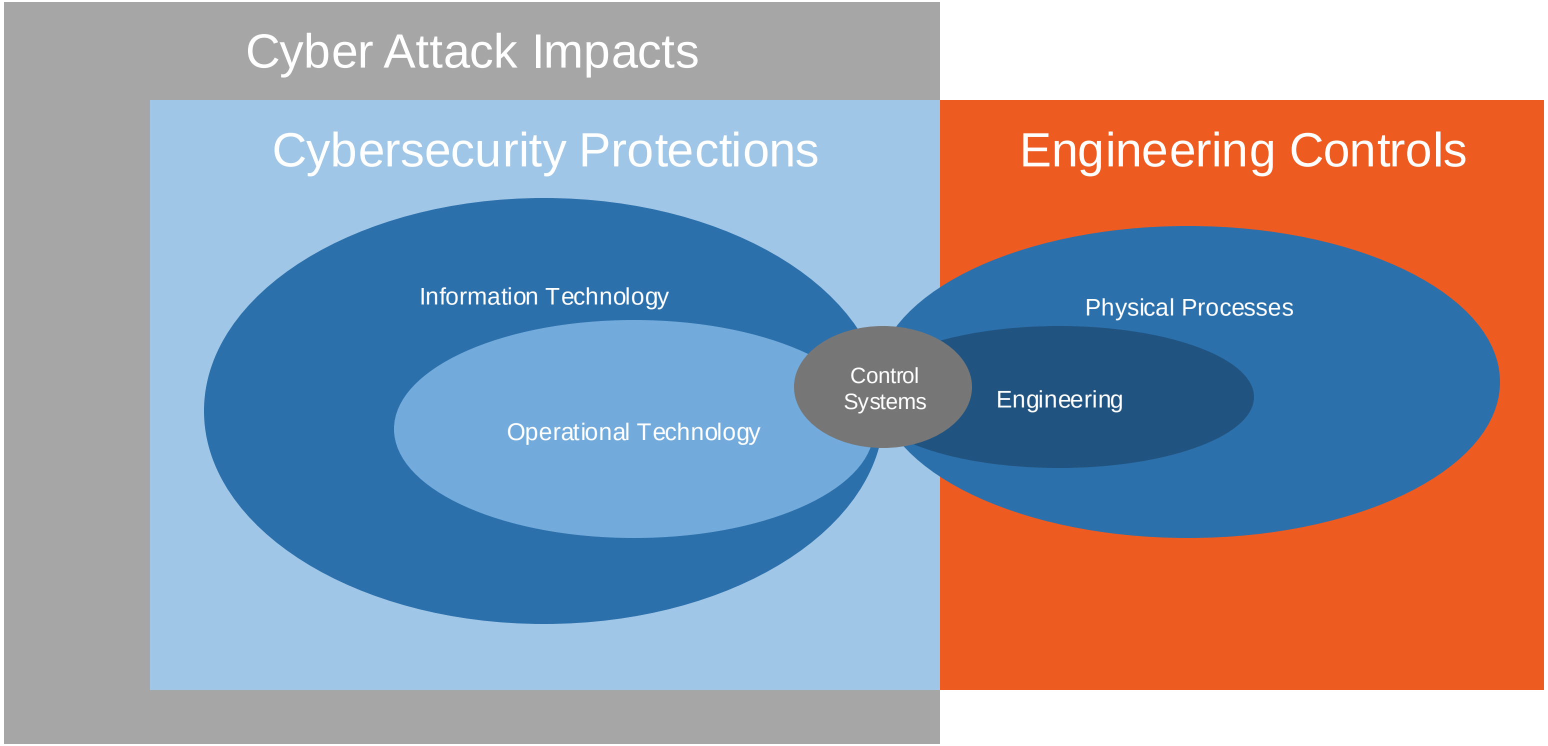
Joe Slowick, MITRE

- Ransomware attacked business data on an IT network
- However, pipeline operations were curtailed.
- Why?

Cybersecurity in Operational Technology



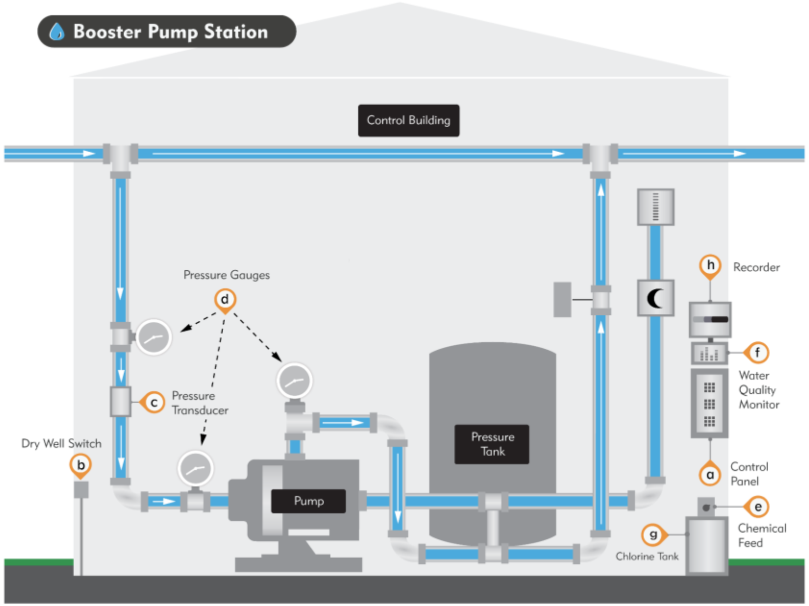
Cyber-Informed Engineering



How does Cyber-Informed Engineering Work?

Water Booster Pump Station

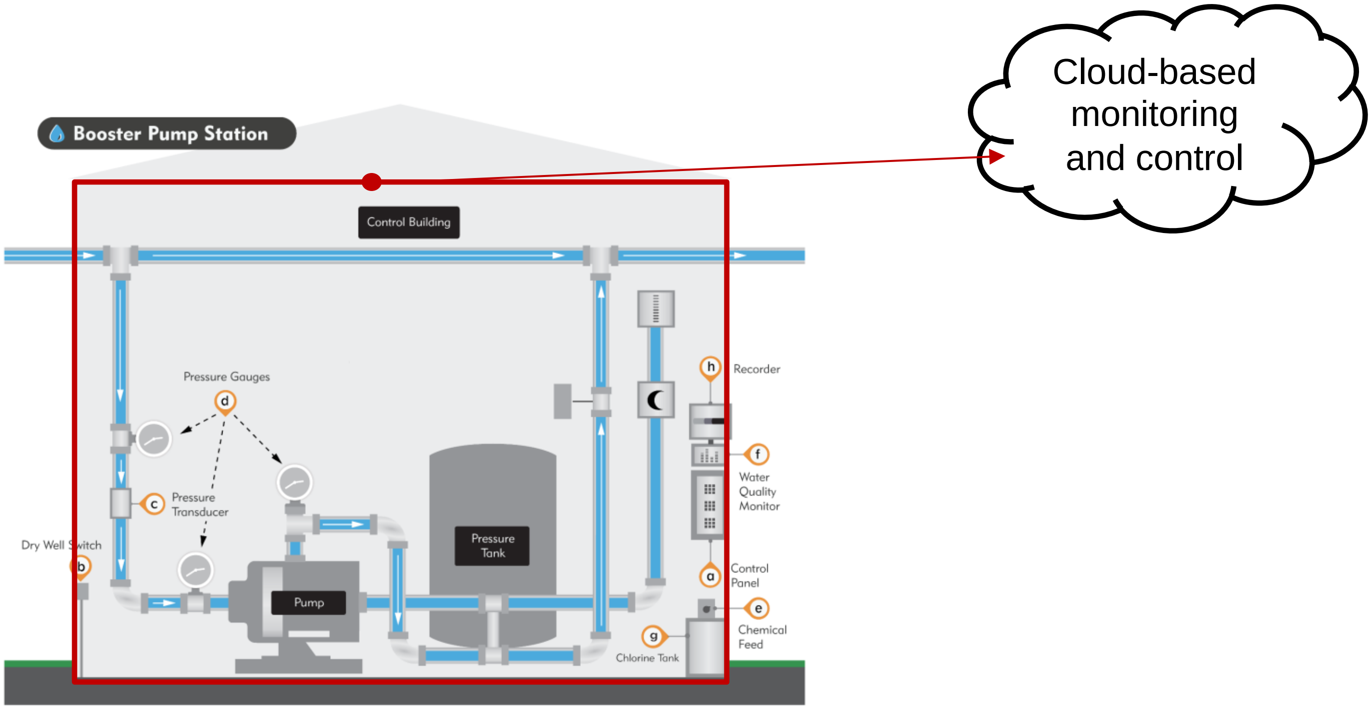
Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

Water Booster Pump Station



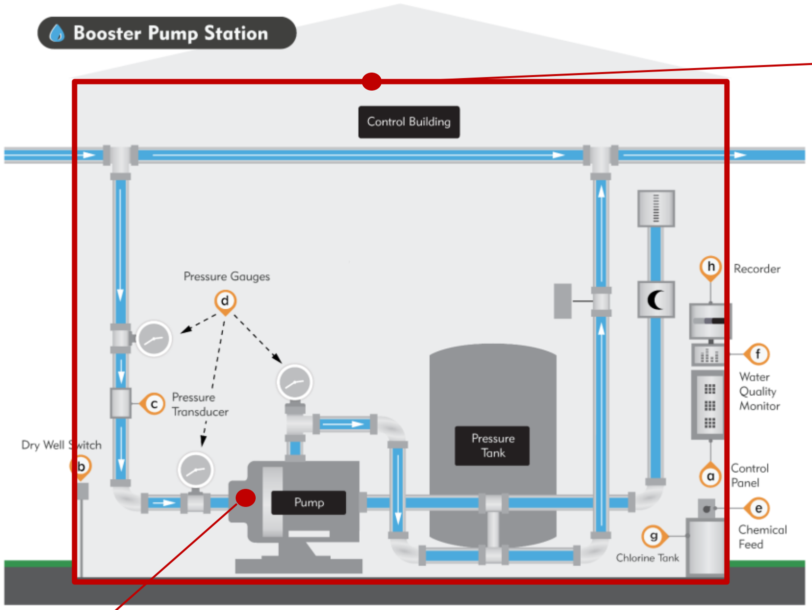
Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

INCOSE

Water Booster Pump Station

Cloud-based monitoring and control



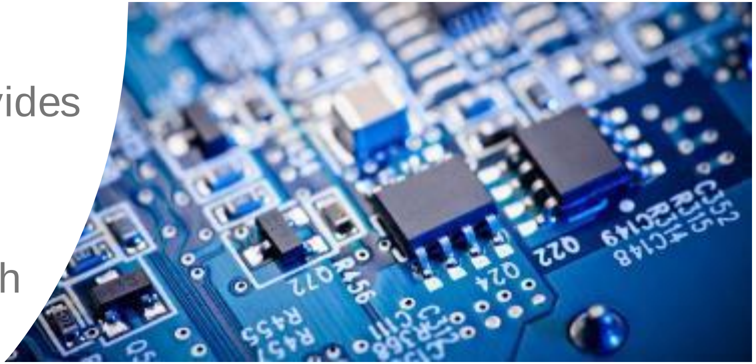
Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

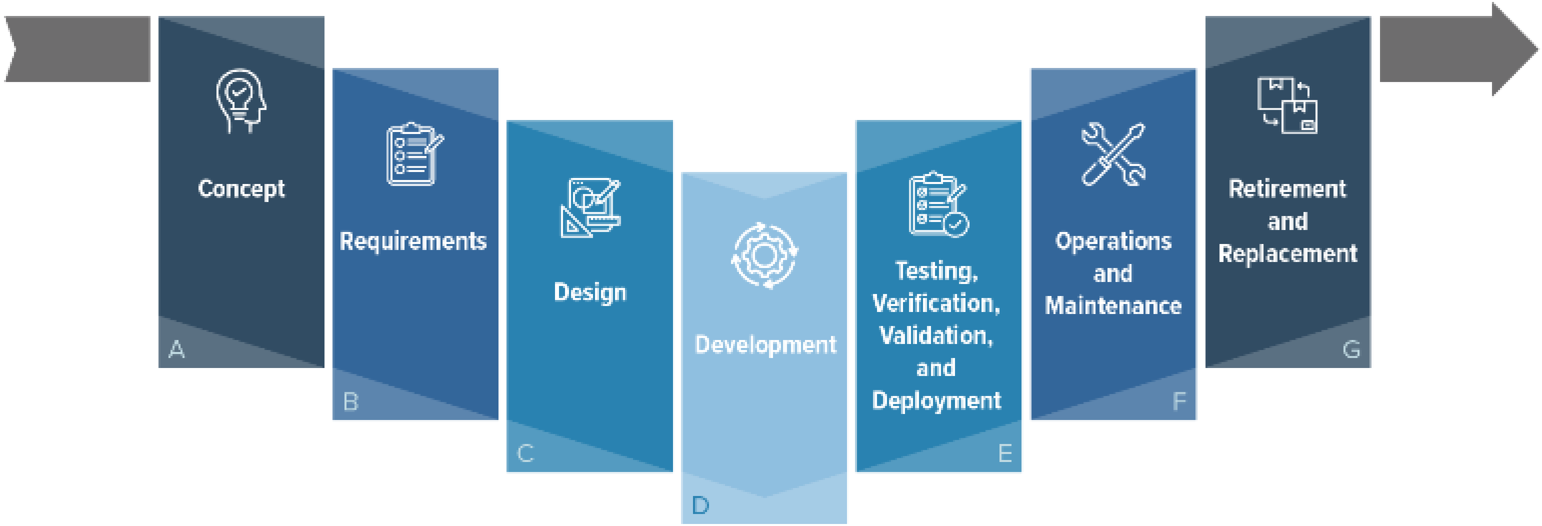
Mechanical Time Delay Relay

Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to build a **culture of security** aligned with the existing industry safety culture.



CIE and the Systems Engineering Lifecycle



CIE and the Systems Engineering Lifecycle

OT Cybersecurity risk mitigations are usually applied here…

CIE and the Systems Engineering Lifecycle

...but they are more effective and efficient when applied here.

OT Cybersecurity risk mitigations are usually applied here...

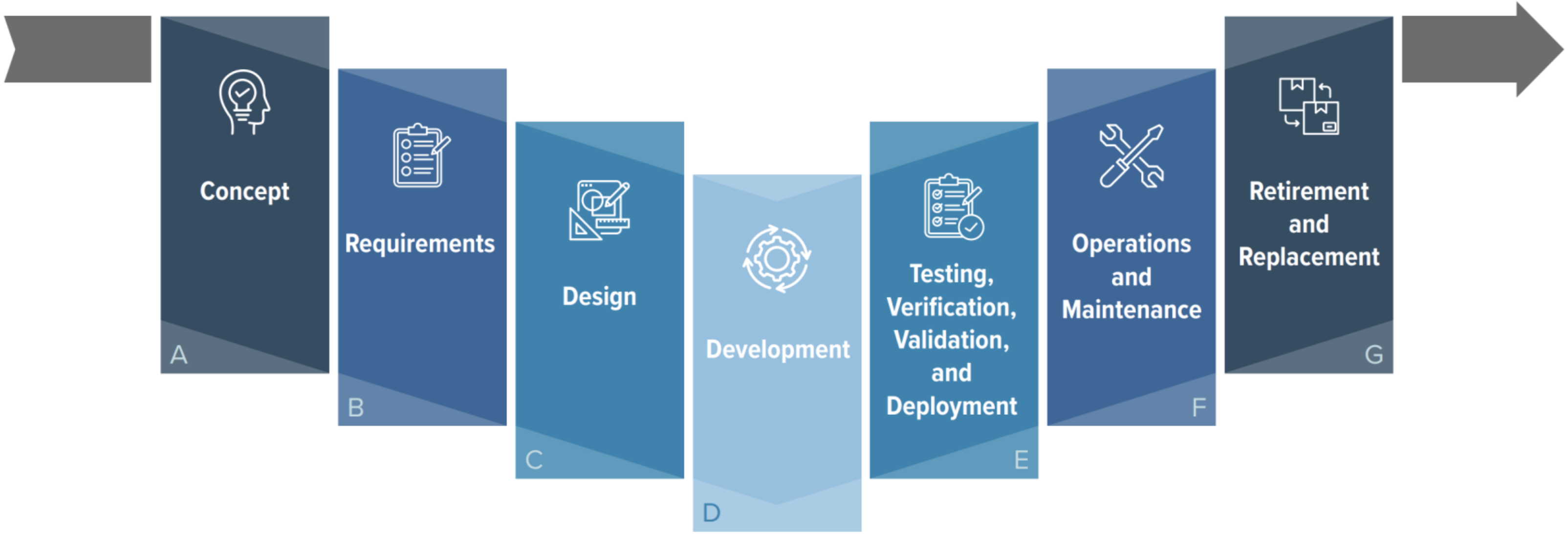
CIE Principles

Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
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?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

CIE Implementation Guide

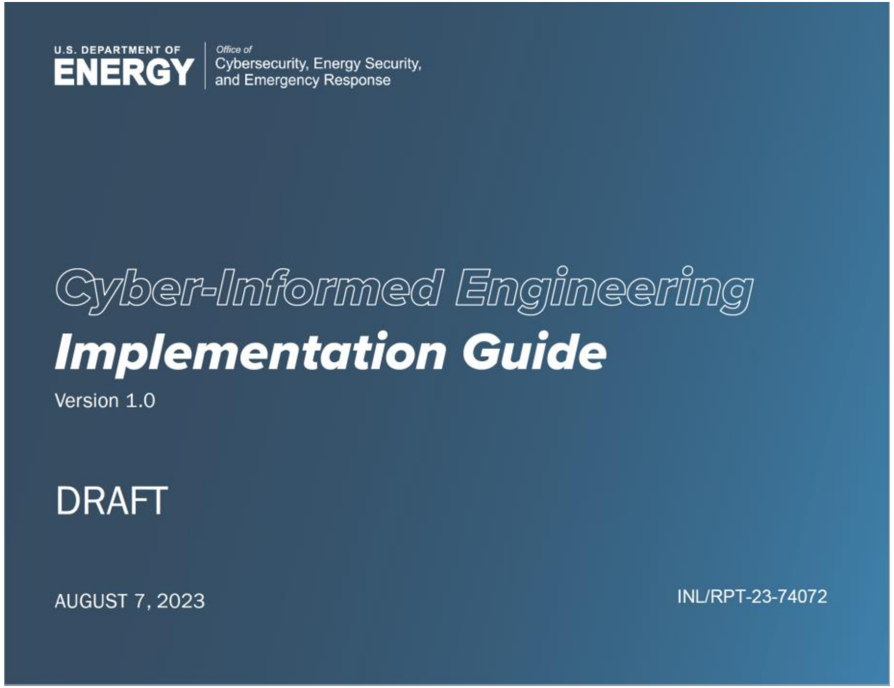
Applying CIE across the SE Lifecycle

Figure 2. CIE Systems Engineering Lifecycle Model



CIE Implementation Guide

https://www.osti.gov/servlets/purl/1995796


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

Cyber-Informed Engineering

Implementation Guide

Version 1.0

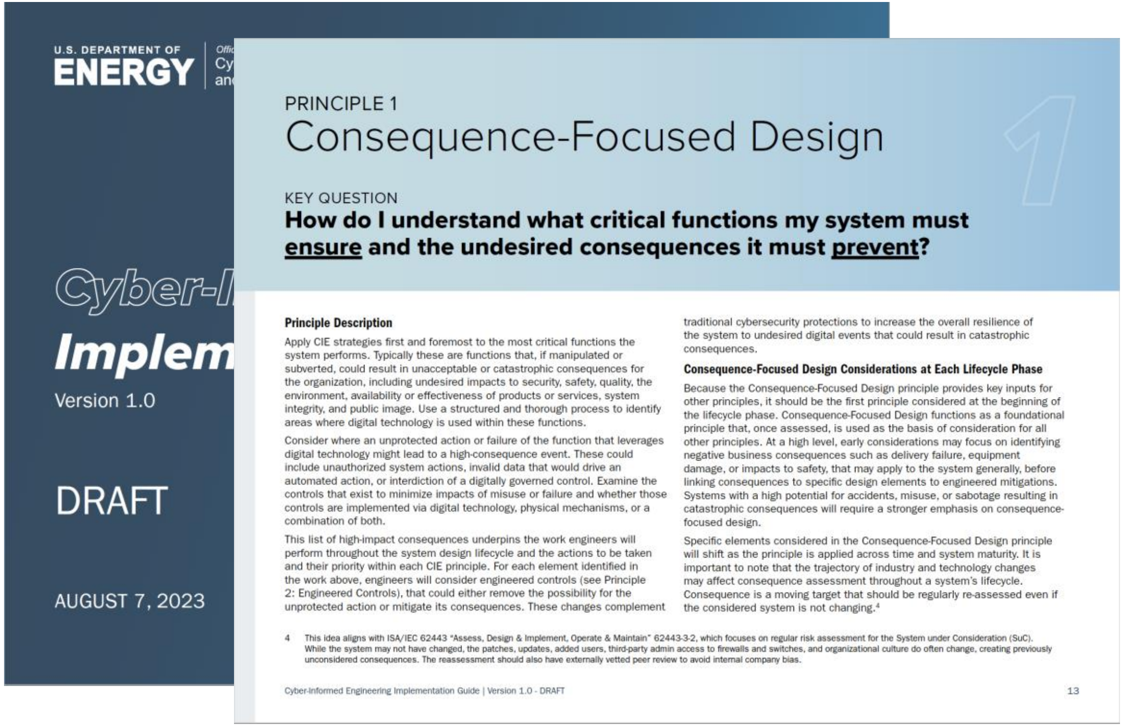
DRAFT

AUGUST 7, 2023

INL/RPT-23-74072

CIE Implementation Guide

https://www.osti.gov/servlets/purl/1995796



U.S. DEPARTMENT OF ENERGY

Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1

Consequence-Focused Design

KEY QUESTION

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

Principle 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.

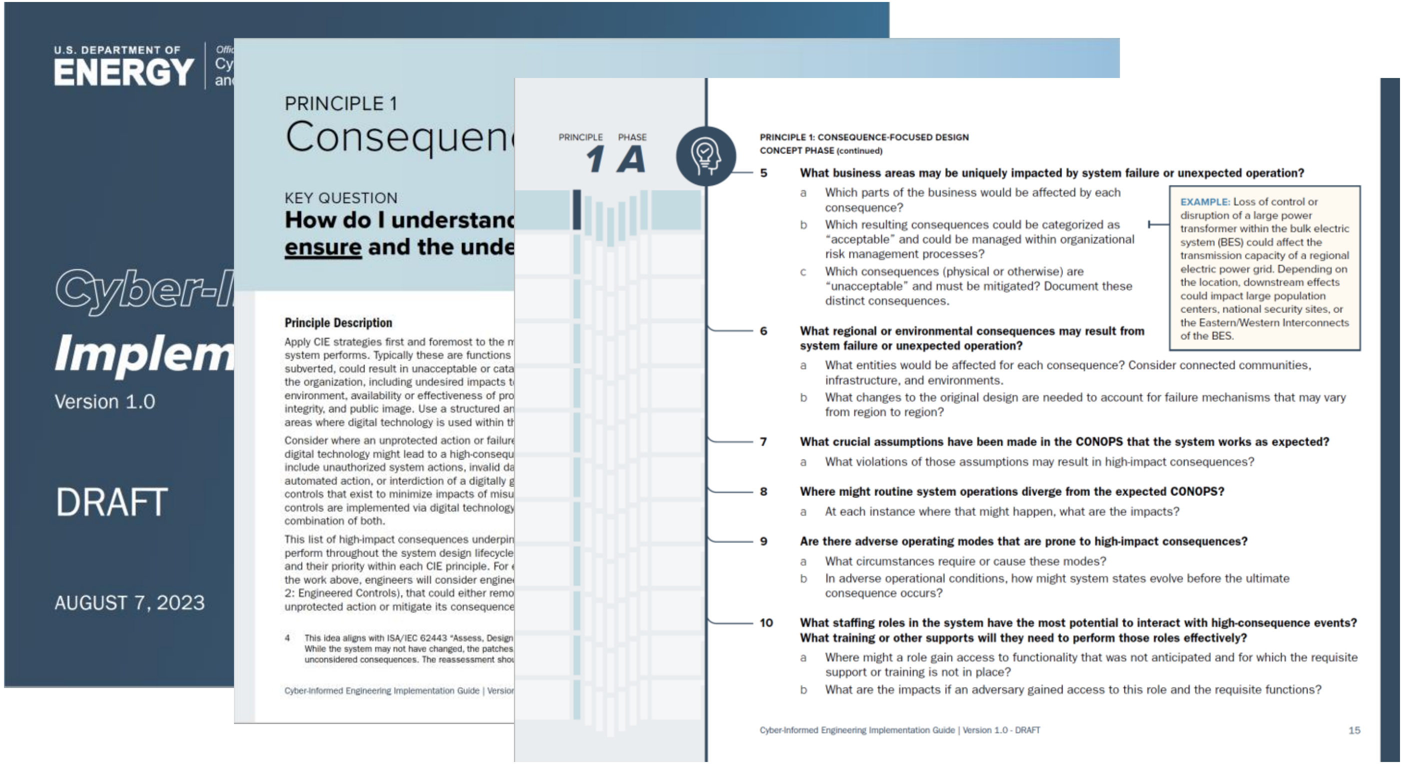
Specific elements considered in the Consequence-Focused Design principle will shift as the principle is applied across time and system maturity. It is important to note that the trajectory of industry and technology changes may affect consequence assessment throughout a system's lifecycle. Consequence 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.

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT 13

CIE Implementation Guide

https://www.osti.gov/servlets/purl/1995796



U.S. DEPARTMENT OF ENERGY

Cyber-I
Implem
Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1
Consequen

KEY QUESTION
How do I understand
ensure and the unde

Principle Description

PRINCIPLE PHASE
1 A

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?

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT 15

CIE Questions (Example)

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?

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.

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?

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

CIE Questions (Systems Engineering)

PRINCIPLE 1
PHASE ALL

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

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

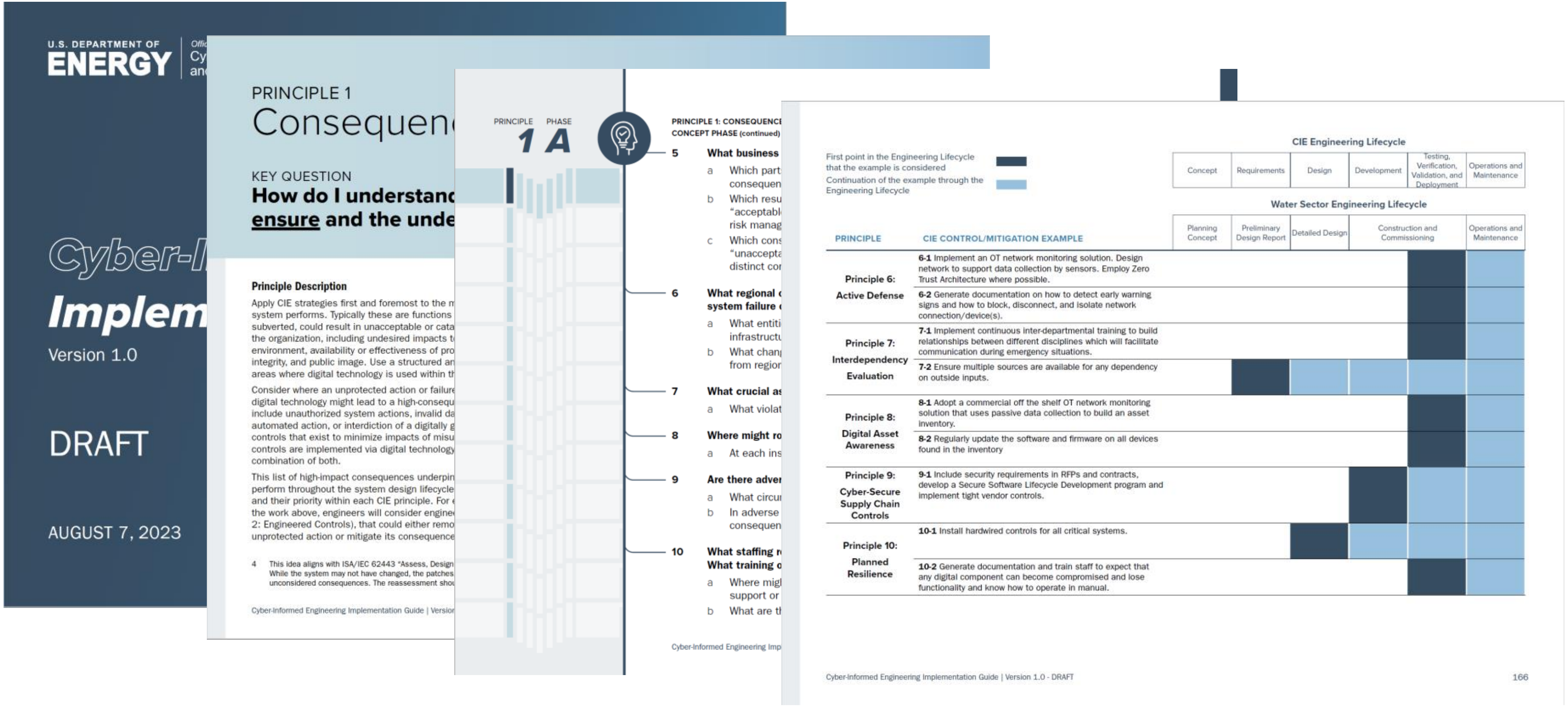
1. Do project processes allow for continual reassessment of consequence paths as mitigations and redesigns are performed?
2. How can downstream implications from changes to mitigate undesired consequences be avoided?

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?

CIE Implementation Guide

https://www.osti.gov/servlets/purl/1995796



CIE COP and Working Group Purpose

Cyber-Informed Engineering COP

Quarterly

11 AM ET on the 2nd Wednesday of January, April, July, and October

Multi-stakeholder team to aid the translation of CIE into technical requirements that can inform guidance, practices, and standards development

CIE Standards WG

Monthly

1st Wednesday, 9 AM MT / 11 AM ET

Support integration of CIE into engineering and cybersecurity standards

CIE Education WG

Monthly

3rd Wednesday, 9 AM MT / 11 AM ET

Develop curricula and materials that integrate CIE principles into engineering degree programs

CIE Implementation WG

Monthly

4th Wednesday, 9 AM MT / 11 AM ET

Develop CIE implementation guidance and an open-source library of resources

Current Activities

Working with Standards Bodies

- IEEE PES, and others
- ISA99 – 62443

Working with Universities

- Developing curriculum guidance
- Incorporating CIE into engineering education

Working with Asset Owners

- Incorporate CIE into ongoing efforts
- Templates for cyber-informed designs
- Coming Soon: CIE module within CSET, Microgrid Analysis Workflow, CIE for OT in the Cloud

CIE Resources

Websites

- DOE CESER CIE Website – https://www.energy.gov/ceser/cyber-informed-engineering
- INL CIE Website - https://inl.gov/cie/
- NREL CIE Website - https://www.nrel.gov/security-resilience/cyber-informed-engineering.html

Publications

- CIE Implementation Guide: https://www.osti.gov/biblio/1995796
- CIE Workbook for ADMS: https://www.osti.gov/biblio/1986517
- CIE Workbook for MicrOgrids: https://www.osti.gov/biblio/2315001
- CIE Workbook for Water Systems: https://www.osti.gov/biblio/2371031

Articles and Briefings

- SANS ICS Concepts Video: https://youtu.be/o_vlxW6UTeg
- Industrial Cyber: CIE and CCE Methodologies Can Deliver Engineered Industrial Systems for Holistic System Cybersecurity (June 11, 2023) with interviews from INL, 1898, and West Yost
- Harvard Business Review: Engineering Cybersecurity into U.S. Critical Infrastructure (April 17, 2023) by Ginger Wright, Andrew Ohrt, and Andy Bochman
- Shift Left video podcast on GrammaTech blog: Shifting Left for Energy Security (April 4, 2023) with Ginger Wright, Idaho National Lab and Marc Sachs, Auburn University
- For more CIE articles and publications, visit: inl.gov/cie

incose.org

Thank You!

CIE@inl.gov

https://www.energy.gov/ceser/cyber-informed-engineering

Q&A Session

Please submit your questions in the Zoom's Q&A feature.

Quick Reminders

- All the previous webinars are now located in the [Professional Development Portal (PDP).]()
- Attending a Webinar does count as 1 PDU credit towards your SEP renewal

Thank you to our 2024 Webinar Sponsors!

DASSAULT SYSTEMES

Platinum Partner

SPEC INNOVATIONS

Corporate Sponsor

INCOSE.org