INL/CON-24-78119-Revision-0

CIE Basic Presentation - University Days

May 2024

Virginia L Wright

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-24-78119-Revision-0

CIE Basic Presentation - University Days

Virginia L Wright

May 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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

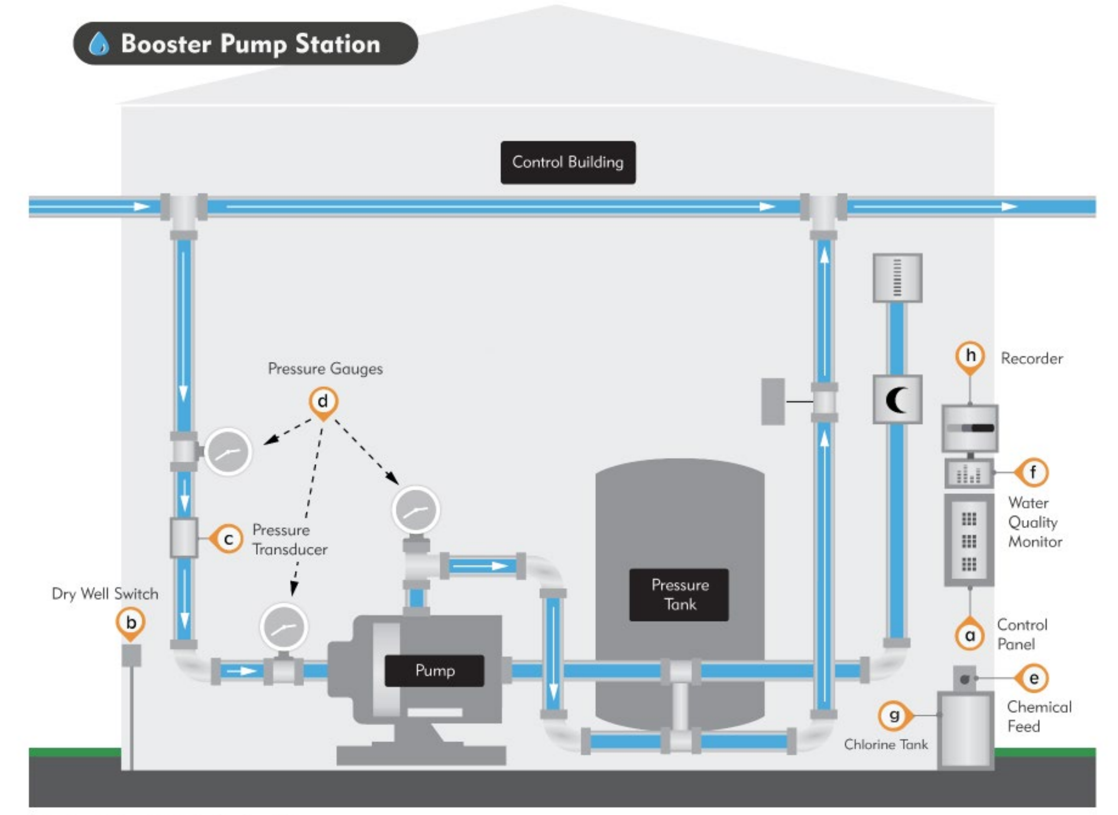
Cyber-Informed Engineering

Cyber-Informed Engineering

What is Cyber-Informed Engineering?

Water Booster Pump Station

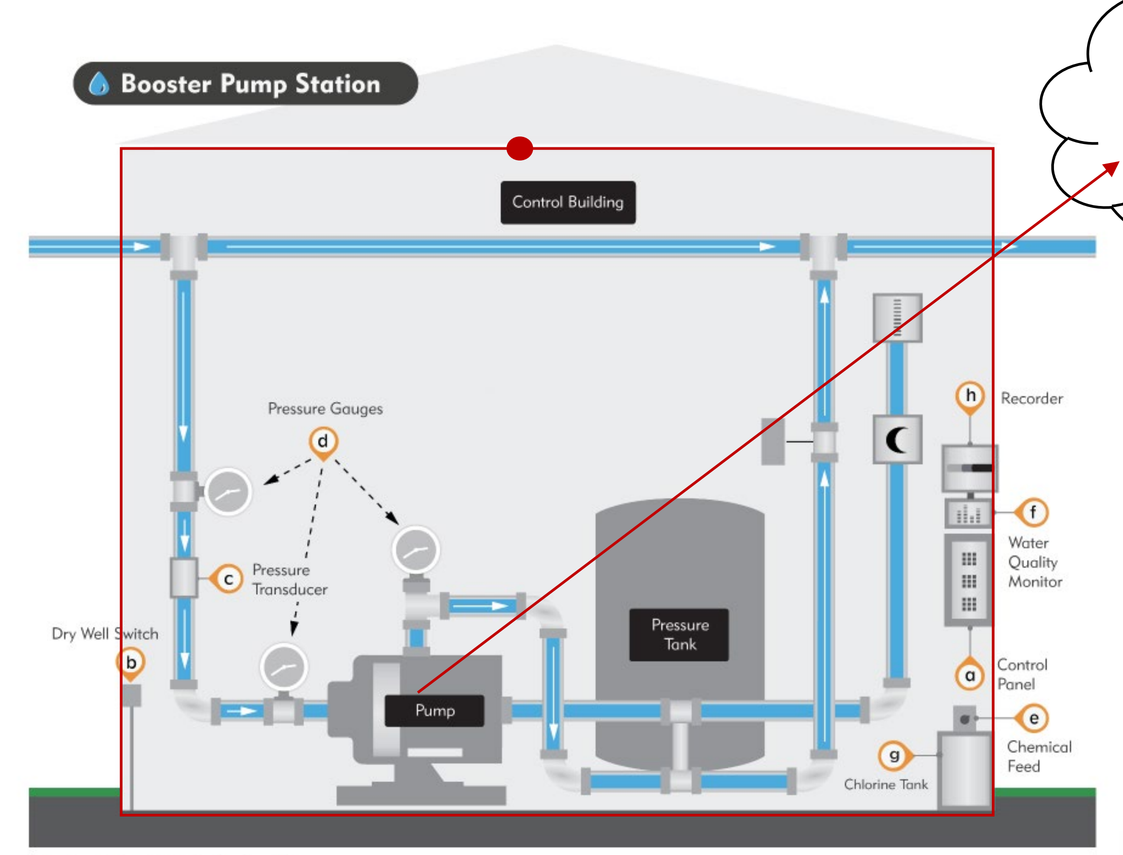
Water Booster Pump Station



Water Booster Pump Station Archives App4Water

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

Water Booster Pump Station

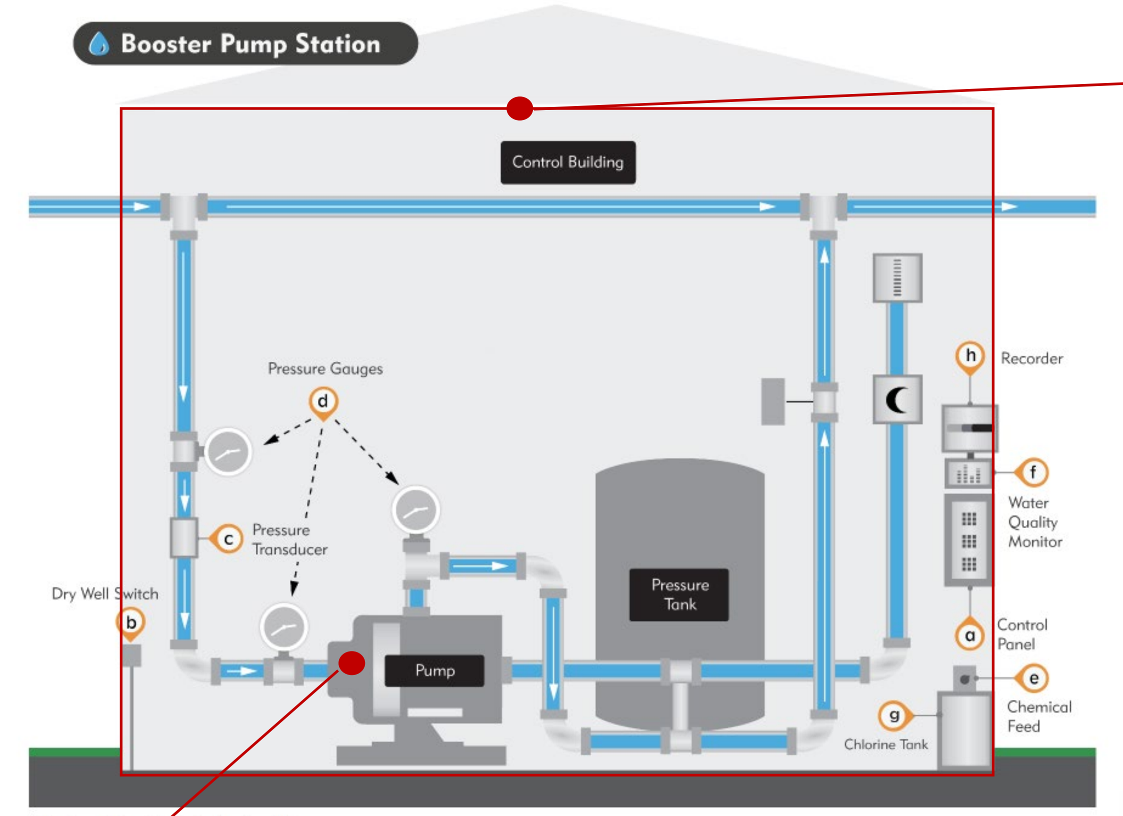


Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

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

Water Booster Pump Station



Water Booster Pump Station Archives App4Water

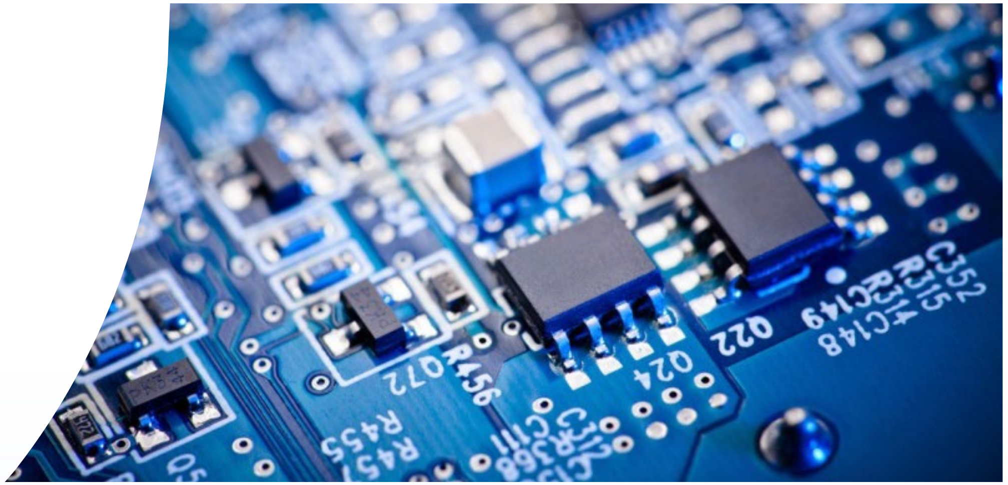
https://bmxlovesk.xyz/product_details/13200675.html

Cloud-based monitoring and control

Mechanical Time Delay Relay

Cyber-Informed Engineering (CIE)

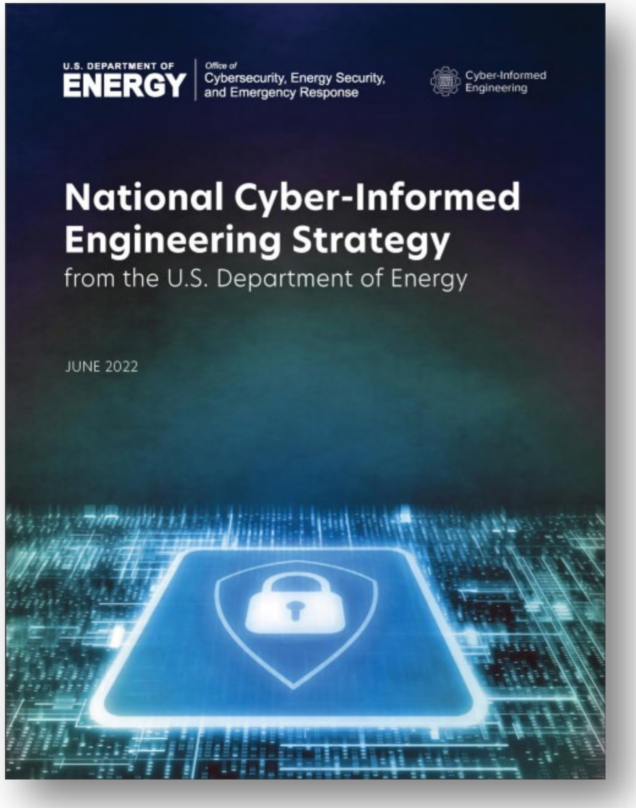
- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after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



How is it being applied?

National CIE Strategy

- Directed by the U.S. Congress in the Fiscal Year 2020 National Defense Authorization Act
- Outlines core CIE concepts
  - Defined by a set of design, operational, and organizational principles
  - Placed cybersecurity considerations at the foundation of control systems design and engineering
- Five integrated pillars offer recommendations to incorporate CIE as a common practice for control systems engineers
  - Intended to drive action across the industrial base stakeholders—government, owners and operators, manufacturers, researchers, academia, and training and standards organizations
- DOE issued the National CIE Strategy June 15, 2022
- CIE has been named in the National Cyber Strategy and the National Cyber Strategy Implementation Plan and in the report on cyber-physical systems by the President's Council of Advisors on Science and Technology



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

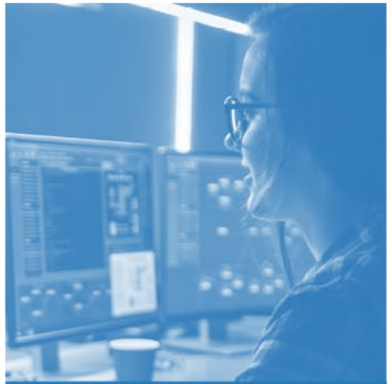
JUNE 2022

https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

Pillars of the National CIE Strategy

Awareness

Promulgate a universal and shared understanding of CIE



Education

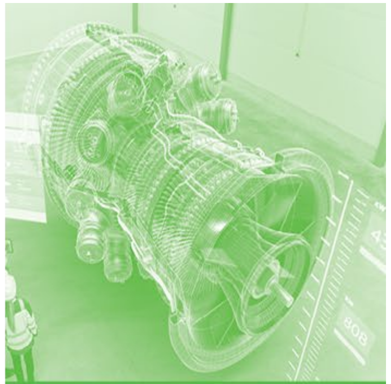
Embed CIE into formal education, training, and credentialing

Development

Build the body of knowledge by which CIE is applied to specific implementations

Current Infrastructure

Apply CIE principles to existing systemically important critical infrastructure



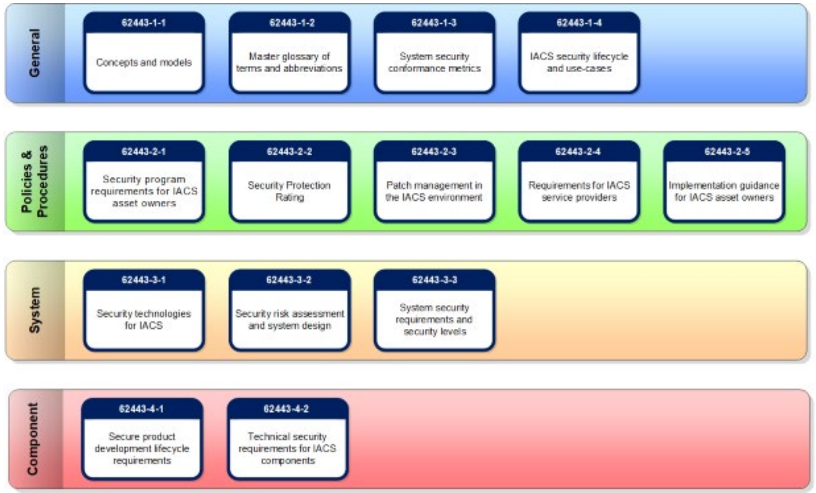
Future Infrastructure

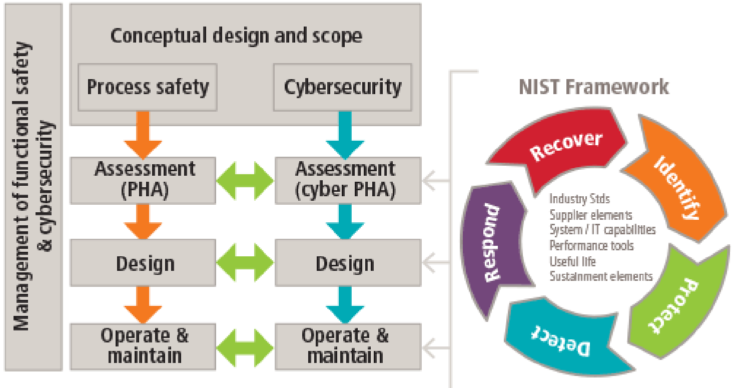
Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology

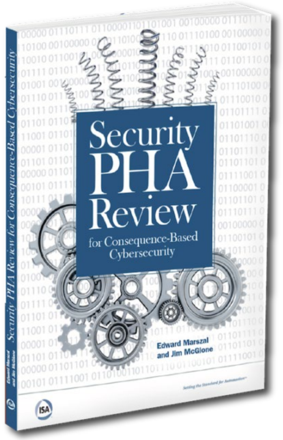
CIE Principles

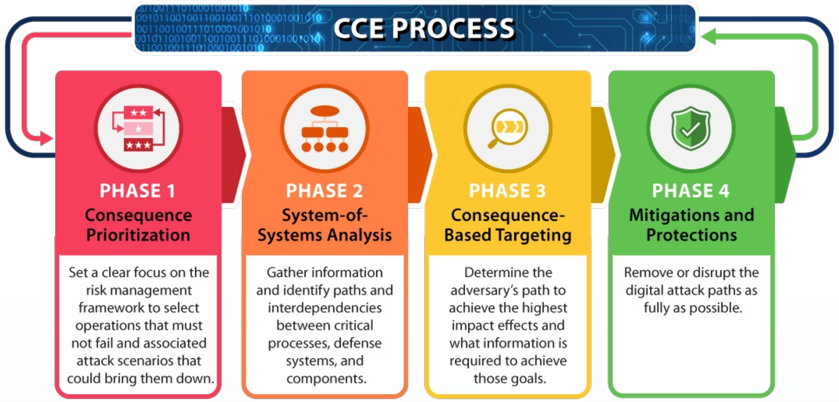
Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	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?

OK, But How Do You CIE?


General
62443-1-1
Concepts and models
62443-1-2
Master glossary of terms and abbreviations
62443-1-3
System security conformance metrics
62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
62443-2-1
Security program requirements for IACS asset owners
62443-2-2
Security Protection Rating
62443-2-3
Patch management in the IACS environment
62443-2-4
Requirements for IACS service providers
62443-2-5
Implementation guidance for IACS asset owners
System
62443-3-1
Security technologies for IACS
62443-3-2
Security risk assessment and system design
62443-3-3
System security requirements and security levels
Component
62443-4-1
Secure product development lifecycle requirements
62443-4-2
Technical security requirements for IACS components




Security PHA Review
for Consequence-Based Cybersecurity
Edward Marszal and Jim McGlone
ISA



PHASE 1
Consequence Prioritization

Set a clear focus on the risk management framework to select operations that must not fail and associated attack scenarios that could bring them down.

PHASE 2
System-of-Systems Analysis

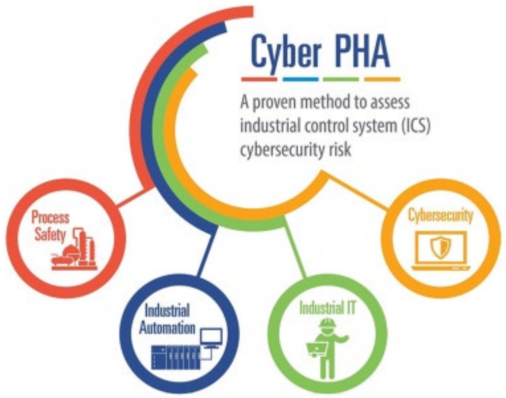
Gather information and identify paths and interdependencies between critical processes, defense systems, and components.

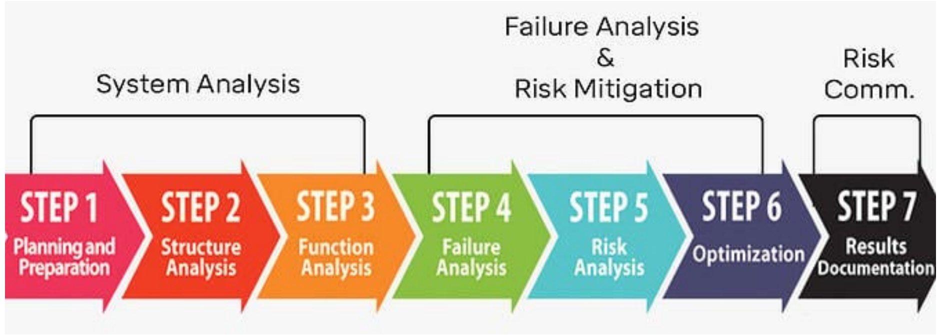
PHASE 3
Consequence-Based Targeting

Determine the adversary's path to achieve the highest impact effects and what information is required to achieve those goals.

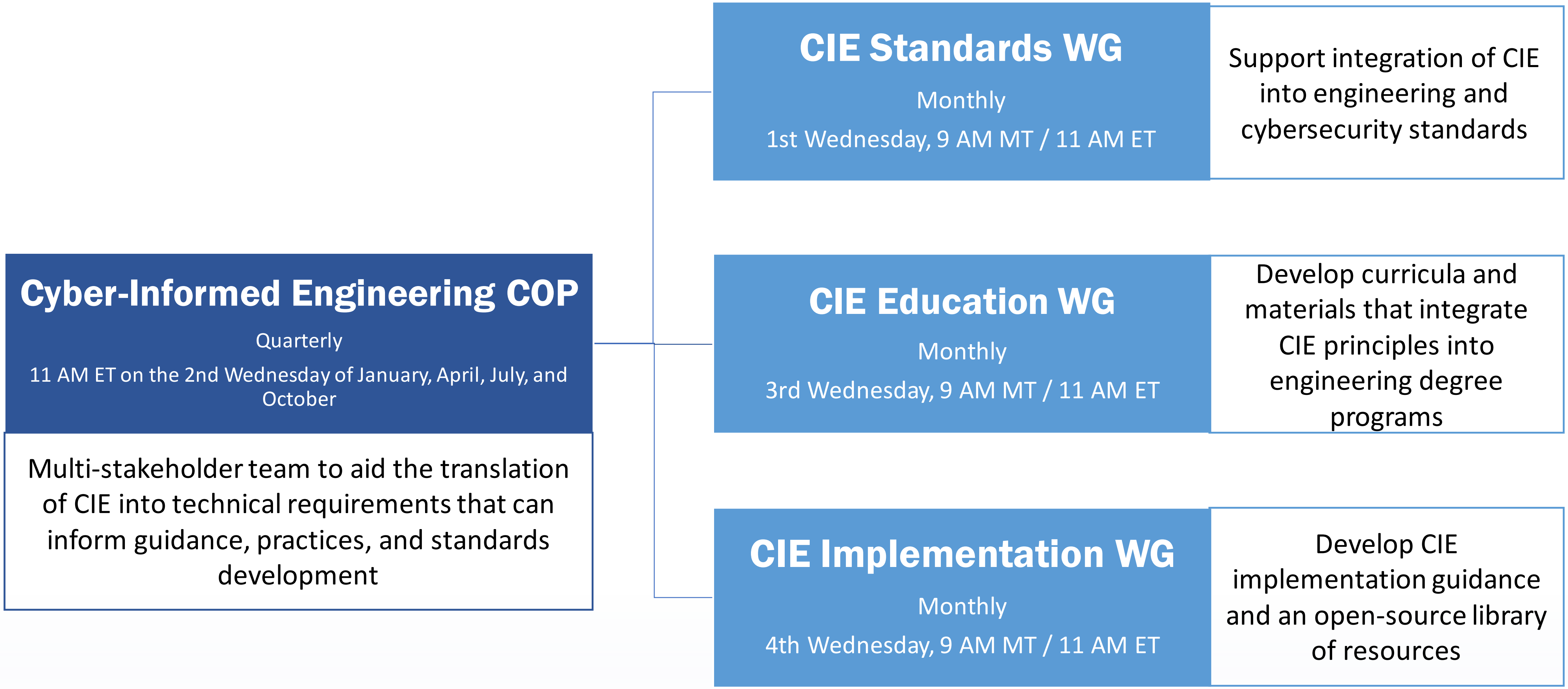
PHASE 4
Mitigations and Protections

Remove or disrupt the digital attack paths as fully as possible.


Cyber PHA
A proven method to assess industrial control system (ICS) cybersecurity risk
Process Safety
Industrial Automation
Industrial IT
Cybersecurity


System Analysis
Failure Analysis & Risk Mitigation
Risk Comm.
STEP 1 Planning and Preparation
STEP 2 Structure Analysis
STEP 3 Function Analysis
STEP 4 Failure Analysis
STEP 5 Risk Analysis
STEP 6 Optimization
STEP 7 Results Documentation

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

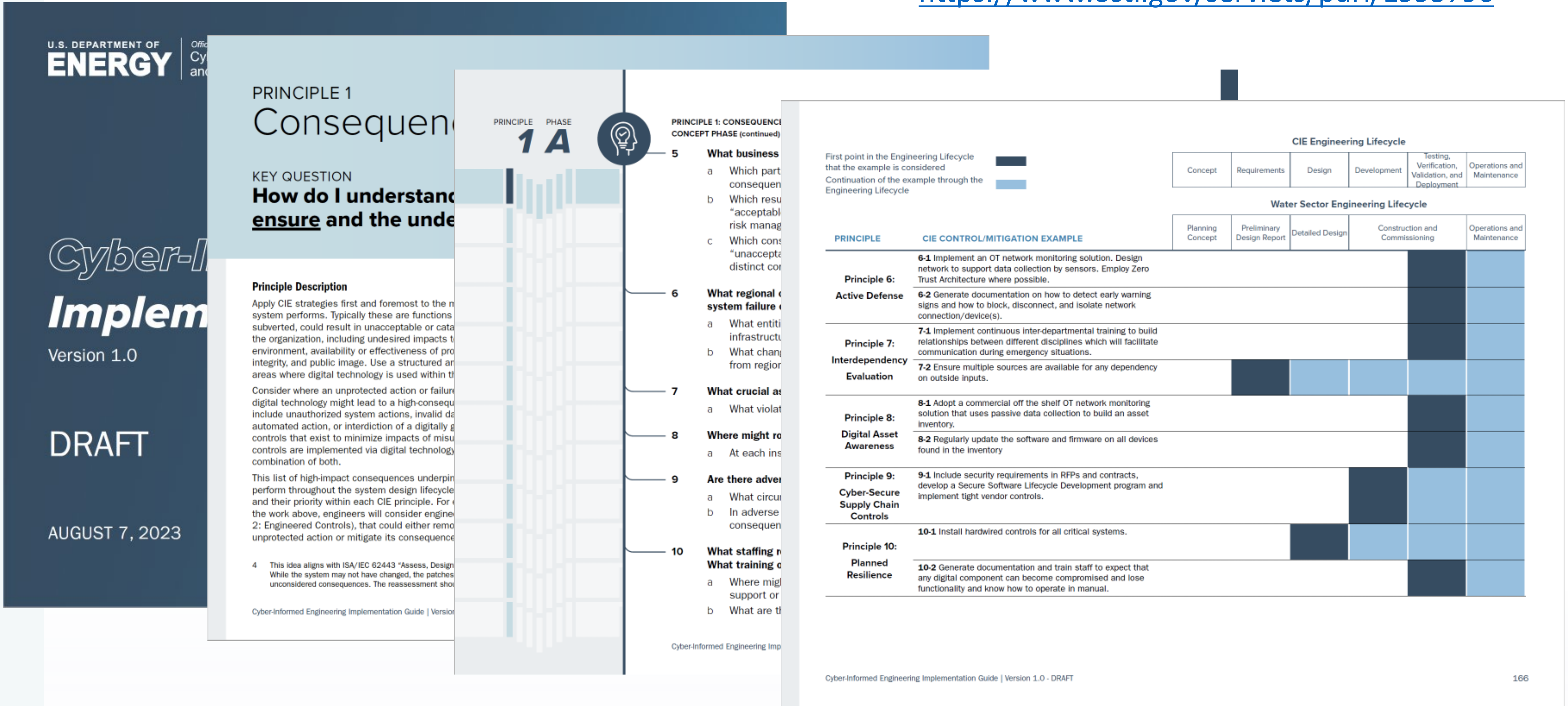
Monthly

4th Wednesday, 9 AM MT / 11 AM ET

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

CIE Implementation Guide

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



U.S. DEPARTMENT OF ENERGY | Offi Cy an

Cyber-I

Implem

Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1

Consequen

KEY QUESTION

How do I understan
ensure and the unde

Principle Description

Apply CIE strategies first and foremost to the m
system performs. Typically these are functions
subverted, could result in unacceptable or cata
the organization, including undesired impacts t
environment, availability or effectiveness of pro
integrity, and public image. Use a structured ar
areas where digital technology is used within th

Consider where an unprotected action or failure
digital technology might lead to a high-consequ
include unauthorized system actions, invalid da
automated action, or interdiction of a digitally g
controls that exist to minimize impacts of misu
controls are implemented via digital technology
combination of both.

This list of high-impact consequences underpin
perform throughout the system design lifecycle
and their priority within each CIE principle. For
the work above, engineers will consider engine
2: Engineered Controls), that could either remo
unprotected action or mitigate its consequence

4 This idea aligns with ISA/IEC 62443 "Assess, Design
While the system may not have changed, the patches
unconsidered consequences. The reassessment sho

Cyber-Informed Engineering Implementation Guide | Versio

PRINCIPLE PHASE
1 A

PRINCIPLE 1: CONSEQUENC
CONCEPT PHASE (continued)

5 **What business**
a Which part
consequen
b Which resu
"acceptabl
risk manag
c Which cons
"unaccepta
distinct cor

6 **What regional**
system failure
a What entiti
infrastructu
b What chang
from region

7 **What crucial a**
a What violat

8 **Where might ro**
a At each ins

9 **Are there adver**
a What circu
b In adverse
consequen

10 **What staffing r**
What training
a Where mig
support or
b What are th

Cyber-Informed Engineering Imp

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 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.					■	▨

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT 166

Cyber-Informed Engineering

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
- Refine products
- Templates for cyber-informed designs

Recent CIE Publications

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:** Cyber-Informed Engineering Implementation Guide (Program Document) | OSTI.GOV
- **CIE Workbook (Distribution, ADMS):** https://www.osti.gov/biblio/1986517
- **CIE Workbook (Microgrids):** https://www.osti.gov/biblio/2315001

Articles and Briefings

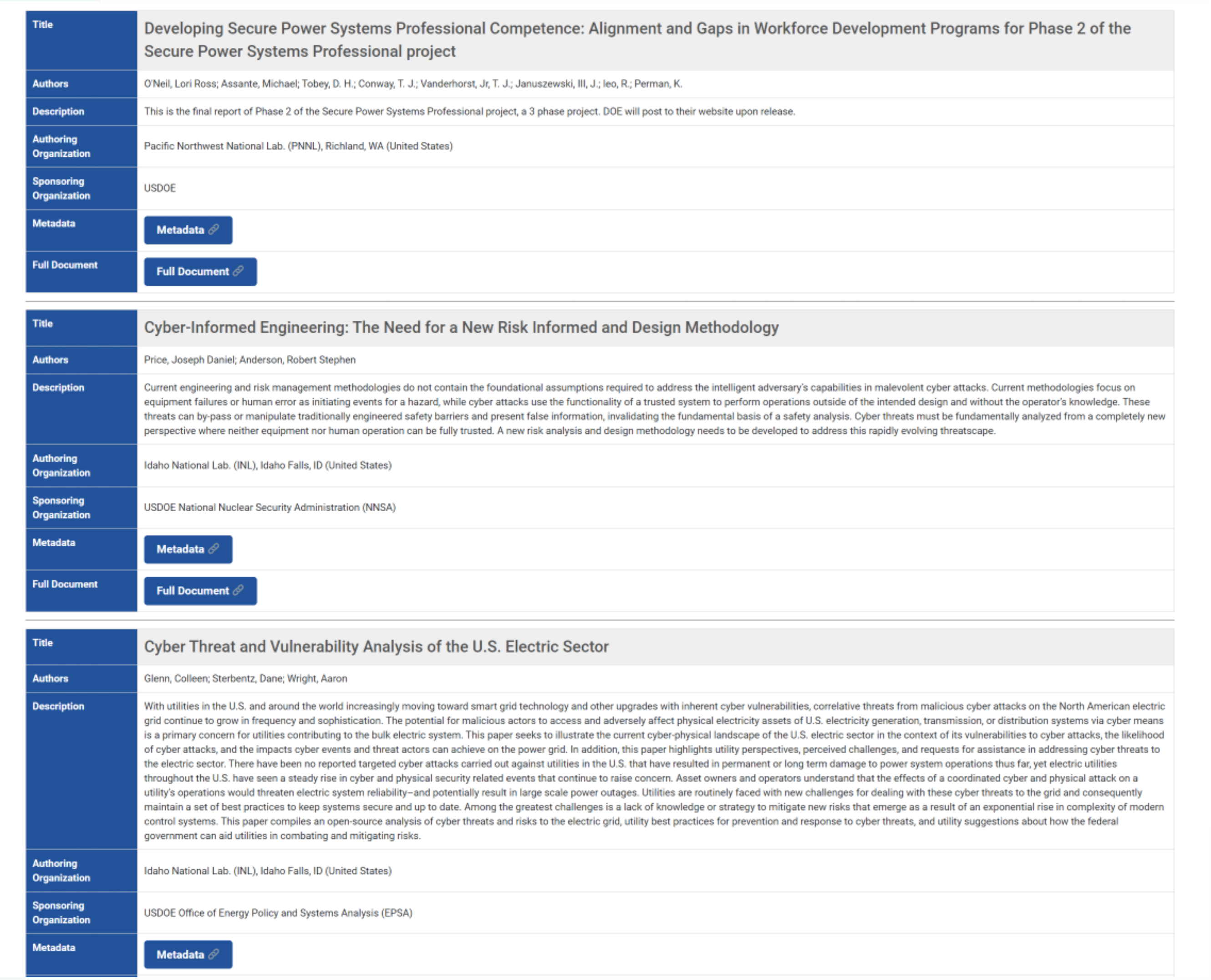
- **SANS ICS Concepts Video:** https://youtu.be/o_vlxW6UTeg
- **Industrial Cyber**: CIE and CCE Methodologies Can Deliver Engineered Industrial Systems for Holistic System Cybersecurity (June 11, 2023) with interviews from INL, 1898, and West Yost
- **Harvard Business Review:** Engineering Cybersecurity 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

Thank You!

CIE@inl.gov

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

CIE Open-Source Library



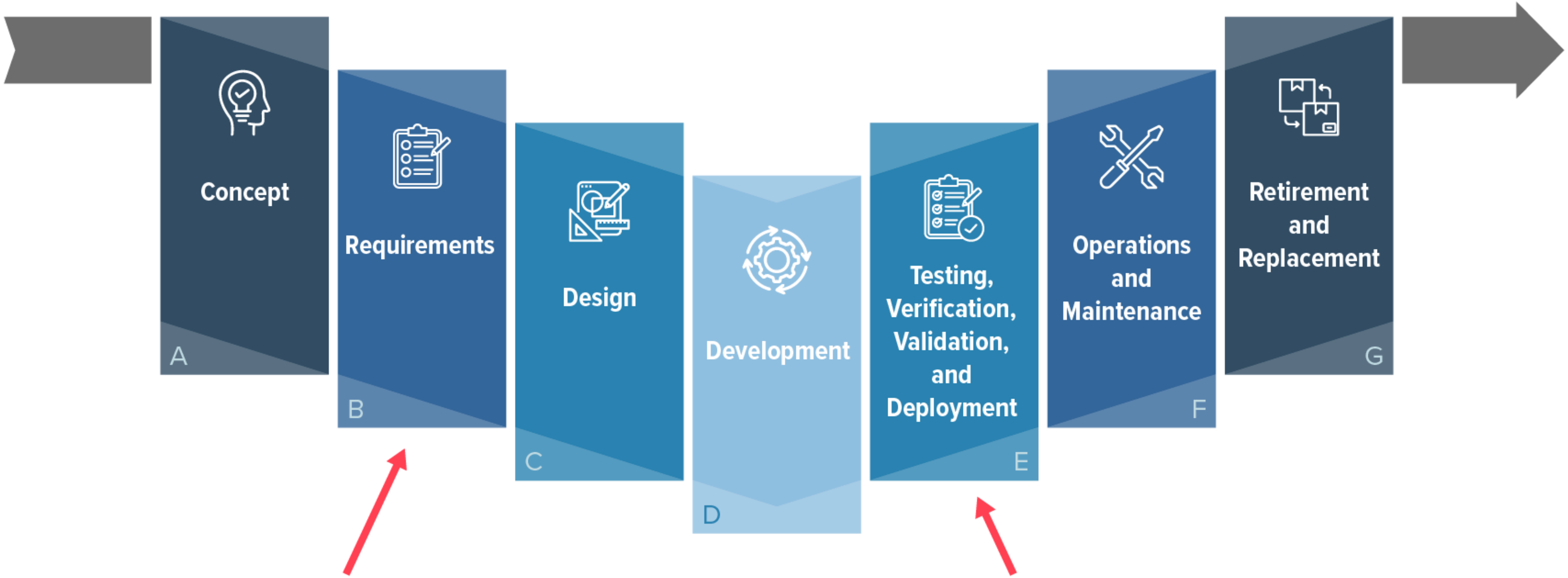
Title	Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs for Phase 2 of the Secure Power Systems Professional project
Authors	O'Neil, Lori Ross; Assante, Michael; Tobey, D. H.; Conway, T. J.; Vanderhorst, Jr, T. J.; Januszewski, III, J.; Ieo, R.; Perman, K.
Description	This is the final report of Phase 2 of the Secure Power Systems Professional project, a 3 phase project. DOE will post to their website upon release.
Authoring Organization	Pacific Northwest National Lab. (PNNL), Richland, WA (United States)
Sponsoring Organization	USDOE
Metadata	Metadata
Full Document	Full Document

Title	Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology
Authors	Price, Joseph Daniel; Anderson, Robert Stephen
Description	Current engineering and risk management methodologies do not contain the foundational assumptions required to address the intelligent adversary's capabilities in malevolent cyber attacks. Current methodologies focus on equipment failures or human error as initiating events for a hazard, while cyber attacks use the functionality of a trusted system to perform operations outside of the intended design and without the operator's knowledge. These threats can by-pass or manipulate traditionally engineered safety barriers and present false information, invalidating the fundamental basis of a safety analysis. Cyber threats must be fundamentally analyzed from a completely new perspective where neither equipment nor human operation can be fully trusted. A new risk analysis and design methodology needs to be developed to address this rapidly evolving threatscape.
Authoring Organization	Idaho National Lab. (INL), Idaho Falls, ID (United States)
Sponsoring Organization	USDOE National Nuclear Security Administration (NNSA)
Metadata	Metadata
Full Document	Full Document

Title	Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector
Authors	Glenn, Colleen; Sterbentz, Dane; Wright, Aaron
Description	With utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyber attacks on the North American electric grid continue to grow in frequency and sophistication. The potential for malicious actors to access and adversely affect physical electricity assets of U.S. electricity generation, transmission, or distribution systems via cyber means is a primary concern for utilities contributing to the bulk electric system. This paper seeks to illustrate the current cyber-physical landscape of the U.S. electric sector in the context of its vulnerabilities to cyber attacks, the likelihood of cyber attacks, and the impacts cyber events and threat actors can achieve on the power grid. In addition, this paper highlights utility perspectives, perceived challenges, and requests for assistance in addressing cyber threats to the electric sector. There have been no reported targeted cyber attacks carried out against utilities in the U.S. that have resulted in permanent or long term damage to power system operations thus far, yet electric utilities throughout the U.S. have seen a steady rise in cyber and physical security related events that continue to raise concern. Asset owners and operators understand that the effects of a coordinated cyber and physical attack on a utility's operations would threaten electric system reliability–and potentially result in large scale power outages. Utilities are routinely faced with new challenges for dealing with these cyber threats to the grid and consequently maintain a set of best practices to keep systems secure and up to date. Among the greatest challenges is a lack of knowledge or strategy to mitigate new risks that emerge as a result of an exponential rise in complexity of modern control systems. This paper compiles an open-source analysis of cyber threats and risks to the electric grid, utility best practices for prevention and response to cyber threats, and utility suggestions about how the federal government can aid utilities in combating and mitigating risks.
Authoring Organization	Idaho National Lab. (INL), Idaho Falls, ID (United States)
Sponsoring Organization	USDOE Office of Energy Policy and Systems Analysis (EPSA)
Metadata	Metadata

- Find at: https://inl.gov/cie-resource-library/
- DOE-sponsored research on Cyber-Informed Engineering as far back as 2013
- Multiple laboratories
- Multiple Application Areas

CIE and the Systems Engineering Lifecycle


Concept
A
Requirements
B
Design
C
Development
D
Testing, Verification, Validation, and Deployment
E
Operations and Maintenance
F
Retirement and Replacement
G

OT Cybersecurity risk mitigations are usually applied here…

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