USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

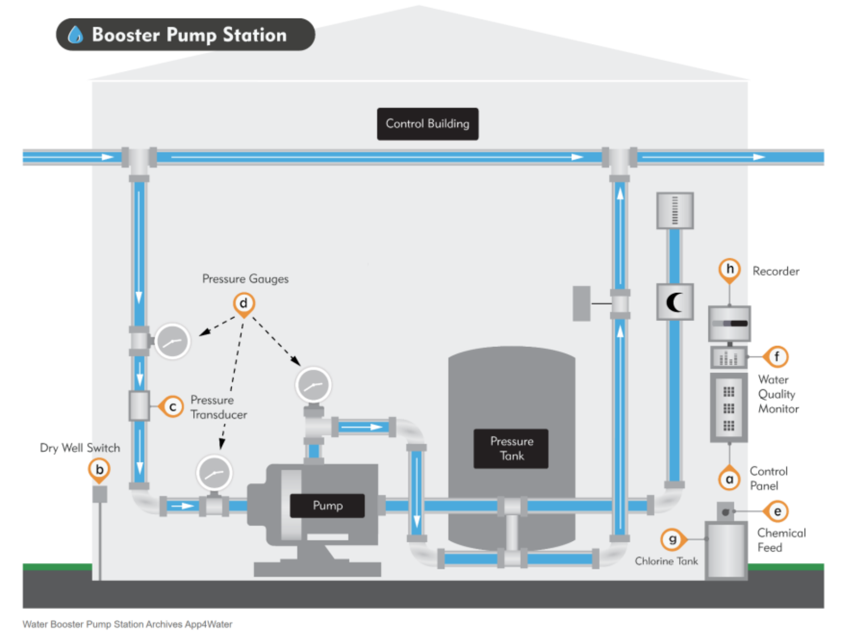
Cyber-Informed Engineering

Cybersecurity and Digitalization:
Supply Chain Risks in the Electricity Sector

What is Cyber-Informed Engineering?

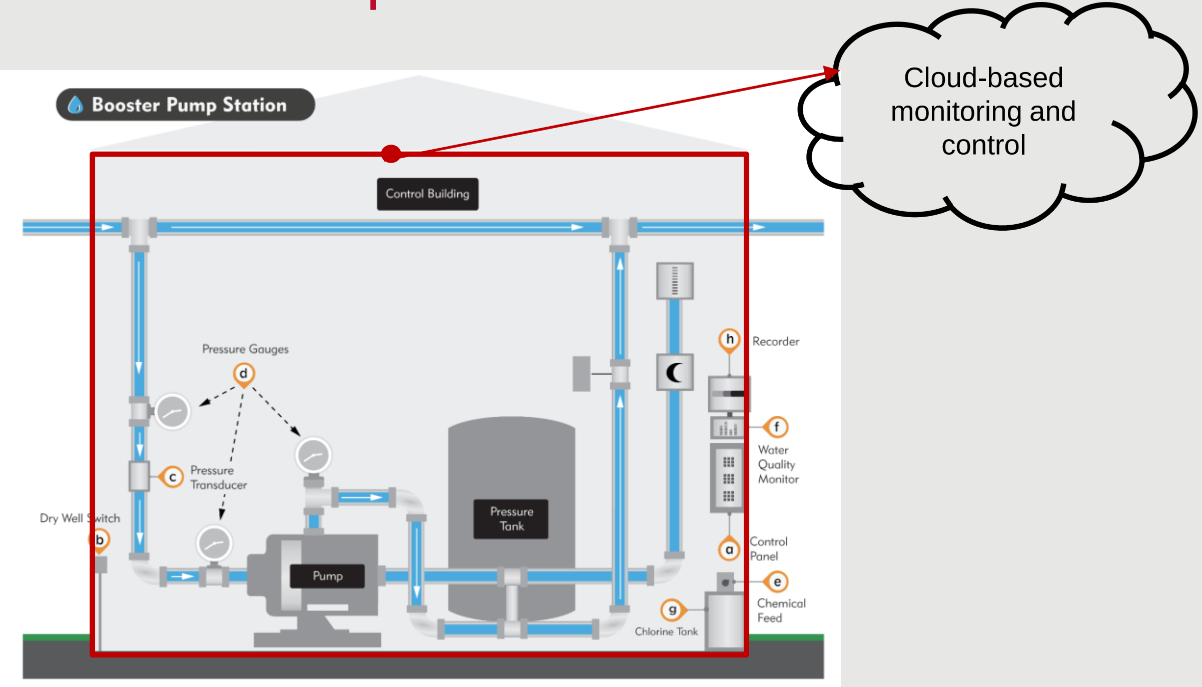
Water Booster Pump Station

Water Booster Pump Station



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

Water Booster Pump Station



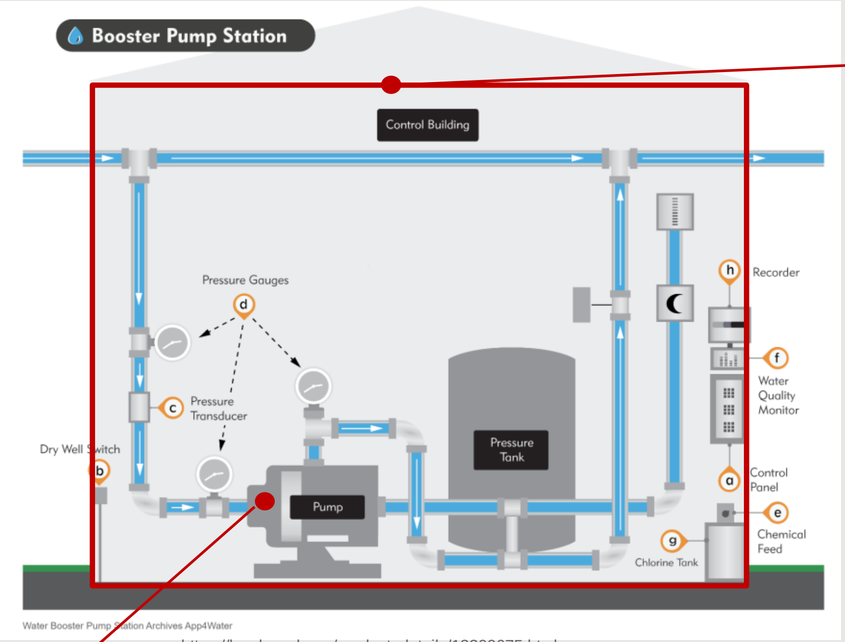
Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

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

Water Booster Pump Station

Cloud-based monitoring and control



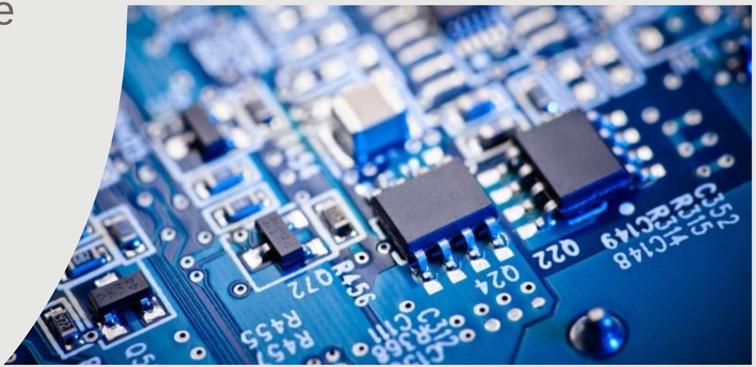
Water Booster Pump Station Archives App4Water

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 align the **culture of security** with the existing industry safety culture.



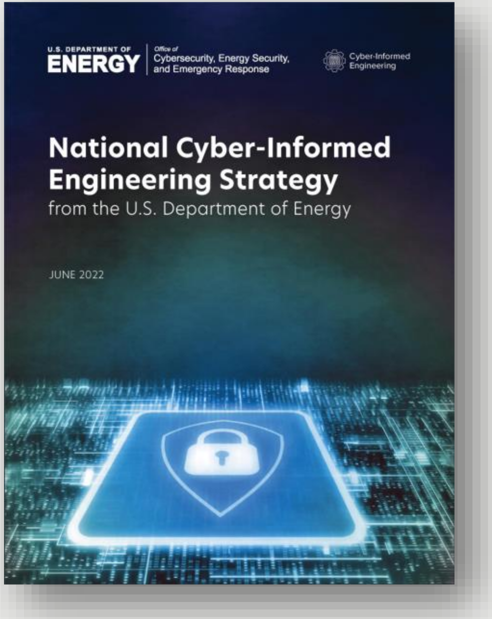
USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

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

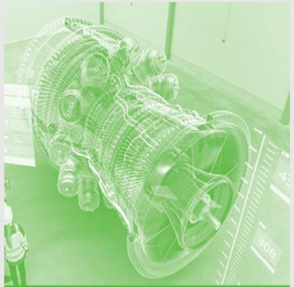
National Cyber-Informed Engineering Strategy

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

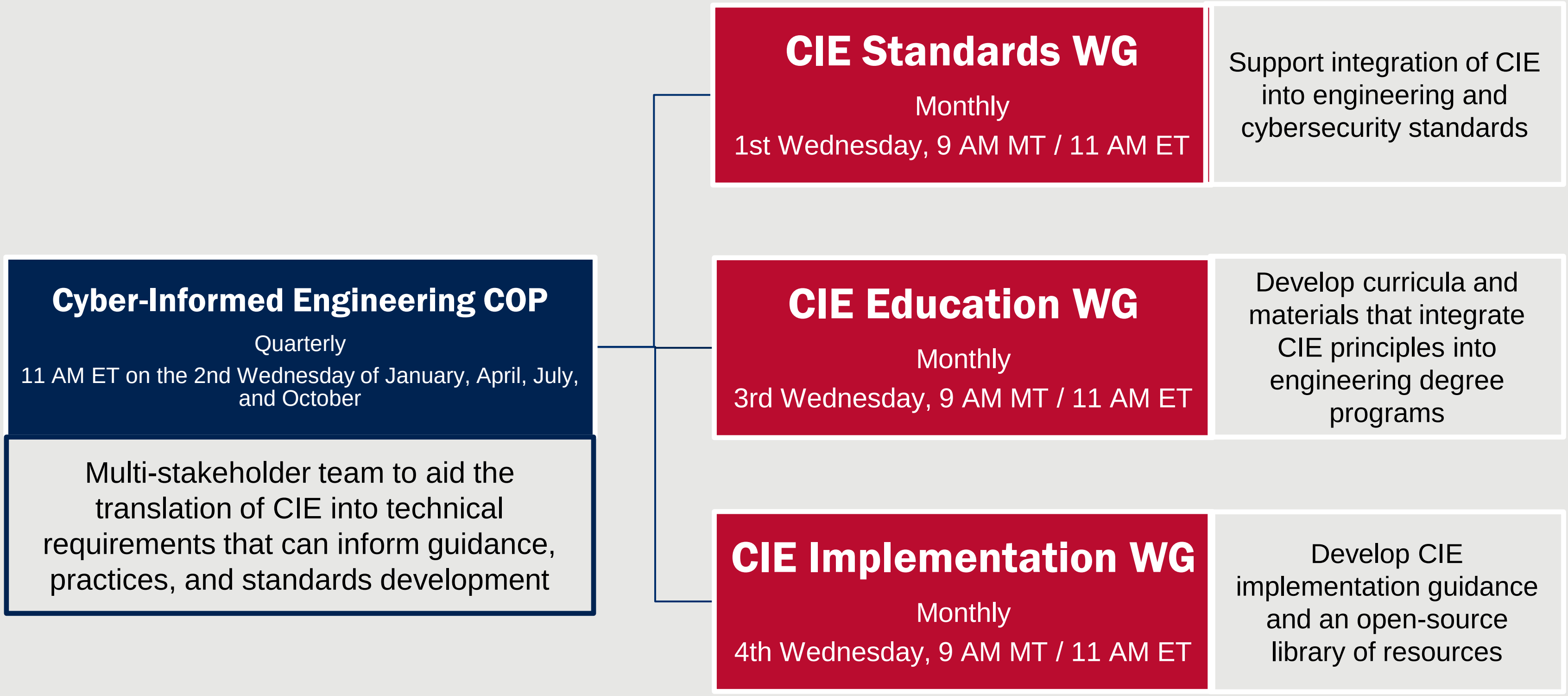


Awareness	Education	Development	Current Infrastructure	Future Infrastructure
Promulgate a universal and shared understanding of CIE	Embed CIE into formal education, training, and credentialing	Build the body of knowledge by which CIE is applied to specific implementations	Apply CIE principles to existing systemically important critical 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?

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

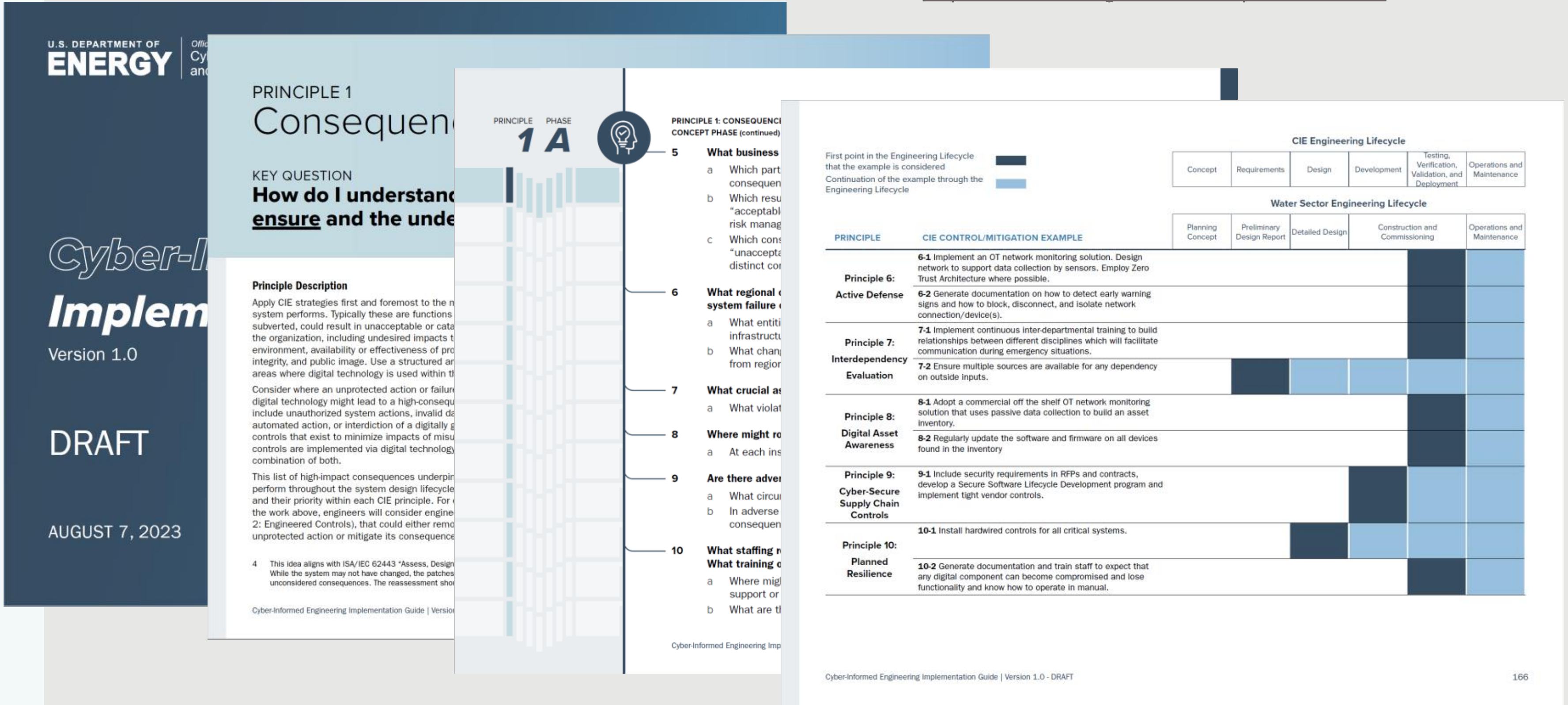
Monthly

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 understanc ensure and the unde

Principle Description

Apply CIE strategies first and foremost to the n 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 tl

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 shou

Cyber-Informed Engineering Implementation Guide | Versio

PRINCIPLE 1 A PHASE 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 chan from regior

7 **What crucial as**
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 c**
a Where mig support or
b What are tl

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

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_vIxW6UTeg
- **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

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

Thank you!

To Join our Communities of Practice or ask questions about CIE, please email: CIE@INL.gov

Current Activities

Working with Standards Bodies

- IEEE PES, and others
- ISA99 – 62443

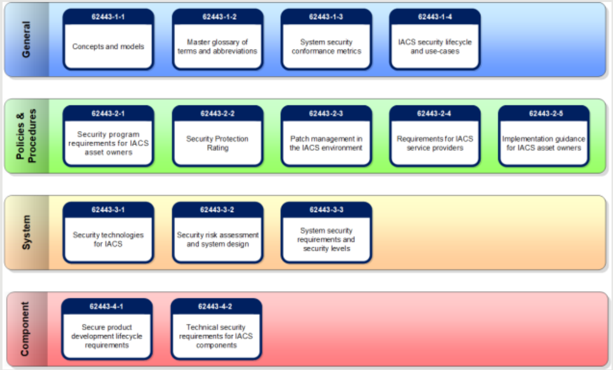
Working with Universities

- Developing curriculum guidance
- Incorporating CIE into engineering education

Working with Asset Owners

- Incorporate CIE into ongoing efforts
- Refine products
- Templates for cyber-informed designs

OK, But How Do You CIE?

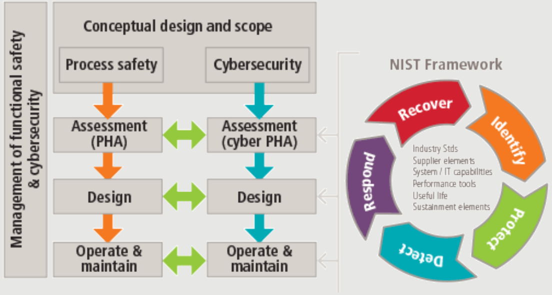


General
- 62443-1-1 Concepts and models
- 62443-1-2 Master glossary of terms and abbreviations
- 62443-1-3 System security conformance metrics
- 62443-1-4 IACS security lifecycle and use-cases

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



Management of functional safety & cybersecurity

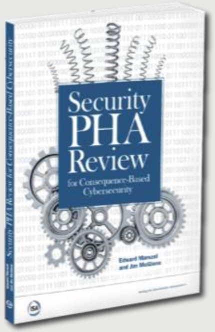
Conceptual design and scope

Process safety	Cybersecurity
Assessment (PHA)	Assessment (cyber PHA)
Design	Design
Operate & maintain	Operate & maintain

NIST Framework

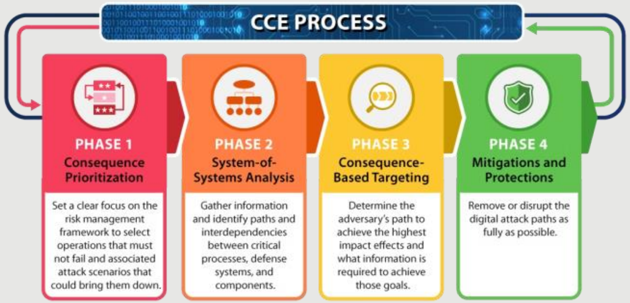
Recover · Identify · Protect · Detect · Respond

Industry Stds
Supplier elements
System / IT capabilities
Performance tools
Useful life
Sustainment elements



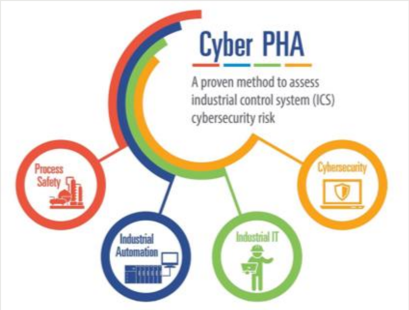
Security PHA Review for Consequence-Based Cybersecurity

Edward Marszal and Jim McGlone



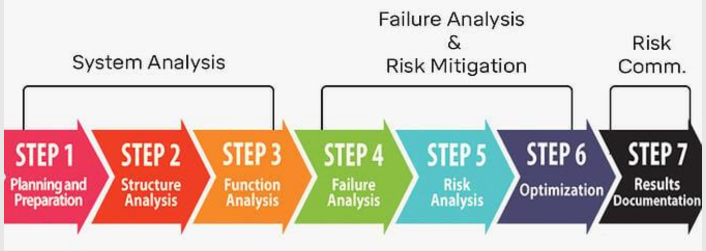
CCE PROCESS

PHASE 1 Consequence Prioritization	PHASE 2 System-of-Systems Analysis	PHASE 3 Consequence-Based Targeting	PHASE 4 Mitigations and Protections
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.	Gather information and identify paths and interdependencies between critical processes, defense systems, and components.	Determine the adversary's path to achieve the highest impact effects and what information is required to achieve those goals.	Remove or disrupt the digital attack paths as fully as possible.



Cyber PHA

A proven method to assess industrial control system (ICS) cybersecurity risk



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