



# Cyber-Enabled Sabotage, Critical Function Assurance, and Cyber-Informed Engineering

August 2024

*Changing the World's Energy Future*

Sam Chanoski



*INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC*

#### **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.

# **Cyber-Enabled Sabotage, Critical Function Assurance, and Cyber-Informed Engineering**

**Sam Chanoski**

**August 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-Enabled Sabotage, Critical Function Assurance, and Cyber-Informed Engineering

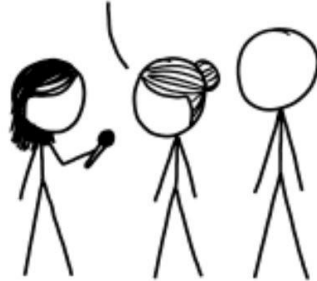


**Sam Chanoski**



ASKING AIRCRAFT DESIGNERS  
ABOUT AIRPLANE SAFETY:

NOTHING IS EVER FOOLPROOF,  
BUT MODERN AIRLINERS ARE  
INCREDIBLY RESILIENT. FLYING IS  
THE SAFEST WAY TO TRAVEL.



ASKING BUILDING ENGINEERS  
ABOUT ELEVATOR SAFETY:

ELEVATORS ARE PROTECTED BY  
MULTIPLE TRIED-AND-TESTED  
FAILSAFE MECHANISMS. THEY'RE  
NEARLY INCAPABLE OF FALLING.



ASKING SOFTWARE  
ENGINEERS ABOUT  
COMPUTERIZED VOTING:

THAT'S TERRIFYING.



WAIT, REALLY?

DON'T TRUST VOTING SOFTWARE AND DON'T  
LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.

WHY?

I DON'T QUITE KNOW HOW TO PUT THIS, BUT  
OUR ENTIRE FIELD IS BAD AT WHAT WE DO,  
AND IF YOU RELY ON US, EVERYONE WILL DIE.



THEY SAY THEY'VE FIXED IT WITH  
SOMETHING CALLED "BLOCKCHAIN."

AAAAA!!!

WHATEVER THEY SOLD  
YOU, DON'T TOUCH IT.  
BURY IT IN THE DESERT.

WEAR GLOVES.



<https://xkcd.com/2030/>



Cyber-Informed  
Engineering



*Centrifuges in an  
Iranian nuclear plant.  
Photo credit: Tasnim  
News Agency*



*Damaged Natanz  
enrichment facility  
Iran Atomic Energy  
Organization, via Agence  
France-Presse*



**Cyber-Informed  
Engineering**

# Background and Context

# The Realities of Cyberspace

## INL's technical doctrine is based on the following assumptions:

- **Existing security efforts are insufficient** to protect control systems and the infrastructure they support against catastrophic technical attacks.
- **A determined, well-resourced and patient adversary WILL succeed** in penetrating and exploiting a critical infrastructure network.

*Given time and resources, cyber attackers WILL have success*



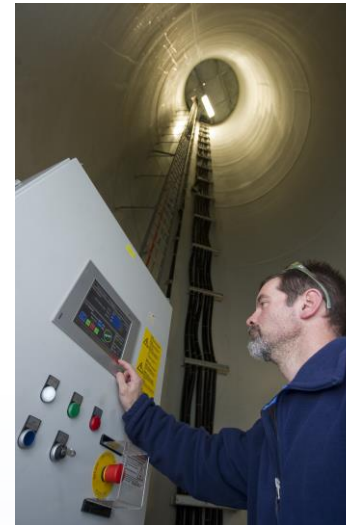
# Start with Why

- Consistent observation that **engineers and technical staff** are **not aware** of how cyber threats affect digital designs and operations
- Need to ensure that **inherent risks of digital technology** (which manifest through failure, error, malign disruption, or compromise) are considered and mitigated in the **earliest possible stages** of the design lifecycle



# Our Origin Story

- Conducted hundreds of **assessments** over more than a decade
- Saw **common themes** with outsized impact on security
- These shaped our **worldview** and most subsequent work
- First **codified** in the Consequence-driven, Cyber-informed Engineering (CCE) methodology



# Keeping the Acronyms Straight

- **Critical Function Assurance** – managing the risks inherent from using digital technology in a world with adversaries – is *the why*
- CIE is *the what*
  - Principles distilled from trends in years of work
- CCE is *a how*
  - Based on and developed by many of the same people as CIE
- There are *other how's!*



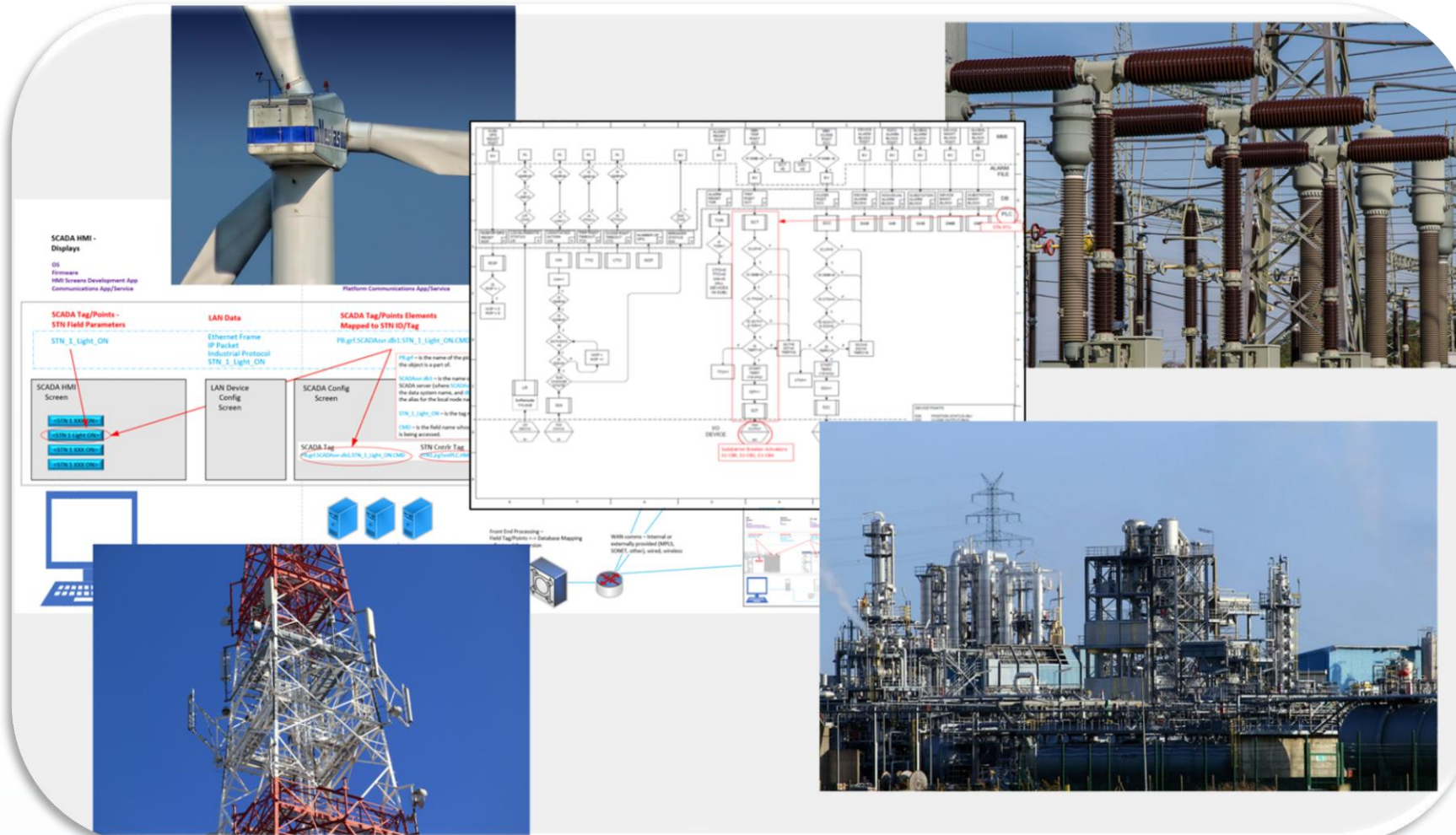
# Why? Critical Function Assurance!

# Critical Functions



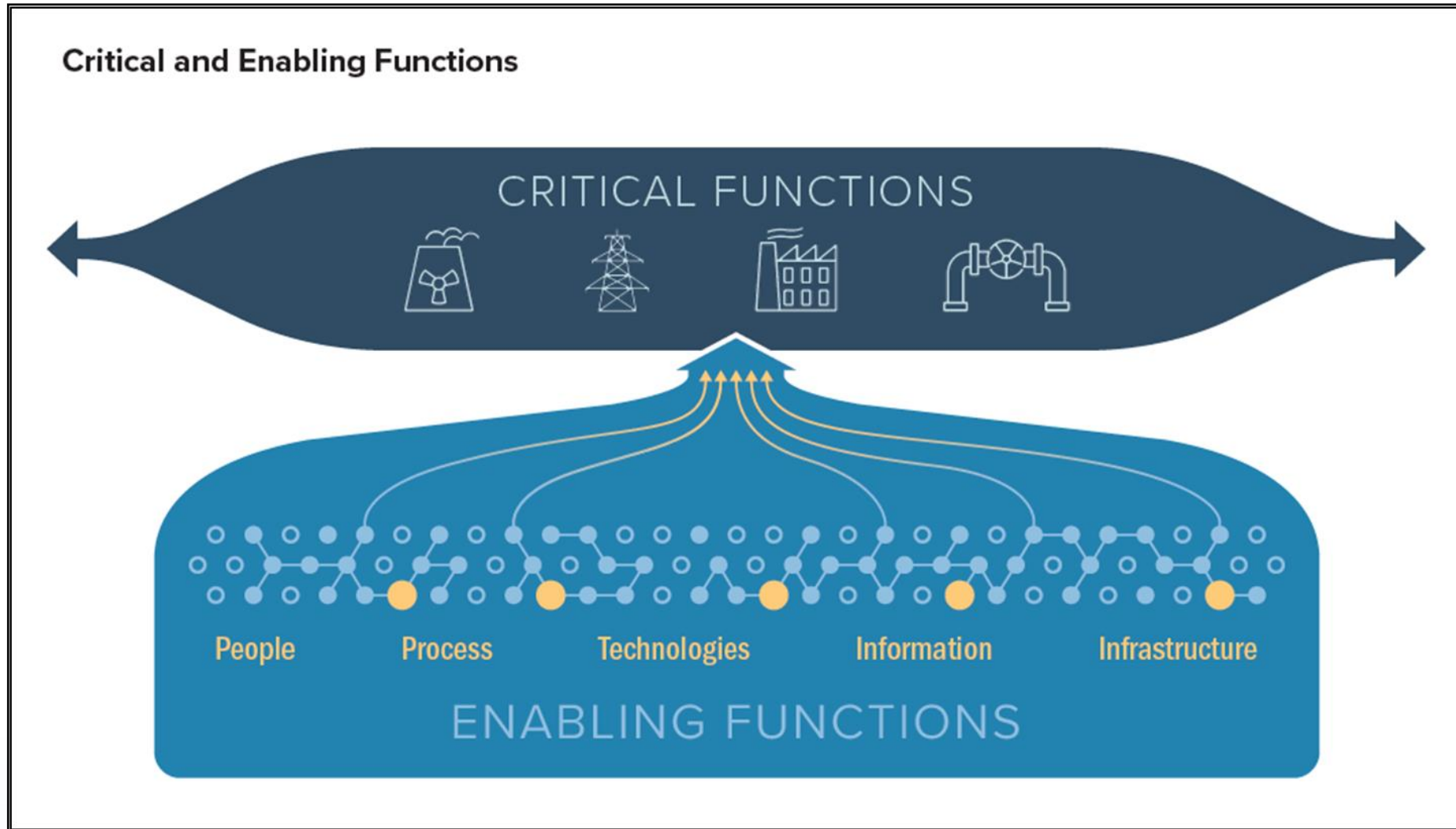
**Adversary – Targeting Critical Functions**

# An adversary exploits our Enabling Functions AND impacts our Critical Functions

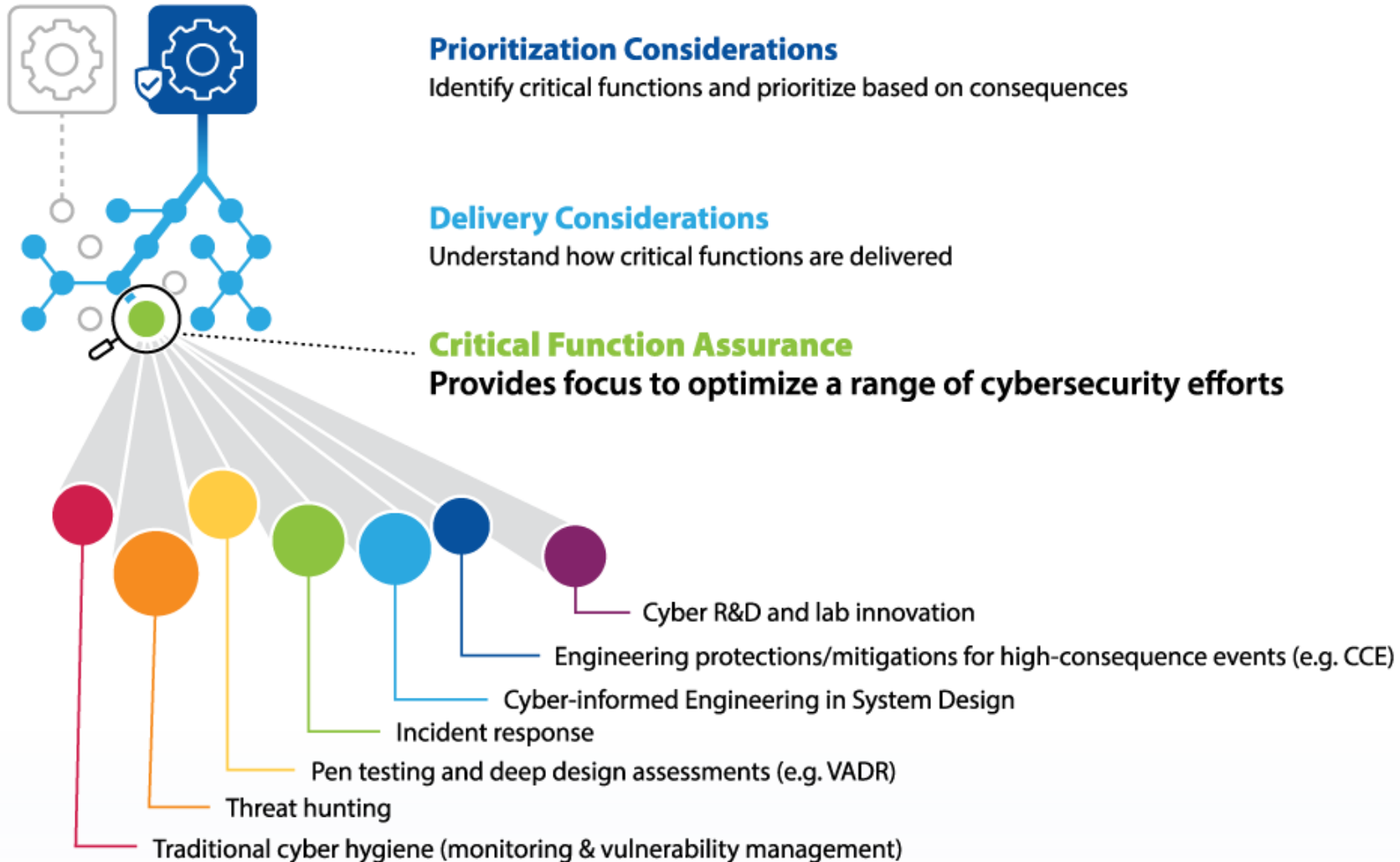


Exploiting how we deliver our critical functions.

# Enabling Functions are PPTII



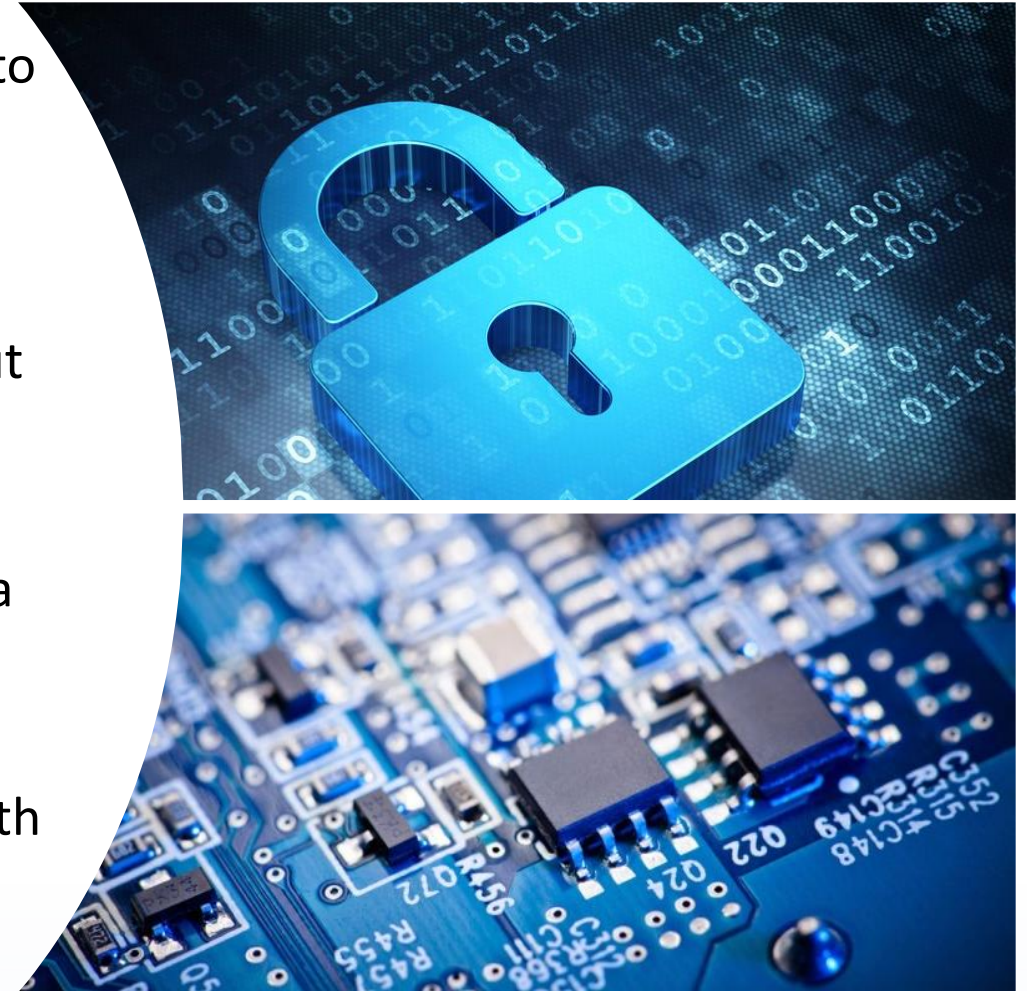
# Critical Function Assurance Guides Our Activities



What? What exactly is CIE?

# Cyber-Informed Engineering (CIE)

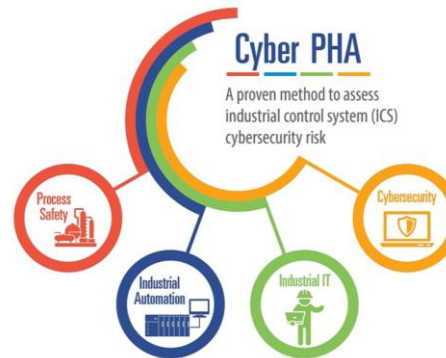
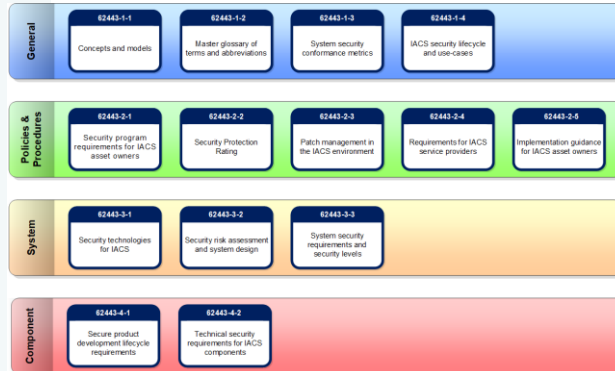
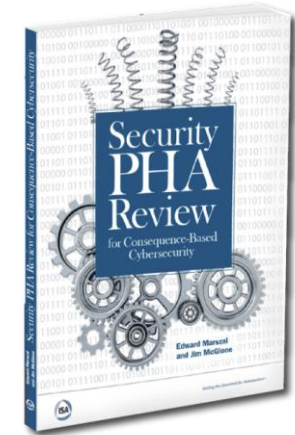
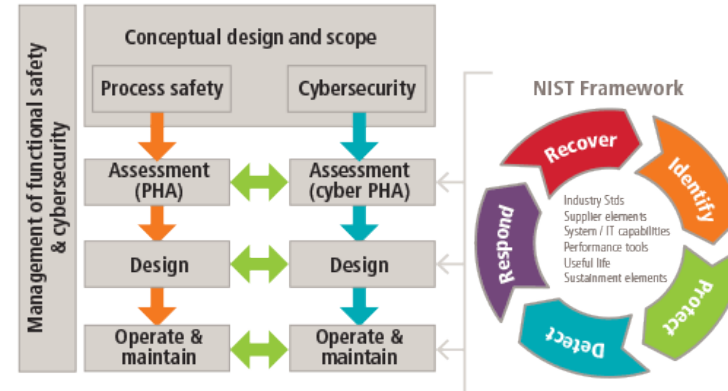
- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after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



# CIE Principles

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

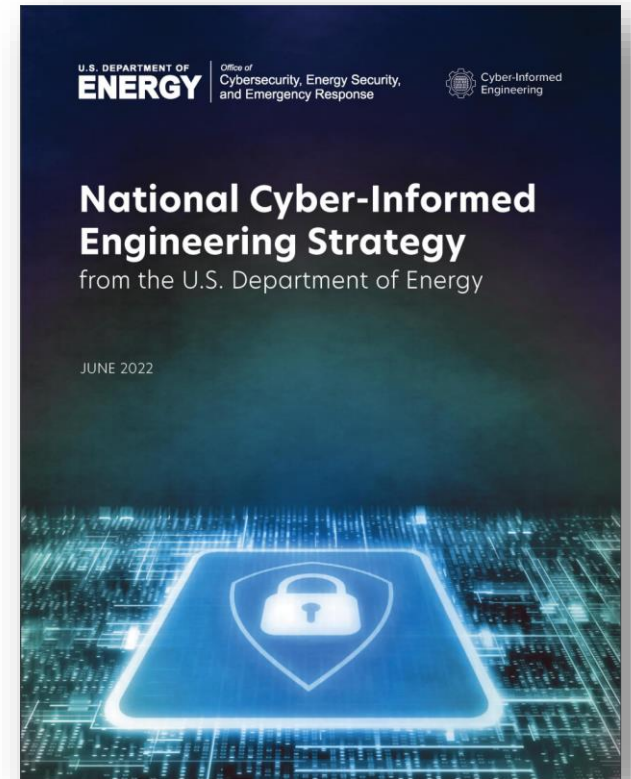
# #HowDoYouCIE?



# 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

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



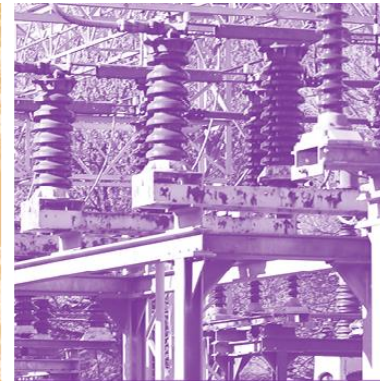
## Education

Embed CIE into formal education, training, and credentialing



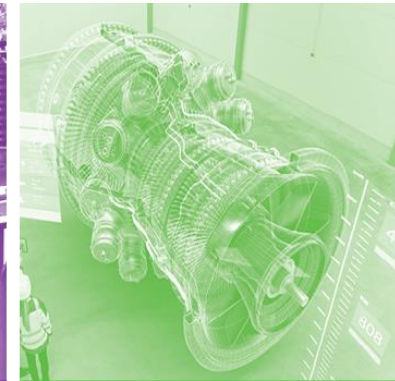
## Development

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

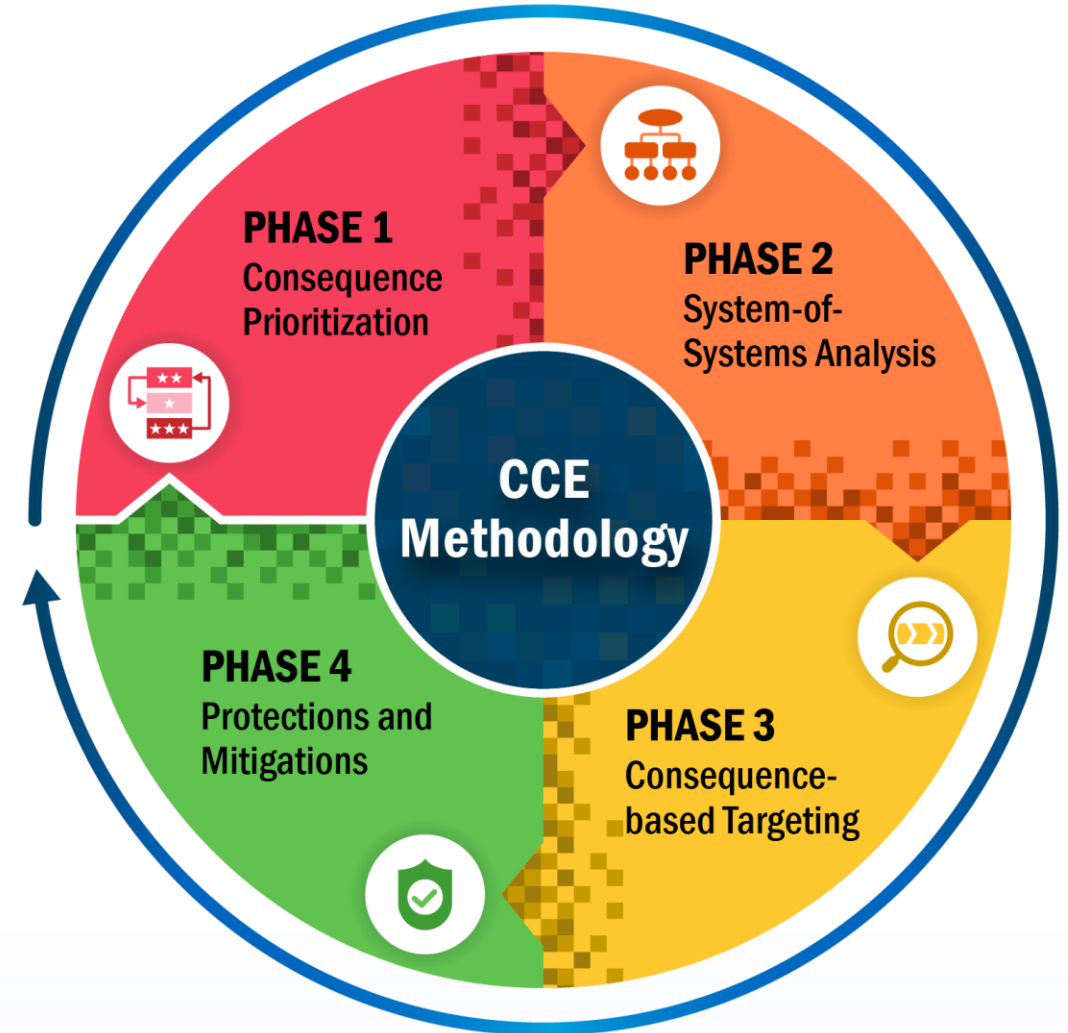
Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology



# *Our* how: Consequence-driven Cyber-informed Engineering

# Consequence-driven Cyber-informed Engineering

The goal of CCE is to protect critical functions from existing and emerging threats and proactively prepare for the next generation of cyber-enabled sabotage.



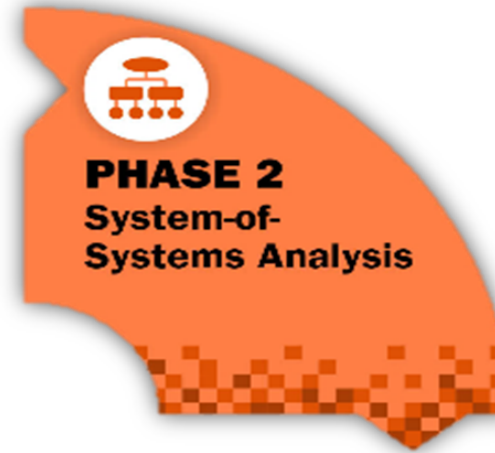
# CCE Phase 1: Consequence Prioritization



**Process of identifying and ranking potential adverse cyber-Events**

The goal of this phase is to identify disruptive Events that would significantly inhibit an organization's ability to provide its critical functions.

# CCE Phase 2: System-of-Systems Analysis



**Focuses on decomposing the High Consequence Event(s) (HCE) to enabling functions to collect and analyze relevant details.**

The goal of this phase is to accurately understand and describe in detail the functionality of all HCE-related systems.

# CCE Phase 3: Consequence-based Targeting



**Process of evaluating the information collected in Phase 2 from an adversarial perspective.**

The goal is to describe what an adversary must do, where they must be, how they get there, and what they must know.

# CCE Phase 3: Consequence-based Targeting

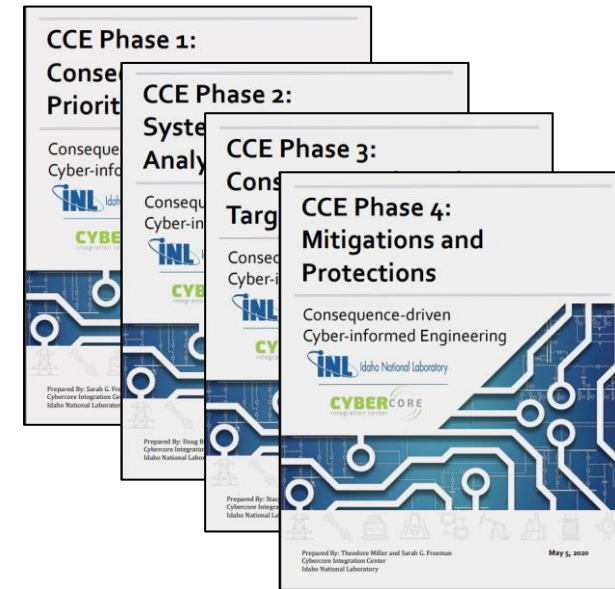


**Making recommendations to remove or reduce possible impacts of HCE(s).**

The goal is to protect or mitigate impacts through application of cyber-informed engineering principles and good engineering.

# Ways to Conduct CCE

- INL-supported and DOE-sponsored (Tier 1) engagement
- Self-driven (Tier 2) engagement
  - Licensed partner support
  - Internally resourced with reference materials
- ACCELERATE training



# Free, Available Resources

# Read Up at the Open-Source Library

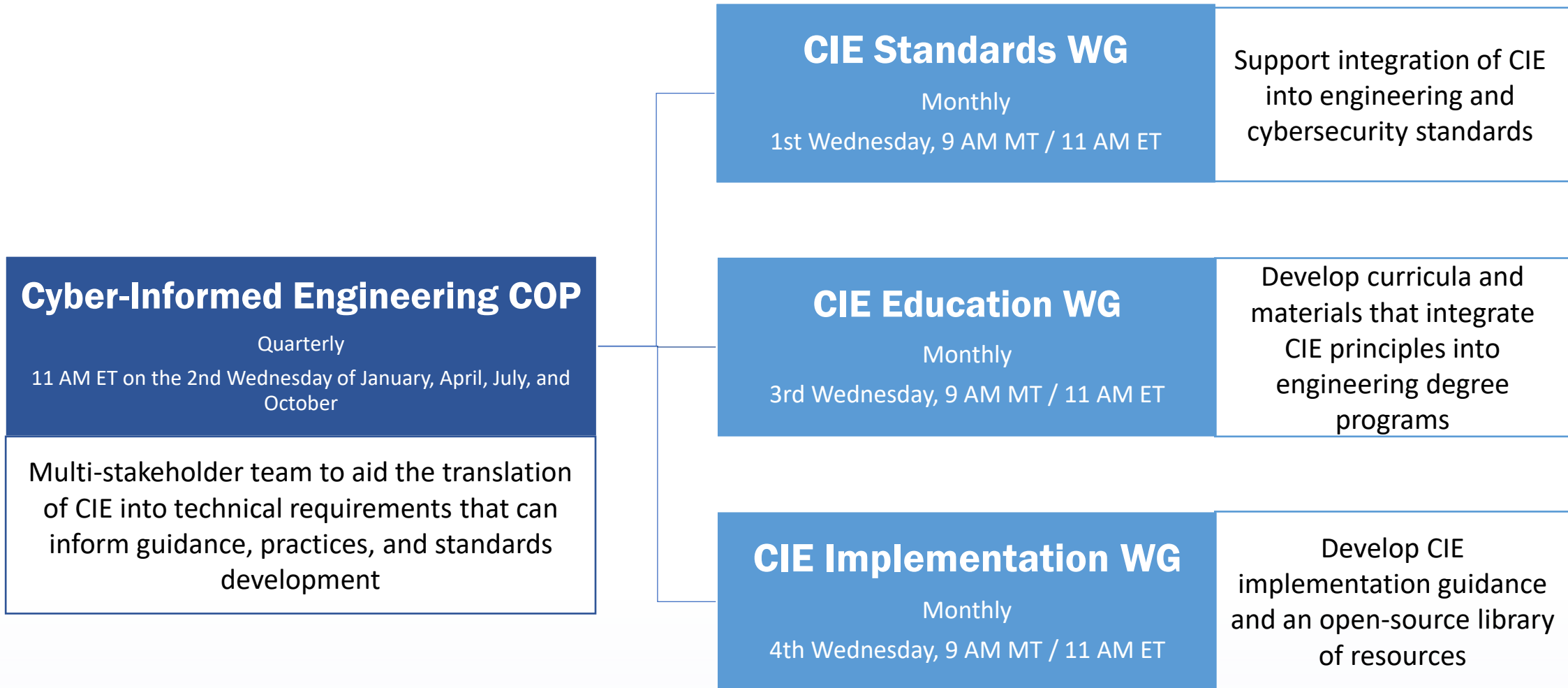
Title	Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs for Phase 2 of the Secure Power Systems Professional project
Authors	O'Neil, Lori Ross; Assante, Michael; Tobey, D. H.; Conway, T. J.; Vanderhorst, Jr, T. J.; Januszewski, III, J.; Ileo, 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	<a href="#">Metadata</a>
Full Document	<a href="#">Full Document</a>

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	<a href="#">Metadata</a>
Full Document	<a href="#">Full Document</a>

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	<a href="#">Metadata</a>

- 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

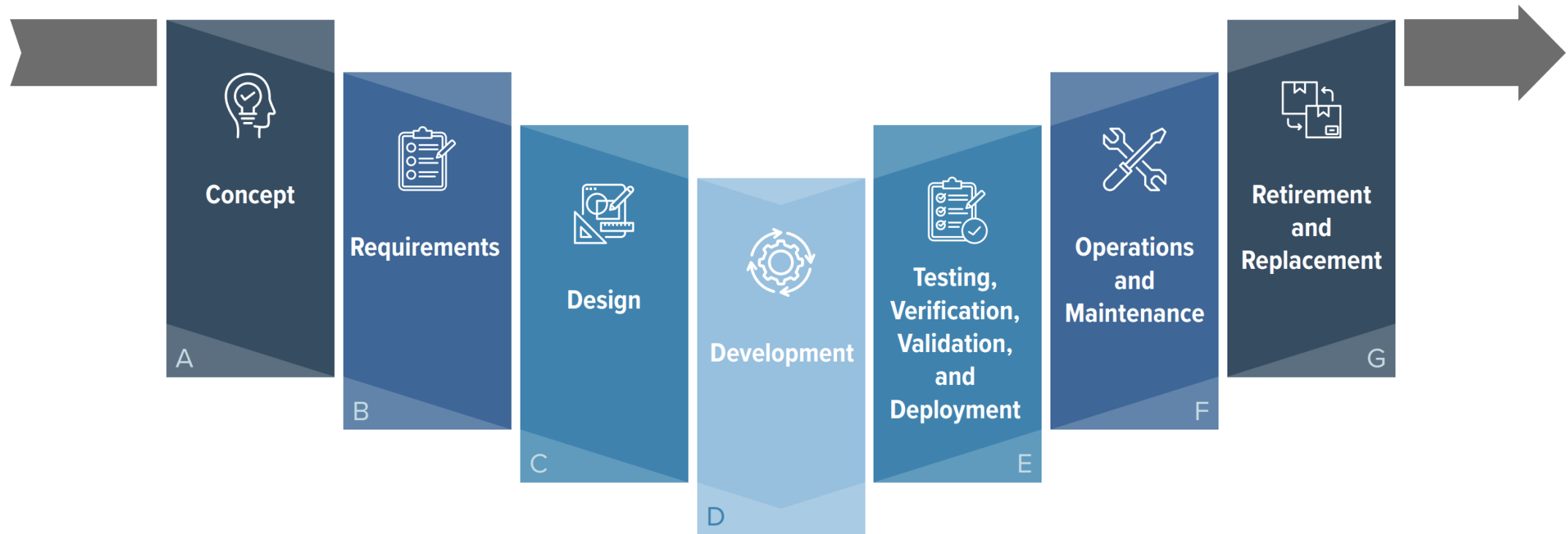
# Join our Community of Practice



# CIE Implementation Guide: A Self-Help Tool

## Applying CIE across the SE Lifecycle

Figure 2. CIE Systems Engineering Lifecycle Model



# CIE Implementation Guide: A Self-Help Tool

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

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



Cyber-Informed  
Engineering

# CIE Implementation Guide: A Self-Help Tool

U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Cybersecurity  
and Energy

Cyber-Informed  
Implementation

Version 1.0

DRAFT

AUGUST 7, 2023

## 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.<sup>4</sup>

<sup>4</sup> 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.



# CIE Implementation Guide: A Self-Help Tool

U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Cybersecurity and  
Energy Reliability

**Cyber-Informed  
Engineering  
Implementation Guide**  
Version 1.0

**DRAFT**

AUGUST 7, 2023

PRINCIPLE 1  
Consequences

KEY QUESTION  
**How do I understand  
consequences and the underlying  
risks?**

**Principle Description**  
Apply CIE strategies first and foremost to the system performs. Typically these are functions subverted, could result in unacceptable or catastrophic impacts to the organization, including undesired impacts to the environment, availability or effectiveness of products, integrity, and public image. Use a structured approach to identify areas where digital technology is used within the system. Consider where an unprotected action or failure of digital technology might lead to a high-consequence event, including unauthorized system actions, invalid data, automated action, or interdiction of a digitally enabled control that exist to minimize impacts of misuse. Controls are implemented via digital technology or a combination of both.

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

4 This idea aligns with ISA/IEC 62443 "Assess, Design, Implement, Operate, Maintain, and Improve" (ADOMIP) process. While the system may not have changed, the patches and updates are considered consequences. The reassessment should be performed.

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT

PRINCIPLE 1 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.

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?

**EXAMPLE:** Loss of control or disruption of a large power electric 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.

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT

# CIE Implementation Guide: A Self-Help Tool

U.S. DEPARTMENT OF

ENERGY

Office of Cybersecurity and Critical Infrastructure Protection

Cyber-Informed Engineering Implementation Guide

Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1

Consequences

KEY QUESTION

How do I understand consequences and ensure and the understanding of consequences

Principle Description

Apply CIE strategies first and foremost to the system performs. Typically these are functions subverted, could result in unacceptable or catastrophic impacts to the organization, including undesired impacts to the environment, availability or effectiveness of products, integrity, and public image. Use a structured approach to identify areas where digital technology is used within the system. Consider where an unprotected action or failure of digital technology might lead to a high-consequence event, including unauthorized system actions, invalid data, automated action, or interdiction of a digitally enabled control that exist to minimize impacts of misuse. controls that exist to minimize impacts of misuse. controls are implemented via digital technology combination of both.

This list of high-impact consequences underpin the system perform throughout the system design lifecycle and their priority within each CIE principle. For the work above, engineers will consider engineering controls (e.g., 2: Engineered Controls), that could either remove or mitigate the consequences of an unprotected action or failure of digital technology.

4 This idea aligns with ISA/IEC 62443 "Assess, Design, Implement, Operate, Maintain, and Improve" (ADOMIP) model. While the system may not have changed, the patches and updates are considered consequences. The reassessment should be done after the system is updated.

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT

PRINCIPLE 1 PHASE 1 A

PRINCIPLE 1: CONSEQUENCES (continued)

5 What business consequences are there?  
a Which part of the system is the consequence?  
b Which results in "acceptable" risk management?  
c Which consequences are "unacceptable" distinct consequences?

6 What regional or system failure consequences are there?  
a What entities are impacted by the failure?  
b What changes from regional to system failure?

7 What crucial assets are there?  
a What violations of the system are there?

8 Where might consequences occur?  
a At each instance of the system?

9 Are there adverse consequences?  
a What circumstances lead to adverse consequences?  
b In adverse consequences?

10 What staffing or training consequences are there?  
a Where might support or training be needed?  
b What are the consequences of staffing or training?

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT

CIE Engineering Lifecycle

Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance
---------	--------------	--------	-------------	---	----------------------------

Water Sector Engineering Lifecycle

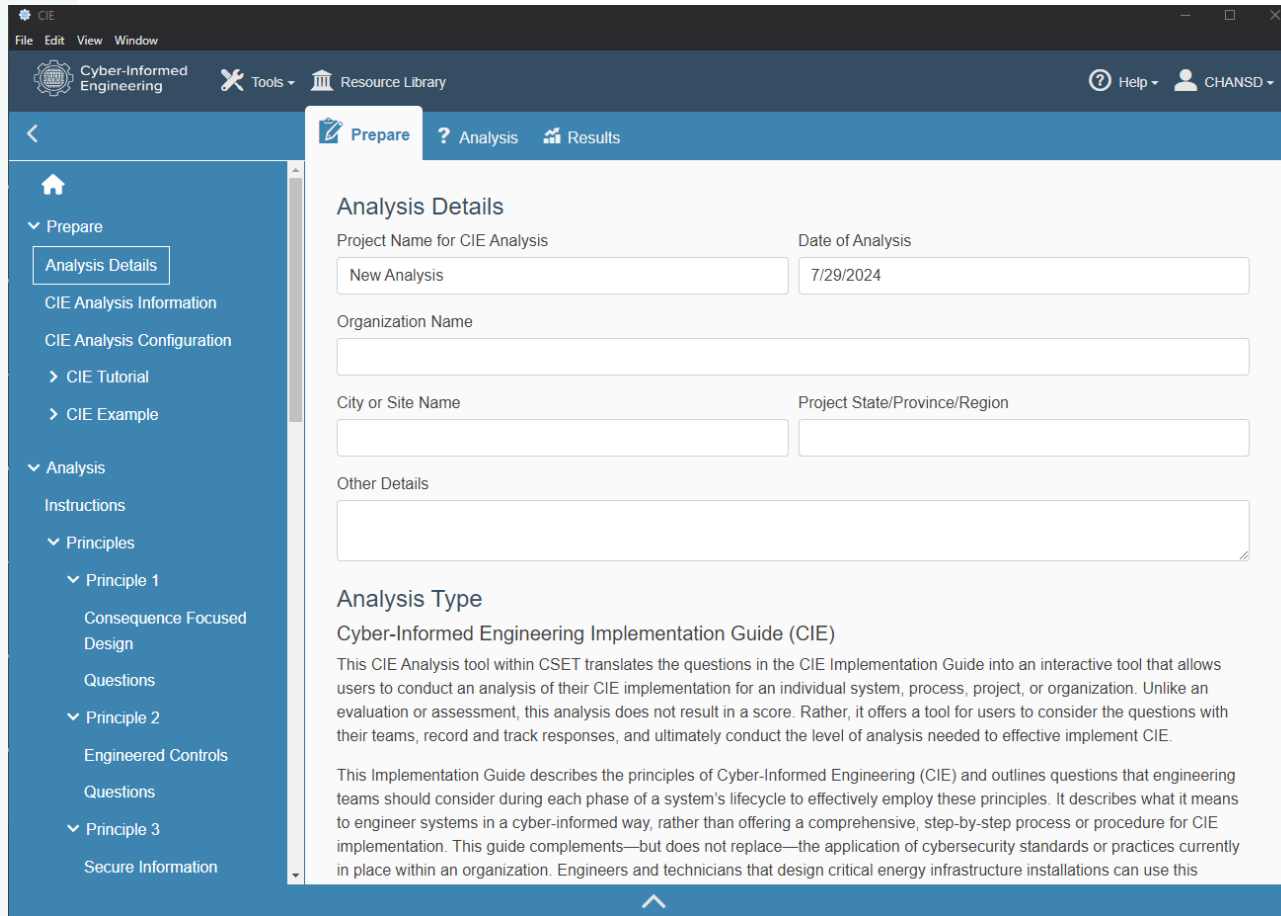
Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning	Operations and Maintenance
------------------	---------------------------	-----------------	--------------------------------	----------------------------

PRINCIPLE CIE CONTROL/MITIGATION EXAMPLE

PRINCIPLE	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

# CIE Analysis Tool



The screenshot displays the CIE Analysis Tool interface. The top menu bar includes 'File', 'Edit', 'View', and 'Window'. Below it, a toolbar shows icons for 'Tools' and 'Resource Library', along with 'Help' and 'CHANSD' user information. The main interface is divided into a left sidebar and a central content area. The sidebar contains a 'Prepare' section with 'Analysis Details' selected, and an 'Analysis' section with 'Instructions', 'Principles', and 'Secure Information' options. The central content area shows the 'Analysis Details' form with fields for 'Project Name for CIE Analysis' (set to 'New Analysis'), 'Date of Analysis' (set to '7/29/2024'), 'Organization Name', 'City or Site Name', 'Project State/Province/Region', and 'Other Details'. Below the form is the 'Analysis Type' section, which describes the tool's purpose and provides instructions for use.

**Analysis Details**

Project Name for CIE Analysis:  Date of Analysis:

Organization Name:

City or Site Name:  Project State/Province/Region:

Other Details:

**Analysis Type**

**Cyber-Informed Engineering Implementation Guide (CIE)**

This CIE Analysis tool within CSET translates the questions in the CIE Implementation Guide into an interactive tool that allows users to conduct an analysis of their CIE implementation for an individual system, process, project, or organization. Unlike an evaluation or assessment, this analysis does not result in a score. Rather, it offers a tool for users to consider the questions with their teams, record and track responses, and ultimately conduct the level of analysis needed to effectively implement CIE.

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

- Find at:  
<https://github.com/inlguy/CIE>
- Interactive application of the CIE Implementation Guide
- Local installation, no external data transfers

# For More Information

- Critical Function Assurance
  - <https://inl.gov/national-security/cfa/>
- Cyber-Informed Engineering
  - <https://inl.gov/national-security/cie/>
- Consequence-driven Cyber-informed Engineering
  - <https://inl.gov/national-security/cce/>



# Thank You!



CIE@inl.gov  
Samuel.Chanoski@inl.gov



<https://www.linkedin.com/in/sdchanoski/>



<https://inl.gov/cie/>

