



Cyber-Informed Engineering Principles: Whats in it for me?

October 2023

Changing the World's Energy Future

Samuel Douglas 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-Informed Engineering Principles: Whats in it for me?

Samuel Douglas Chanoski

October 2023

**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 Principles: What's in it for me?

Sam Chanoski, Idaho National Laboratory

OCTOBER 23-26, 2023 | ATLANTA



INL/CON-23-75161

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
- **Codified** in the Consequence-driven, Cyber-informed Engineering (CCE) methodology



Keeping the Acronyms Straight



- Critical function assurance – managing 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!*

CIE Principles

PRINCIPLE	KEY QUESTION
Consequence-Focused Design	How do I understand what critical functions my system must <u>ensure</u> and the undesired consequences it must <u>prevent</u> ?
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?
Resilient 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 : 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

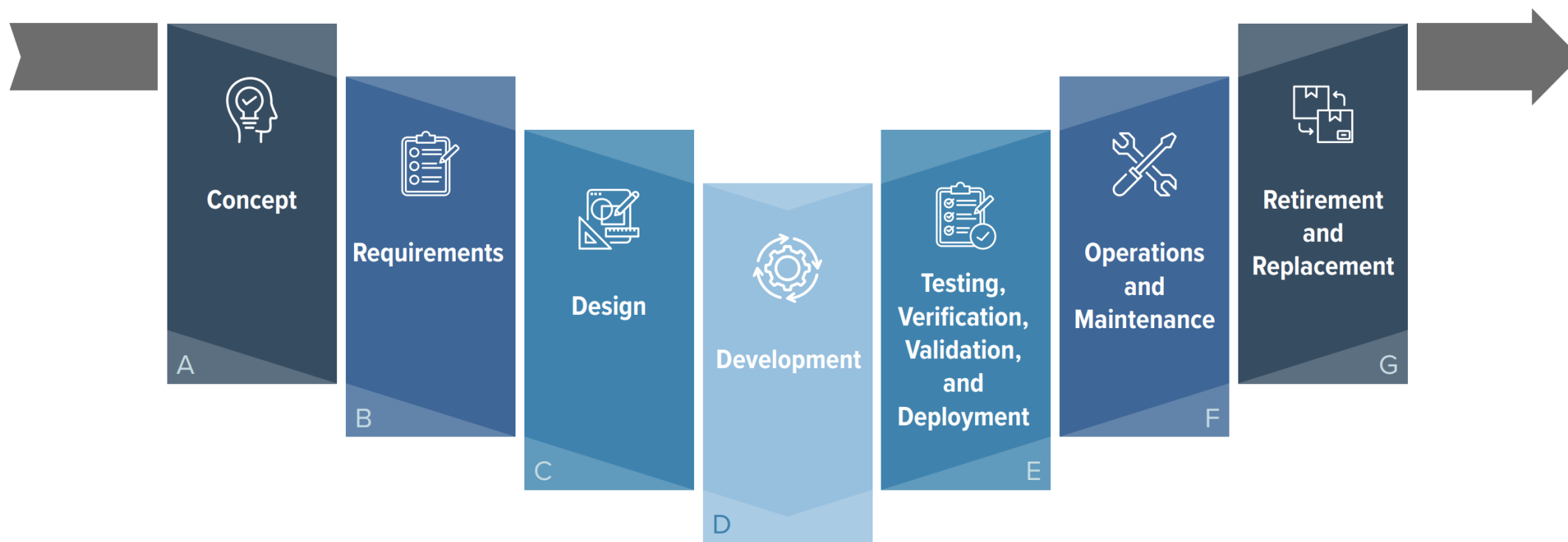
DRAFT

AUGUST 7, 2023

INL/RPT-23-74072

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

CIE Implementation Guide: A Self-Help Tool



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.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.

CIE Implementation Guide : A Self-Help Tool

U.S. DEPARTMENT OF
ENERGY

Official
Cybersecurity
and Energy
Security
Agency

Cyber-Informed
Engineering
Implementation
Guide
Version 1.0
DRAFT
AUGUST 7, 2023

PRINCIPLE 1
Consequence-Focused Design


KEY QUESTION
How do I understand the consequences of system failure and the underlying risks to the system?

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 product, 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 the unprotected action or mitigate its consequences.

4 This idea aligns with ISA/IEC 62443 "Assess, Design, Implement, Operate, Maintain, and Improve" phases. While the system may not have changed, the patches and updates could lead to new, previously unconsidered 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 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

Consequence

KEY QUESTION

How do I understand and ensure and the under

Principle Description

Apply CIE strategies first and foremost to the system performs. Typically these are functions subverted, could result in unacceptable or catastrophic consequences to the organization, including undesired impacts to the environment, availability or effectiveness of product 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 are implemented via digital technology or a combination of both.

This list of high-impact consequences underpin system performance 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) model. While the system may not have changed, the patches and updates are considered consequences. The reassessment should be performed.

PRINCIPLE 1

PHASE 1 A

PRINCIPLE 1: CONSEQUENCE

CONCEPT PHASE (continued)

5

What business

a

Which part of the system could be subverted, could result in unacceptable or catastrophic consequences to the organization, including undesired impacts to the environment, availability or effectiveness of product integrity, and public image. Use a structured approach to identify areas where digital technology is used within the system.

b

Which result in unacceptable or catastrophic consequences to the organization, including undesired impacts to the environment, availability or effectiveness of product integrity, and public image. Use a structured approach to identify areas where digital technology is used within the system.

c

Which consequences to the organization, including undesired impacts to the environment, availability or effectiveness of product integrity, and public image. Use a structured approach to identify areas where digital technology is used within the system.

6

What regional or system failure

a

What entities or infrastructure could be subverted, could result in unacceptable or catastrophic consequences to the organization, including undesired impacts to the environment, availability or effectiveness of product integrity, and public image. Use a structured approach to identify areas where digital technology is used within the system.

b

What changes from regional or system failure

7

What crucial assets

a

What violations of critical assets

8

Where might controls

a

At each instance of controls

9

Are there adverse consequences

a

What circumstances

b

In adverse consequences

10

What staffing or training

a

Where might support or training

b

What are the staffing or training

First point in the Engineering Lifecycle that the example is considered

Continuation of the example through the Engineering Lifecycle

CIE Engineering Lifecycle

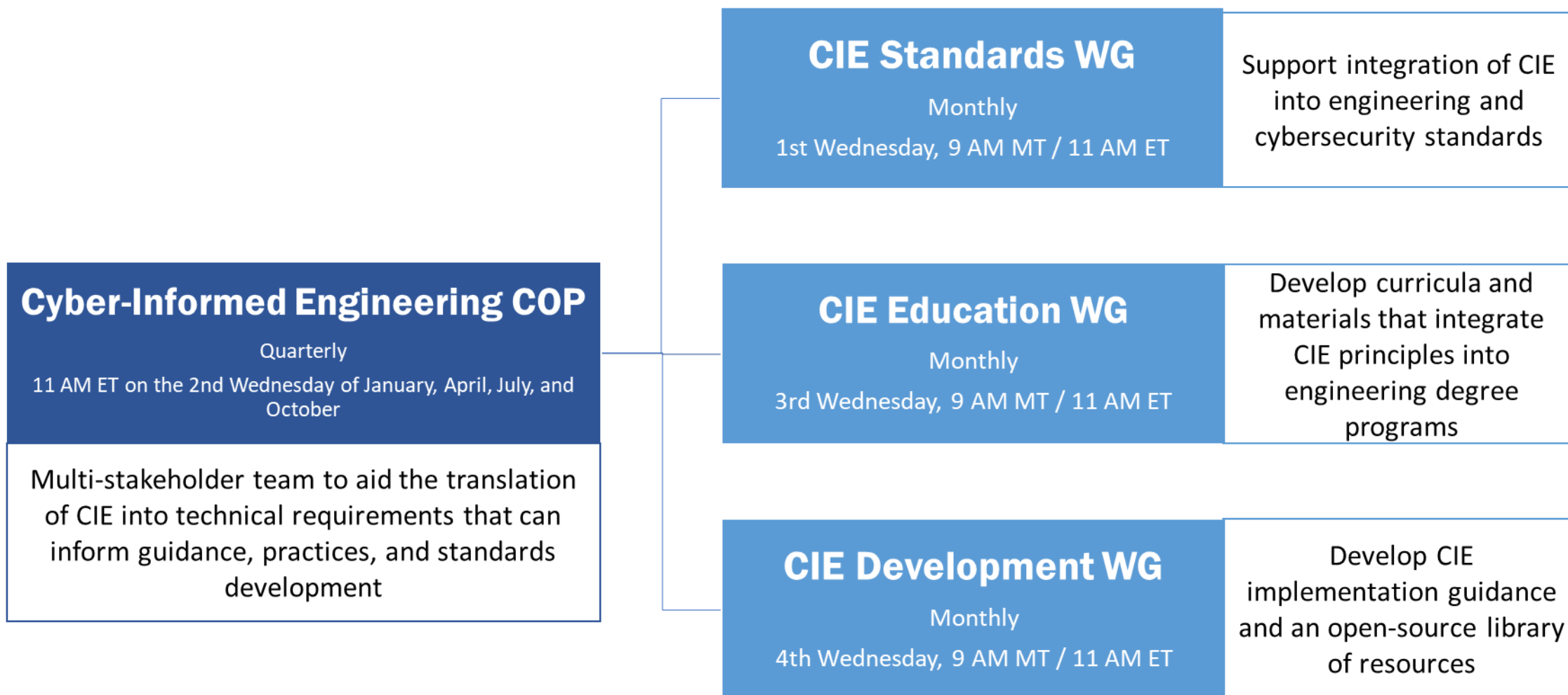
Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance
---------	--------------	--------	-------------	---	----------------------------

Water Sector Engineering Lifecycle

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

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE	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.					

Community of Practice: Get Involved



Open-Source Library: Learn

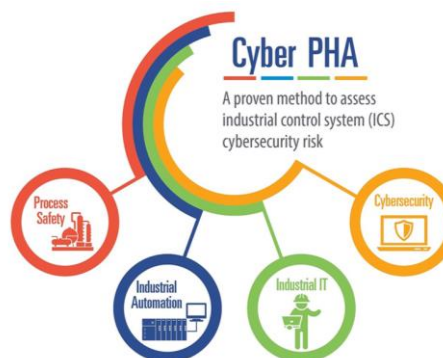
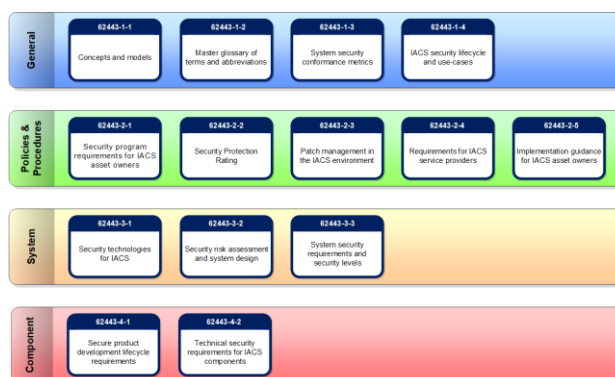
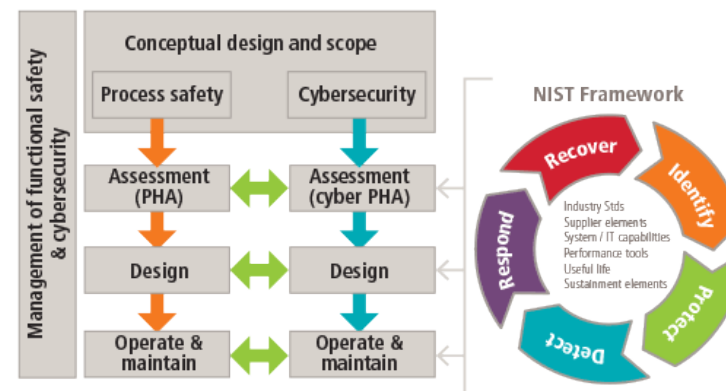
Title	Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs for Phase 2 of the Secure Power Systems Professional project
Authors	O'Neil, Lori Ross; Assante, Michael; Tobey, D. H.; Conway, T. J.; Vanderhorst, Jr, T. J.; Januszewski, III, J.; leo, 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

So, #HowDoYouCIE?



Questions? Suggestions?!

Visit <https://inl.gov/cie/>
Email CIE@inl.gov

Sam Chanoski, CISSP, GCIP, GICSP, C|EH
Technical Relationship Manager
Idaho National Laboratory
samuel.chanoski@inl.gov