INL/CON-23-73416-Revision-0

Cyber-Informed Engineering for Design and Operations

July 2023

Samuel Douglas Chanoski

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-23-73416-Revision-0

Cyber-Informed Engineering for Design and Operations

Samuel Douglas Chanoski

July 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 for Design and Operations

Sam Chanoski, CISSP, GCIP, GICSP, C|EH
Technical Relationship Manager
Idaho National Laboratory

IEEE Power & Energy Society General Meeting 2023

INL/CON-23-73416

Agenda

- Why, What, and How
- Implications for Design and Operation
- Moving Forward

Why, What, and How

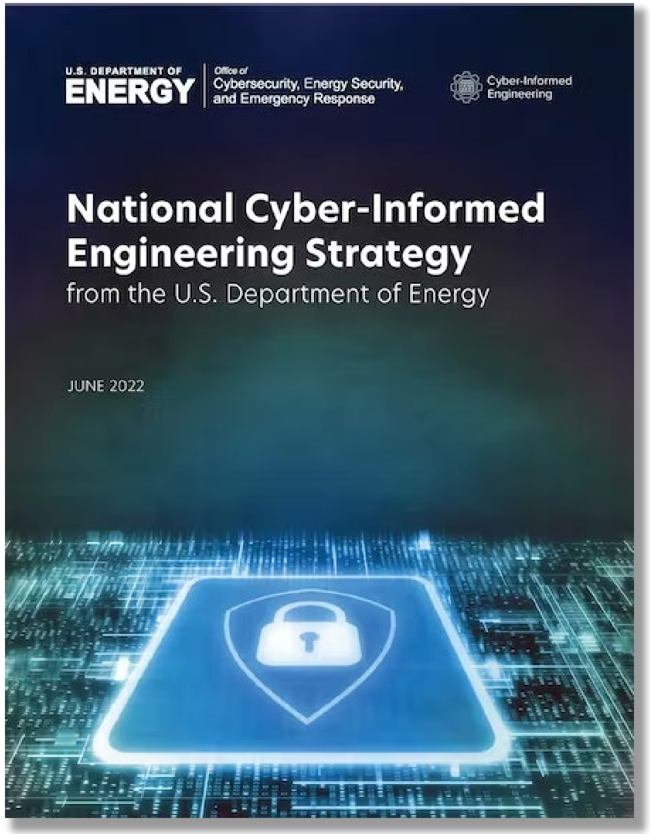
Why Cyber-Informed Engineering?

- 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

What is Cyber-Informed Engineering?

- CIE uses **design decisions** and **engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to "engineer out" cyber risk** 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.



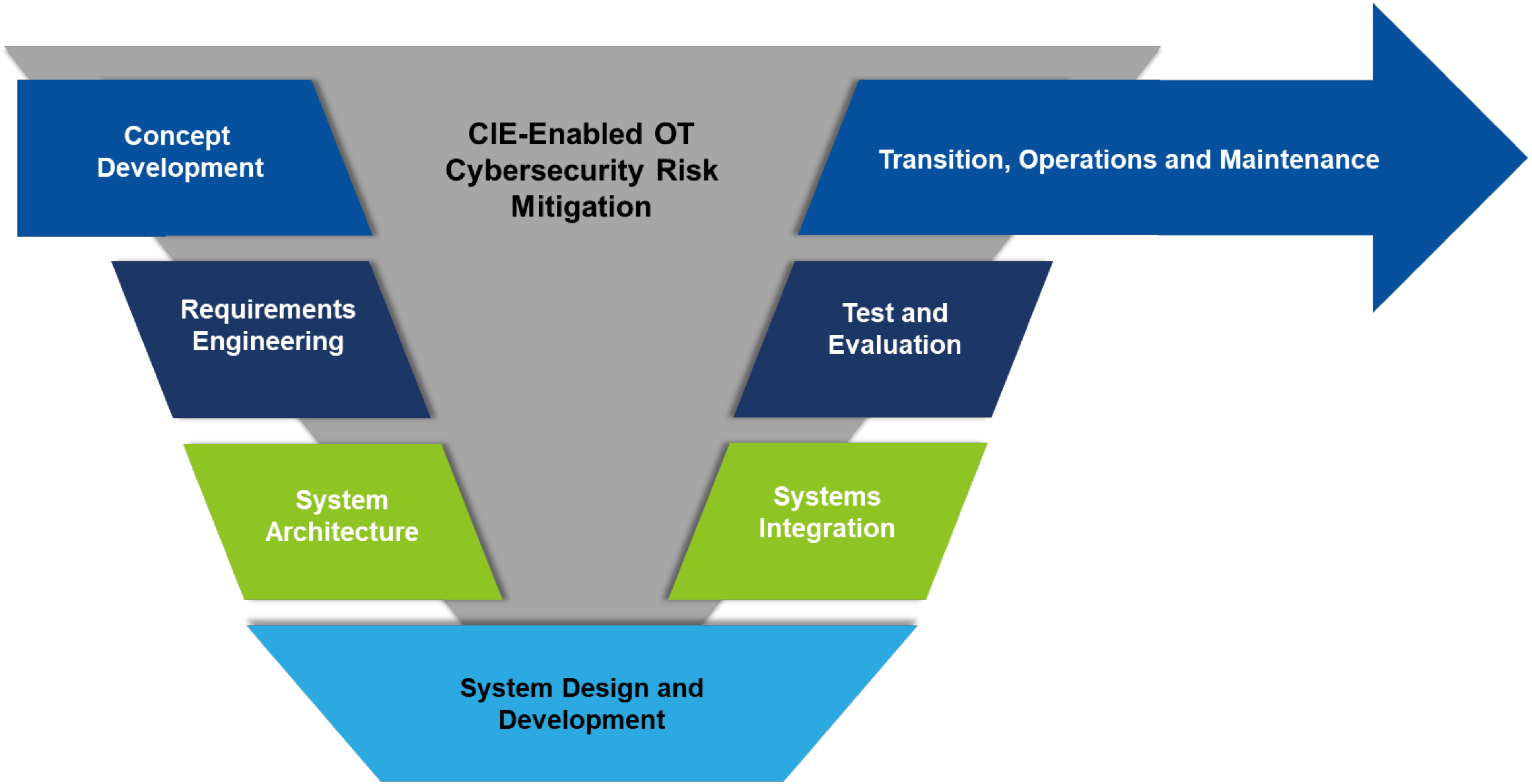
U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Cyber-Informed Engineering

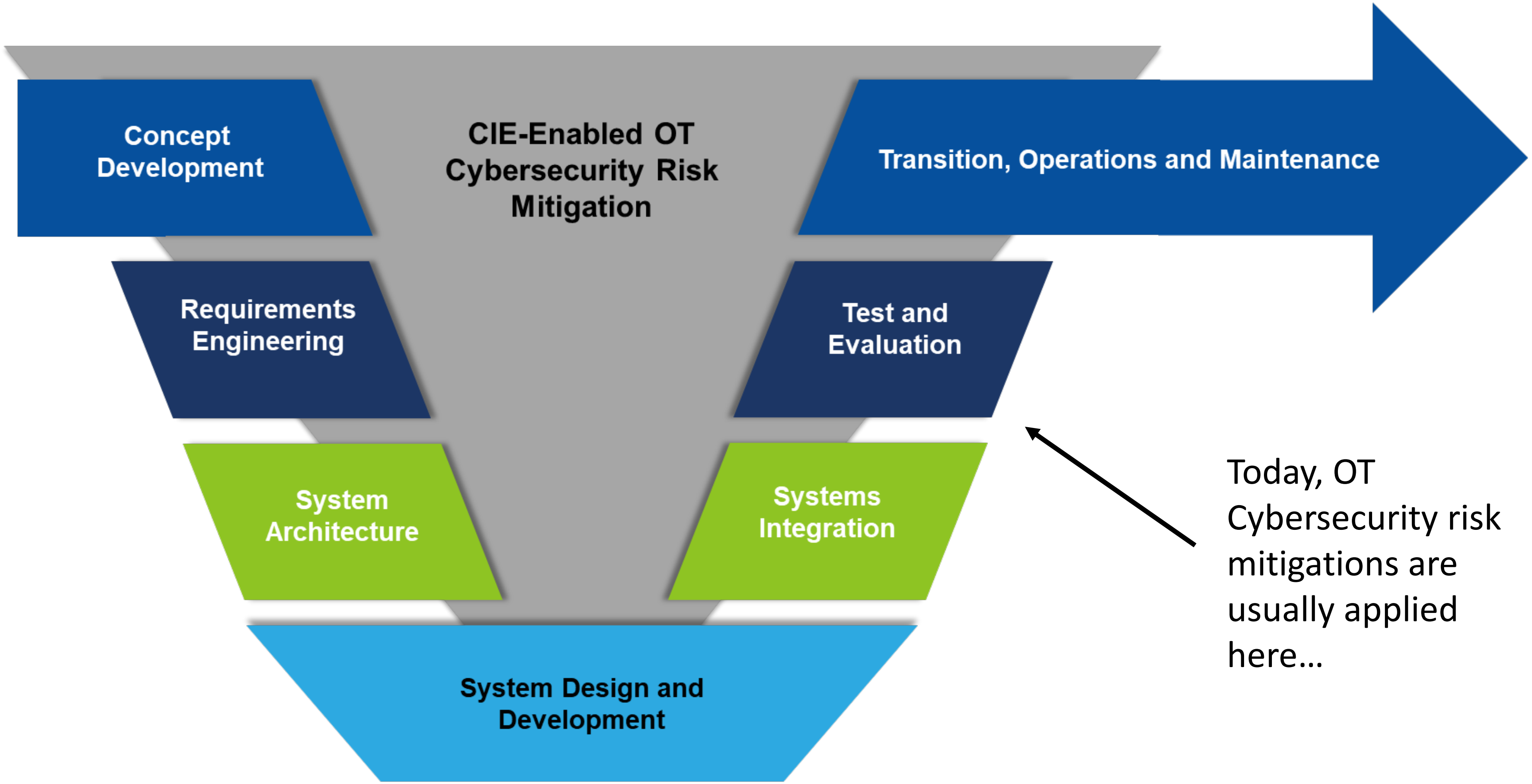
National Cyber-Informed Engineering Strategy
from the U.S. Department of Energy

JUNE 2022

CIE in Systems Engineering

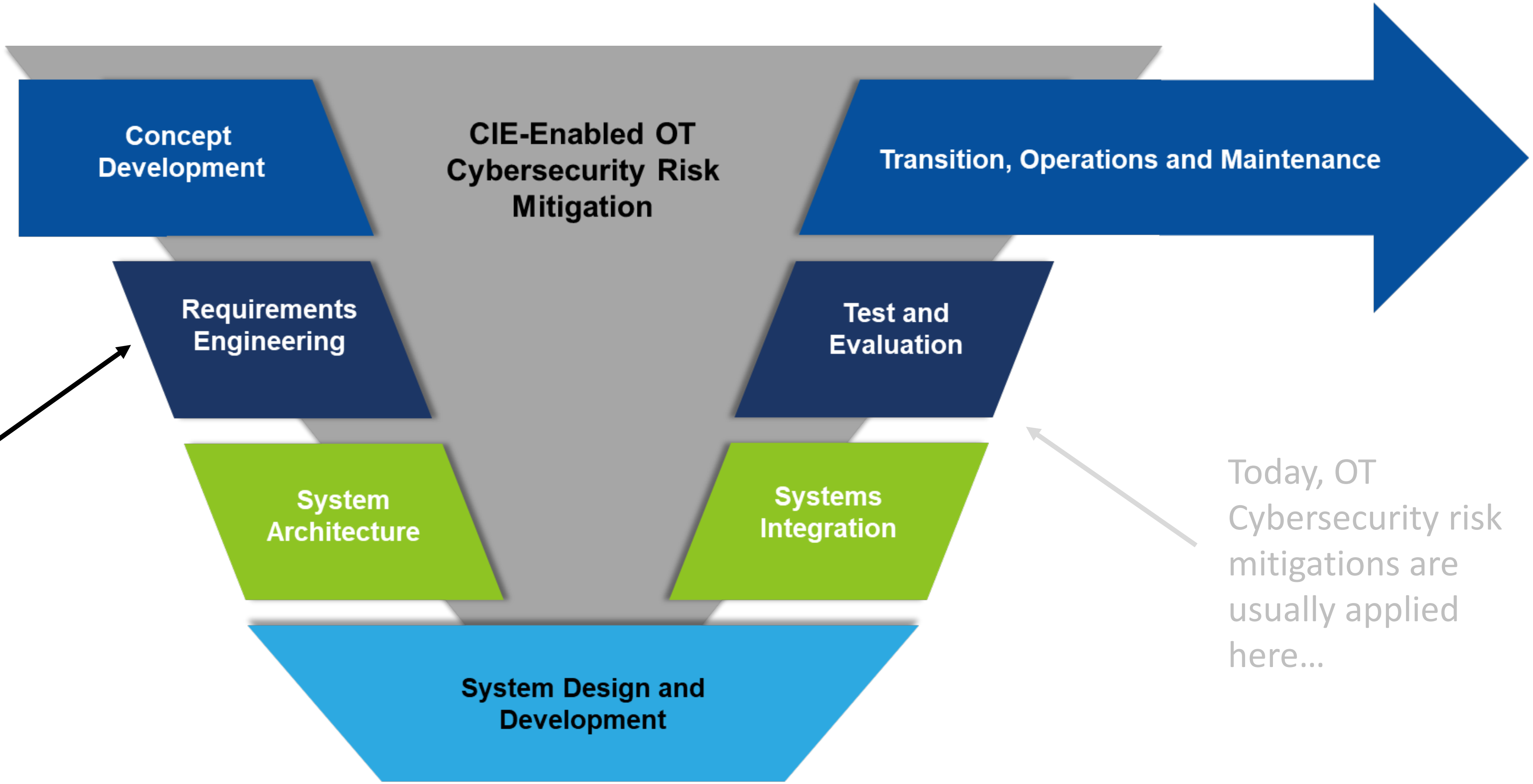

CIE-Enabled OT Cybersecurity Risk Mitigation
Concept Development
Requirements Engineering
System Architecture
System Design and Development
Systems Integration
Test and Evaluation
Transition, Operations and Maintenance

CIE in Systems Engineering


Concept Development
CIE-Enabled OT Cybersecurity Risk Mitigation
Transition, Operations and Maintenance
Requirements Engineering
Test and Evaluation
System Architecture
Systems Integration
System Design and Development

Today, OT Cybersecurity risk mitigations are usually applied here…

CIE in Systems Engineering


Concept Development
CIE-Enabled OT Cybersecurity Risk Mitigation
Transition, Operations and Maintenance
Requirements Engineering
Test and Evaluation
System Architecture
Systems Integration
System Design and Development

… but mitigations are more effective and efficient when applied here!

Today, OT Cybersecurity risk mitigations are usually applied here…

Principles of CIE

Design and Operations

Consequence-focused Design

Engineered Controls

Secure Information Architecture

Design Simplification

Resilient Layered Defenses

Active Defense

Organizational

Interdependency Evaluation

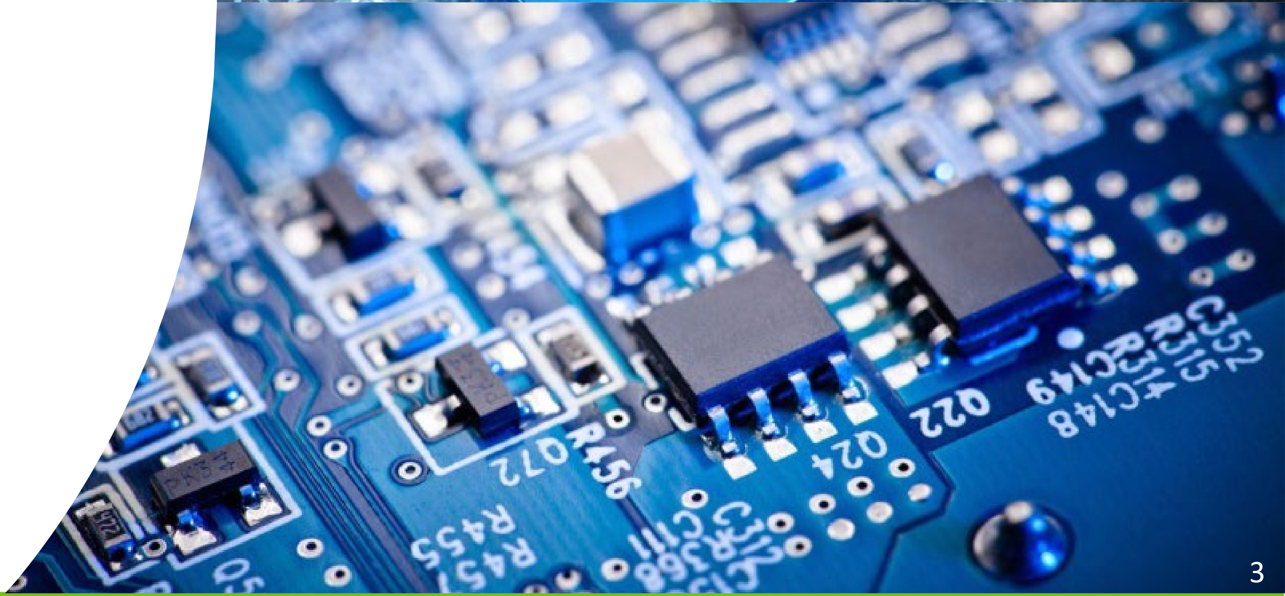
Digital Asset Awareness

Cyber-secure Supply Chain Controls

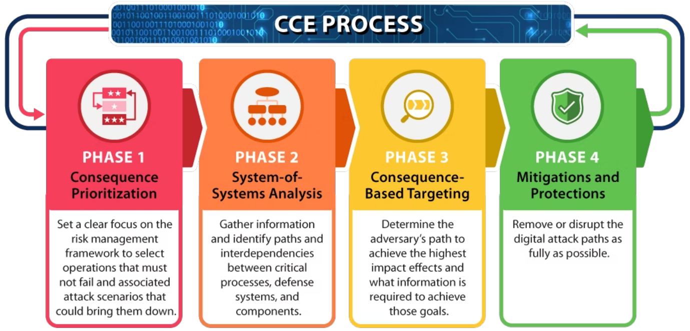
Planned Resilience

Engineering Information Control

Security Culture



How do *YOU* CIE?

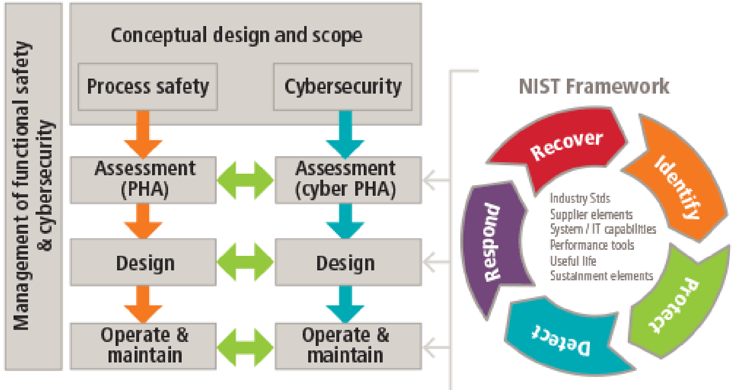

CCE PROCESS
PHASE 1
Consequence Prioritization
PHASE 2
System-of-Systems Analysis
PHASE 3
Consequence-Based Targeting
PHASE 4
Mitigations and Protections

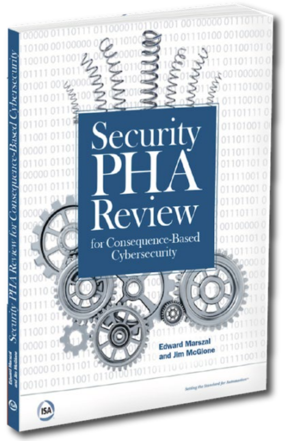
Set a clear focus on the risk management framework to select operations that must not fail and associated attack scenarios that could bring them down.

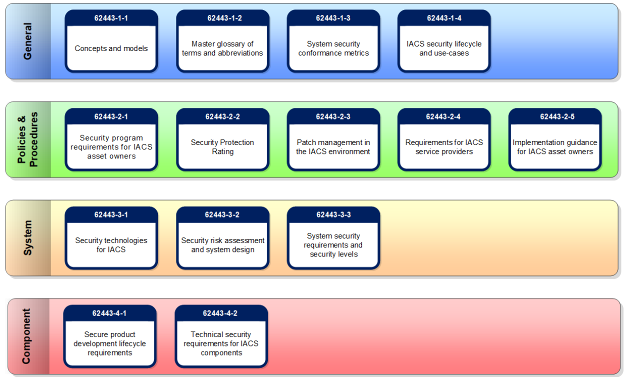
Gather information and identify paths and interdependencies between critical processes, defense systems, and components.

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.




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



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

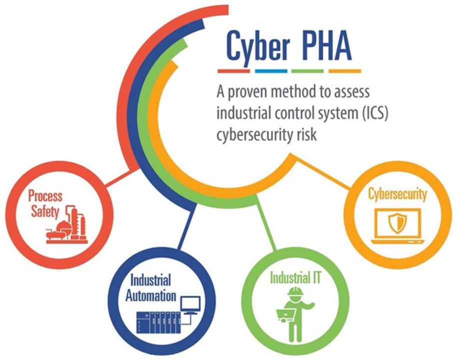
62443-3-2 Security risk assessment and system design

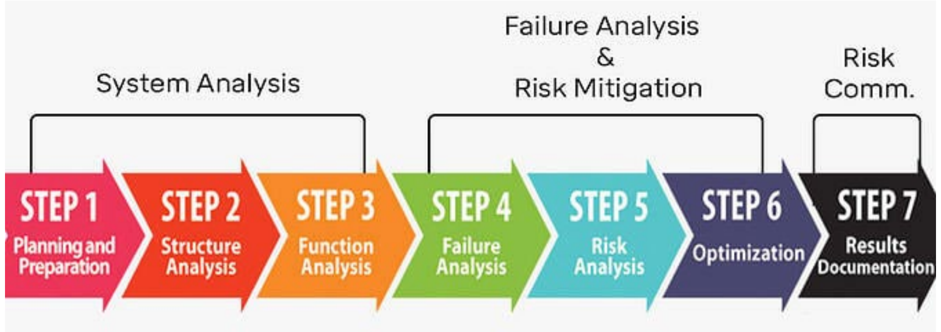
62443-3-3 System security requirements and security levels

Component

62443-4-1 Secure product development lifecycle requirements

62443-4-2 Technical security requirements for IACS components


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

Remember the Why!

- 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

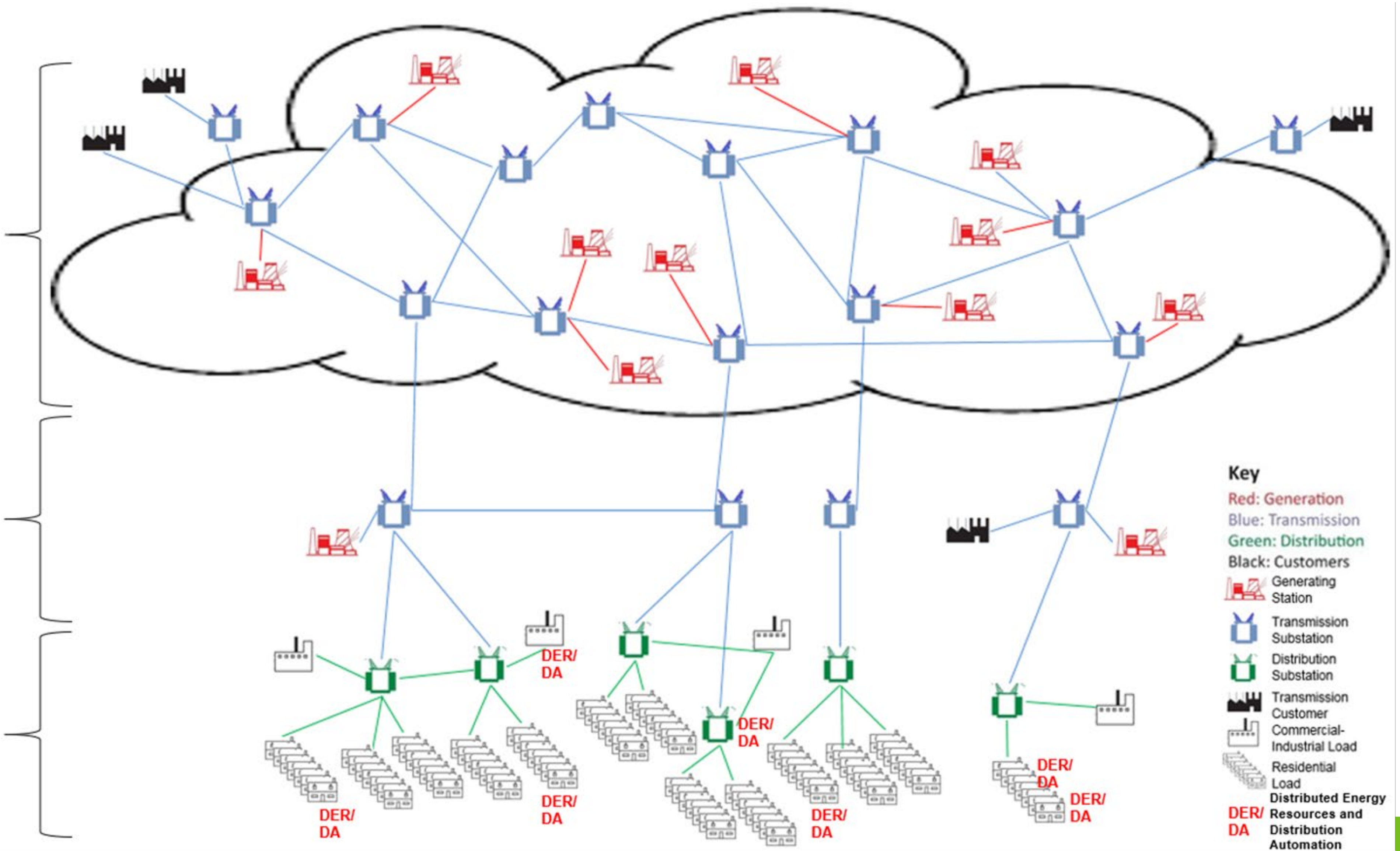
Implications for Design and Operation

Increasing Grid Complexity

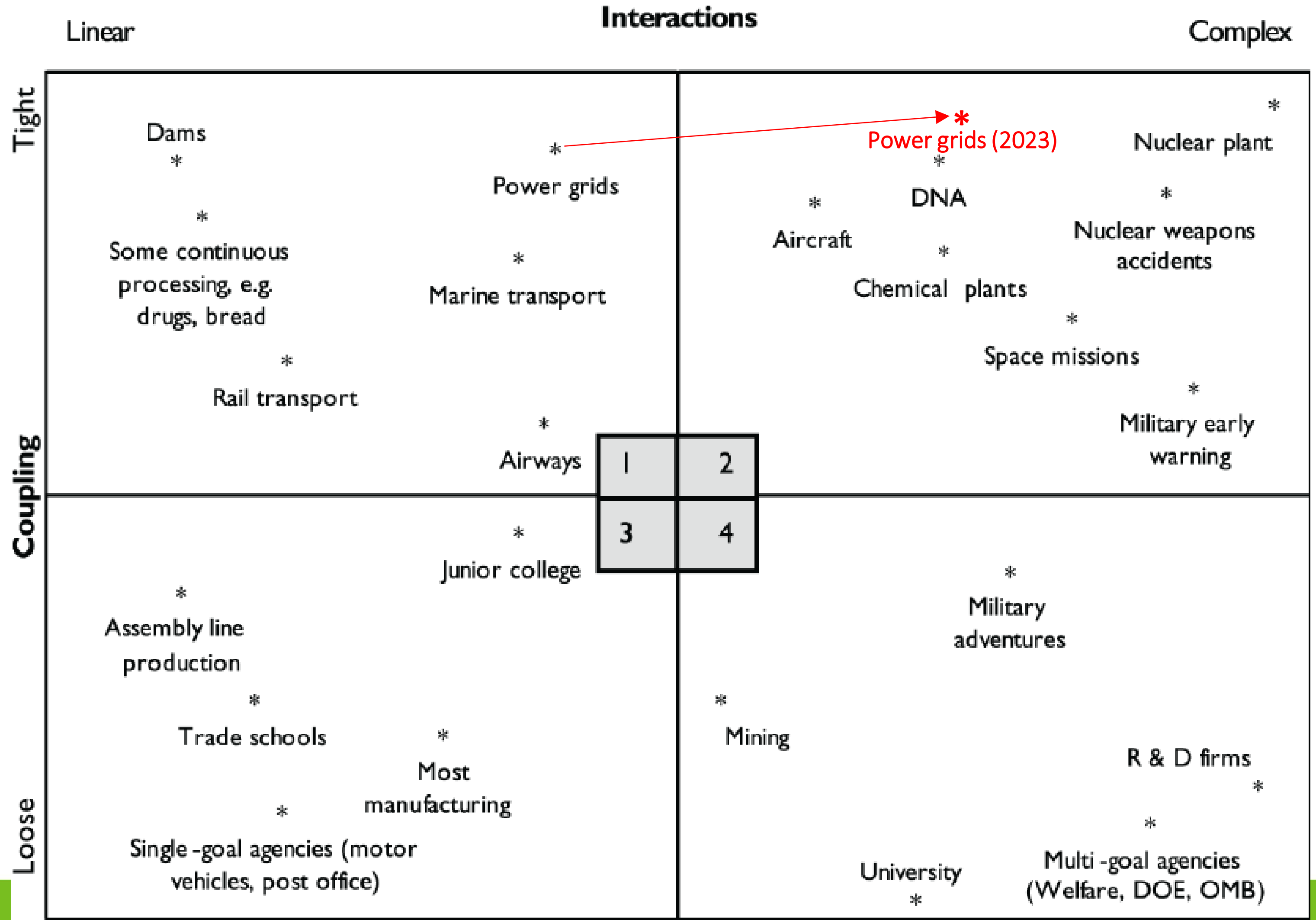
Bulk Electric System (BES): densely interconnected, highly reliable, redundant, NERC-regulated

Subtransmission: series-parallel paths from the BES to the lowest-voltage substations

Distribution: radially connected load and DERs

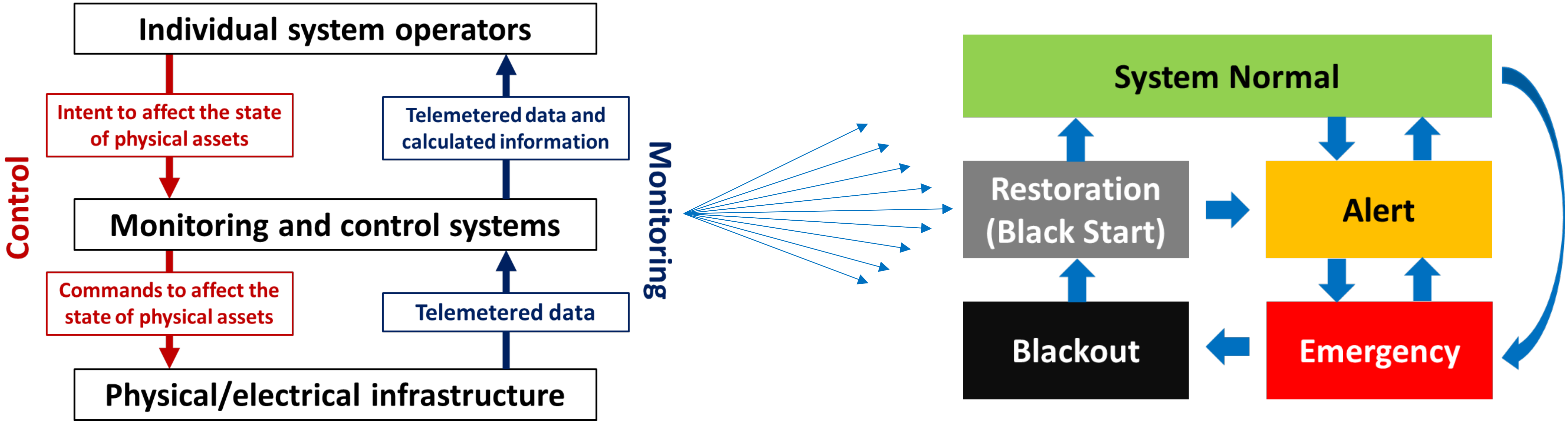


Digitization Increases Interaction and Coupling



Perrow, C. *Normal Accidents: Living with High-Risk Technologies.* 1984.

Humans and Machines Operate a Dynamic Grid



Individual system operators

Intent to affect the state of physical assets

Telemetered data and calculated information

Monitoring and control systems

Commands to affect the state of physical assets

Telemetered data

Physical/electrical infrastructure

System Normal

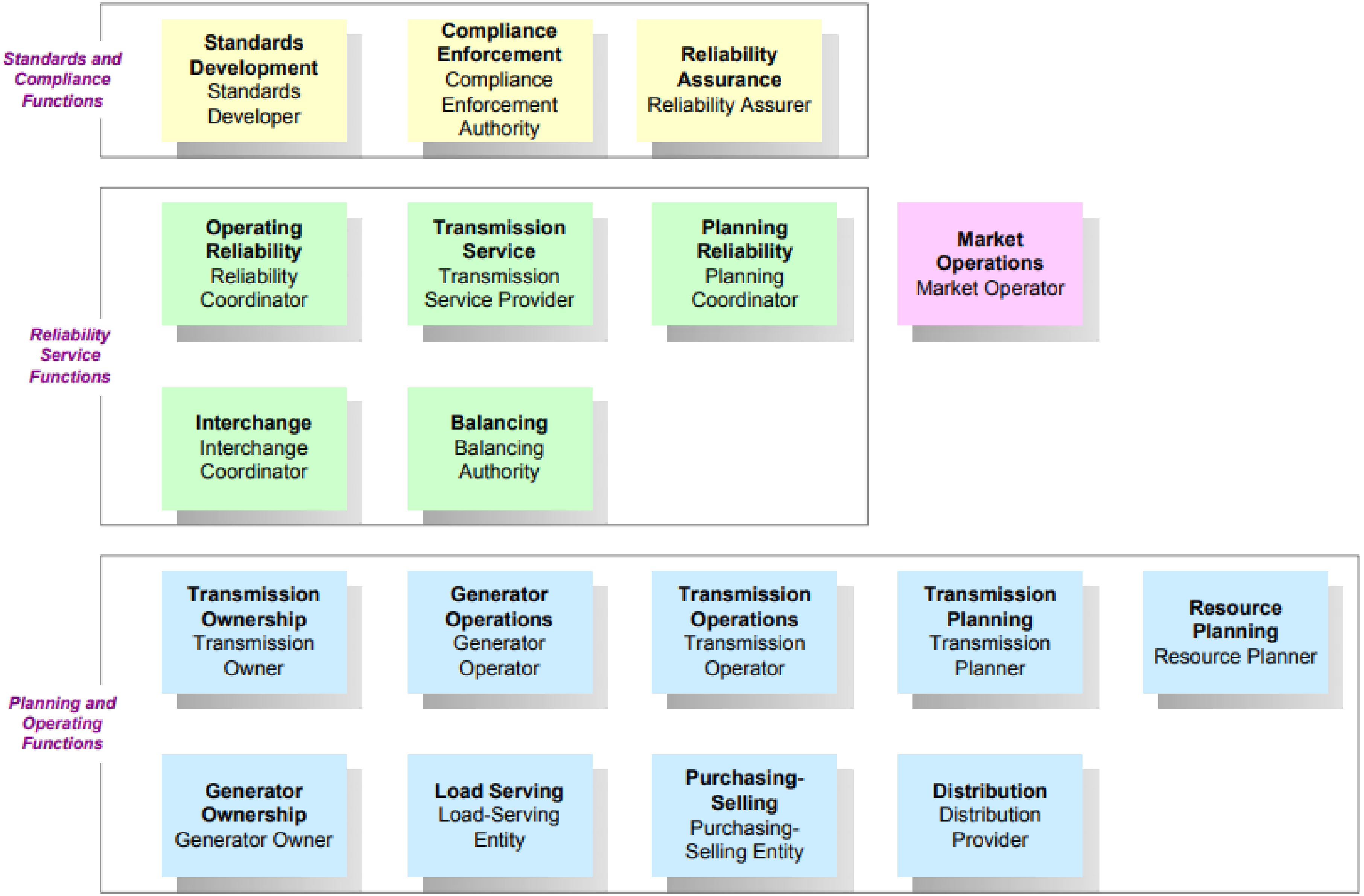
Restoration (Black Start)

Alert

Blackout

Emergency

Functional Roles



Standards and Compliance Functions

Standards Development Standards Developer

Compliance Enforcement Compliance Enforcement Authority

Reliability Assurance Reliability Assurer

Reliability Service Functions

Operating Reliability Reliability Coordinator

Transmission Service Transmission Service Provider

Planning Reliability Planning Coordinator

Market Operations Market Operator

Interchange Interchange Coordinator

Balancing Balancing Authority

Planning and Operating Functions

Transmission Ownership Transmission Owner

Generator Operations Generator Operator

Transmission Operations Transmission Operator

Transmission Planning Transmission Planner

Resource Planning Resource Planner

Generator Ownership Generator Owner

Load Serving Load-Serving Entity

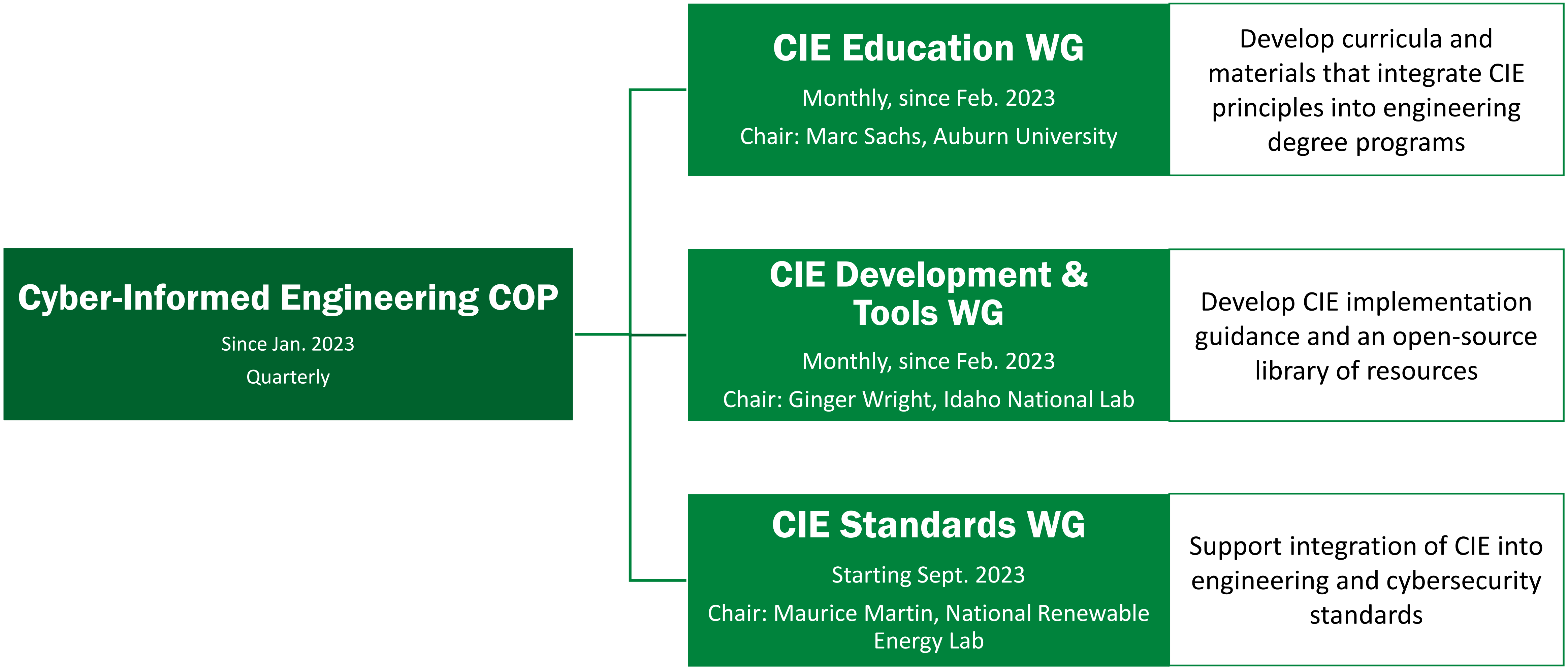
Purchasing-Selling Purchasing-Selling Entity

Distribution Distribution Provider

NERC. *Functional Model Technical Document*. 2018

Moving Forward

Working Groups



Cyber-Informed Engineering COP

Since Jan. 2023

Quarterly

CIE Education WG

Monthly, since Feb. 2023

Chair: Marc Sachs, Auburn University

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

CIE Development & Tools WG

Monthly, since Feb. 2023

Chair: Ginger Wright, Idaho National Lab

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

CIE Standards WG

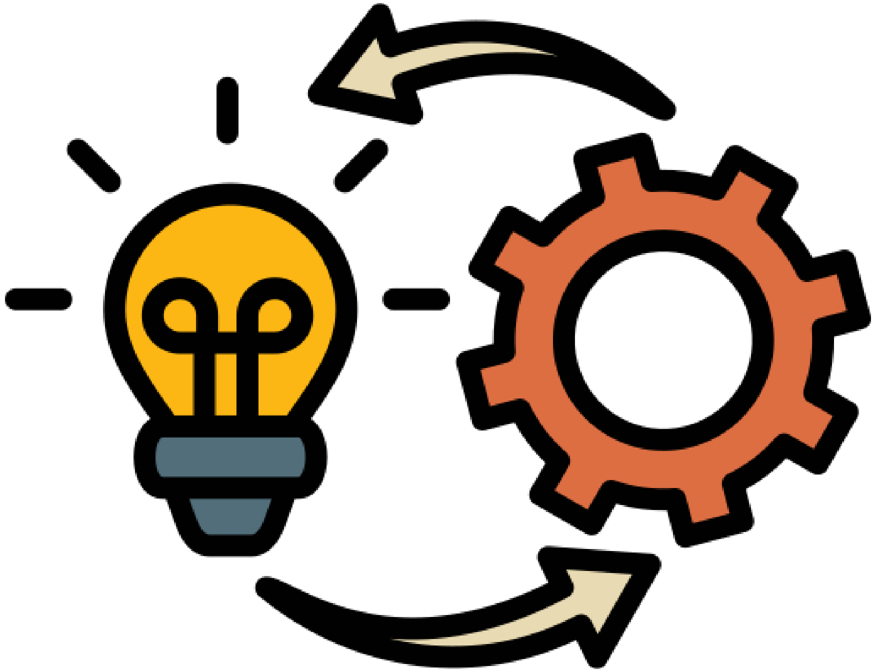
Starting Sept. 2023

Chair: Maurice Martin, National Renewable Energy Lab

Support integration of CIE into engineering and cybersecurity standards

Implementation Guide

- Guidance to help an organization **assess their application of CIE principles** in whatever framework or standards they follow
- Organized as a **series of questions** across the systems engineering lifecycle phases, for each principle
- Public release planned for **this fall**



Save the Date!

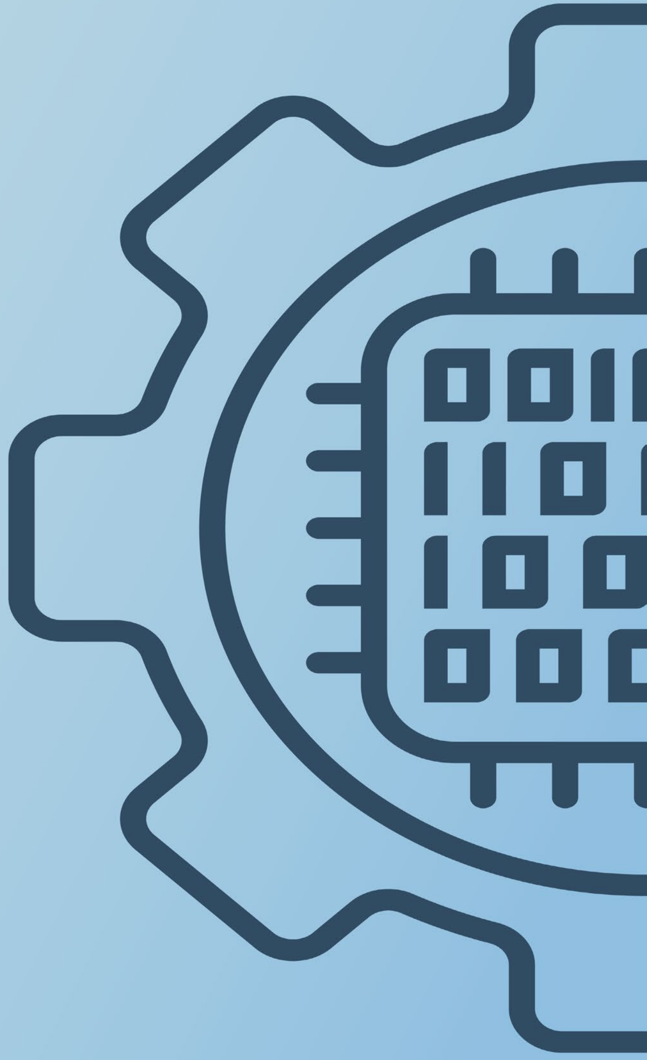
IEEE PES Power & Energy Society® | IEEE

Cyber-Informed Engineering Practitioner's Workshop

Save the Date

Sept. 6, 2023

11am - 5pm ET



Questions?

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

https://inl.gov/cie/