March 23, 2023

Sam Chanoski

Technical Relationship Manager

Idaho National Laboratory Energy Cybersecurity Programs Update

NERC RSTC Security Groups Summit

Idaho National Laboratory

INL/MIS-23-71834

INL’s Position Nationally

Network of 17 DOE National Laboratories

Center for National Security & Clean Energy

Lead Laboratory for Nuclear Energy R&D

Labs are Capability Machines

Labs innovate to solve multi-disciplinary problems

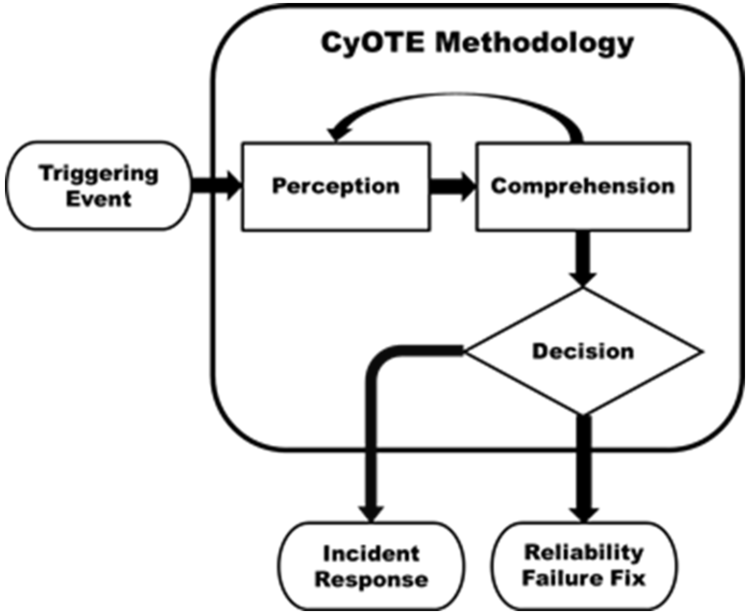
Do what others can’t, won’t, or shouldn’t do

Cybersecurity for the Operational Technology Environment (CyOTE)

Cybersecurity for Operational Technology Environments (CyOTE™)

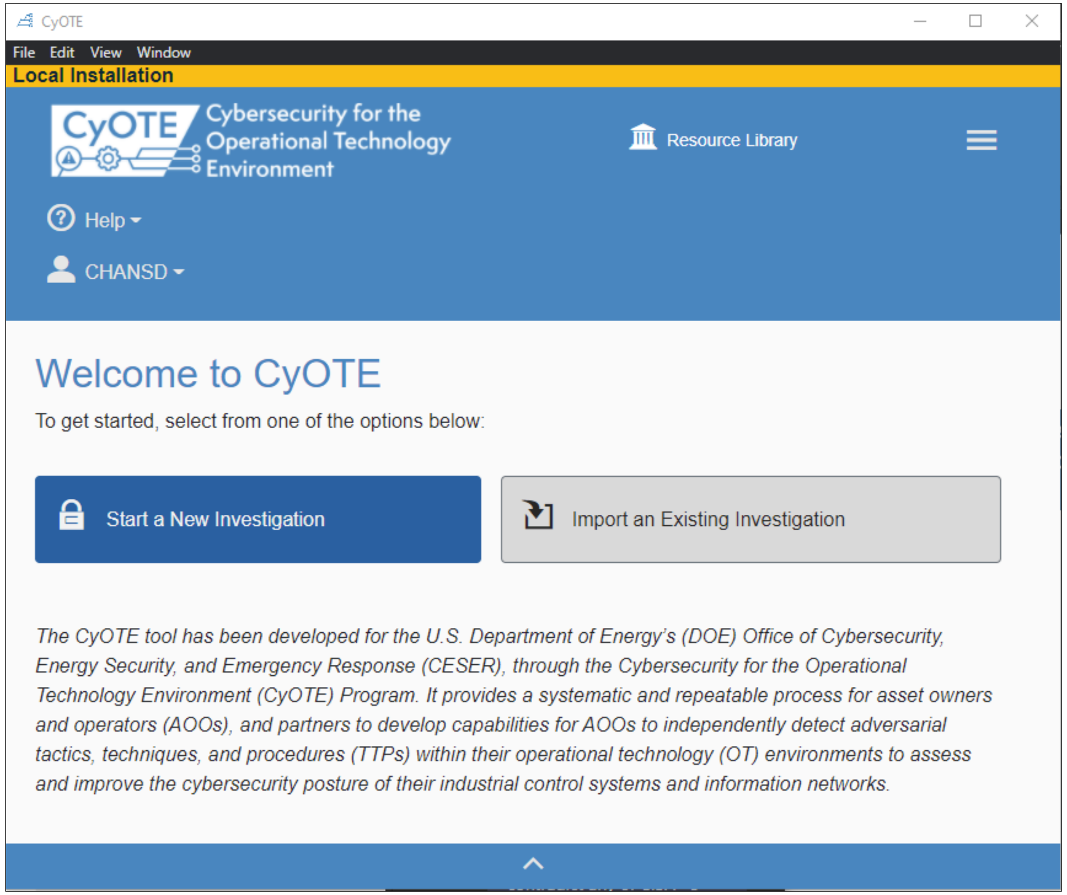
- Continuing to produce **Precursor Analysis Reports** identifying observables and artifacts correlated to adversary techniques
- Job aid **Application tool** in beta testing
  - Anticipate industry release in the next month
- **”Alexandria” library of observables** in development
  - Anticipate industry release in late 2023
- For more information: https://inl.gov/cyote/

CyOTE Cybersecurity for the Operational Technology Environment



CyOTE Application

- Structured job aid to implement CyOTE methodology
  - Real-world investigation
  - Post-mortem review
  - Exercises
- Provides suggestions and produces documentation
- Similar look and feel to CSET


CyOTE
File Edit View Window
Local Installation
CyOTE Cybersecurity for the Operational Technology Environment
Resource Library
Help
CHANSD
Start a New Investigation
Import an Existing Investigation

Welcome to CyOTE

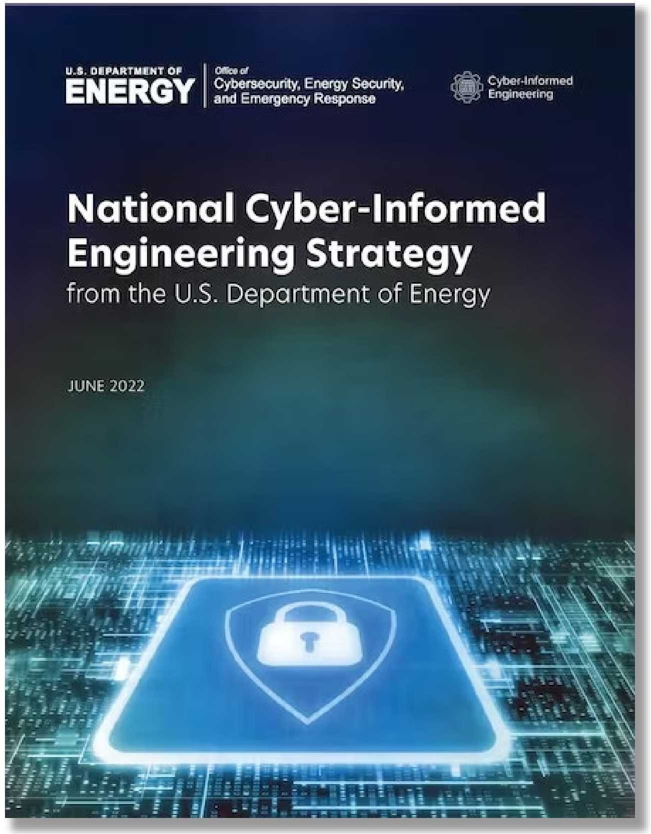
To get started, select from one of the options below:

The CyOTE tool has been developed for the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), through the Cybersecurity for the Operational Technology Environment (CyOTE) Program. It provides a systematic and repeatable process for asset owners and operators (AOOs), and partners to develop capabilities for AOOs to independently detect adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments to assess and improve the cybersecurity posture of their industrial control systems and information networks.

Cyber-Informed Engineering (CIE)

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.
- For more information: https://inl.gov/cie/



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

Key Premises of the CIE Strategy

Today's risk landscape calls for systems that are engineered to continue operating critical functions while faced with increasingly severe and sophisticated cyber attacks from intelligent, determined adversaries.

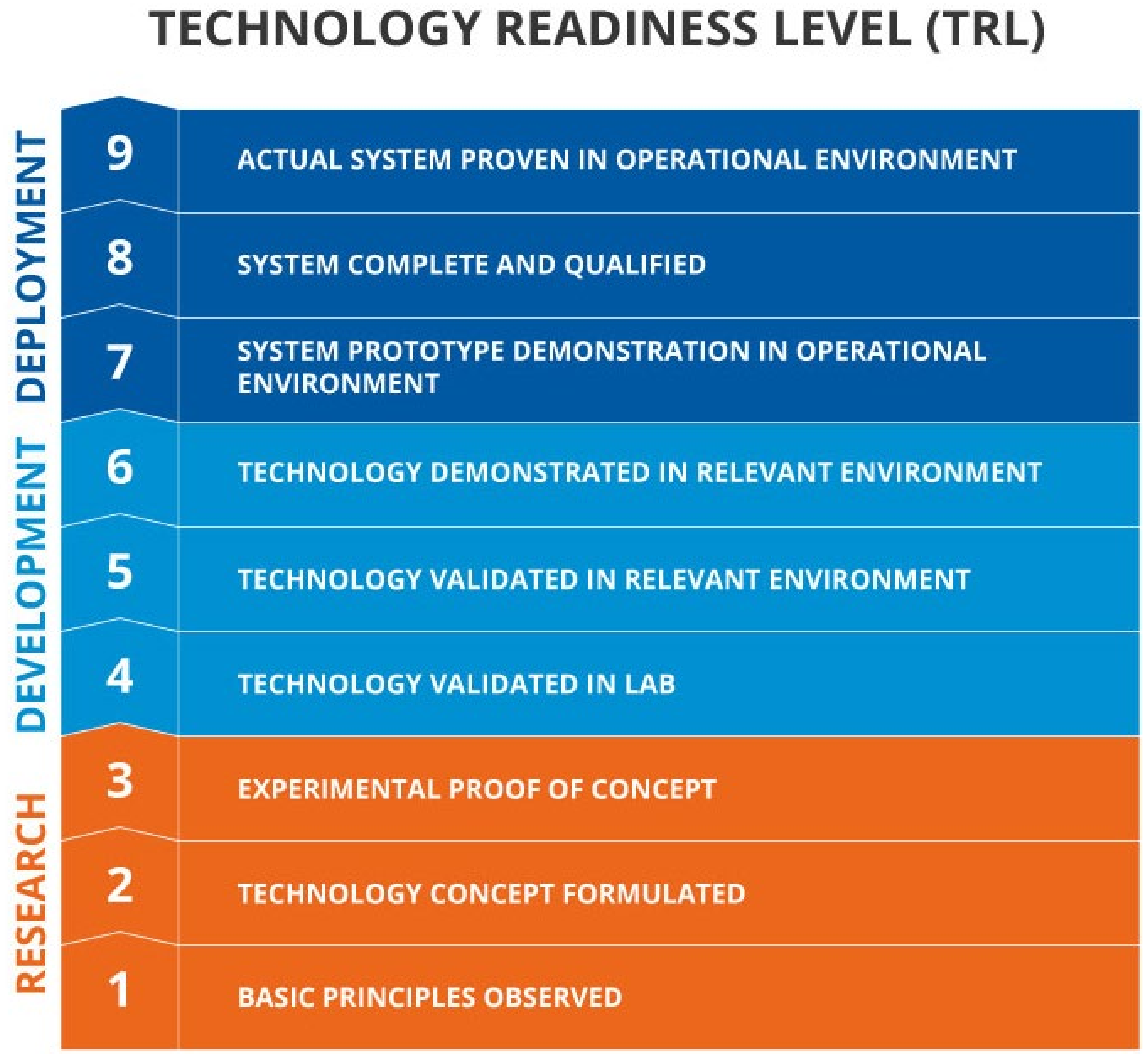
While specialized IT and OT cybersecurity experts bring strong skills, **many engineers and technicians who design and operate control systems with digital components currently lack sufficient cybersecurity education** and training to adequately address the risk of cyber-enabled sabotage, exploitation, failure, and misuse in the design, development, and operational lifecycle.

Accelerating industry's adoption of a culture of cybersecurity by design—complementing industry's strong culture of safety—offers the ability to maintain secure design even as systems evolve and grow in functionality.

CIE offers an opportunity to reduce risk across the entire device or system lifecycle, starting from the earliest possible phase of design.

Early in the design phase is often the most optimal time to achieve low cost and effective cybersecurity, compared to solutions introduced late in the engineering lifecycle.

CIE and Technology Readiness Levels

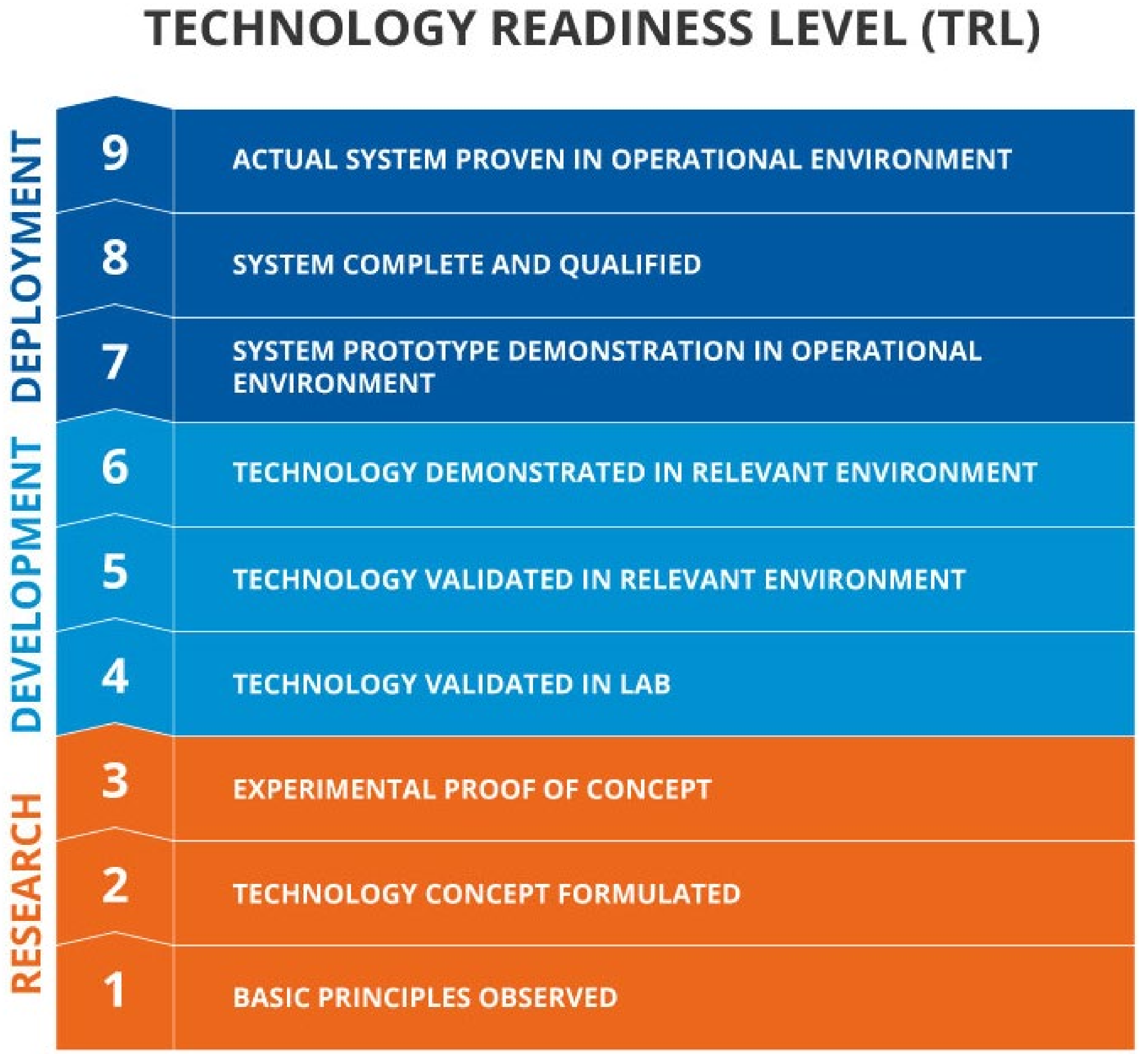


TECHNOLOGY READINESS LEVEL (TRL)

DEPLOYMENT	9	ACTUAL SYSTEM PROVEN IN OPERATIONAL ENVIRONMENT
	8	SYSTEM COMPLETE AND QUALIFIED
	7	SYSTEM PROTOTYPE DEMONSTRATION IN OPERATIONAL ENVIRONMENT
DEVELOPMENT	6	TECHNOLOGY DEMONSTRATED IN RELEVANT ENVIRONMENT
	5	TECHNOLOGY VALIDATED IN RELEVANT ENVIRONMENT
	4	TECHNOLOGY VALIDATED IN LAB
RESEARCH	3	EXPERIMENTAL PROOF OF CONCEPT
	2	TECHNOLOGY CONCEPT FORMULATED
	1	BASIC PRINCIPLES OBSERVED

Traditional OT Cybersecurity risk mitigations are usually applied here…

CIE and Technology Readiness Levels



TECHNOLOGY READINESS LEVEL (TRL)

DEPLOYMENT

9 ACTUAL SYSTEM PROVEN IN OPERATIONAL ENVIRONMENT

8 SYSTEM COMPLETE AND QUALIFIED

7 SYSTEM PROTOTYPE DEMONSTRATION IN OPERATIONAL ENVIRONMENT

DEVELOPMENT

6 TECHNOLOGY DEMONSTRATED IN RELEVANT ENVIRONMENT

5 TECHNOLOGY VALIDATED IN RELEVANT ENVIRONMENT

4 TECHNOLOGY VALIDATED IN LAB

RESEARCH

3 EXPERIMENTAL PROOF OF CONCEPT

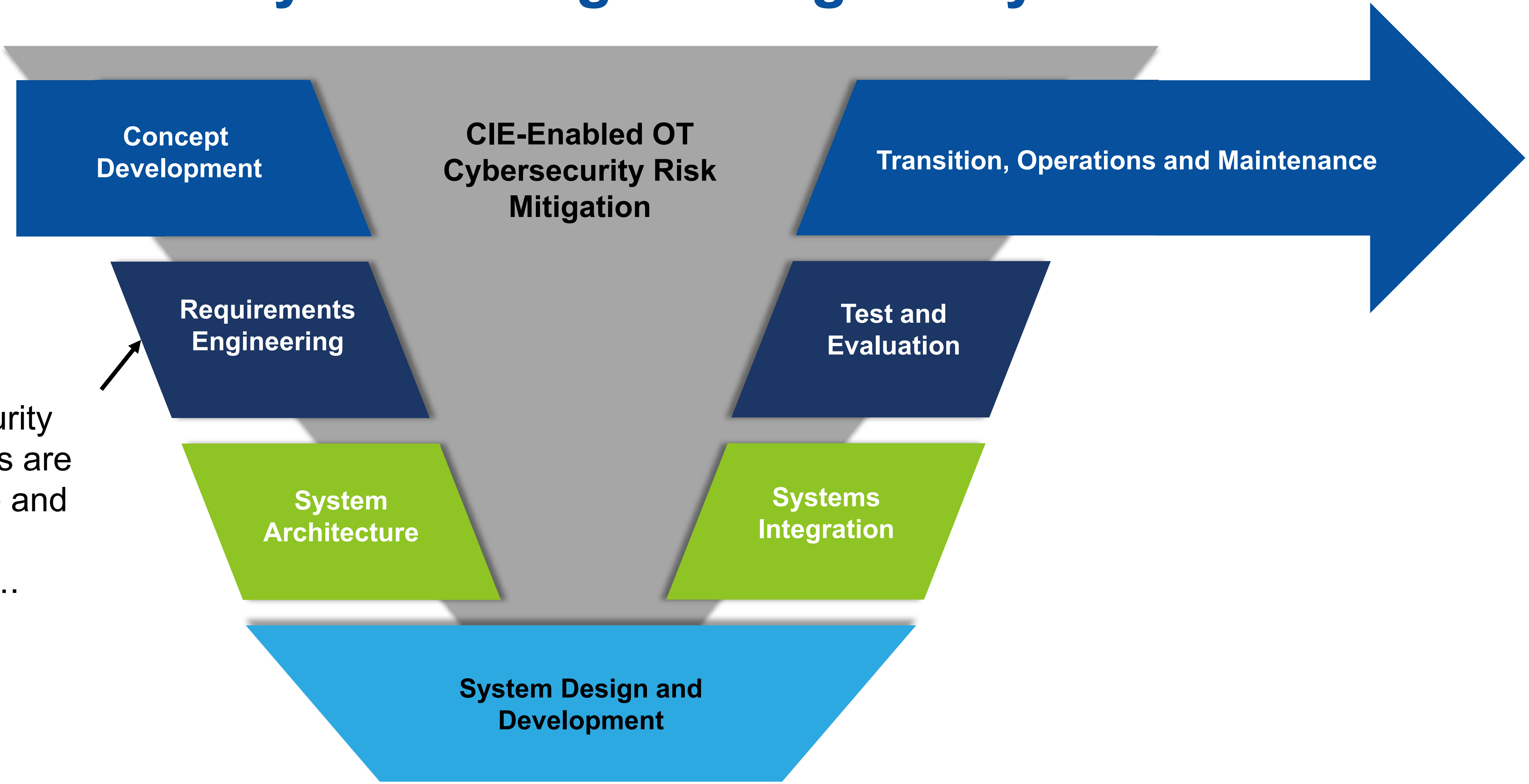
2 TECHNOLOGY CONCEPT FORMULATED

1 BASIC PRINCIPLES OBSERVED

Traditional OT Cybersecurity risk mitigations are usually applied here…

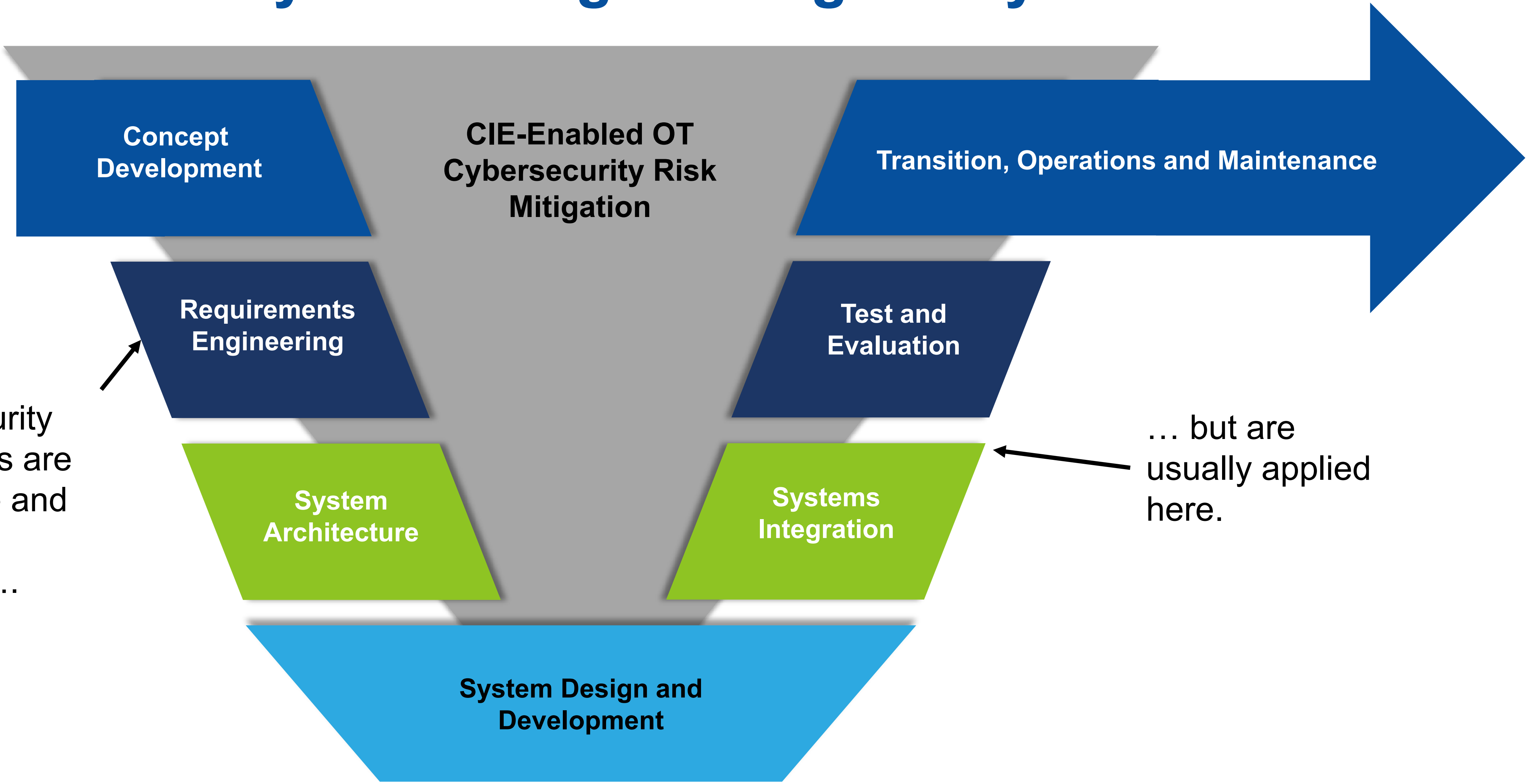
… but are more effective and efficient when applied here.

CIE and the Systems Engineering Lifecycle


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

OT Cybersecurity risk mitigations are more effective and efficient when applied here….

CIE and the Systems Engineering Lifecycle


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

OT Cybersecurity risk mitigations are more effective and efficient when applied here….

… but are usually applied here.

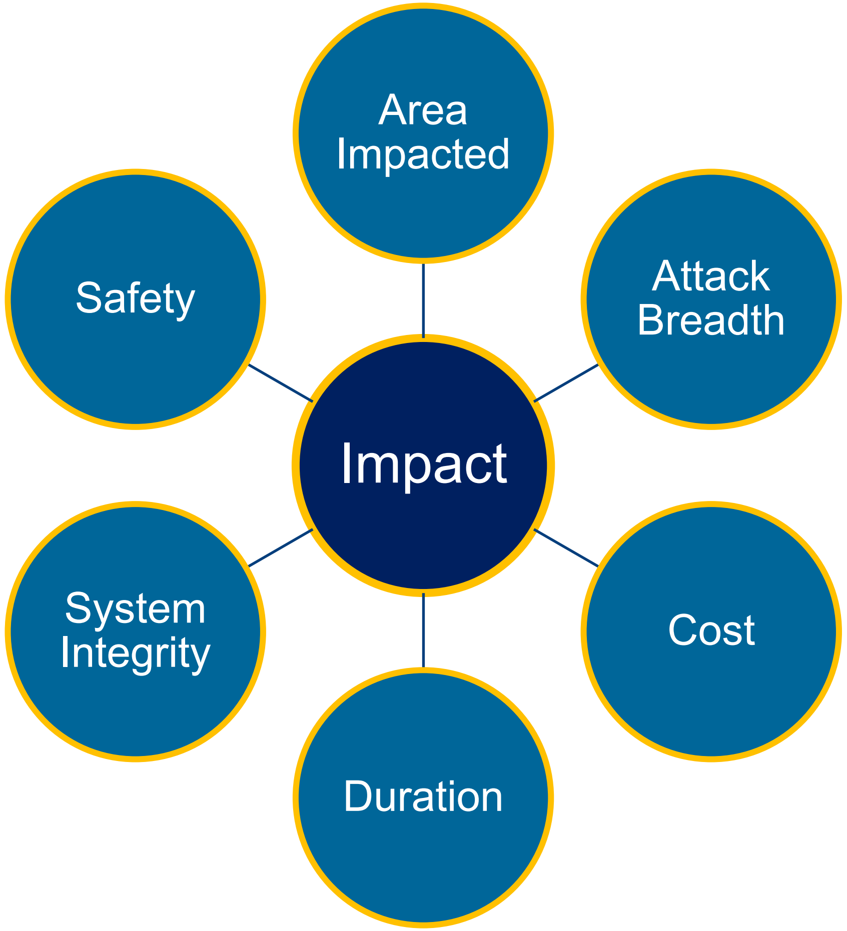
Principles of CIE

- **Consequence-focused design**
- Engineered Controls
- Secure information architecture
- Design Simplification
- Resilient layered defenses
- Active defense

- Interdependency evaluation
- Digital asset awareness
- **Cyber-secure supply chain controls**
- Planned resilience with no assumed security
- Engineering information control
- Security culture

Consequence-Focused Design

- What must happen?
- What must not happen?
- What governs my risk appetite?



Cyber-Secure Supply Chain

- Cyber security requirements must flow down to vendors, integrators, and third-party contractors
  - You are only as secure as your least secure vendor
- Procurement language must specify the exact requirements a vendor must comply with as part of the system design, build, integration, or support
- These requirements can raise procurement costs, but without them, caveat emptor
- Be aware of what a subcontractor leaves behind on your network
  - You don't know where subcontractor devices were before today
- Consider vendor tools such as calibration equipment or diagnostic equipment

Cybersecurity Procurement Language for Energy Delivery Systems

April 2014

Energy Sector Control Systems Working Group (ESCSWG)

Cyber Security Procurement Methodology, Rev. 1

ICAL REPORT

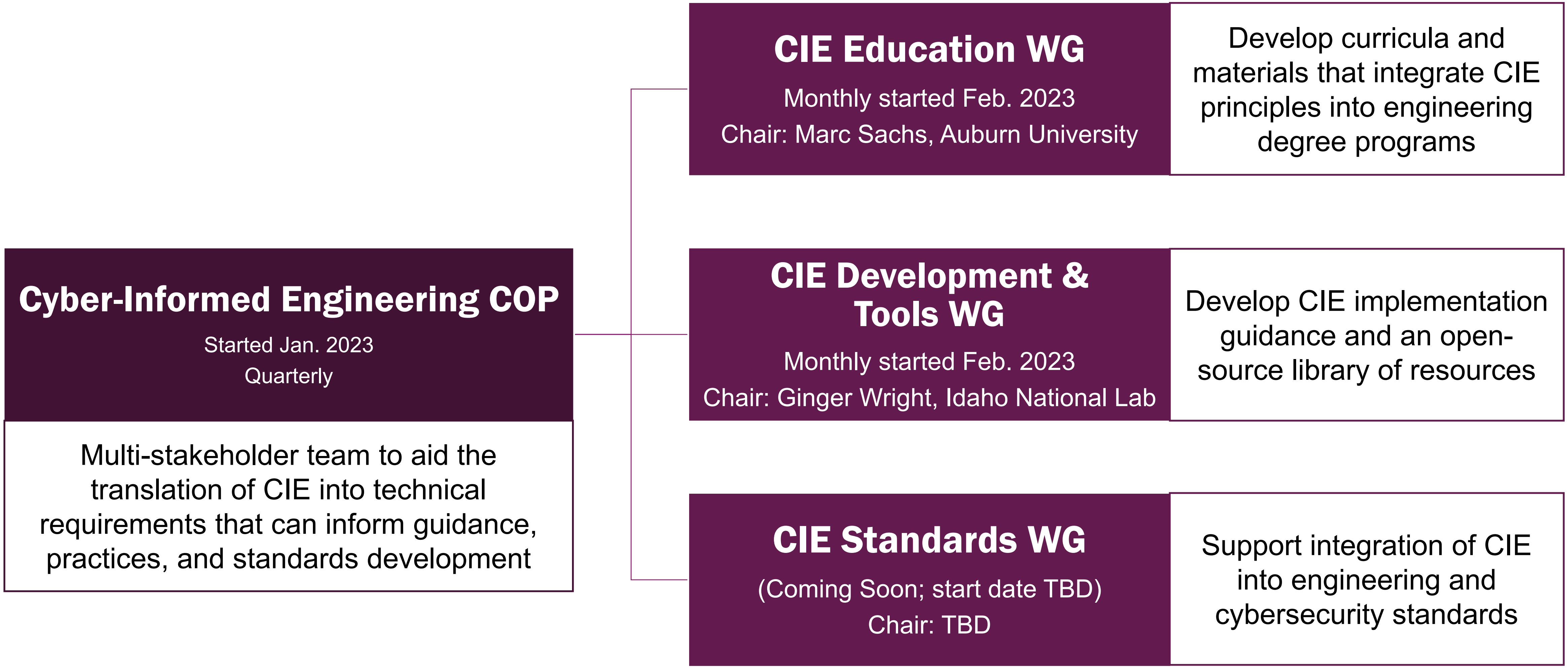
Department of Homeland Security: Cyber Security Procurement Language for Control Systems

September 2009

Homeland Security

Control Systems Security Program
National Cyber Security Division

CIE Community of Practice and Working Groups



Cyber-Informed Engineering COP

Started Jan. 2023

Quarterly

Multi-stakeholder team to aid the translation of CIE into technical requirements that can inform guidance, practices, and standards development

CIE Education WG

Monthly started Feb. 2023

Chair: Marc Sachs, Auburn University

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

CIE Development & Tools WG

Monthly started Feb. 2023

Chair: Ginger Wright, Idaho National Lab

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

CIE Standards WG

(Coming Soon; start date TBD)

Chair: TBD

Support integration of CIE into engineering and cybersecurity standards

Supply Chain Security

Cyber Testing for Resilient Industrial Control Systems (CyTRICS)

- Work with manufacturers and asset owners to discover, mitigate, and ultimately engineer out cyber vulnerabilities in digital components in energy sector critical supply chains
- Synergies with **Energy Cyber Sense Program** (IIJA, Section 40122)
- **SBOM Proof of Concept** for Energy Sector
- For more information: https://inl.gov/cytrics/

CyTRICS™

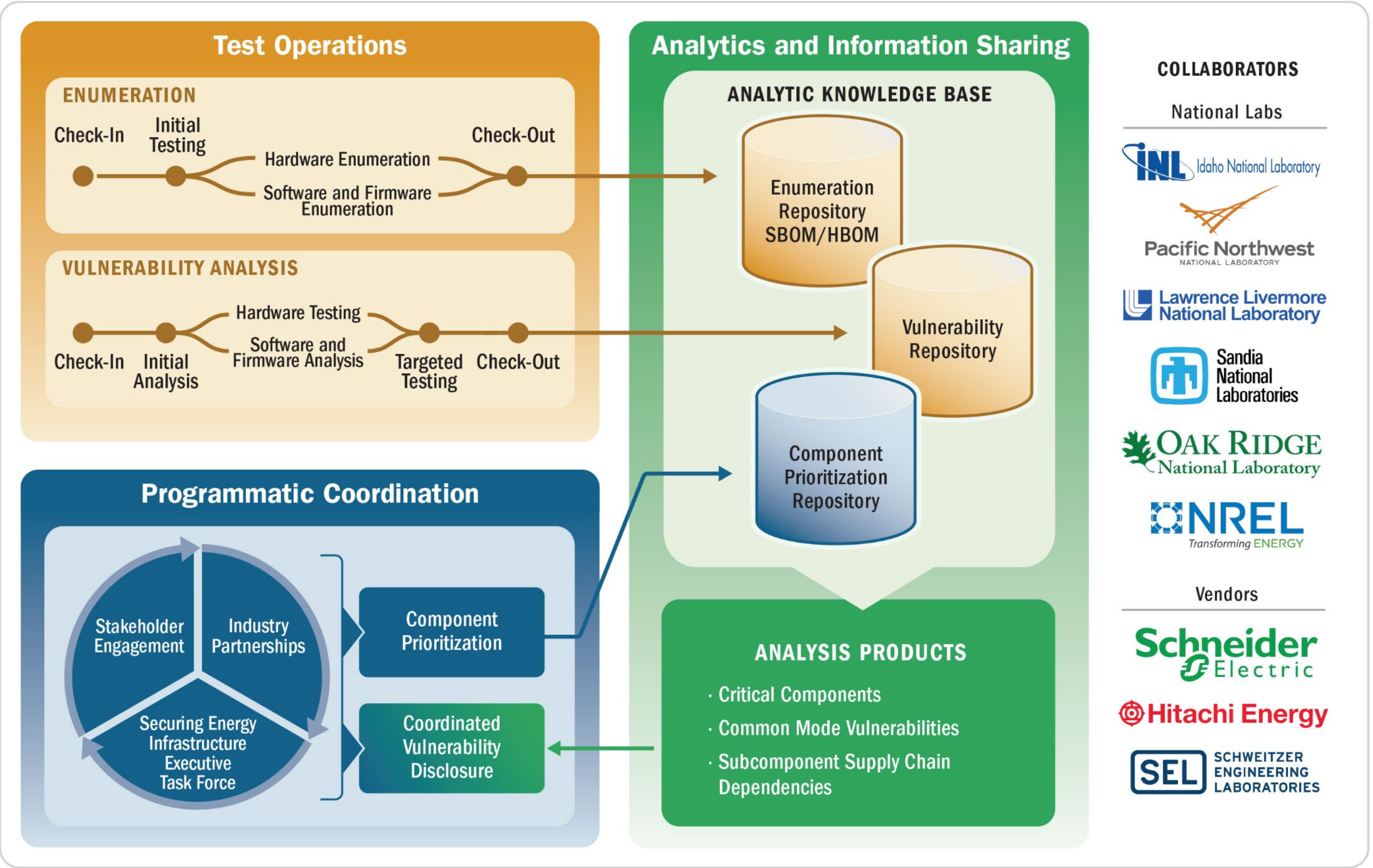
Cyber Testing for Resilient Industrial Control Systems

CyTRICS Program Overview

Standardized Repository and Reporting

Standardized Testing Process

Prioritization Methodology

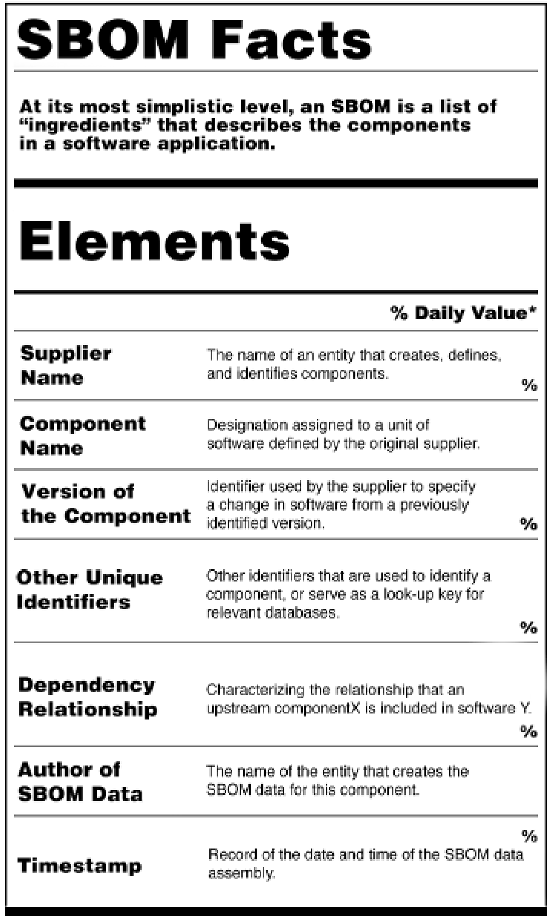

Test Operations
ENUMERATION
Check-In
Initial Testing
Hardware Enumeration
Software and Firmware Enumeration
Check-Out
VULNERABILITY ANALYSIS
Hardware Testing
Software and Firmware Analysis
Check-In
Initial Analysis
Targeted Testing
Check-Out
Programmatic Coordination
Stakeholder Engagement
Industry Partnerships
Securing Energy Infrastructure Executive Task Force
Component Prioritization
Coordinated Vulnerability Disclosure
Analytics and Information Sharing
ANALYTIC KNOWLEDGE BASE
Enumeration Repository SBOM/HBOM
Vulnerability Repository
Component Prioritization Repository
ANALYSIS PRODUCTS
· Critical Components
· Common Mode Vulnerabilities
· Subcomponent Supply Chain Dependencies
COLLABORATORS
National Labs
INL Idaho National Laboratory
Pacific Northwest NATIONAL LABORATORY
Lawrence Livermore National Laboratory
Sandia National Laboratories
Oak Ridge National Laboratory
NREL Transforming ENERGY
Vendors
Schneider Electric
Hitachi Energy
SEL SCHWEITZER ENGINEERING LABORATORIES

Multi-Laboratory Cooperation

Vendor Agreements

Energy Sector Software Bill of Materials Proof of Concept (SBOM POC)

- Started at NTIA, now a partnership between DOE CESER and DHS CISA
  - Broad and open participation
- S4x23 SBOM challenge: Five participants, three artifacts, three tasks
  - No "one tool to rule them all"
  - Firmware-based device enumeration is far less mature than software enumeration
  - VEX
  - Significant maturation year over year
- For more information: https://sbom.inl.gov/



SBOM Facts

At its most simplistic level, an SBOM is a list of "ingredients" that describes the components in a software application.

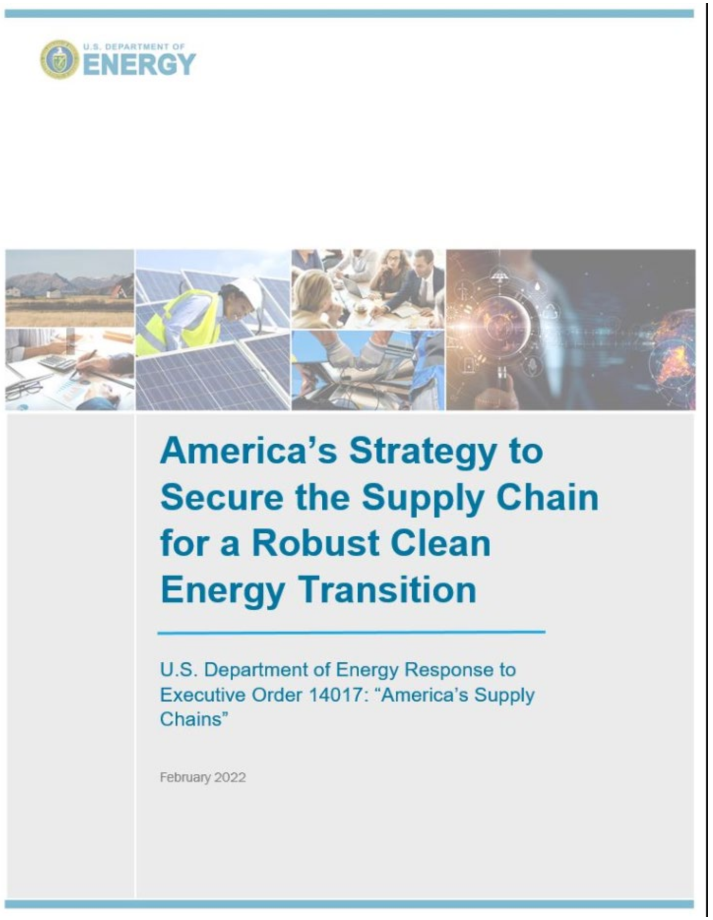
Elements

		% Daily Value*
Supplier Name	The name of an entity that creates, defines, and identifies components.	%
Component Name	Designation assigned to a unit of software defined by the original supplier.	
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.	%
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.	%
Dependency Relationship	Characterizing the relationship that an upstream componentX is included in software Y.	%
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.	
Timestamp	Record of the date and time of the SBOM data assembly.	%

https://soos.io/sbom-101-what-is-an-sbom-why-are-they-important

EO 14017 and Energy Cyber Sense

- Executive Order 14017 directives to strengthen the resilience of America’s supply chains
  - DOE strategy, 13 topical reports
- Bipartisan Infrastructure Law Section 40122 requires DOE to “establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, and for other purposes.”
  - Testing
  - Vulnerability reporting and tracking
  - Technical assistance
  - Guidance



U.S. DEPARTMENT OF ENERGY

America’s Strategy to Secure the Supply Chain for a Robust Clean Energy Transition

U.S. Department of Energy Response to Executive Order 14017: “America’s Supply Chains”

February 2022

Questions and Discussion

Sam Chanoski

Technical Relationship Manager | Cybercore Integration Center

samuel.chanoski@inl.gov | 404-904-2480

Idaho National Laboratory | Atlanta, GA

Idaho National Laboratory