Cyber-Informed Engineering

2025 CAE Community Symposium

Cyber-Informed Engineering

Dr. Sharon R. Hamilton, Norwich University
Dr. Shankar Banik, The Citadel
Dr. Ginger Wright, Cyber-Informed Engineering Program Manager, Idaho National Lab
Colin Chinn, Cyber Assurance & Resiliency, Savannah River National Laboratory

Contains public information about the Cyber-Informed Engineering program sponsored by DOE-CESER and performed by the Idaho National Laboratory and the National Renewable Energy Laboratory

Cybersecurity Threats are no longer Just Theoretical

Attackers May Be Coming for Your Plant. Time to Tighten Cyber Defenses.

The water and wastewater sectors are targets for a variety of cyber attacks. Some simple measures can go a long way to protect critical

Every "Thing" Everywhere All at Once

Every asset in an organization's inventory that is not accounted for and protected is a potential attack vector that an attacker can use to gain access or move undetected.

BY ANDY GREENBERG SECURITY APR 17, 2024 6:00 AM

Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities

Cyber Army of Russia Reborn, a group with ties to the Kremlin's Sandworm unit, is crossing lines even that notorious cyberwarfare unit wouldn't dare to.

Cybersecurity

US warns hackers are carrying out attacks on water systems

Russia-linked hackers claim cyberattacks on U.S., French and Polish water utilities

CYBERSECURITY ADVISORY

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Release Date: May 24, 2023 **Alert Code:** AA23-144a

Arkansas City water treatment facility hit by cyberattack

While disruptions are limited, the attack on the water treatment facility highlights how the critical infrastructure sector remains a popular target for threat actors.

By **Arielle Waldman,** News Writer Published: **24 Sep 2024**

Russian hackers breached, sabotaged Texas water treatment plant, cyber firm says

What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

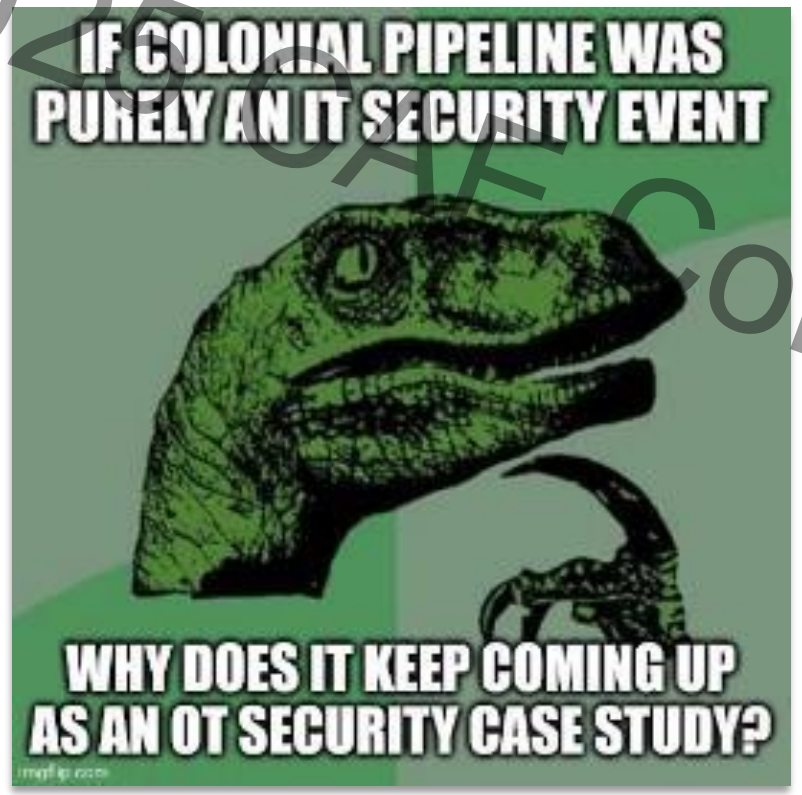
-- Cybersecurity and Infrastructure Security Agency (CISA)

What's missing in this picture?

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Cyber-Informed Engineering

Cybersecurity is not just about data and networks



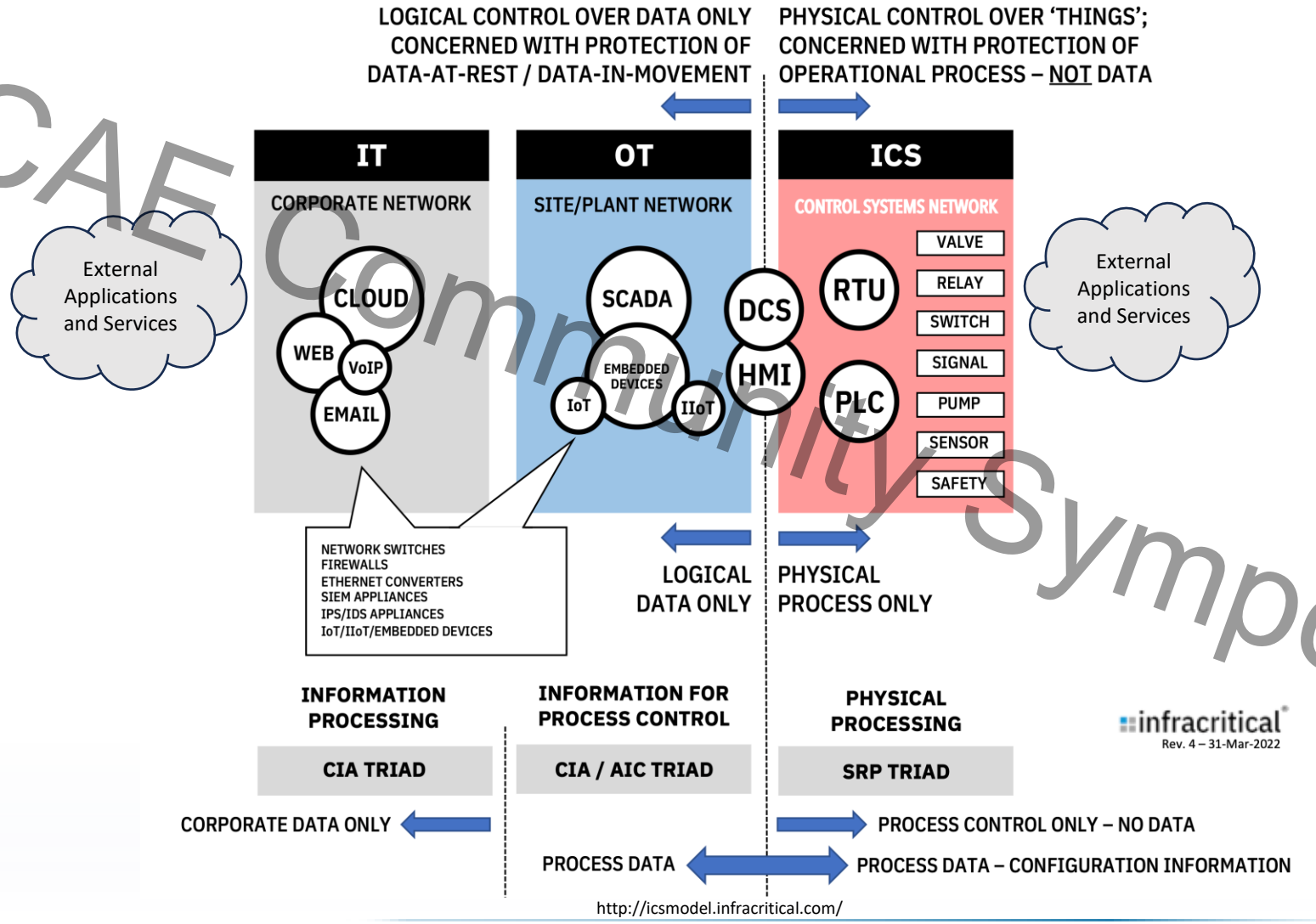
Joe Slowick, MITRE

- Ransomware attacked business data on an IT network
- However, pipeline operations were curtailed.
- Why?

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Operational Technology vs Information Technology

Confidentiality
Integrity
Availability



Safety
Reliability
Performance

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

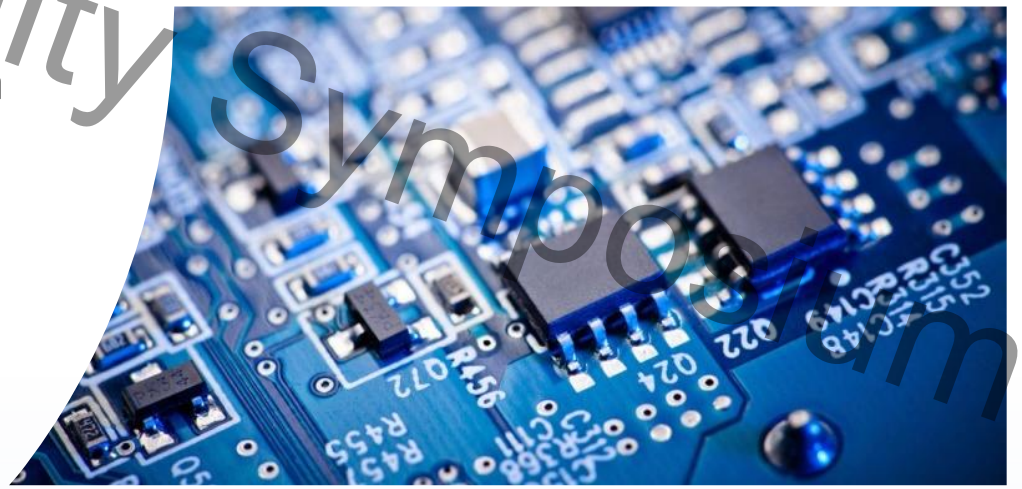
Cyber-Informed Engineering

2025 CAE Community Symposium

Introduction to Cyber-Informed Engineering

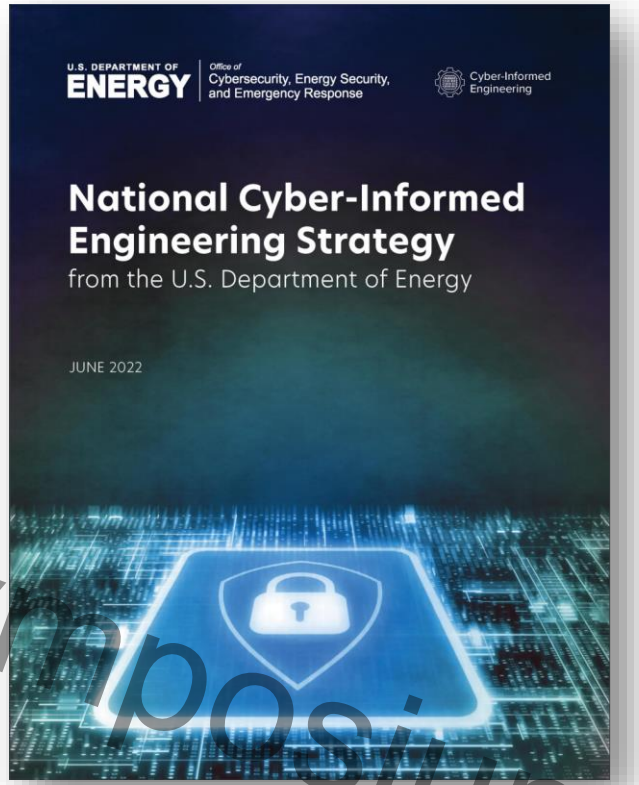
Cyber-Informed Engineering (CIE)

- 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 create a **culture of security** aligned with the existing industry safety culture.



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



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

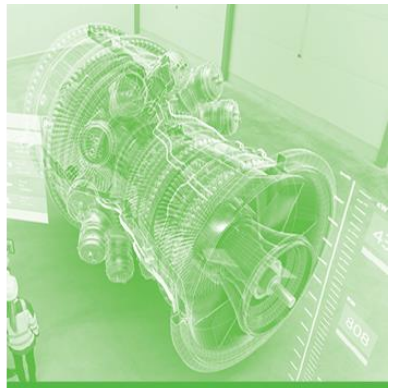
Embed CIE into formal education, training, and credentialing

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



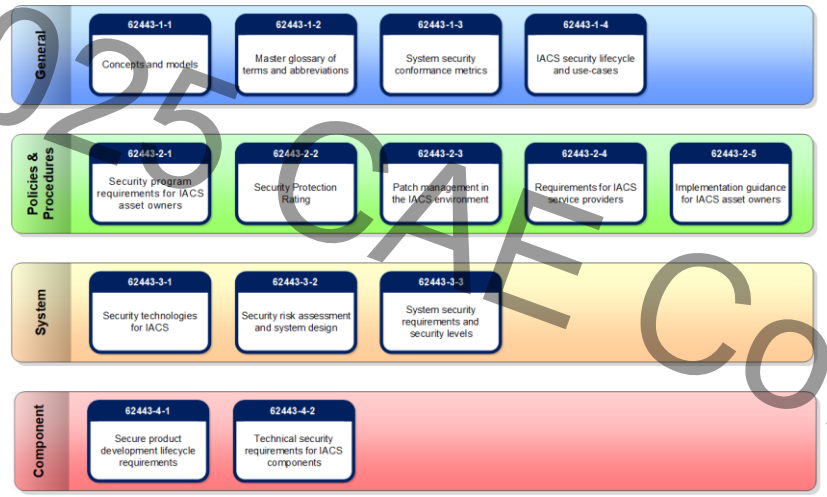
Future Infrastructure

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

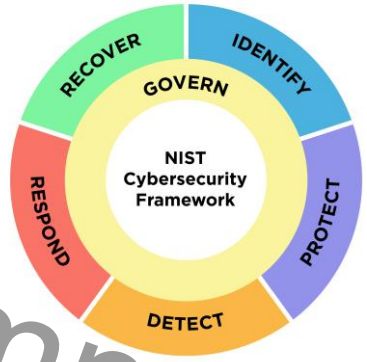
CIE Principles

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?

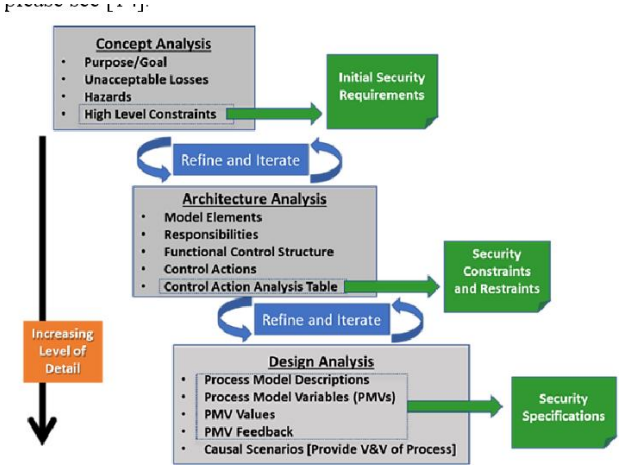
OK, But How Do You CIE?



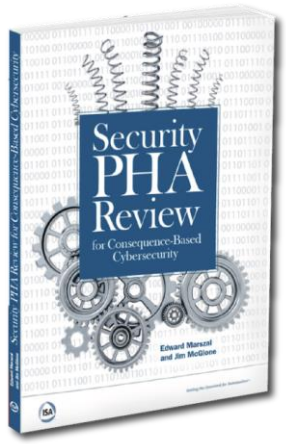
https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards

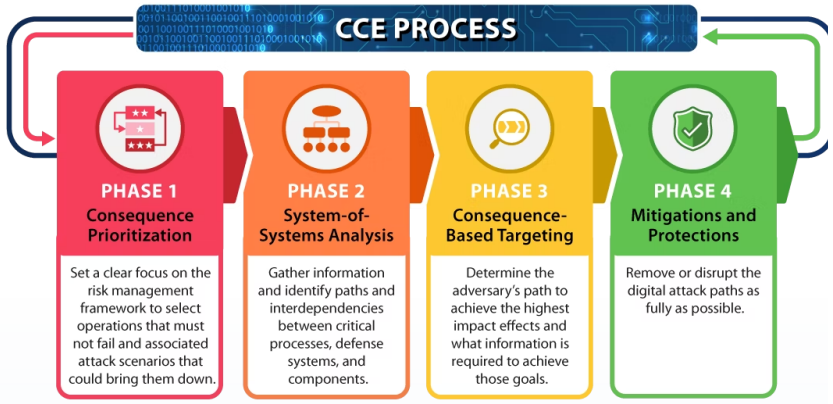


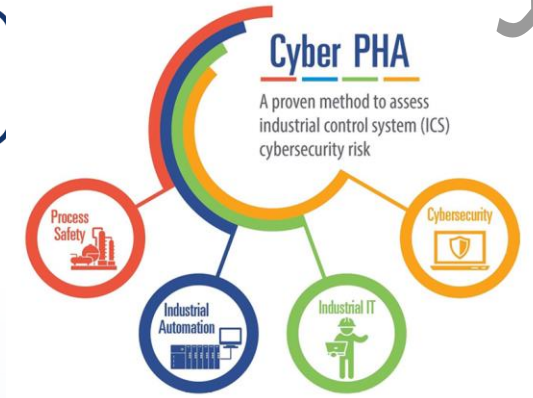
https://www.nist.gov/image/nist-cybersecurity-framework-20



https://incose.onlinelibrary.wiley.com/doi/epdf/10.1002/j.2334-5837.2021.00839.x







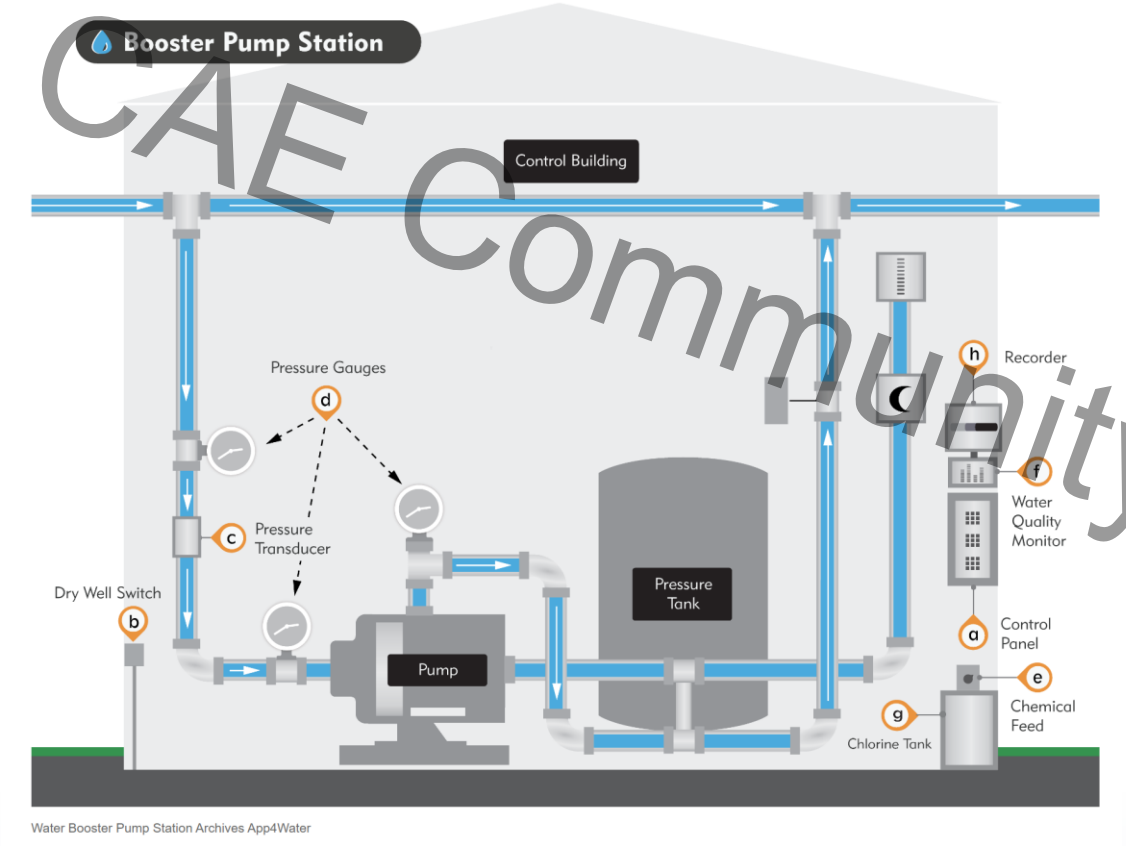
https://www.linkedin.com/pulse/cyber-pha-perfect-technique-ensure-your-safety-sis-kramer-mba/

2025 CAE Community Symposium

How does this work in practice?

Water Booster Pump Station

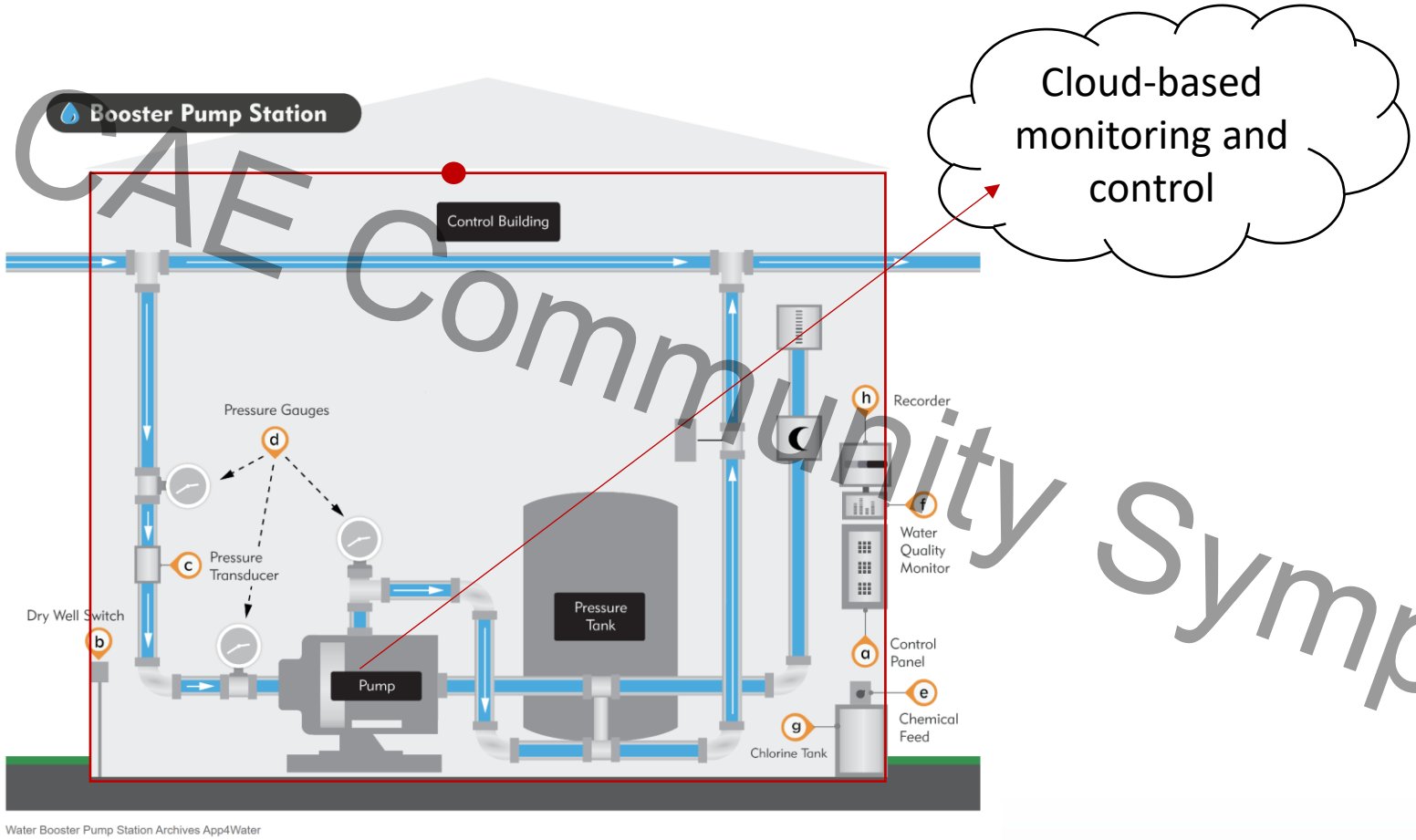
Water Booster Pump Station



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

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Water Booster Pump Station



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

Cloud-based monitoring and control

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Cyber Solution Review

- Control System Software has a qualifying secure development lifecycle.
  - Very mature demonstrated processes
  - Provided SBOM
  - Component infrastructure is up to date
  - Mature vulnerability release process – with regular patches
  - 24/7 Support availability

- Cloud provider is reputable and qualified
  - SOC Type 2 and Fedramp (if needed), great physical security
  - Very mature, experienced in hosting critical infrastructure services
  - Demonstrated response and restoration capabilities

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

IT Installation Review

- Network entry point has standard security package
- Monitoring and logging traffic on this interface according to standard practice
  - Logging interfaces with organizational logging system
- Traffic in and out is encrypted between the cloud provider and the internal network boundary

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Goal 1 –
Use CIE to Improve Energy Sector Cyber Resilience

Supporting Tools:

- CIE Strategy - https://www.energy.gov/sites/default/files/2022-06/FINAL DOE National CIE Strategy - June 2022_0.pdf
- CIE Implementation Guide - https://www.osti.gov/biblio/1995796
- Benefits Quantification Methodology - https://www.osti.gov/biblio/2480936
- Targeted R&D Guidance for CIE Principles - https://www.osti.gov/biblio/2448074
- CIE Guidance to Defeat Systemic Operational Technology Weaknesses - https://www.osti.gov/biblio/2481275
- Web-based Implementation Guide - https://github.com/inlguy/CIE/releases/tag/v12.2.4.0
- CIEMAT – CIE for Microgrids Tool - https://github.com/idaholab/CIEMAT/tree/main
- CIEBAT – CIE for Battery Energy Storage Systems Tool - https://github.com/idaholab/CIEBAT/tree/main
- Cyber-Informed Engineering Workbook: Microgrids - https://www.osti.gov/biblio/2315001
- Cyber-Informed Engineering Workbook: Substations - https://www.osti.gov/biblio/2448237
- Cyber-Informed Engineering Workbook: ADMS - https://www.osti.gov/biblio/2453879

Strategic Alignment:

Goal 2 –
Teach CIE Principles at Leading US Engineering Universities

Supporting Deliverables:

- CIE Curriculum Guide - https://www.osti.gov/biblio/2478665
- CIE Quarterly Webinar: What is Cyber-Informed Engineering? - https://www.youtube.com/watch?v=P4dpA7-vjig
- CIE Presentation: Water Booster Pump Station - https://www.osti.gov/biblio/2447693
- CIE Workbook: Water Booster Pump Station - https://www.osti.gov/biblio/2371031
- Engage Universities to Integrate Curriculum (Adoption Report) - https://www.osti.gov/biblio/2478666

Strategic Alignment:

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Goal 3 –
Incorporate CIE into International Digital Design and Engineering Standards

Supporting Deliverables:

- CIE Requirements Analysis Framework - https://www.nrel.gov/docs/fy25osti/90317.pdf
- Tool for Applying CIE at Varying Criticality Levels - https://www.osti.gov/biblio/2480935
- CIE Validation Methods - https://www.osti.gov/biblio/2480931

Strategic Alignment:

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

FY-24 Goal 4 –
Conduct CIE Outreach and Grow the Community of Practice

Key Outcome: Achievement of regular and consistent outreach and robust partnerships with key stakeholder groups to accelerate implementation

Supporting Deliverables:

- CIE Outreach
  - 22 conference presentations, panels, or workshops
- Support CIE COP and Working Groups
  - 290 COP members
  - 3 Working Groups met 32 times
- CIE Success Stories

Strategic Alignment:

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

2025 CAE Community Symposium

What's Ahead for CIE:

FY25 Scope

FY-25 Goal 1 –
Use CIE to Improve Energy Sector Cyber Resilience

Key Outcome: Continued engagement to apply CIE to critical energy systems being deployed on the US grid, especially the systems and supply chains of systems being added to the grid to serve new energy functions and creating and updating tools and guidance to aid those applying CIE. Additionally, engagement with DOE research, development, and deployment programs desiring Cyber-Informed Engineering integration.

Supporting Deliverables:

- CIE Adoption Pathway
- CIE Procurement Strategies
- Cyber-Informed Sensor Placement
- Engineering Controls Database
- Model-Based Systems Engineering
- CIE for Process Control and Optimization
- CIE for Process Automation
- CIE-Based Control and Optimization Algorithms
- Cyber Conservative Operations
- CIE Engagements with Asset Owners

Strategic Alignment:

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Cyber-Informed Engineering

FY-25 Goal 2 –
Teach CIE Principles at Leading US Engineering Universities

Key Outcome: Expand work with universities and educational institutions to add CIE into the engineering and technical curriculum at more US universities and to develop an initial capability for a student competition to apply CIE to engineering infrastructure.

Supporting Deliverables:

- CIE Curriculum Advancement
- CIE Centers of Academic Excellence
- Professional Engineers (PE) CIE Enhancement
- Lab-Based Assessment Use Cases for CIE-Based Mitigation Strategies
- CyberForce-Style CIE Student Competitions

Strategic Alignment:

Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Cyber-Informed Engineering

FY-25 Goal 3 –
Incorporate CIE into International Digital Design Standards

Key Outcome: Continue collaboration with standards organizations to build CIE into the standards that guide the development and deployment of secure energy infrastructure with the goal of publishing white papers, examples, and working with accreditation bodies to add CIE into engineering.

Supporting Deliverables:

- Advance Integration of CIE into Existing Standards
  - Establish CIE Presence within Governing Bodies of Standards
  - CIE Standards Case Study White Paper
  - CIE Standards Quick Start Guide
- Process Hazard Analysis and CIE
- CIE Requirements Analysis Use Cases

Strategic Alignment:

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

Email CIE@inl.gov to request membership to any or all