Operational Technology at Risk: Building a High-Assurance Future with the Pitt's Cyber Energy Center

Daniel G. Cole
Swanson School of Engineering

Greater PGH CISO Group

28 October 2025

University of Pittsburgh | Cyber Energy Center

Ex-CISA head thinks AI might fix code so fast we won't need security teams

Jen Easterly says most breaches stem from bad software, and smarter tech could finally clean it up

Joe Fay

Mon 27 Oct 2025 // 11:43 UTC

Ex-CISA head Jen Easterly claims AI could spell the end of the cybersecurity industry, as the sloppy software and vulnerabilities that criminals rely on will be tracked down faster than ever.

Speaking at AuditBoard's user conference in San Diego, Easterly said the threat landscape has never stopped evolving.

The proliferation of data, platforms, and devices meant "we've expanded the attack surface for cyber threat actors like China and Russia and Iran and North Korea and gangs of cybercriminals." Easterly said that if cybercrime was a country, it would be the third biggest in the world, just behind the US and China.

Cybersecurity is no longer just about protecting data—it's about securing the machines and systems that power our critical infrastructure

TECH + ENGINEERING

Cyber Attack on German Steel Mill Leads to 'Massive' Real World Damage

A steel mill in Germany lost control of its blast furnace. Hackers had infiltrated the mill's control system, according to the German government's office for information security.

BY R.A. BECKER THURSDAY, JANUARY 8, 2015 NOVA NEXT

Energy | Data Privacy | Regulatory Oversight | Governance | Grid & Infrastructure

US electric grid growing more vulnerable to cyberattacks, regulator says

By **Laila Kearney**

April 4, 2024 5:48 PM EDT · Updated 11 days ago

Updated

Foreign hackers breached a US nuclear weapons plant via SharePoint flaws

News Analysis

Oct 20, 2025 • 8 mins

Cyberattacks | Data Breach | Government IT

A foreign actor infiltrated the National Nuclear Security Administration's Kansas City National Security Campus through vulnerabilities in Microsoft's SharePoint browser-based app, raising questions about the need to solidify further federal IT/OT security protections.

University of Pittsburgh | Cyber Energy Center

CISA defines 16 critical infrastructure sectors vital to the U.S., whose disruption would severely impact national security, the economy, or public health and safety


Chemical sector


Commercial Facilities Sector


Communications Sector


Critical Manufacturing Sector


Dams Sector


Defense Industrial Base Sector


Emergency Services Sector


Energy Sector


Financial Services Sector


Food and Agriculture Sector


Government Services and Facilities Sector


Healthcare and Public Health Sector


Information Technology Sector


Nuclear Reactors, Materials, and Waste Sector


Transportation Systems Sector


Water and Wastewater Systems

University of Pittsburgh® | Cyber Energy Center

Operational technology (OT) refers to hardware and software systems that monitor and control physical devices, processes, and infrastructure

SOC

IT/OT convergence

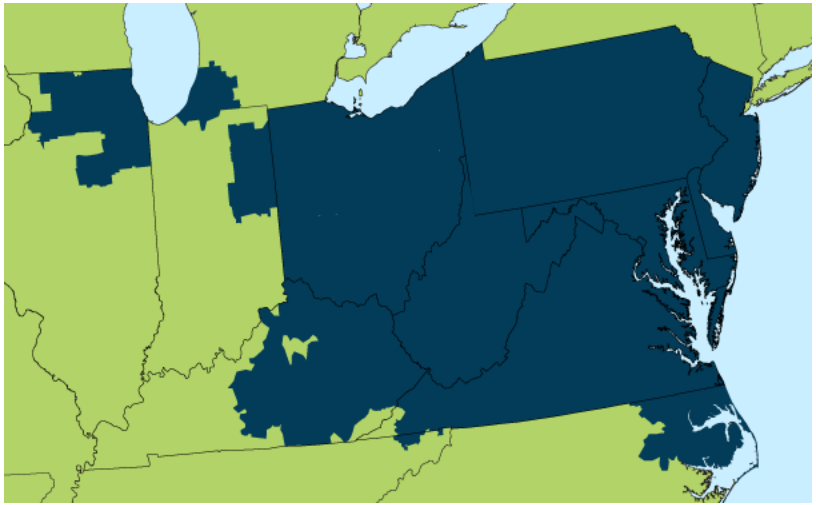
Operational technology


CYBER
ENERGY
CENTER

The goal of the project is to ...

- create a Cyber Energy Center based at Pitt that will
- produce a collaborative ecosystem for regional energy industries and stakeholders,
- enhance educational opportunities for cybersecurity technologists and professionals, and
- improve cybersecurity for the region's energy system.

The Center brings together regional industry and university researchers to drive innovation for new cybersecurity capabilities



Security vendors	
GrayMatter	Cybersecurity, OT
MxD	Cybersecurity, OT
Energy systems	
Eaton Corporation PLC	Energy systems
MEPPI	Energy systems
Siemens	Energy systems
Westinghouse	Energy systems, nuclear power
Energy	
EQT Corp.	Energy, natural gas
PJM Interconnection LLC	Energy, RTO
Duquesne Light DLC	Energy, utility
ICS/SCADA	
Emerson	ICS and SCADA systems
Digital Twins	
ANSYS Digital Twins	Simulation and digital twins
FFRDC	
INL	Cybersecurity, energy
Sandia	Cybersecurity, energy

University of Pittsburgh | Cyber Energy Center

Intrusion Detection and Tolerance

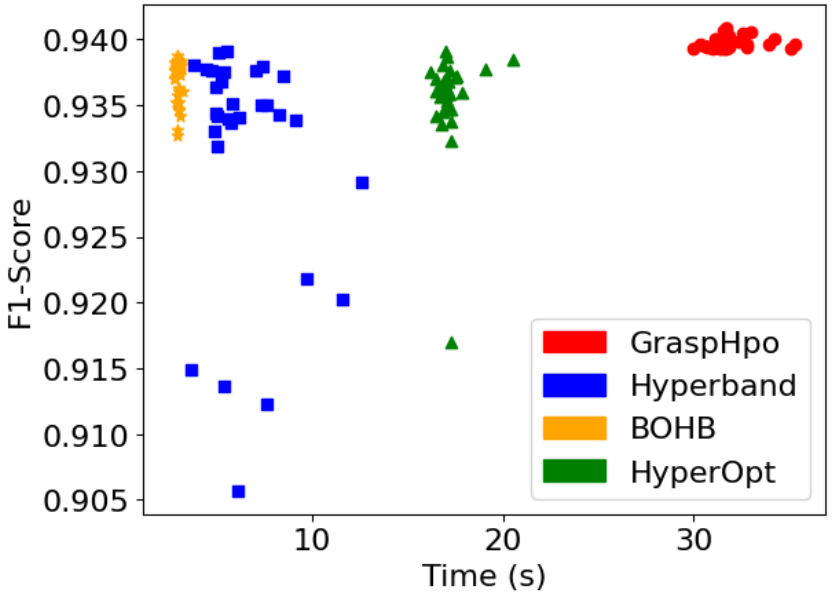
Intrusion detection is the ability to determine if an intrusion to the OT system has occurred.

Intrusion tolerance is the ability to continue to operate correctly while partially compromised.

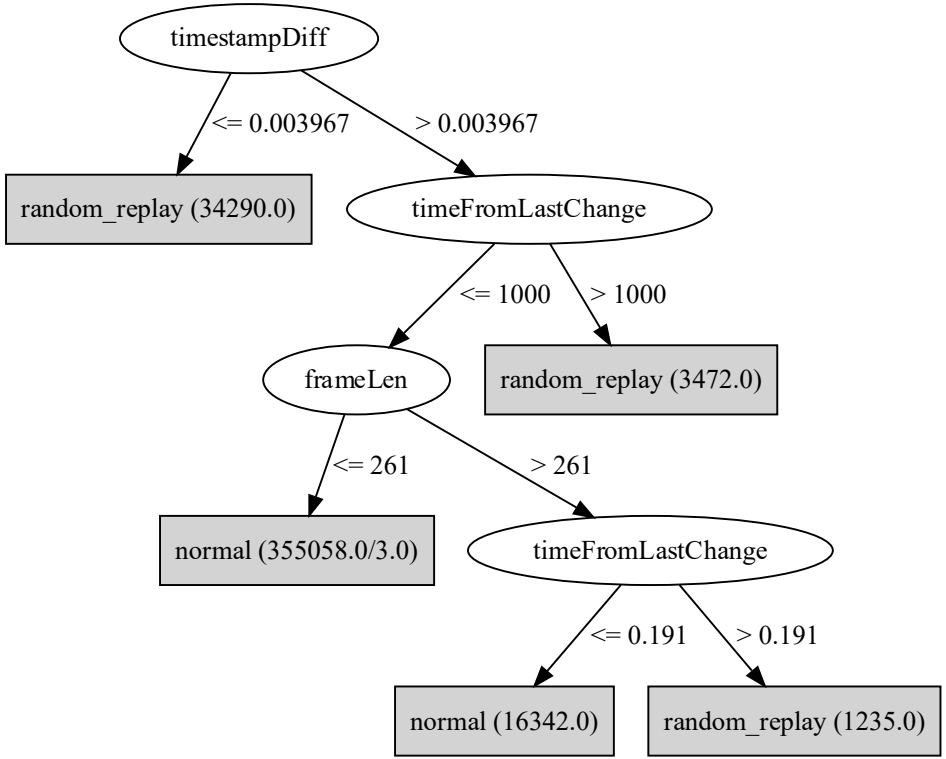
Challenges exist for both processing the large amounts of data that can come from modern OT systems and the means for managing system architecture to ensure tolerance. Digital twins provide useful tools to address both challenges.

Generating synthetic and realistic datasets helps develop machine-learning-based Intrusion Detection Systems

Hyperparameter Optimization



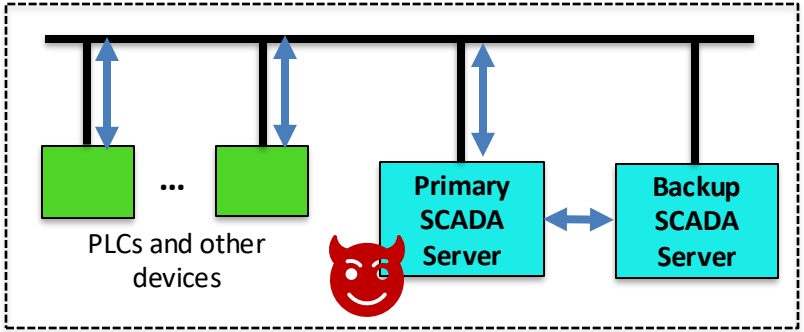
Explainable ML IDS model



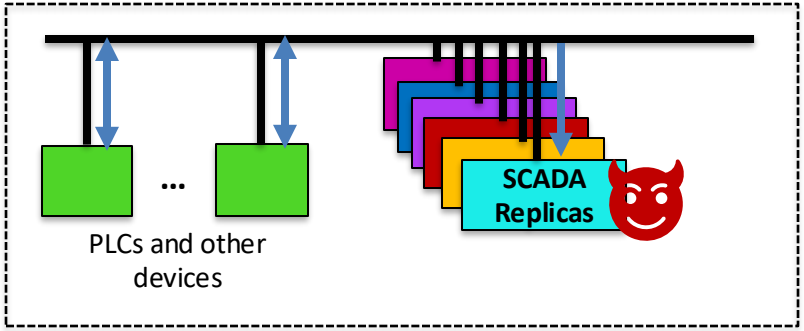
University of Pittsburgh | Cyber Energy Center

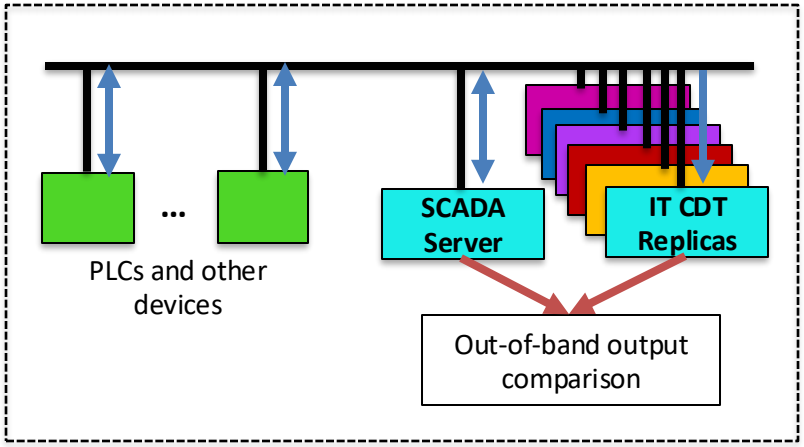
CDTs will enable us to transition today's vulnerable SCADA systems to intrusion-tolerant architectures

Today's systems are vulnerable to cyberattacks



We know how to build more resilient systems



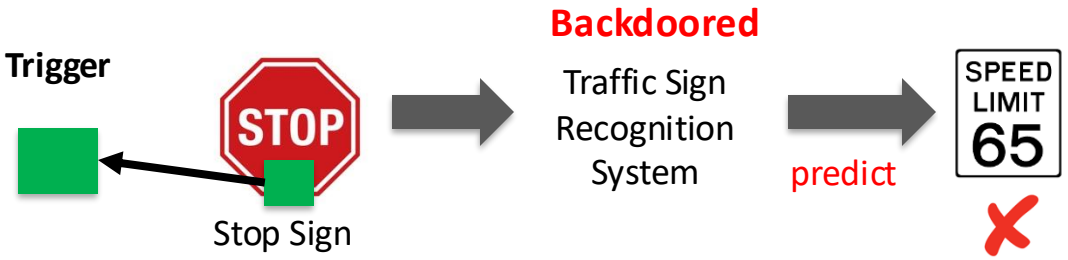


CDTs can provide a safe transition and upgrade path

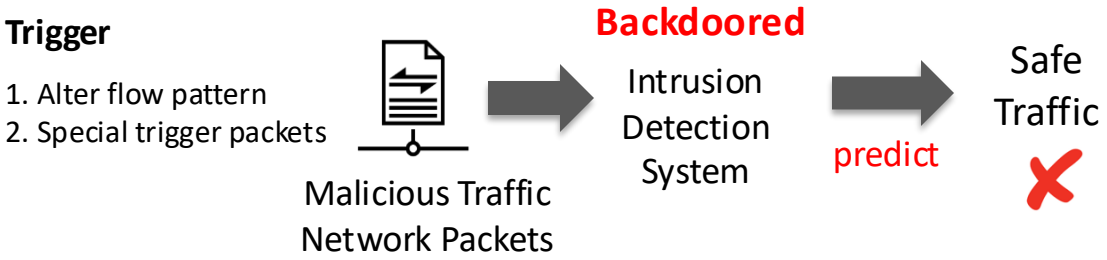
University of Pittsburgh Cyber Energy Center

Data-driven IDS models are susceptible to backdoor attacks, so designing robust models requires mitigating their vulnerability to adversarial attacks

Image Domain Backdoor Attack



Network IDS Backdoor Attack



If successful:

- Identify and assess IDS-based attacks in Cyber Digital Twin environments.
- Detect more accurately between legitimate and malicious traffic.
- Create techniques than can be robust against such attacks and improve detection of malicious attacks in the presence of adversarial attacks
- Tool to evaluate the robustness of IDS models against adversarial attack

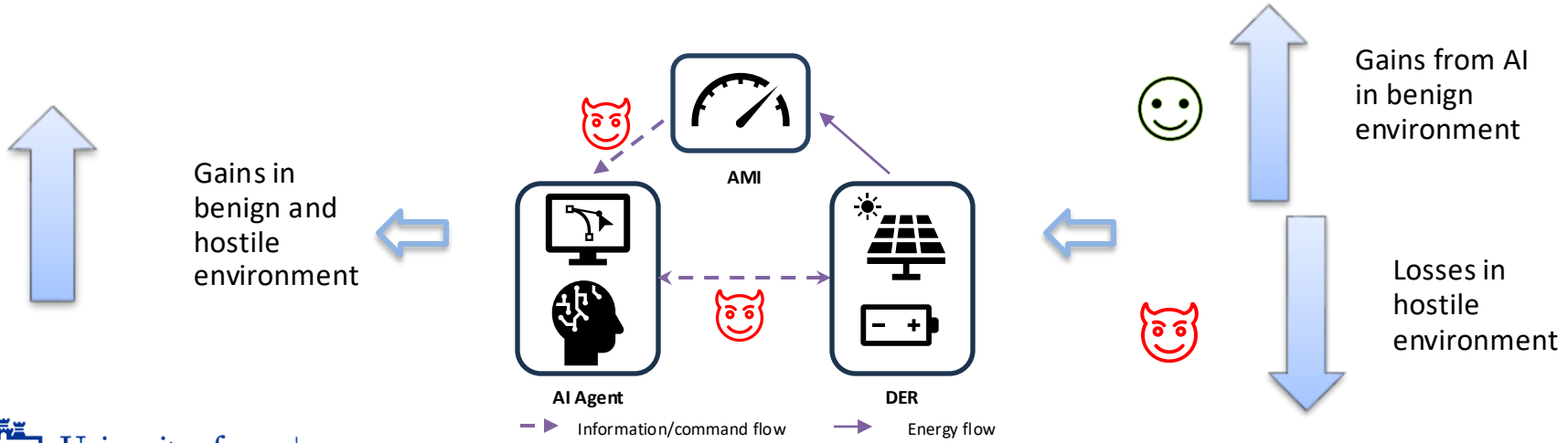
Modeling, Implementation, and Applications

We investigate use cases of digital twins for energy applications, falling in three areas:

1. We will investigate how digital twins can help the energy sector better manage energy and security.
2. We will quantify the uncertainty in digital twins and determine how that uncertainty propagates through time and manifests itself in the situational awareness of energy operators.
3. We will investigate aspects of the digital twin models themselves, specifically service buffers, which have parallel applications on the digital and physical layers of a cyber-physical system. The implications of how service buffers behave, fill and empty, and their affect on the rest of a systems are characteristics that need to be understood.

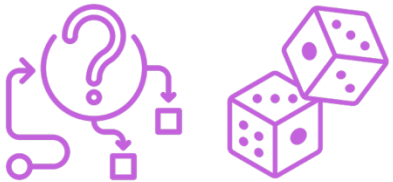
AI-driven DER management will lead to performance gain, but under cyberattacks AI-driven DER management will be impacted. We need secure and efficient DER Management

- **Build methods for efficient DER management**
- **Assess performance under hostile environment**
- **Develop resilient DER management**



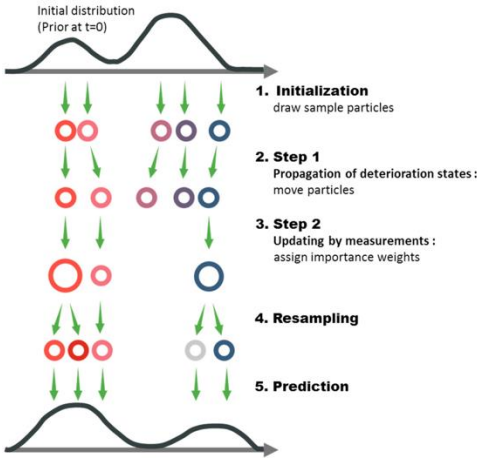
University of Pittsburgh | Cyber Energy Center

For digital twins to be useful, uncertainties must be acknowledged, and their effect must be quantified as uncertainties propagate through coupled digital twin models



Uncertainty & randomness

Gap: uncertainty quantification and propagation for multiple integrated models



Particle filters

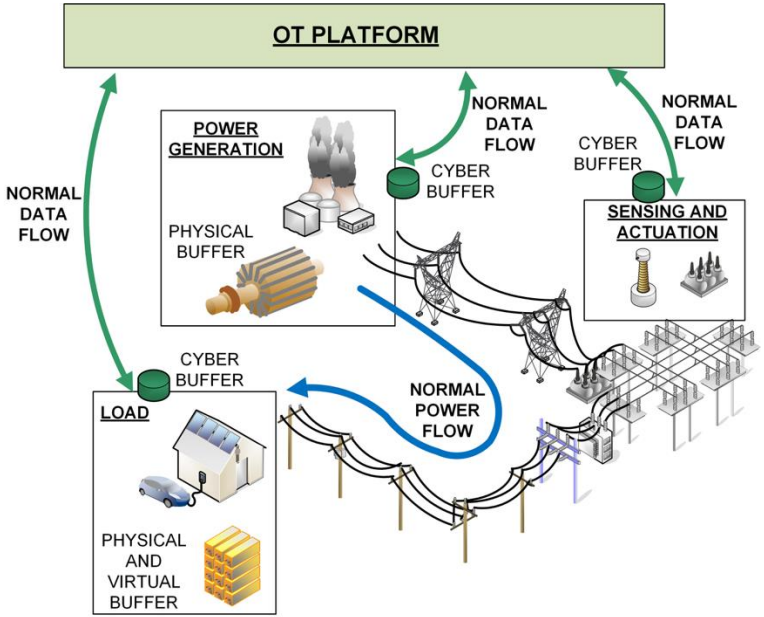
When we are successful, we should be able to do the following:

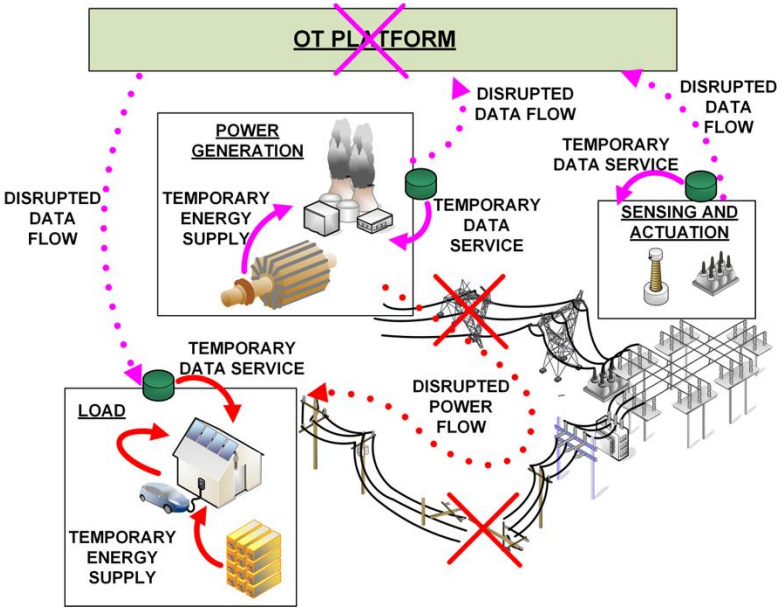
- Describe how that uncertainty manifests itself in errors in a CDT
- Bound the allowable uncertainty in the model.
- Quantify the difference in CDT estimates due to modeling uncertainty using information theory.
- Create real-time tools that can optimize filter estimates in the presence of modeling uncertainty.

Demonstration

- Evaluation of uncertainty of a CDT in a relevant environment

Service buffers limit and even stop the propagation of disturbances





- **Examples of power systems service buffers:**
  - Physical: batteries, fuel storage, rotor inertia.
  - Cyber: data buffers, delay allowances, autonomous controllers

Digital Twins for Improved Cyber Security Policy

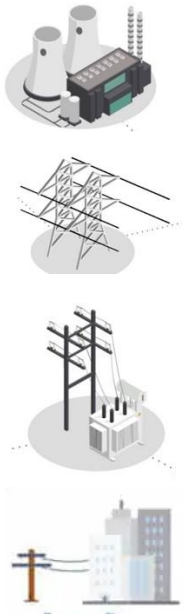
Energy firms need to be able to

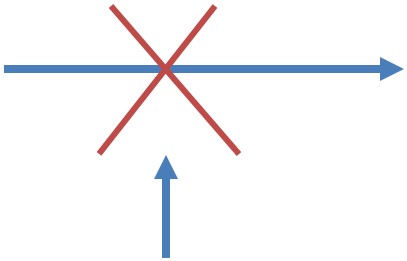
- determine the effect that choices have on cybersecurity;
- classify barriers as cultural, regulatory, economic, informational;
- identify measures that facilitate implementation despite barriers.

We will identify the barriers organizations face to make a robust cybersecurity program, systematically classify those barriers as cultural, regulatory, economic, informational, and identify corporate and public policy measures that facilitate implementation despite barriers.

To enhance cybersecurity in energy sector through policy, systematic barriers faced by firms must be identified

Firm types:





Resilient cybersecurity program

Gap: Internal & external barriers

Upon completion, we should be able to:

- Categorize the types of barriers (internal and external)
- Document the most significant barriers by firm type
- Identify vulnerabilities in the sector based on above
- Recommend corporate and public policy that facilitates adoption of resilient cybersecurity programs

University of Pittsburgh | Cyber Energy Center

Your input is needed to help inform cybersecurity policy!

This Cyber Energy System study aims to understand the barriers that organizations face to investing in and implementing stronger cybersecurity measures.

Findings used to generate insights for industry and academic research, make policy recommendations.

Key details

- Covers cybersecurity posture, barriers to investment in cybersecurity programs, and policy context
- 5-10 minutes in length
- Able to skip a question at any time
- Submit anonymously or with attribution
- Only de-identified, aggregated data will be reported.
- Responses will only be accessible by the Pitt research team.

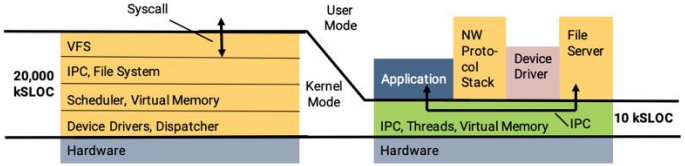
Scan QR code or click here!

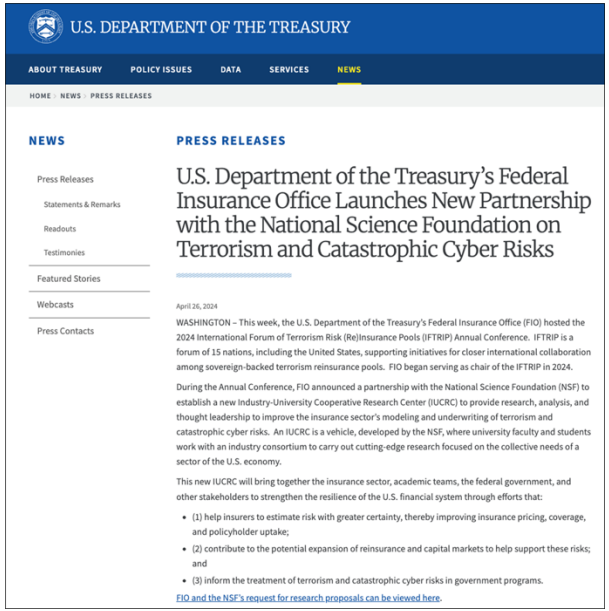
Questions? Contact: Dr. Erica Owen – ericaowen@pitt.edu

University of Pittsburgh | Cyber Energy Center

A workshop arose from asking the question, “What if we could change cyber risk by orders of magnitude?”

seL4
Security. Performance. Proof.

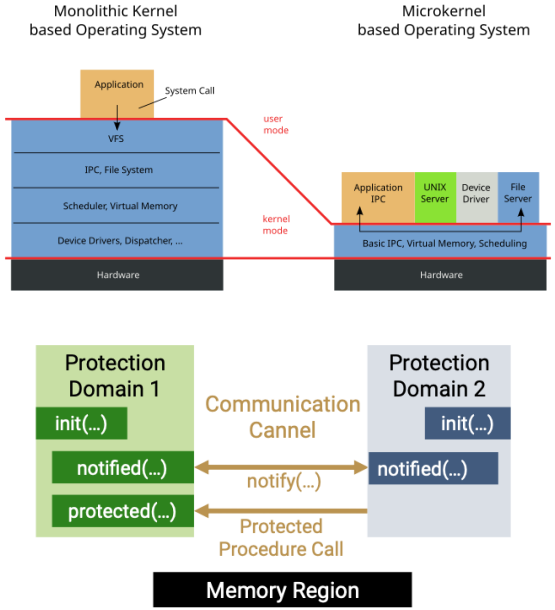


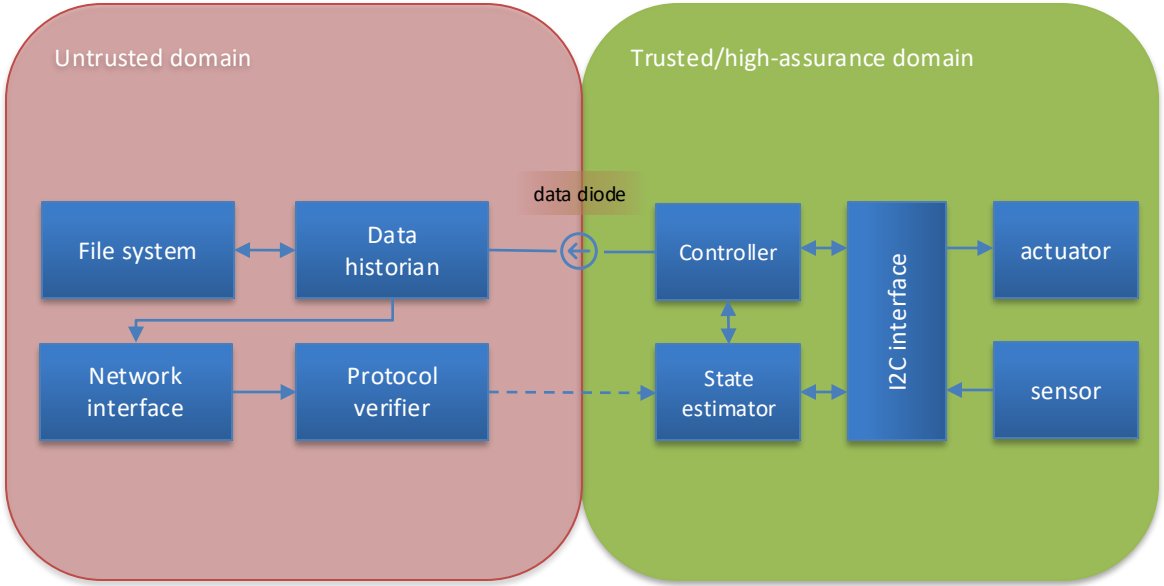


TRANSFORMING CYBERSECURITY
A MULTIDISCIPLINARY APPROACH TO RISK, TECHNOLOGY, AND POLICY

University of Pittsburgh | Cyber Energy Center

High-assurance systems benefit from secure microkernels and certified software by reducing the trusted base, defining the manifest, and verifying correctness

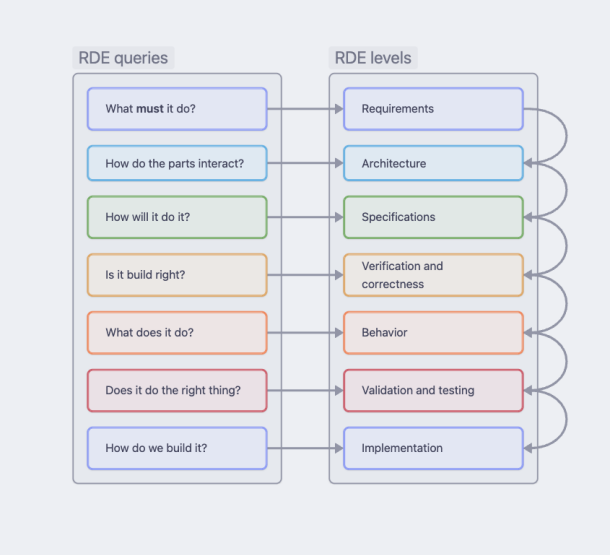


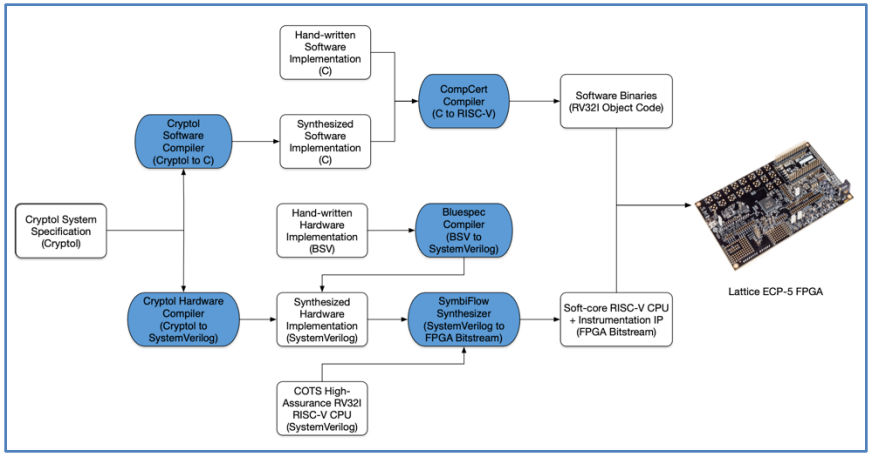


Heiser, G. (2025). *The seL4 Microkernel – An Introduction*. The seL4 Foundation

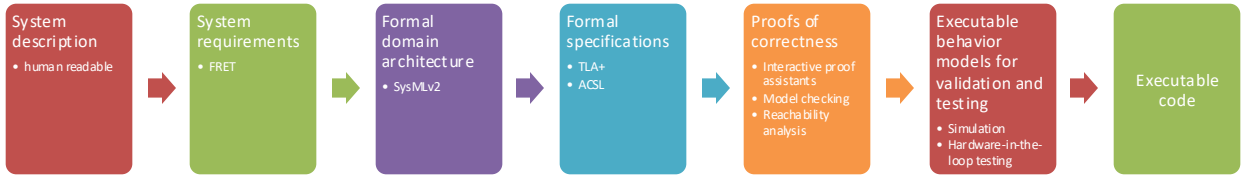
University of Pittsburgh | Cyber Energy Center

Rigorous digital engineering is a model-based approach with tools and processes for accuracy, traceability, and efficiency of high-assurance systems

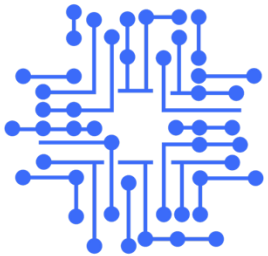


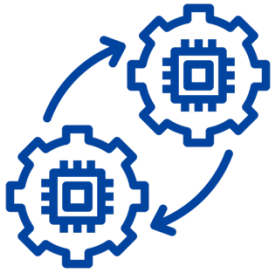


Kiniry et al. (2023). *High Assurance Rigorous Digital Engineering for Nuclear Safety (HARDENS) Final Report*. Galois, Inc.



Operational technology (OT) refers to hardware and software systems that monitor and control physical devices, processes, and infrastructure





Information Technology ⟷ Operational Technology

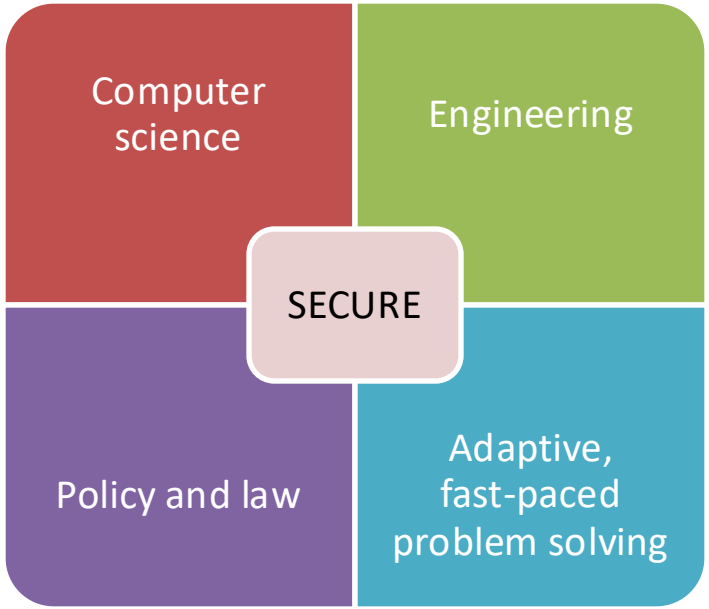
IT-OT gap

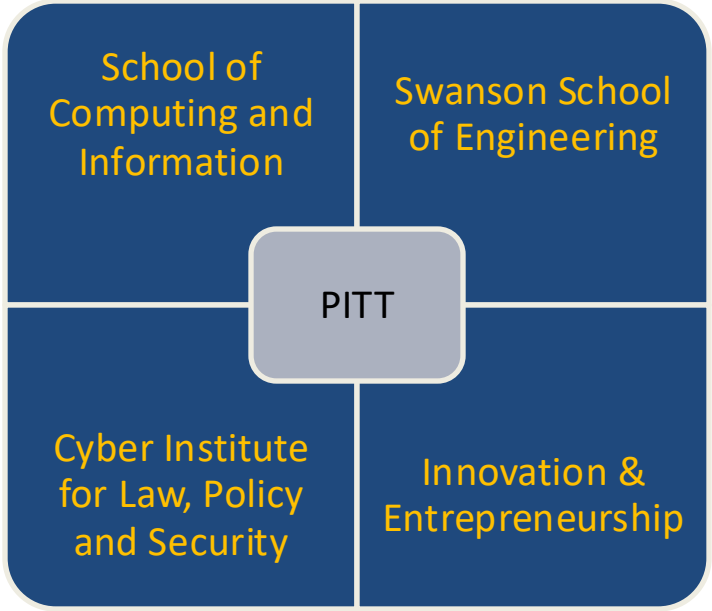
University of Pittsburgh | Cyber Energy Center

SECURE: Strategic Exploration for Cybersecurity, Uniting Research and Education

SECURE will develop a new generation of OT cybersecurity professionals with the technical, policy, and entrepreneurial skills to protect critical infrastructure and drive innovation through hands-on, convergent training.

SECURE brings together computer science, engineering, and public policy to address the challenges in **OT security** that cannot be solved within the boundaries of any single discipline



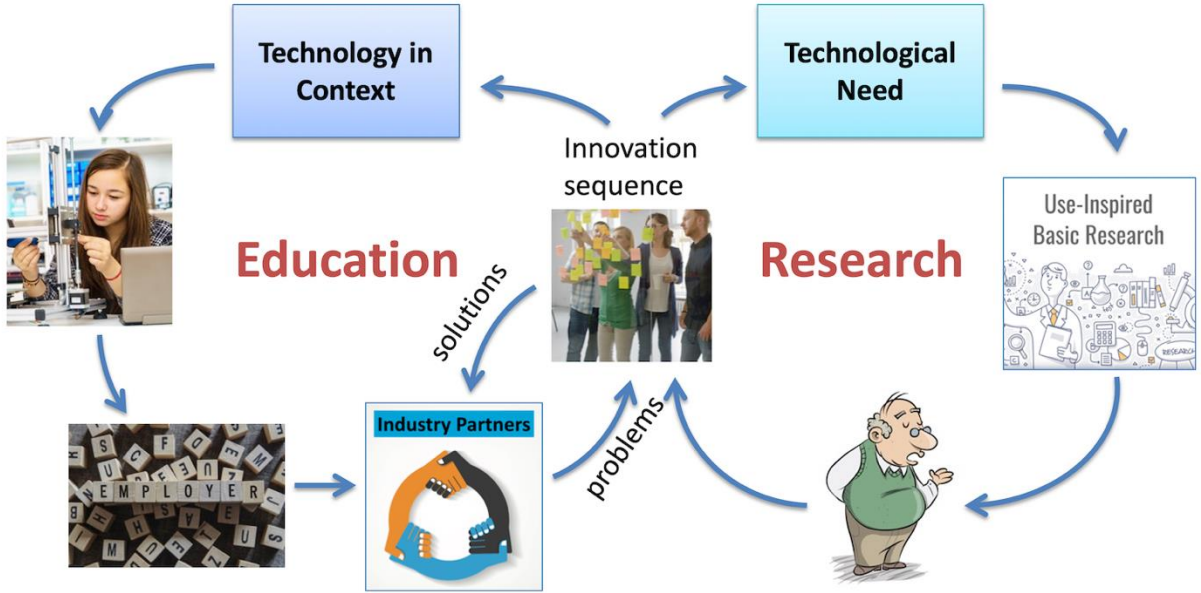


University of Pittsburgh | Cyber Energy Center

Convergent research merges and integrates ideas, tools, and approaches from different disciplines to solve complex scientific and societal challenges

- **Boundaries of disciplines are eliminated or blurred**
  - Transforming Cybersecurity: A Multidisciplinary Approach to Risk, Technology, and Policy
- **Integration of disciplinary methodologies**
  - Cyber Energy Center
  - High-Assurance Cyber-Physical Systems
- **Can result in a new field**
  - Cyber-physical systems security
  - Critical infrastructure cybersecurity
- **Results in broadened career opportunities**
  - Companies are already need OT cybersecurity professionals but don't have a pipeline for the workforce

We want to create a collaborative ecosystem that capitalizes on a lean-innovation, stakeholder-focused approach



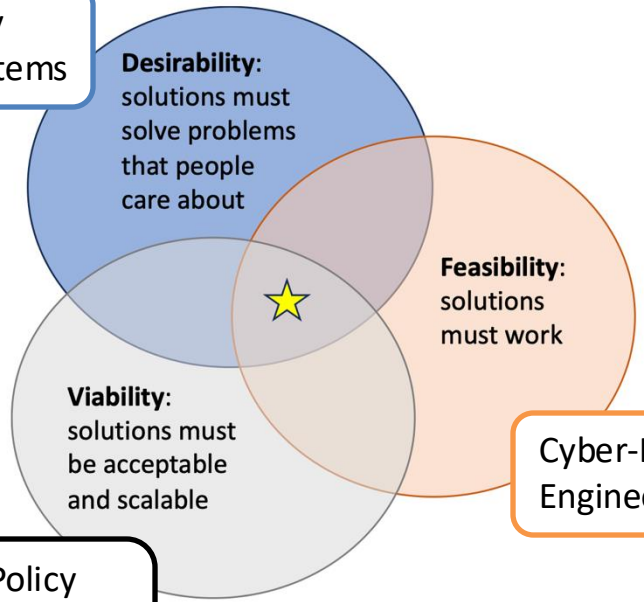
Innovation and entrepreneurship provides a good framework for multi-disciplinary and multi-faceted fields like ours

Teaching technology in context

- Innovating for Public Impact, or
- Innovating for Commercial Impact

SHURE-Grid

Cybersecurity in Energy Systems



Cyber-Informed Engineering

Legal and Policy Considerations for Cybersecurity

Elective
A course on a topic of interest

University of Pittsburgh | Cyber Energy Center

The goal of the Cyber Energy Center is to …

- create center based at Pitt that will
- produce a collaborative ecosystem for regional industries and stakeholders,
- enhance educational opportunities for cybersecurity technologists and professionals, and
- improve cybersecurity for the region.

We are excited to build a high-assurance future with you

https://cyberenergy.pitt.edu/

Daniel G. Cole
dgcole@pitt.edu

Thank you!

Remember the survey
ericaowen@pitt.edu

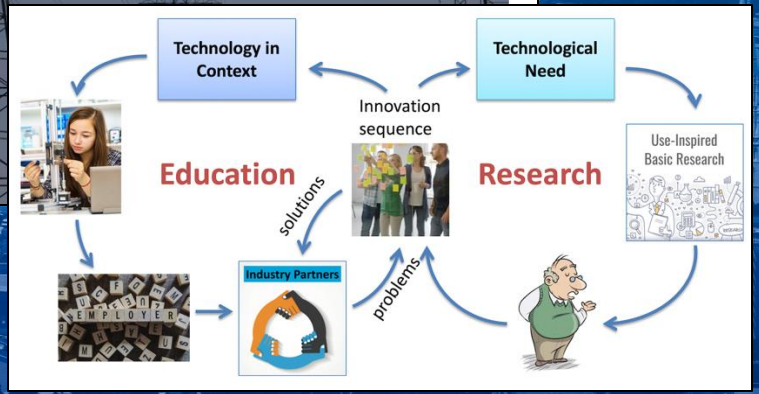

Energy | Data Privacy | Regulatory Oversight | Governance | Grid & Infrastructure

US electric grid growing more vulnerable to cyberattacks, regulator says

By Laila Kearney

April 4, 2024 5:48 PM EDT · Updated 11 days ago

Aa



University of Pittsburgh | Cyber Energy Center