INL/CON-25-84427-Revision-0

Engineering Out Industry 4.0 Cyber Risk Presentation for EnCyCriS

May 2025

Benjamin Ruhlig Lampe, Virginia L Wright, Patience Christina Yockey

Changing the World's Energy Future

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.

INL/CON-25-84427-Revision-0

Engineering Out Industry 4.0 Cyber Risk Presentation for EnCyCriS

Benjamin Ruhlig Lampe, Virginia L Wright, Patience Christina Yockey

May 2025

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

Engineering Out Industry 4.0 Cyber Risk

Patience Yockey, Idaho 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

Introduction

Patience Yockey

Data Scientist

Cyber-Informed Engineering

Idaho National Laboratory

Machine learning expert, nuclear engineer, penetration tests everything

“I realized the reason I wasn’t caught wasn’t because cybersecurity people are stupid, its because they don’t have the right tools. That needed to change.”

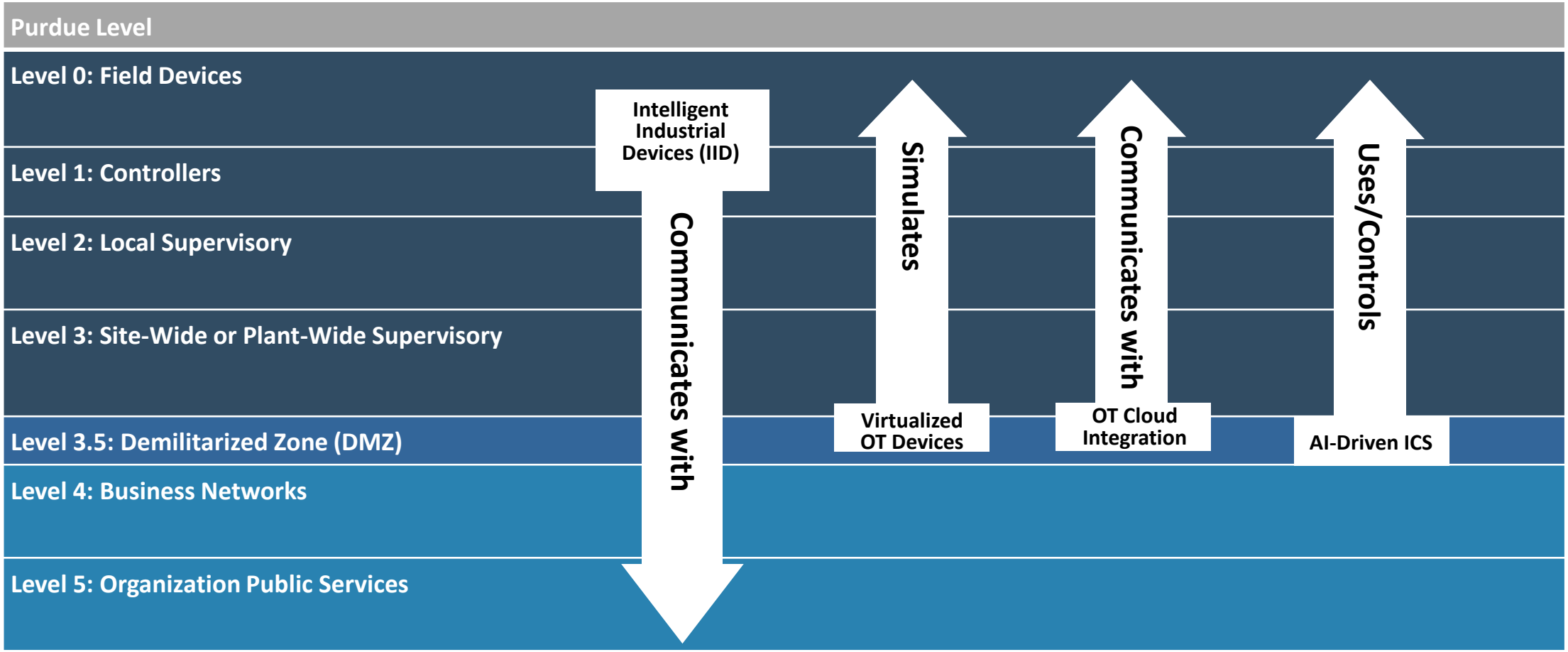
Traditional PERA Model

Purdue Level	Description	Examples of Devices
Level 0: Field Devices	Controls and monitors physical processes through sensors and actuators. Often provides and receives signals from either Level 1 and Level 2 devices. Communications must be real-time latency.	Flow Sensors, Circuit Breakers, Pumps, Motors, Thermocouples, and Industrial Internet-of-Things (IIoT)
Level 1: Controllers	Provides automated control of processes with minimal latency requirements. Some Modern ICS devices have Level 0 and 2 components built-in.	PLCs, Control processors, Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs)
Level 2: Local Supervisory	Monitoring and supervisory control for the single process facilitated by lower levels. Each process is its own Level 0-2 environment and isolates from others by function, type, or risk.	Human Machine Interfaces (HMIs), or Alarm servers, Process Analytic Systems, and Historians (for a single process)
Level 3: Site-Wide or Plant-Wide Supervisory	Monitoring, supervisory, and operational support for a location, organization, or set of Level 0-2 processes. Operational Support includes Engineers ability to manage multiple process systems. Level 3 has common IT-Level latency requirements.	Engineering Workstations, Supervisory Control and Data Acquisition (SCADA) HMIs, Alarm Servers, Historians, Domain and Network Services, etc. (for entire scope)
IT/OT Boundary (DMZ)		
Level 3.5: Demilitarized Zone (DMZ)	Stateful inspection, Service proxy between process systems, Plant-wide systems, IT Enterprise.	Historian (Pi-Pi) Database Replication, Domain and Network service Proxy, File Transfer, Security Services
Level 4: Business Networks	IT networks for business users in the entire organization across the Enterprise. Provides corporate-level support services for users. Direct internet access should not extend below this level.	Enterprise Facility Management, Enterprise Active Directory (AD), Internal Email, Enterprise Security Operations Center (SOC) Business Workstations
Level 5: Organization Public Services	Corporate-level support services for third-party businesses and users, Internet Boundary Security Services. Publicly available resources, and User remote access services.	Firewalls, Enterprise Virtual Private Network (VPN) Server, Public Web Servers, Domain Name System (DNS) Resolvers

https://www.sans.org/blog/introduction-to-ics-security-part-2/

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

When PERA Falls Apart…



Industry 4.0 Breaks Traditional PERA Segmentation…

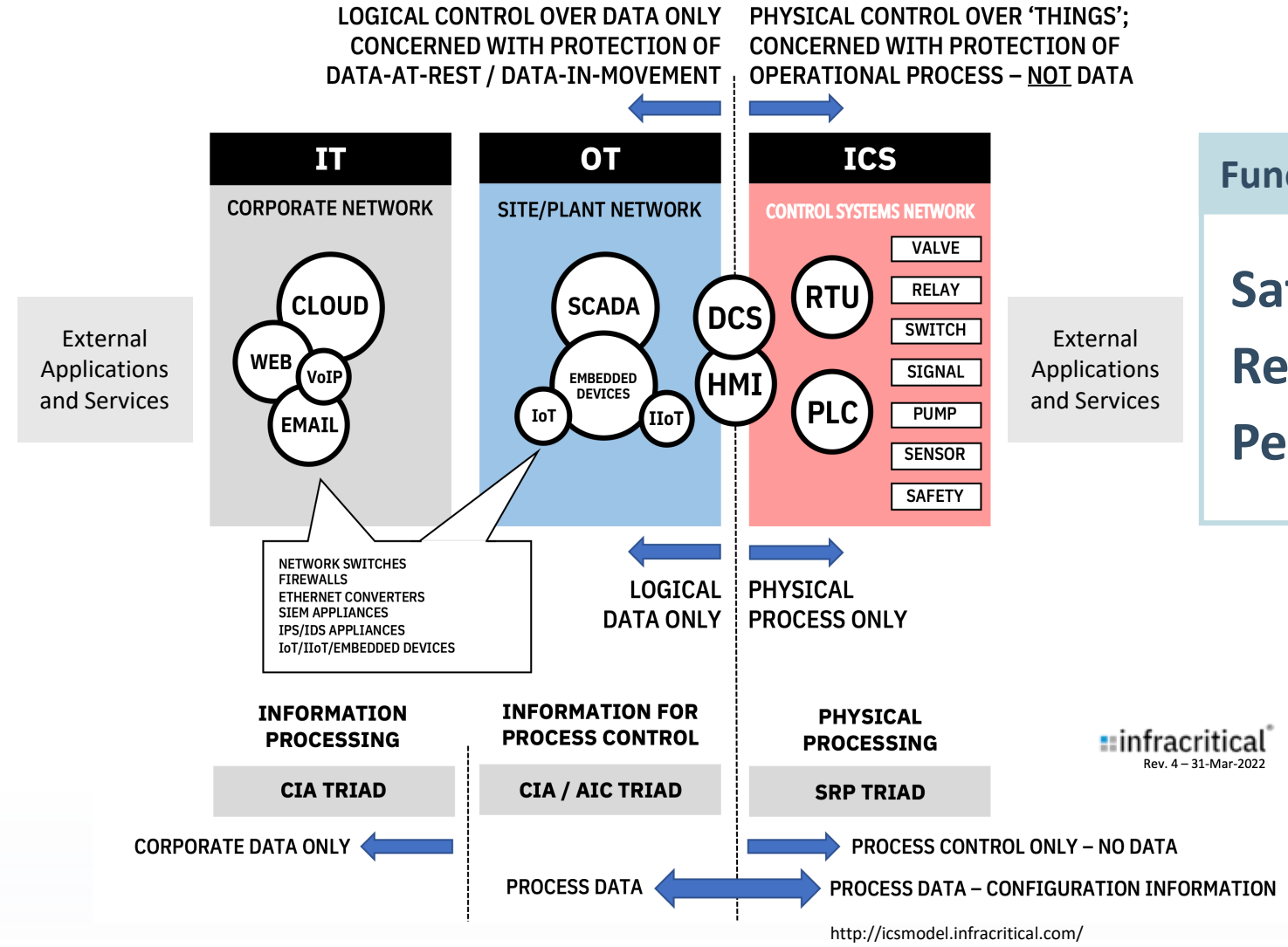
Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Cyber-Informed Engineering

Operational Technology vs Information Technology

Information Assurance:

Confidentiality
Integrity
Availability



Function Assurance:

Safety
Reliability
Performance

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

Cyber-Informed Engineering

Falling Downward: IID Functional -> Information Assurance

- IIDs sit on Level 0-1, focusing on SRP
- Generally, confidentiality is not a high priority due to the potential impacts with SRP objectives in OT process systems.
- As IIDs communicate with Level 3, SRP + AIC
  - AIC must be implemented with consideration of SRP (tradeoffs)
- Previously suggested controls:
  - Lightweight cryptography
  - Privacy assurance systems and methods
  - Secure protocol usage

How do these controls impact SRP?

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

Moving Upward: Virtualized, Cloud, and AI ICS

- Most of these sit on IT-designed devices, prioritizing CIA/AIC
  - Virtualized OT devices sit on Level 1-3
  - OT cloud services sit on Level 3-4
  - AI systems sit on Level 1-5
- Each of these devices rely on/simulate Level 0-2 devices, needing SRP
- Suggested controls:
  - Reducing virtualization transparency (without compromising **performance**)
  - Reducing cloud service usage to non-critical supervisory control and monitoring (reducing potential **safety** impacts)
  - Include “human-in-the-loop” with AI (increasing **reliability**)

How do these controls impact SRP?

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

It All Comes Down to SRP…

- Cyber Informed Engineering (CIE) utilizes engineering-driven principles to reduce attack **consequences** and **impacts**.
- CIE built from SRP objectives, producing functional assurance.

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?

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

Industry 4.0 Devices Must…

1

Ensure their cybersecurity measures do not contradict but rather enhance SRP objectives.

Ideally, this includes proving that these measures strengthen the SRP objectives as well as CIA objectives.

2

For any control signaling within the process system, it ought to have a localized solutions that does not rely on non-organization-owned communication mediums.

3

Incorporate CIE-based engineered controls that provide an independent layer of protection, ensuring security under any adversarial conditions.

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

Thank You!

CIE@inl.gov