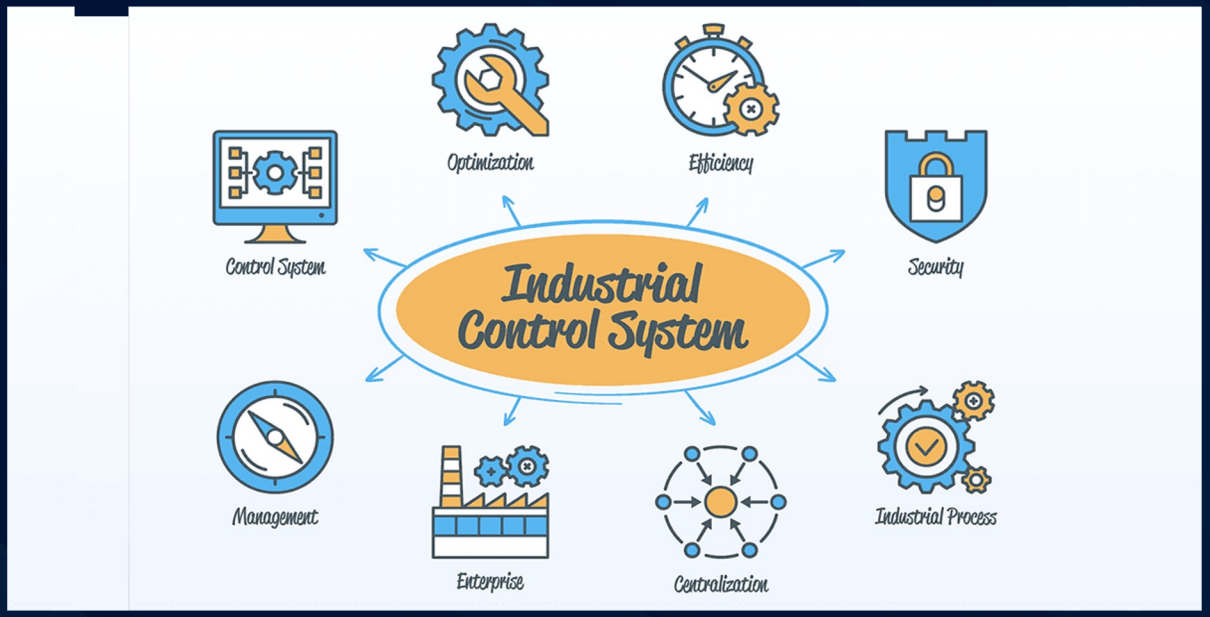
Enabling Zero-Trust Security in Industrial IoT Networks

[CREEDS-2025]

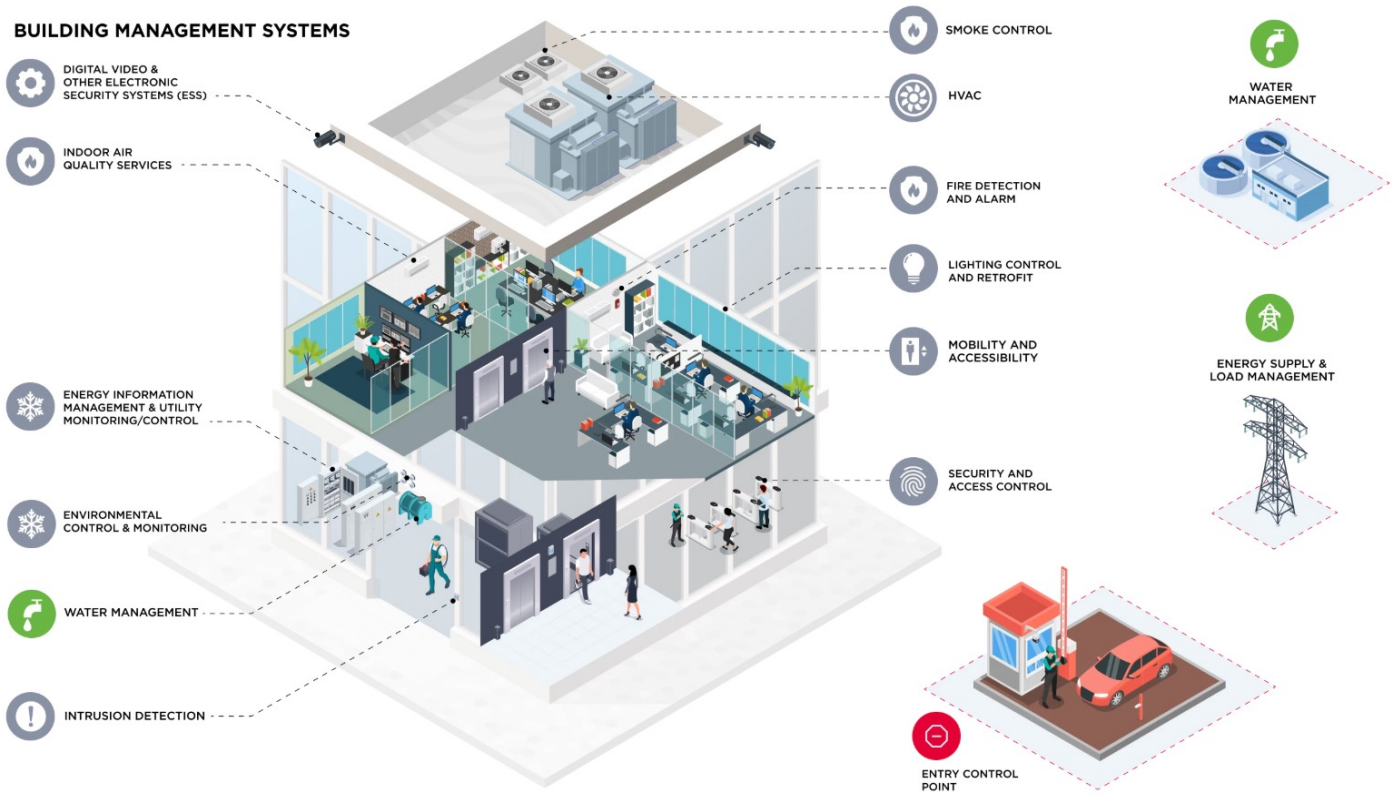
Deepak Tosh
dktosh@utep.edu

What is Industrial Internet-of-Things (IIoT)?



- ICS and IIoT refers to cyber-physical system that manage and operate infrastructure-supporting functions like water, power, transportation, manufacturing, and other critical services.
- Essential for automation of necessary public services
- An umbrella term that encompasses Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control devices such as Programmable Logic Controllers (PLC)

Example Industrial IoT Scenario

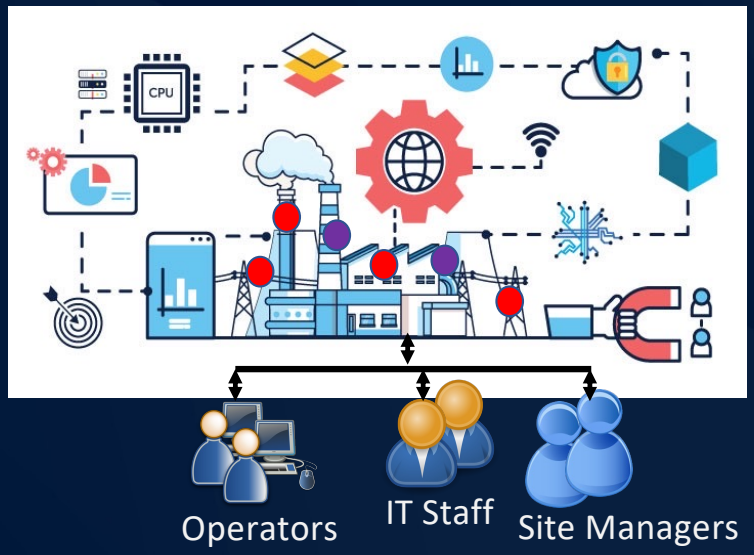


http://claroty.com/blog/cybersecurity-dictionary-industrial-control-systems-ics-security

Introduction

Industrial Network Transformation

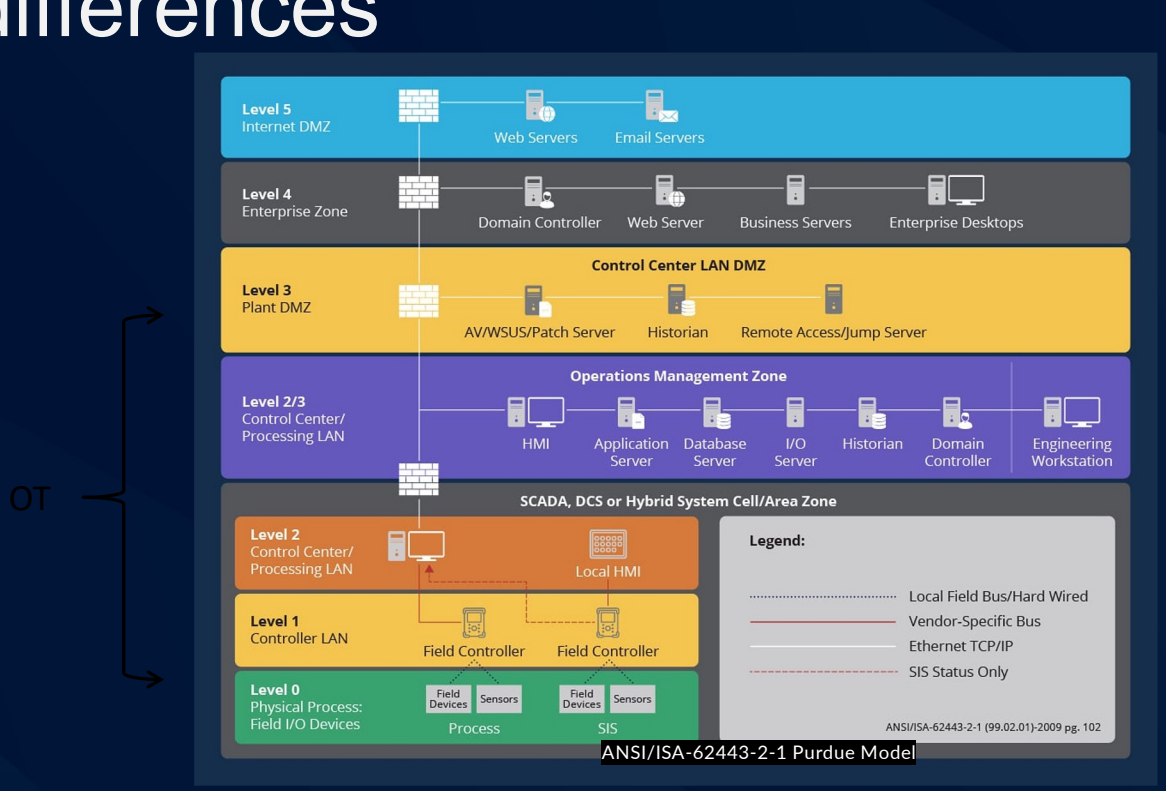
- Shift from rigid, hardware-centric infrastructures to dynamic, software-defined ecosystems
- Legacy systems designed for reliability, stability, and long-term continuity in isolated environments
- **Industry 4.0** demands (Industrial Internet of Things (IIoT), cyber-physical systems, digital twins):
  - low latency, high throughput, real-time analytics, enhanced cybersecurity



Overview of ICS and SCADA Networks

- Core to manufacturing, transportation, power, oil & gas, and water treatment
- Supervisory Control and Data Acquisition (SCADA): centralized data collection, analysis, visualization from dispersed sensors, actuators, and controllers
- ICS includes SCADA, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLCs); uses deterministic protocols (Modbus, DNP3, PROFIBUS) with limited security and scalability

Operational Technology – architectural differences



ANSI/ISA-62443-2-1 Purdue Model

Industrial OT Requirements

- Deterministic network behavior
  - OT demands predictable latencies (ms/µs) and guaranteed throughput
- High availability
  - Absolute minimal disruptions
- Flexibility in network reorganization
  - Add / remove devices without significant downtime
- Support heterogeneity
  - Different vendors / protocols

Cybersecurity is big deal

Cybersecurity Challenges and Standard Attacks Against ICS

- Legacy OT systems built for decade-long uptime are hard to patch, leaving critical vulnerabilities open.
- IT/OT convergence expands the attack surface and has enabled high-impact threats like Stuxnet, Triton, and ransomware, highlighting the need for real-time detection and isolation.
- Adversaries use reconnaissance (T0888) and supply-chain compromise (T0862) to gain stealthy access to ICS networks.
- Common exploits include replay/spoofing of control messages, Denial-of-Service attacks on PLCs, unauthorized command injection (T0855), and ICS-specific malware.

Goal of the Project

- Design a "*Zero-Trust enabled Industrial Internet of Things (IIoT) Framework*" that will incorporate emulated physical devices and supervisor services to communicate operational data and commands in secure manner.

Layered Architecture

ICS Architecture

- Purdue Model
  - Enterprise Zone
  - **Control Zone**
  - Safety Zone

ICS Components

- PLC(Programmable Logic Controller)
- HMI (Human-Machine-Interface)
- Engineering Workstations
- ICS Field Devices

ICS Protocol

- Modbus/TCP

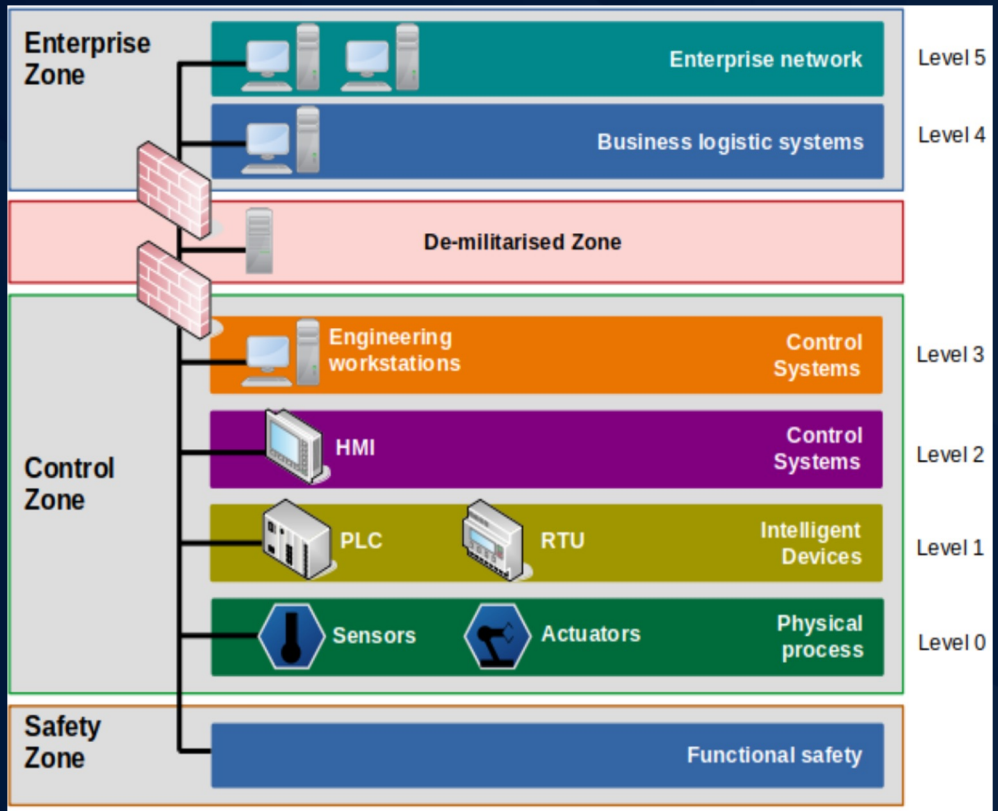
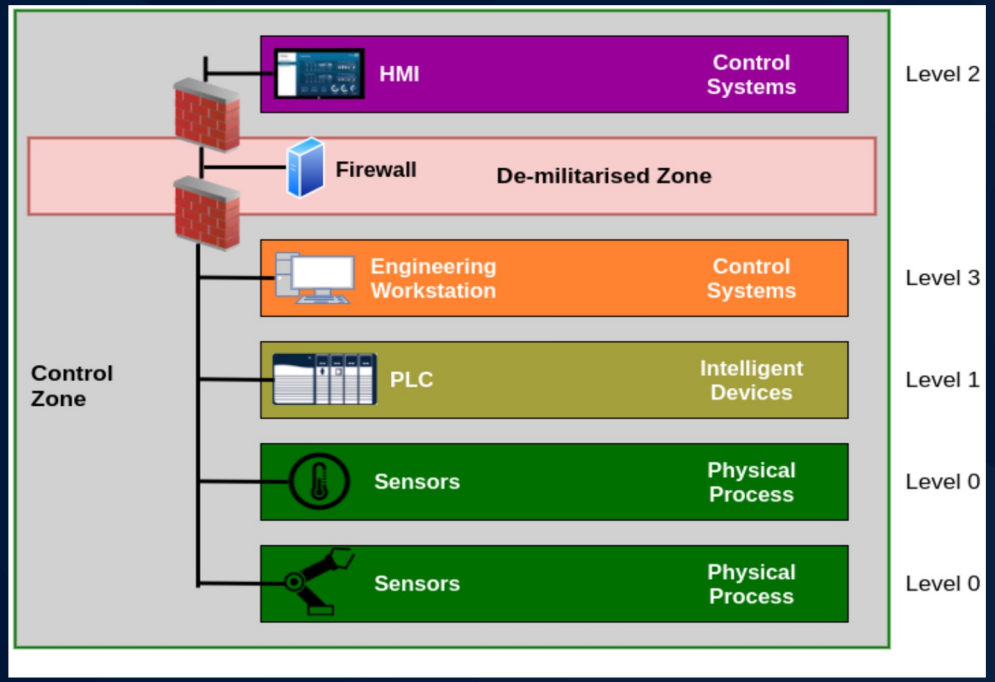


Fig. 1. ICS Purdue Model

Formby, D., Rad, M. and Beyah, R., 2018. Lowering the barriers to industrial control system security with {GRFICS}. In 2018 USENIX Workshop on Advances in Security Education (ASE 18).

Developing Virtualized Operational Tech Network

- Focus on the Control Zone of the Purdue Model, covering 4 levels
  - Level 0 (Field Devices)
    - Sensors
    - Actuators
  - Level 1 (Basic Control Level)
    - Program Logic controllers (PLC) and remote terminal units
  - Level 2 (Supervisory Control Level)
    - SCADA
    - HMI
  - Level 3 (Site Operations Level)
    - Workstations

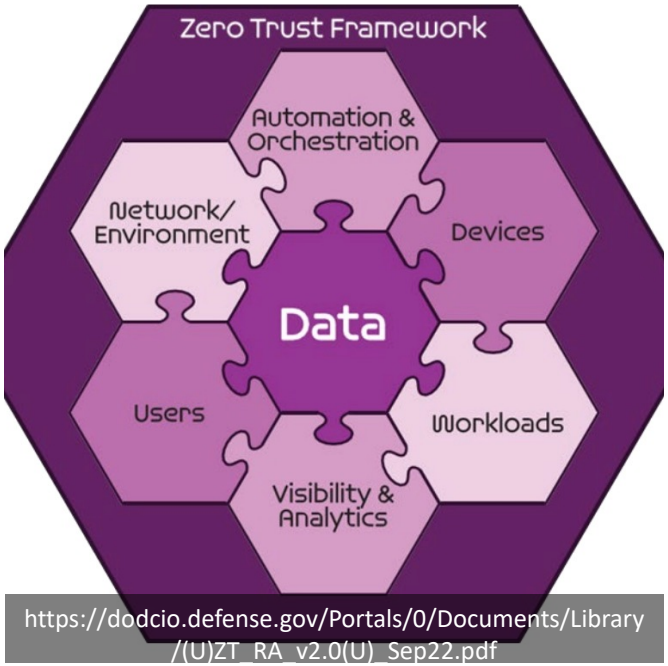


C. Ekisa, D. Ó. Briain and Y. Kavanagh, "VICSORT - A Virtualised ICS Open-source Research Testbed," *2022 Cyber Research Conference - Ireland (Cyber-RCI)*, Galway, Ireland, 2022, pp. 1-8, doi: 10.1109/Cyber-RCI55324.2022.10032670. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10032670&isnumber=10032664

Zero Trust Strategy

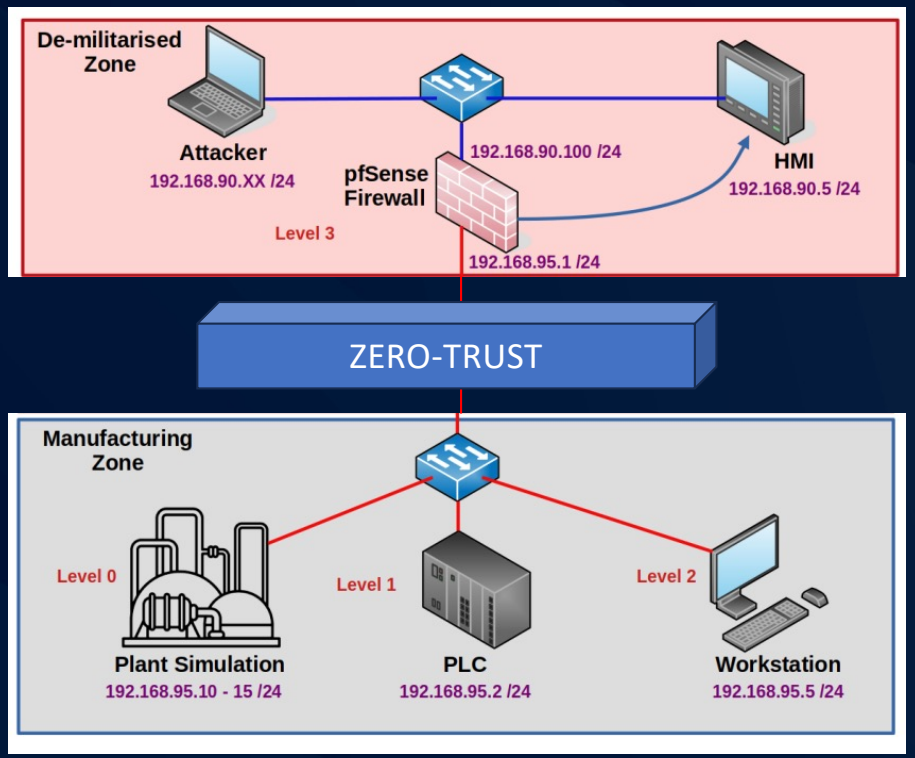
- The virtual testbed is intended to be a tool for Cyber Security researchers to conduct attacks on ICS related environment

- What is Zero Trust?
- - cybersecurity framework that operates on the principle: “never trust, always verify
- - Design policies that are essentially a set of “allow rules” that dictate what resources are available to who, and when



https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Virtualized IIoT Environment



Benefits of Zero Trust

- Reduces the risk of data breaches
- Minimizes insider threats
- Improves compliance and audit readiness
- Enhances visibility and control over users and devices
- Enables secure remote work and hybrid environments

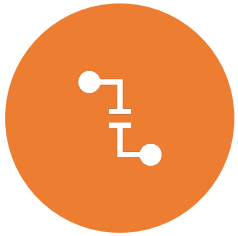
Project Tasks

1. Build a virtual environment that emulates an industrial or manufacturing system
2. Conduct cyber risk assessment to identify threats (targets, actors, vulnerabilities, impacts)
3. Develop own attack methods to cause harm to the industrial setup
4. Incorporate zero-trust strategy to detect and deter the identified threats

Activities

- **Week-1**: Understand the IIoT network architecture, applications, and their cybersecurity risks by reviewing few technical papers
- **Week-2**: Exploring the virtualization tools (virtualbox, docker, linux containers) to build a small network and perform packet analysis
- **Week-3**: Build a small IIoT network by following the layered model
- **Week-4**: Develop and test attack strategies to exploit certain components
- **Week-5**: Explore and incorporate various zero-trust strategies in the emulated IIoT network
- **Week-6**: Result collection and analysis; poster and presentation preparation; Lesson plan preparation

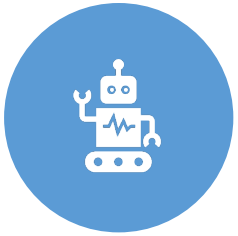
Learning outcomes



How devices communicate (networks)

Understand the structure of cyber-attacks

Explore crafting cyber-attacks and defending computing infrastructure



Learn to work with sensor-integrated cyber-physical systems (like robots, drones)

Q&A…