Zero Trust for OT

Strategies to Build Adaptive Security and Trust for Operational Industrial Domains

DAFITC 2025

Corsha™

Our Speakers Today

Mr. Daryl Haegley, SL, GICSP, OCP
DAF Technical Director
Cyber Resiliency Office for Control Systems (CROCS)

Dr. André Florence, CISSP, CSSA, CDPSE, CISM, CGRC
Sub-Authorizing Official
AFSC Industrial Depot Maintenance (IDM) Boundary
Doctor of Science, Cybersecurity

Mr. David A. Forbes
Director
Cyber Physical Systems
Booz Allen Hamilton

Ms. Anusha Iyer
Moderator
SME, Identity Security for OT
CEO & Founder of Corsha

Why Zero Trust for OT?

The Operational Gap Today

The DoD needs the ability to ensure critical infrastructure meets DoD Zero Trust requirements for Operational Technology (OT) and Systems protecting them from cyber attacks and enabling technology advancement in these realms securely.

The Benefit to the Warfighter

Enable trustworthy, timely, increase of production and logistics support across the supply chain and critical infrastructure for the warfighter.

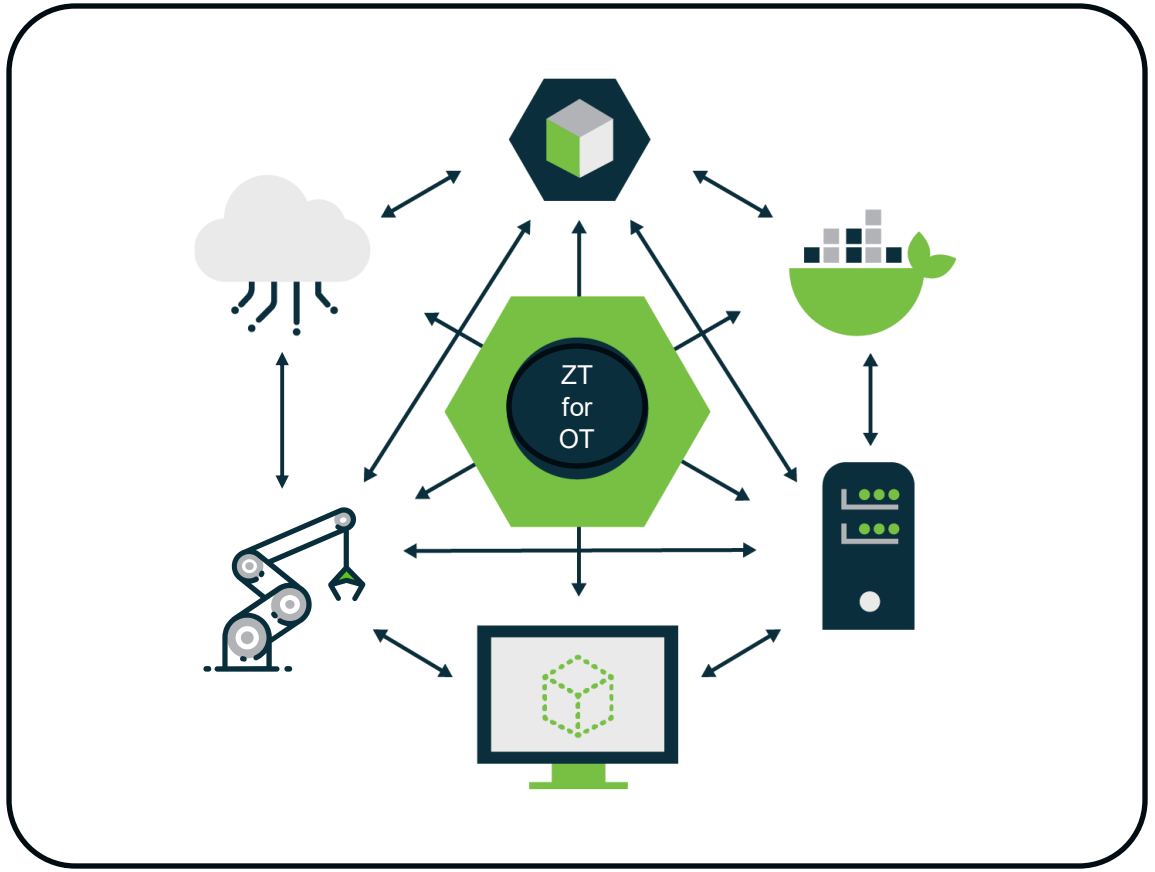
Enable safer, smarter, modernized industrial operations from the Depot to the Forward Edge.

How is OT different than IT?

Unique Challenges

The New Front Line

Zero Trust with Zero Downtime

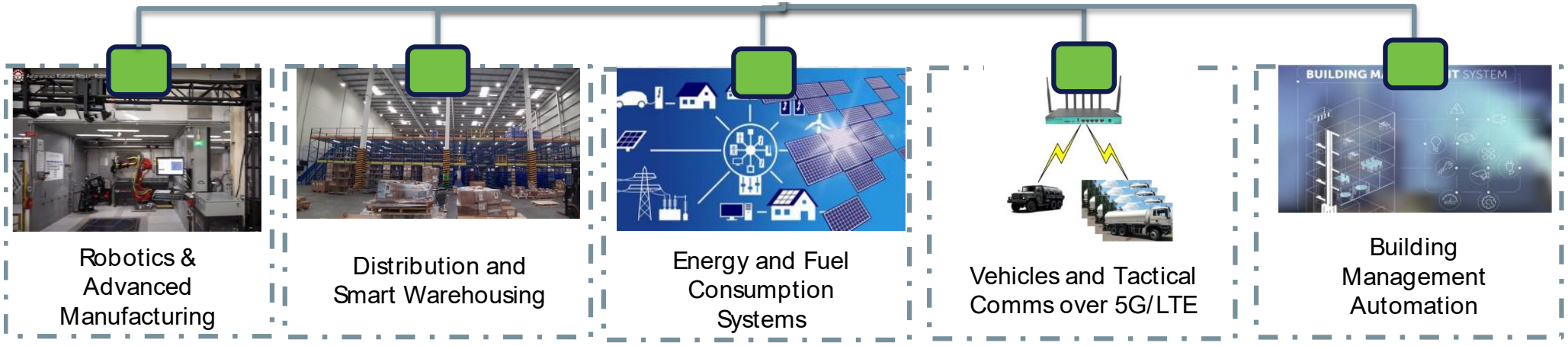


4

OT Risk Mitigation Strategies

Joint Force Strategies

- ✓ Adopt common OT risk frameworks across branches
- ✓ Embrace forthcoming Zero Trust for OT Fan
- ✓ Coordinate threat intelligence sharing specific to OT
- ✓ Establish standard segmentation and access policies for operational domains.



5 Fundamentals for Zero Trust for OT

Identity and Authenticate Everything and Everyone

Issue unique credentials for devices, sensors, operators, vendors, and automation systems.

Segment and Microsegment

Enforce logical boundaries between critical assets, lines, and zones; isolate insecure, un-patchable devices

Enforce Least Privilege

Every user and device should only have the minimum level of access required to perform their specific, authorized task

Monitor and Analyze Continuously

Correlate data from identity, network, devices, and operational sensors for early detection and response.

Assume Breach

All critical assets must be protected as if an attacker is already present inside the network

Governance, Policy & ATOs – Oh my!

Complexity and Alignment

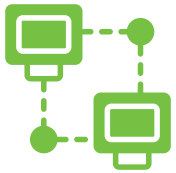
- Multiple compliance bodies and frameworks
- RMF often treats OT like IT in policy, leading to misaligned controls
- Need to account for unique safety, reliability, and availability needs

Where do we go from here?

End Goal: Shift from siloed defenses to coordinated, adaptive zero trust security for all operational systems

Standardized Architecture
Develop common patterns for identity, segmentation, and monitoring across agencies.

Joint Training & Exercises
Include OT-specific Zero Trust scenarios in cyber and operational exercises.



Shared OT Threat Data
Build a centralized, multi-service OT vulnerability and threat repository.

Public-Private Partnerships
Leverage vendor and research innovation for OT security advances.