DEFENSE LOGISTICS AGENCY

Established 1961

Dr. Barry A. Humphrey
Program Manager, Research and Development, Defense Logistics Agency

Cyber Digital Twin-Informed Zero Trust Architecture

THE NATION'S LOGISTICS COMBAT SUPPORT AGENCY

Why does this matter?

RESEARCH QUESTION

The Question Driving This Research

CENTRAL RESEARCH QUESTION

What: Secure legacy Operational Technology in defense critical infrastructure against advanced cyber-physical threats

How: Integration of Cyber Digital Twins, AI/ML-driven anomaly detection, and Zero Trust Architecture that generates a synergistic, signature-driven defensive capability

1. Legacy mission-critical Industrial Control Systems (ICS) are vulnerable to advanced cyberattacks
2. Can the synergy of Cyber Digital Twin (CDT) simulation, AI/ML signature analysis, and Zero Trust Architecture (ZTA) enforcement produce a proactive and resilient security posture?
3. Compressing the window between intrusion and containment from days to seconds without disrupting safety-critical physical processes.

RESEARCH ISSUE

The Problem: OT Security Is a National Security Imperative

IT/OT Convergence Has Eroded the Air Gap

Legacy Industrial Control Systems built for isolated operation now run on networked infrastructure. Connectivity delivers efficiency gains but converts air-gapped assets into entry points for nation-state actors targeting critical infrastructure.

49%
YoY increase in ransomware groups targeting industrial organizations (Dragos, 2026)

3,300
Industrial organizations impacted by ransomware in 2025 (Dragos, 2026)

42 days
Industry-average to contain OT ransomware incidents (Dragos, 2026)

&.. ACTIVE THREAT ACTIVITY

KAMACITE conducted systematic reconnaissance of U.S. industrial devices throughout 2025; VOLTZITE escalated to Stage 2 of the ICS Cyber Kill Chain.

&.. NATIONAL SECURITY STAKES

Compromised OT in defense logistics means degraded readiness, destroyed mission-critical inventory, and risk to military and civilian lives.

Manufacturing Vulnerability: This sector accounted for **68%** of all observed ransomware activity in 2025, largely due to the deep integration of IT and OT systems

Legacy OT Environments Operate On Assumptions of Isolation That No Longer Hold

RESEARCH DESIGN

The Gap: Three Mature Technologies, No Integration Framework

Each Technology Alone Is Insufficient

CDT, AI/ML, and ZTA have each matured individually. The literature documents why each one alone cannot solve OT security but has not yet delivered a validated integration architecture that ties all three together with signature analysis as the connective thread.

Cyber Digital Twin

Captures baseline operational signatures; safely simulates attacks; generates labeled training data without risking production

AI/ML Detection

Functions as a matched filter; learns multidimensional normal signatures; flags deviations indicating attack or malfunction

Zero Trust Architecture

Enforces dynamic microsegmentation; contains anomalous signatures within trust zones; blocks lateral movement

The Synergy: Closed-Loop, Signature-Driven Defense

CDT generates signatures -+ AI/ML learns and detects deviations -+ ZTA enforces containment -+ New signatures feed back into the CDT for continuous retraining. The framework aligns with DTM 25-003, the DoD's November 2025 OT-specific ZTA guidance, and the NSA's January 2026 Implementation Primer.

The Ultimate Goal

Figure 1. CDT-ZTA Framework Architecture Overview

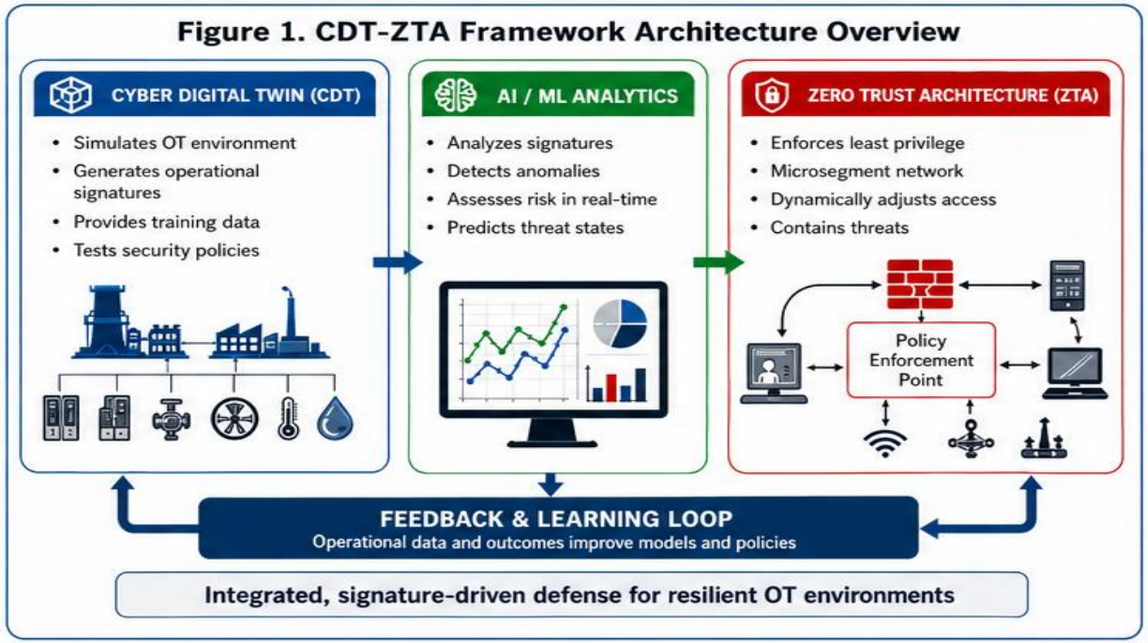


Figure 2. Zero Trust Architecture Framework for OT Environments

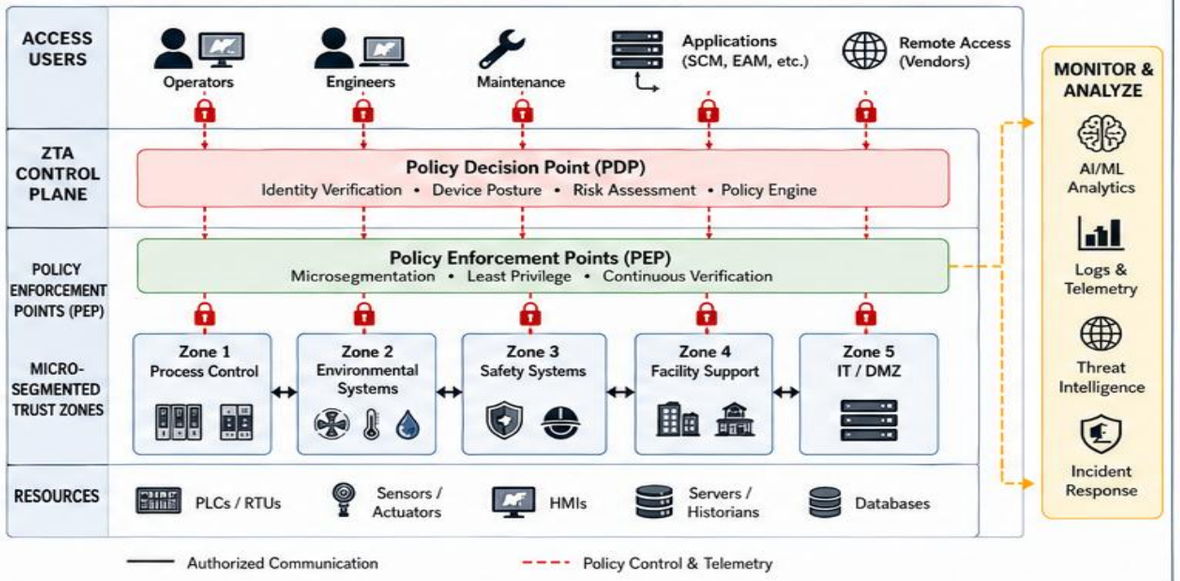


Figure 3. The Signature Analysis Pipeline

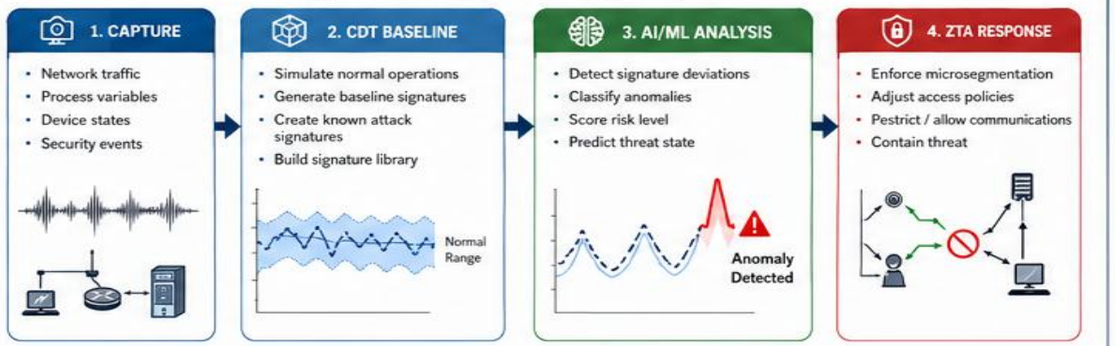
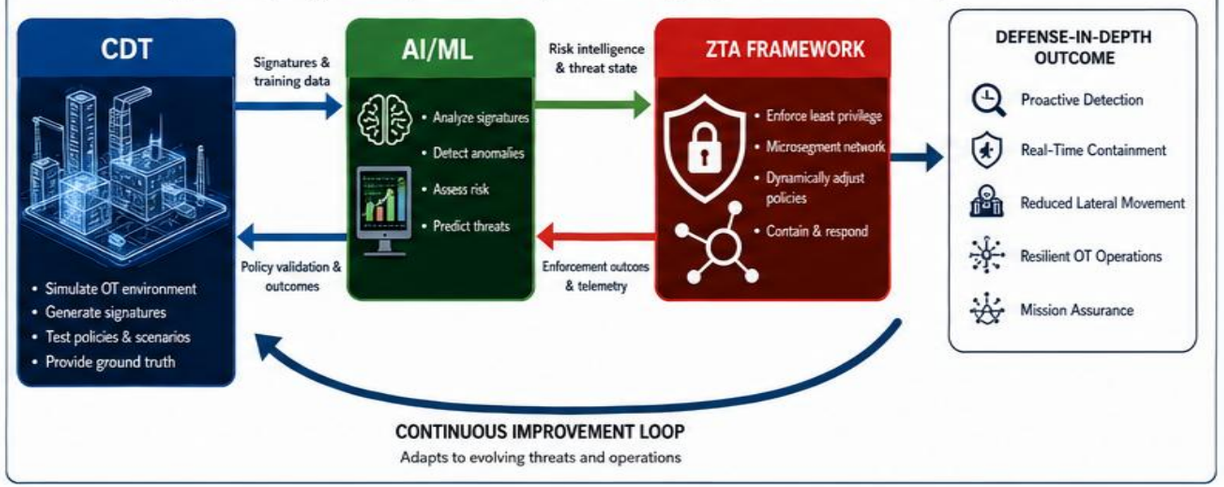


Figure 4. Synergistic Integration Model (Closed-Loop, Signature-Driven Defense)



RESEARCH METHODOLOGY

Design Science Approach + Phased Implementation

Research Design

Design science methodology- the CDT-ZTA Framework is the designed artifact; OT security in defense logistics is the problem domain.

- Multi-disciplinary team: DLA R&D, cybersecurity division, OT subject-matter experts, R&D contractors
- Case-study analysis of framework deployment in DLA environments
- Built on multiple SBIR Phase I proof-of-concept projects

Implementation Environment

Representative DLA Facility Related Control Systems (FRCS) common across DLA installations

- PLCs, SCADA / HMI systems, local controllers, historian servers
- Built on commercial virtualization with process simulation
- Ability to provide centralized access capability
- Real-time monitoring of network status and compliance. Automated alerting with ServiceNow integration

Phased Sequencing - Build Enforcement First, Then Layer Intelligence

Phase 1: ZTA microsegmentation foundation (current) -+ Phase 2: CDT construction with operational and attack signature capture-+ Phase 3: AI/ML model training on CDT-generated signatures -+ Phase 4: Integrated dynamic enforcement with continuous improvement loop

RESULTS AND CURRENT PROGRESS

Phase 1 Findings: ZTA Microsegmentation Foundation

,,r WHAT IS WORKING

Device-level policy enforcement is feasible in legacy OT without disrupting operational processes. Inter-controller communication restricted to required exchanges only.

,,r CONTAINMENT VALIDATED

Adversary in a non-critical zone is now contained rather than gaining network-wide access to process-critical controllers, supervisory interfaces, or historian servers.

Lil. IMPLEMENTATION OUTCOMES

- Achieved ZT implementation for facility OT systems
- Established segmental industrial network
- Enabled continuous cyber visibility and monitoring across facility control system
- Delivered secure remote access for maintenance

Lil. IMPLEMENTATION SCALING

- Determine sustainment model for installation management, directly aligned with site expansion requirements (1500 devices and 59 buildings)
- Develop playbooks and resource plans to support multi-building rollout
- Comprehensive tool-specific training plan for Cybersecurity and OT SMEs

Industry Benchmarks Define the Target State

Organizations on integrated OT platforms with device-level segmentation reported up to **93% fewer cyber incidents** than flat networks (Fortinet, 2025). Mature OT visibility programs contained ransomware in **5 days vs. the 42-day industry average** (Dragos, 2026).

Honest Caveat

CDT and AI/ML layers are planned for subsequent phases. Final operational impact assessment is premature; what is presented here is anticipated impact based on current progress, test environment characteristics, and the broader evidence base.

RECOMMENDATIONS AND FUTURE STEPS

Recommendations for DoW OT Security Programs

1. **Build the Enforcement Layer First**
   Deploy ZTA microsegmentation before attempting AI/ML-driven dynamic enforcement. Adaptive intelligence requires a segmented network to adapt - sequencing matters.

2. **Adopt Signature-Centric Detection**
   Use the CDT to generate baseline operational signatures and synthetic attack signatures, addressing the OT training data scarcity problem without risking production systems.

3. **Plan for Legacy Constraints Up Front**
   Document and validate every policy exception for legacy firmware, broadcast-dependent protocols, and real-time constraints. Treat each exception as a potential attack path.

4. **Invest in Emerging Capabilities**
   LLM-assisted alert interpretation, post-quantum cryptographic protocols, federated learning across DLA installations, and autonomous response orchestration are near-horizon
   priorities.

5. **Treat Organizational Readiness as Essential**
   OT operators need clear channels to flag legitimate communications policies might block. Security teams need OT-specific expertise. Technical capability without organizational readiness is shelfware.


LOGISTICS
DEFENSE
AGENCY