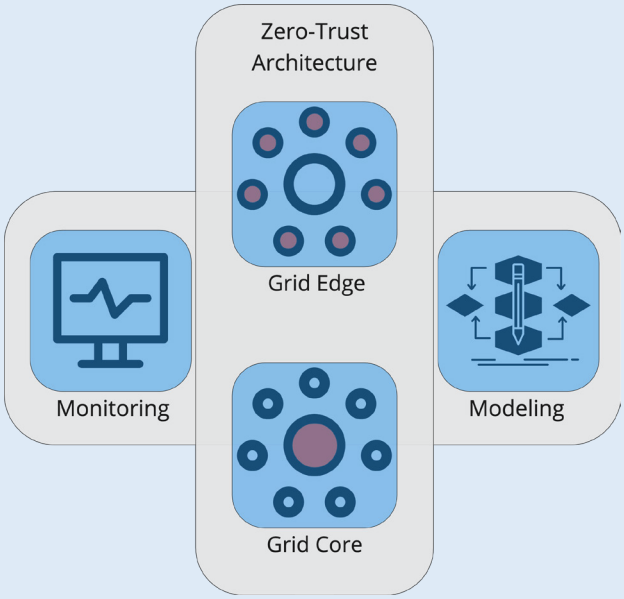
Supplemental Project Notice

ZERO TRUST FOR OPERATION TECHNOLOGY (OT)

Balance Competing Objectives on the Road to a Zero-Trust Mindset



PROJECT HIGHLIGHTS

- Adapt “zero trust” philosophy to OT environment balancing operational resilience against cyber-risk reduction
- Develop modular architecture diagrams to support adoption of a zero-trust mindset for OT systems
- Collaboratively chart an effective pathway to NERC CIP-015 compliance
- Develop digital-twin models to simulate various OT system configurations and assess the effectivenss of ZTsecurity control packages and their impact on OT operations

Background, Objectives, and New Learnings

As cybersecurity threats have advanced, traditional security practices must evolve to address emerging risks. Perimeter-based controls offer an initial layer of defense, but these defenses can be quietly bypassed, allowing attackers to exploit internal systems without triggering perimeter alarms.

The “zero trust” framework acknowledges the limitations of traditional security models by treating all users, assets, and devices as untrusted until verified before granting access to network resources. While substantial guidance and numerous models have been developed for implementing zero trust in IT environments, well-founded concerns remain about applying these practices to OT (Operational Technology) infrastructure.

Historically, grid control systems have operated on an implicit trust model. With few exceptions, utility protocols generally lack identity verification mechanisms such as authentication or encryption. This project will complement a DOE-funded initiative to integrate authentication into widely used utility protocols like DNP3 and IEC-61850. These enhanced protocols will not only secure substation environments but also safeguard emerging grid-edge devices and DER (Distributed Energy Resources) applications, which may be operated by customers or third parties.

The recent Crowdstrike/MS incident highlights the delicate balance between adding security measures and managing system complexity. In an effort to mitigate cyber risks, impacted customers unintentionally introduced new failure modes to their systems. It is critical to carefully evaluate zero-trust security implementations to avoid undermining grid resilience while mitigating cyber threats.

Benefits

This project will provide utility subject matter experts with a "zero trust" framework tailored for OT systems, balancing increased complexity with cyber risk mitigation. Architecture guidance and best practices will be developed for various OT environments, including "core" substation or field systems and "edge" distributed energy resources. These frameworks will go beyond topology recommendations, offering support in creating zero-trust policies that effectively balance competing priorities.

As regulatory compliance questions surrounding zero trust begin to affect a subset of utilities, and with the CIP-015 implementation deadline approaching, utilities stand to gain significant value from this collaborative effort. By exploring alternative approaches to the high-availability zero-trust model appropriate for OT environments, this project will equip utilities with the insights needed to make informed decisions about optimal architecture and security controls moving forward.

Project Approach and Summary

This project is broken into three consecutive year-long phases:

1. Launch ZT4OT working group, baseline ZT recommendations, and begin OT architecture development and protocol update.
2. Modify the OT systems architecture based on zero-trust recommendations and develop digital twins to emulate key components and operations. Incorporate a mechanism for monitoring CIP-015 compliance, and compute metrics to evaluate the effectiveness of the digital twin in emulating OT systems.
3. Demonstrate secure architecture and protocols using the digital twin to emulate the impact of ZT on real-world OT operations in a lab environment.

Deliverables

- ZT4OT Modular Substation Architecture
- ZT4OT DER Integration Architecture
- CIP-015 Implementation Guidance
- Digital Twin (Cyber-Cyber-Physical) Models
- Final Report: ZT4OT Strategies and Best Practices

Price of Project

This is a 3-year project with funding set for $100k per year for a total of $300k.

Project Status and Schedule

This project launched in October 15, 2024, with member kickoff planned for mid-January 2025. Expected duration is three years.

Who Should Join

Utilities that are subject to NERC CIP, federal entities subject to U.S. Executive Order, or other utilities focused on improving OT visibility and security.

Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

Technical Contact

John Stewart at 865.279.1447 (jstewart@epri.com)

Technical Advisor Contact Information

Central: Chuck Wentzel at 618.320.0011 (cwentzel@epri.com)

Northeast: Anne Haas at 704.608.6314 (ahaas@epri.com)

Southeast: Barry Batson at 704.595.2879 (bbatson@epri.com)

West: Brian Dupin at 650.906.2936 (bdupin@epri.com)

Product ID: 3002031083 **Project ID:** 01-120170 **April 2025**

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 • USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com