Operational Technology Cybersecurity Coalition

The Zero Trust Mandate: Translating the Philosophy for OT/ICS

Zero Trust has become the premier security model for securing modern Information Technology (IT) environments, representing a fundamental shift in philosophy by relying on the assumption of compromise, strict access controls, and continuous verification of every user and device. Given the convergence between IT and Operational Technology (OT) systems and increasingly connected OT systems, it's natural that organizations are eager to extend these powerful principles into the OT domain.

The Critical Distinction: Where the Carpet Ends

While the boundary between IT and OT systems is often debated and increasingly indistinguishable, the fundamental differences between them are profound. OT systems manage physical processes, from water purification and energy grids to manufacturing and patient care, making availability and safety nonnegotiable priorities. These environments operate on specialized hardware, use legacy protocols, and cannot tolerate the latency or disruption common in IT security implementations. This transition from IT to OT is not seamless. There is a definitive point - often colloquially termed "where the carpet ends" where traditional IT-centric Zero Trust must adapt to the unique realities of industrial control systems (ICS).

Zero Trust in IT vs OT

IT USER-CENTRIC	vs.	OT ASSET-CENTRIC
Protects data		Protects people, processes, and process data
Confidentiality, integrity, and availability (CIA)		Safety, then availability, integrity and confidentiality (AIC)
Assumes no physical access		Physical access assumed
Humans are the risk to the data, not to be trusted		Humans and assets must be trusted for process continuity
Network Segmentation is driven by security		Network Levels are defined by need for speed of access to data
Patching systems is integral to security, and must be done in a timely fashion		Patching systems may introduce instability to physical process, or break interdependencies, and can take time to achieve
Assume environment has already been tainted		Assume the environment is safe to operate
Unsafe operations can be mitigated with technology		Unsafe operations result in shutdown of facilities
Major Risk: Espionage and Financial Loss		**Major Risk:** Strategic disruption and sabotage of national-level functions.

The Necessary Amendments

It is not that Zero Trust fails in OT; rather, its constructs must be amended to address the unique constraints of the OT environment. Applying a full, unmodified Zero Trust model to OT can introduce unacceptable risks to safety and operations. Crucially, this adaptation must be done in concert with not in opposition to, or as a recreation of established OT security frameworks and guidance, such as NIST 80053 and ISA/IEC 62443.

A successful Zero Trust approach for OT will require strategic modifications, including:

- A Holistic Scope: Any elements explicitly scoped out of a Zero Trust Enterprise (ZTE) must be explicitly scoped into equivalent, established OT/ICS guidance, such as ISA/IEC 62443 or NIST SP 80082, in the absence of specific DoW-drafted standards or controls. This ensures no critical components fall through the cracks.
- Acknowledging the "Delta": A clear understanding and widespread acknowledgment of the "delta," the unique differences between IT and OT environments, is paramount. This delta must actively participate in the process of hardening under the scope of ZTE, ensuring that OT-specific requirements drive the adaptation.
- Start with Existing Guidance: To ensure Zero Trust is applied effectively within operational technology (OT) environments, organizations should first enhance and adopt foundational OT cybersecurity standards by building on existing NIST guidance, DoD Instructions, and relevant overlays, while incorporating proven industry frameworks such as ISA/IEC 62443 as reference models. Establishing this baseline will provide comprehensive coverage of OT-specific requirements and clearly define the line of demarcation between OT controls and Zero Trust principles. Once these standards are in place, Zero Trust can then be applied to the remaining areas, ensuring alignment, avoiding overlap, and addressing the delta between IT and OT.

Given the nature of OT/ICS threats, an amended Zero Trust approach is vital for reducing risks and securing critical infrastructure. The OTCC is dedicated to clarifying these differences, providing essential guidance for implementing Zero Trust effectively and appropriately in OT environments.

For more information, please visit www.otcybercoalition.org or email info@otcybercoalition.org.