Zero Trust for OT: Never Trust, Always Verify, Even on the Plant Floor

https://scottslab.io/posts/zero-trust-for-ot-never-trust-always-verify-even-on-the-plant-floor

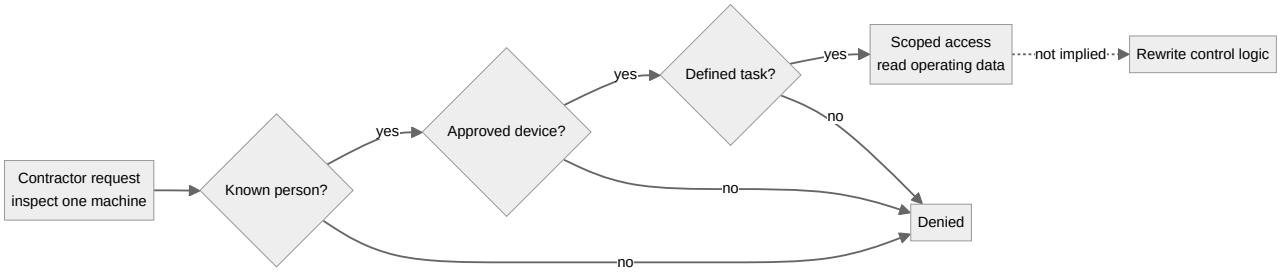
> **TL;DR**
>
> NSA's new guidance applies zero trust to operational technology. What zero trust means, why OT is different, and the practical moves to make first.

> **Watch the 3-minute video:** Zero Trust for OT, Explained in 3 Minutes on The Night Build.

Being inside the network proves nothing.

On October 8, 2026 the NSA published a Cybersecurity Information Sheet, *Hardening Department of War Critical Operational Technology Environments with Zero Trust Principles*. It's aimed at defense networks, but the advice fits anyone running water, power, manufacturing, or building systems. I also made a three-minute video on it for The Night Build. Link below, or keep reading for the written version.

Traditional security works like a castle. Get past the wall and you're trusted everywhere: file shares, operator screens, even the controllers that move physical equipment. Zero trust drops that assumption. Every user, device, and request is verified, every time, and access is scoped to what the task actually needs.



Being inside the network proves nothing.

The Cyber Security Hub write-up has the cleanest example. A maintenance contractor needs to inspect one machine. Under zero trust that access is tied to an identified person, an approved device, a defined task, and only the resources that task needs. Permission to read operating data does not include permission to rewrite control logic.

OT protects the process, not just the data.

Operational technology is the set of computers that control physical things: pumps, valves, power, building automation. In IT we mostly protect data. In OT we protect the process, and the people standing next to it.

That changes the math. A controller may need to run for years without a reboot, inside strict timing limits, next to equipment installed decades ago. A lot of it still works mechanically but has no modern authentication, no encryption, and no easy way to patch. Replacing it can mean engineering reviews, vendor involvement, testing, and a scheduled shutdown.

So you get a bad choice. Leave it alone and the exposure drags on. Change it without understanding the process and you create operational risk.

Wrap what you can't replace.

NSA's central recommendation is to surround legacy equipment with compensating controls: controlled access, segmentation, and monitoring. That buys real protection now while modernization gets planned and funded.

Build bulkheads. Segment so one breach floods one zone, not the whole ship. If a workstation needs production data, that doesn't justify admin access to every device producing it. Then prove the boundaries hold in practice: routing, firewall rules, remote access paths, maintenance arrangements. A diagram that shows separate zones isn't evidence.

Treat remote access as its own risk. An encrypted session can still carry an unauthorized configuration change. A connection that's technically secure and an activity that's operationally authorized are two different things. For every remote path into OT, ask:

1. Who approved it?
2. What can it reach?
3. Is the account still needed?
4. Who can end the session if something looks wrong?

Know what each asset does. An inventory of IP addresses and model numbers is half the picture. Two identical controllers can run lobby lights or chemical dosing. Record what each device controls, what depends on it, who maintains it, and what happens if it goes dark. That context is what tells a responder whether disconnecting something contains a threat or creates an unsafe condition.

Limit authority, not just access. NSA warns that AI is accelerating reconnaissance, exploit development, and full campaigns. Any AI or automation connected to OT should get only the authority its purpose requires. A service that reads telemetry is a very different risk from one that

can change setpoints or issue commands, and that difference belongs in the access policy, written down.

Start with 26, not 84.

NSA picked 26 high-impact activities out of a broader framework of 84 OT zero trust activities as a manageable starting point. They cover remote access, data protection, inventory, visibility, threat intelligence, controller hardening, segmentation, engineering workstations, identity, and safe validation.

My short version: verify, segment, watch, and limit. The goal isn't a perfect architecture. It's keeping safe control of the physical process even when an account, a workstation, or a connected system is compromised.

This is my first post on OT. If you work in this space, I'd like to hear which of those 26 you'd tackle first in your environment.

Sources

- NSA: NSA Releases Zero Trust Guidance for Protecting Operational Technology Systems
- Cyber Security Hub: NSA Urges Zero Trust Defences To Protect Critical Infrastructure and Ageing Industrial Systems
- Industrial Cyber: NSA urges zero-trust controls to protect DoW OT systems

---

Written by Scott S. — Contact: scott@scottschlangen.com — scottslab.io — https://scottslab.io/posts/zero-trust-for-ot-never-trust-always-verify-even-on-the-plant-floor