



WHITE PAPER

Zero Trust Starts at the Purchase Order

How Open Process Automation addresses the root causes behind the NSA's October 2026 guidance on hardening operational technology with zero trust

OPEN • STANDARDS • RESULTS

Trevor Cusworth

Collaborative Systems Integration (CSI)

October 2026

Contents

Executive summary..... 3

1. What the NSA guidance says..... 4

2. The root cause: insecure by design and locked in..... 6

3. O-PAS in brief..... 7

4. Mapping the NSA activities to O-PAS..... 9

5. Legacy coexistence: where the two approaches meet..... 11

6. What OPA does not do..... 12

7. Writing zero trust into the specification..... 13

8. A roadmap for plant owners..... 14

9. Conclusion..... 14

About the author and next steps..... 15

References..... 15

Executive summary

The NSA's October 2026 guidance on hardening operational technology (OT) with zero trust is a plan for protecting systems that cannot protect themselves. Open Process Automation (OPA) is a way to stop buying more of them. The two are complementary, and plant owners need both.

The guidance names 26 high-impact activities, drawn from the Department of War's 84 OT zero trust activities, that organisations can start now. By design they are compensating controls: gateways, enclaves, segmentation, monitoring, and identity and access controls wrapped around legacy assets that lack native encryption, modern authentication or a safe way to patch.

That approach is right for the installed base. It also leaves the root cause in place. The guidance itself says the best fix for an insecure smart controller is usually to upgrade it to the vendor's newest secure model, which takes engineering review, testing, outage coordination and vendor support. In a single-vendor architecture, that upgrade is tied to one supplier's roadmap and often to a system-wide migration.

The Open Process Automation Standard (O-PAS) changes the terms of that upgrade. Security based on ISA/IEC 62443 is part of the conformance requirements for every component and interface. Communication runs on OPC UA, which has authentication, signing and encryption built in. Components are bought separately, certified independently, and replaced without redesigning the system.

This paper maps the NSA activities to the O-PAS mechanisms that support them, sets out where OPA does not help, and gives practical steps for writing zero trust requirements into the next control system specification.

The central idea

The NSA guidance tells owners how to protect the insecure systems they already own. OPA is how they stop buying more of them. Compensating controls make the gap safer; changing what gets bought is what closes it.

A note on scope

The NSA guidance does not mention OPA, O-PAS, ISA/IEC 62443 or OPC UA. Nothing here suggests the NSA endorses OPA. The argument is that OPA addresses the root causes the guidance describes.

1. What the NSA guidance says

The Cybersecurity Information Sheet *Hardening Department of War (DoW) Critical Operational Technology (OT) Environments with Zero Trust (ZT) Principles* (U/OO/6070841-26, version 1.0) was released on 8 October 2026. It is written mainly for owners and operators of National Security Systems, the Department of War and the Defense Industrial Base. The NSA says it also applies to technical leaders and to IT and OT managers more widely.

The threat it responds to

The guidance cites three patterns of attack on critical infrastructure:

- ▶ **Pre-positioning.** Volt Typhoon, a PRC state-sponsored group, gains long-term covert access through IT networks, then pivots to OT using "living-off-the-land" techniques. The aim is the ability to disable systems such as power grids at a time of its choosing.
- ▶ **Exploiting exposed devices.** Iran-affiliated actors targeted PLCs in the water and wastewater sector through internet-exposed devices and default administrator credentials (joint advisory AA26-097A).
- ▶ **Disruption and ransomware.** These include attacks on the Ukrainian grid and on U.S. water systems, and ransomware such as Colonial Pipeline.

It also warns that adversaries now use advanced AI, which it calls super intelligence (SI), to automate reconnaissance and speed up exploit development. It ties its approach to the SANS ICS Cyber Kill Chain. The intent is to break the attack at several stages, not rely on the perimeter.

The approach

Zero trust, as defined in NIST SP 800-207, assumes the environment is already compromised. It continuously verifies users, devices, workloads and communications. The DoW framework organises this into seven pillars: user; devices; applications and workloads; data; network and environment; visibility and analytics; and automation and orchestration.

Those pillars break down into 45 capabilities. DoW OT guidance defines 84 activities. This information sheet picks the 26 with the most immediate effect, chosen because they "wrap legacy assets in protective enclaves without requiring intrusive hardware modifications."

The ten priority areas

1. Securing remote access
2. Protecting OT data
3. Inventorying OT assets
4. Enhancing OT environment visibility
5. Using OT cyber threat intelligence
6. Hardening smart controllers
7. Strengthening networks with segmentation and monitoring
8. Securing engineering workstations and HMIs

9. Hardening Active Directory and domain controllers

10. Verifying zero trust controls safely, by passive means first

The guidance also points to the Operational Technology Assurance Partnership (OTAP). OTAP is an NSA pilot program for conformance testing of OT installed in National Security Systems.

2. The root cause: insecure by design and locked in

The NSA says plainly why OT is hard to secure. Systems often stay in service for more than 50 years. Many "are no longer supported by vendors and are unable to receive vital patches or updates." They often "lack native encryption, modern authentication protocols, or the ability to be patched without disrupting essential services." The guidance calls these "insecure-by-design systems." It describes a "mission-risk paradox": hardware built for decades of physical reliability, running on a cybersecurity architecture that is obsolete.

Its answer for now is to work around that limit: "the path forward lies in utilizing compensating controls that provide modern protection without requiring a total hardware overhaul."

Why the best fix is the hardest one

In the section on hardening smart controllers, the NSA says "upgrading a device to the vendor's newest, secure model is usually the best solution." It then lists what that upgrade takes: "engineering review, testing, outage coordination, contingency planning, and vendor support."

In a traditional distributed control system (DCS), that list describes a lock-in that is built into the architecture. Each vendor supplies the full stack: controllers, I/O, networking, runtime, engineering tools and lifecycle services. Interfaces are tuned internally and rarely standardised externally. Control logic is tied to the platform it was written on.

That coupling has three security consequences:

- ▶ **Security is only as current as one vendor's roadmap.** If the vendor has not built native encryption or modern authentication into its next controller, the owner has no other conformant option.
- ▶ **Replacing one component means revalidating the system.** Hardware, software and tools are co-dependent, so a controller upgrade spreads across the stack. This is why insecure devices stay in service.
- ▶ **Upgrades come in large, rare steps.** Owners are held back by the cost of leaving: engineering effort, revalidation, retraining and operational risk. Upgrades are deferred until they are unavoidable. The exposure the NSA describes is the gap between those steps.

Compensating controls make that gap safer. They do not close it. Closing it means changing what gets bought.

3. O-PAS in brief

In a traditional architecture, the vendor's platform defines the system. In O-PAS, the standard defines the system, and the owner assembles it from components that meet the standard. The Open Process Automation Forum (OPAF) develops the standard under The Open Group. End users set the requirements and suppliers contribute the technology. It is published in fourteen parts that can be revised independently. Version 2.1 became a full standard in February 2023.

Six elements matter for security:

- ▶ **Conformant components.** The basic unit is any hardware or software built and certified to behave according to a profile in the standard. You buy components, not a system.
- ▶ **Distributed control node (DCN).** This is the main execution unit. A DCN is defined by the interfaces it exposes, not by its form factor. It has a Physical Platform (Part 7) with a standard software framework above it, so applications run the same way whichever vendor's hardware sits underneath. A larger DCN, the Advanced Computing Platform (ACP), hosts heavier applications such as historians and advanced control.
- ▶ **O-PAS Connectivity Framework (OCF).** Part 4 sets out how components talk to each other. It is built on OPC UA and covers transport, data structure, quality of service and "the security requirements that apply to every exchange." Diagrams draw the OCF as one fabric. Real plants may build it from segmented networks, VLANs and firewall boundaries.
- ▶ **Information model.** Units, scaling, validity and the equipment a signal belongs to travel with the signal itself. Control logic is expressed as function blocks, supporting both the IEC 61131-3 cyclic model and the IEC 61499 event-driven model. Configuration moves between engineering tools and runtimes in a standard form, so tools and runtimes can be bought separately.
- ▶ **System management.** Every component exposes standard management interfaces based on the DMTF Redfish standard. That gives the owner one consistent way to monitor, configure and update components, instead of a different tool for each vendor.
- ▶ **Profiles, conformance and security.** Part 3 defines profiles, which are testable sets of requirements for a role. The Open Group's O-PAS Certification Program checks independently that components meet them. Part 2 covers security and is built on the ISA/IEC 62443 family. Each profile inherits security requirements from Part 2, and conformance to a profile requires conformance to its security facets. Conformance is kept up over time and has to be renewed as the standard and the components change.

For existing equipment there is the **gateway DCN**. It exposes a legacy DCS, PLC or field device through conformant interfaces without modifying the device. Section 5 returns to this.

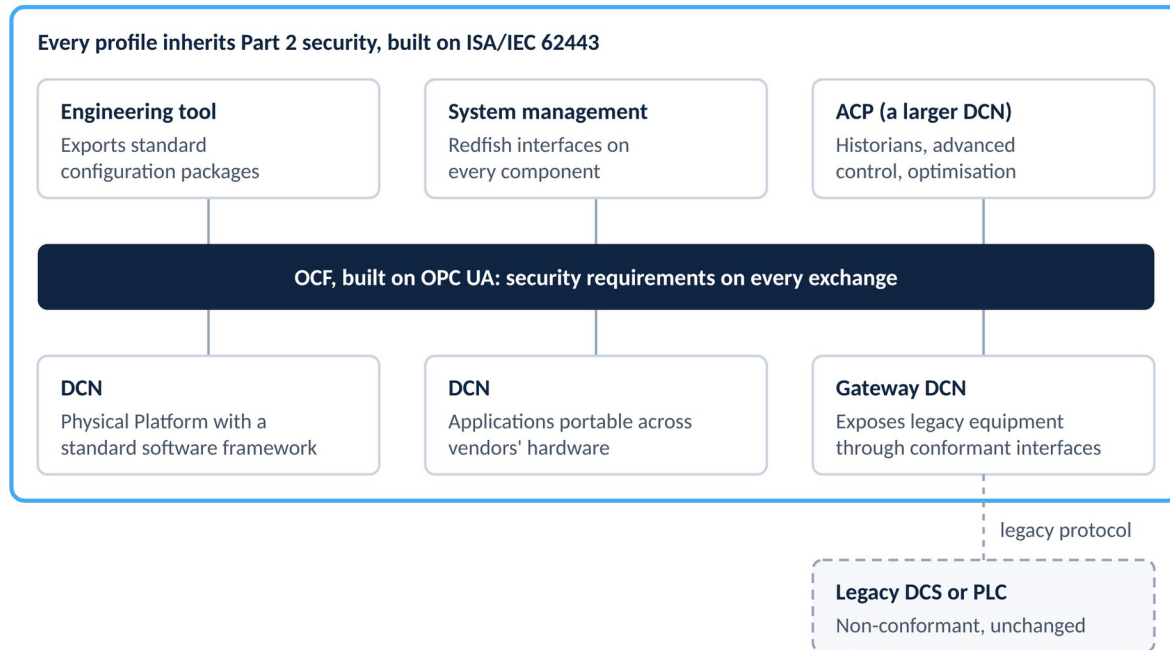
Security is inherited by every component and every exchange

Figure 1. Everything inside the boundary meets profiles that carry Part 2 security requirements. The legacy system sits outside it, reached only through the gateway DCN.

4. Mapping the NSA activities to O-PAS

O-PAS gives strong support to three of the NSA's priority areas and partial support to five. Its certification program runs parallel to the NSA's OTAP pilot. It is neutral on segmentation and offers nothing on identity, threat intelligence or endpoint detection. Activity numbers are those in the NSA's Table 1. "Fit" is CSI's assessment, not the NSA's.

NSA activity	What the NSA asks	What O-PAS provides	Fit
5.4.3 Protect OT data in transit	Confidentiality, integrity, authenticity and availability of OT communications. Where a protocol cannot encrypt, use a broker, enclave, gateway or tunnel	The OCF is built on OPC UA, which has authentication, signing and encryption built in, with security requirements on every exchange. The NSA notes encryption alone does not meet this activity, so availability and timing remain design work	Strong
4.1.1 OT data tagging governance	A governing body to define controlled terminology, file formats and protocols for interoperable data	The O-PAS information model carries units, scaling, validity and equipment context with each signal. OPAF and The Open Group govern it across vendors	Strong
2.5.1 Vulnerability and patch management, plus hardening smart controllers	Patch by risk. Where possible, upgrade to the vendor's newest secure model	Components are bought and replaced one at a time, and logic is portable between conformant runtimes. Upgrading an insecure controller becomes a component change, not a system migration	Strong
2.1.1 Inventory non-person entities; 3.1.1 Application and code inventory	A living inventory of hardware, software, firmware, addresses and services	Every component exposes standard management interfaces based on DMTF Redfish. Check which inventory attributes the relevant O-PAS profiles require	Partial
2.6.2 OT device configuration management	Defined configuration standards and automated configuration management	Standard management interfaces, and a standard way to move configuration between engineering tools and runtimes	Partial
3.3.1 Binaries, code and hardware configurations	Application control; disable unused logic	Logic is expressed as function blocks with defined inputs, outputs, state and parameters, which makes it easier to see. Application control is still a deployment task	Partial
2.2.1 Connection policy for OT	Define and enforce authorised protocols and connection paths	One standard communication framework narrows the set of protocols to approve and baseline. This is CSI's inference, not a stated O-PAS requirement	Partial
Compensating gateways and enclaves (general)	Wrap legacy assets that cannot support zero trust natively	The gateway DCN exposes legacy equipment through conformant interfaces without modifying it. It is an interoperability mechanism and does not by itself count as a security enclave	Partial

NSA activity	What the NSA asks	What O-PAS provides	Fit
OTAP (further reading)	NSA pilot conformance testing for OT in National Security Systems	The O-PAS Certification Program independently verifies conformance to profiles, including their security facets, and requires recertification as things change	Parallel
5.4.1 Micro segmentation; 5.3.1 and 5.3.2 Plane and site segmentation	Logical zones and enforced communication paths	The OCF can be implemented as segmented networks, VLANs and firewall boundaries. O-PAS allows segmentation but does not design it	Neutral
1.1.1 to 1.8.1 Identity, MFA, PAM, deny by default	Inventory accounts, phishing-resistant MFA, privileged access management, least privilege	Not addressed by O-PAS. See section 6	None
2.7.1 EDR; 4.4.x Data loss prevention and file monitoring; 7.1.2 Log parsing; 7.5.x Threat intelligence	Detection, monitoring and threat intelligence across the OT environment	Not addressed by O-PAS. See section 6	None

5. Legacy coexistence: where the two approaches meet

The NSA's compensating controls and OPA's migration model share an assumption: the legacy installed base will keep running for years and cannot be modified safely. Both wrap it rather than replace it at once.

Two forms of wrapping

The NSA wraps legacy assets for security. It uses "ZT-enabled gateways, ruggedized network devices, micro-segmentation, and continuous monitoring" so that a device which cannot authenticate or encrypt is shielded by controls around it.

O-PAS wraps legacy assets for interoperability. A gateway DCN exposes the data and functions of an existing DCS, PLC or field device through conformant interfaces, without changing the device. To the rest of the architecture, the legacy system looks like one more component that provides data and receives commands.

Using them together

CSI's recommendation is to design the two wrappers as one boundary:

- ▶ **Put the gateway DCN at the edge of the NSA enclave.** Legacy protocols stay inside a segmented zone. Traffic leaving the zone goes over the OCF on OPC UA, with the security O-PAS requires on every exchange.
- ▶ **Monitor at the same point.** The gateway is where legacy traffic is translated, so it is the natural place for the baseline and anomaly monitoring the NSA calls for under activities 2.2.1 and 2.7.1.
- ▶ **Shrink the enclave over time.** In OPA migration, control functions move gradually from legacy equipment to conformant DCNs. Each function that moves leaves the compensating-control zone and runs on components with security built into their conformance.

This is migration through coexistence. Risk is spread across smaller steps, each one checked before the next, instead of piling up at a single cutover. The compensating controls protect what remains. They are not there to stay.

6. What OPA does not do

O-PAS is an architecture standard. Much of the NSA guidance concerns identity, operations and detection, which no architecture provides. A plant that adopts OPA and skips these activities is not running zero trust.

- ▶ **Identity and access.** Account inventory (1.1.1), credentialing and role-based access (1.2.1, 1.2.2), phishing-resistant MFA (1.3.1), privileged access management (1.4.1), identity lifecycle (1.5.1), deny by default (1.7.1) and per-session authentication (1.8.1) all remain the owner's job.
- ▶ **Active Directory and domain controllers.** The NSA's advice on tiered administration, Group Policy hardening and attribute-based access applies whatever the control architecture.
- ▶ **Third-party and vendor remote access.** In multi-vendor systems this matters more, not less. More suppliers can mean more remote sessions to approve, time-limit, record and end.
- ▶ **Engineering workstations and HMIs.** Logging, application control, file monitoring and physical security of these machines are outside O-PAS.
- ▶ **Detection and response.** EDR (2.7.1), log parsing (7.1.2), data loss prevention and file monitoring (4.4.x), and an OT cyber threat intelligence program feeding a SIEM (7.5.1, 7.5.2) all have to be built and run.
- ▶ **The installed base.** O-PAS changes what you buy next. It does nothing for a 25-year-old DCS already in service, apart from giving it a route out through the gateway DCN.
- ▶ **The IT-to-OT pivot.** Groups such as Volt Typhoon get into IT networks first and move into OT. Architecture cannot stop that by itself; segmentation and monitoring at the IT/OT boundary still carry the load.

One OPA failure mode also bears on security. Owners can recreate vendor lock-in by letting one supplier provide most components, or by relying on vendor-specific extensions. The system then looks open but behaves as a platform. The security gains in section 4 depend on keeping interfaces standard and conformance current.

7. Writing zero trust into the specification

The cheapest time to meet the NSA's activities is before the purchase order is signed. A traditional DCS specification describes what the system must do and leaves security to the vendor's platform. An OPA-aligned specification describes components, the interfaces between them, and the conformance each must prove. That gives the owner a place to write security requirements that can be tested.

Where security requirements belong

- ▶ **Request for proposal (RFP).** For each component role, state the O-PAS version, the profiles to be certified, and the security facets those profiles inherit from Part 2. Score architectural fit and conformance before cost. That avoids buying the cheapest component that meets the letter of the specification but not its intent.
- ▶ **Conformance Requirements Specification (CRS).** List the profiles each component must meet, with version numbers. Require independent test reports from The Open Group's O-PAS Certification Program as the minimum evidence. Say what happens if a conformance failure is found after award.
- ▶ **Interface Control Document (ICD).** For each interface, record the security requirements alongside data, timing and error handling. Keep the ICD under change control. Uncontrolled change is the main way interfaces drift, and drifted interfaces are where both interoperability and security get weaker.
- ▶ **Lifecycle support clauses.** Require suppliers to maintain conformance as the standard changes, to recertify after updates, and to cooperate with other suppliers on vulnerability fixes. Spell out how these duties survive acquisitions and end-of-life announcements.
- ▶ **Remote access terms.** Write in the NSA's conditions for third-party and OEM access: phishing-resistant MFA, policy-based authorisation, time-bound sessions, recording and immediate termination.

Questions to put to every supplier

1. Which O-PAS profiles is this component certified to, against which version of the standard, and where is the certification evidence?
2. Which of the NSA's 26 activities does this component support natively, and which will need compensating controls?
3. Which OPC UA security modes does it support, and are they on by default?
4. What inventory, firmware and configuration data does it expose through its standard management interface?
5. If we replace it with another supplier's conformant component, what has to be revalidated, and does our control logic move with it?
6. How quickly do you recertify after a security update, and who pays for it?

8. A roadmap for plant owners

Start the NSA activities on the installed base now. Write O-PAS conformance into the next control system purchase. Then use coexistence to move functions out of the compensating-control zone one step at a time.

Compensating controls now, conformance from the next purchase on

Phases are not to scale and overlap in practice

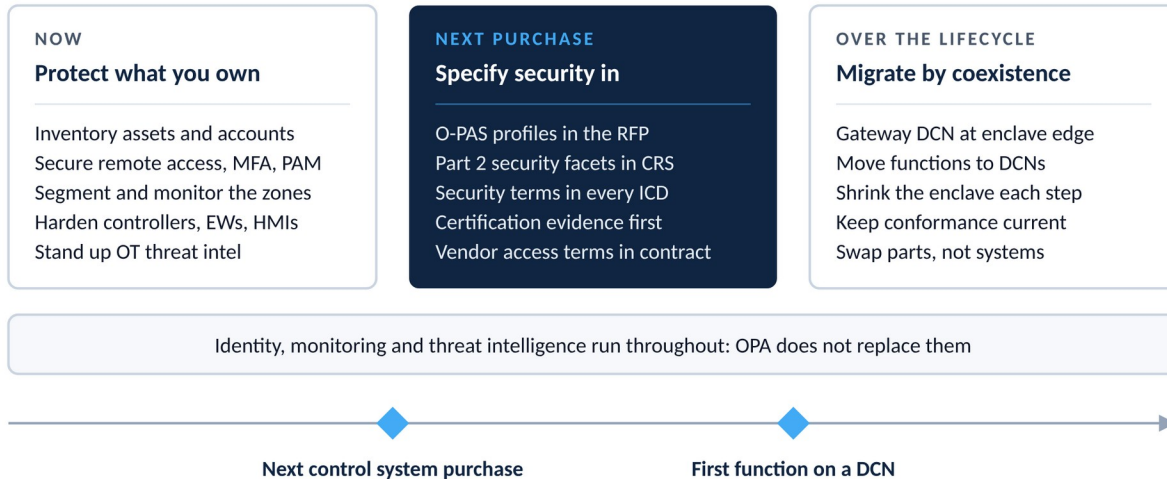


Figure 2. Three phases and two gates. The middle phase is the one most often missed: it costs least and decides how long the first phase has to last.

9. Conclusion

The NSA guidance tells owners how to protect the insecure systems they already own. OPA is how they stop buying more of them. The 26 activities should start now, because the threat is current and the installed base will be in service for years. But compensating controls only manage the exposure. Each new single-vendor system bought with security as a platform feature extends the problem by another lifecycle.

O-PAS moves security from the vendor's roadmap into the owner's specification. Requirements are written against a standard, proved through independent certification, and kept up as components change. When a controller falls behind, it is replaced as a component, not through a system migration.

About the author and next steps

Trevor Cusworth is a Principal at Collaborative Systems Integration (CSI), a vendor-neutral industrial automation consultancy he co-founded with Don Bartusiak. He has 47 years of process manufacturing experience across ICI, Imperial Oil, Aspen Technology, Invensys, Hagen & Company, Deloitte and Schneider Electric. He co-chairs Marketing and Outreach for the Open Process Automation Forum, having served as Forum Co-Chair from 2017 to 2023. CSI is a co-founding member of COPA.

Learn more

- ▶ Start with the free [Introduction to Open Process Automation](https://csi.learnworlds.com) course at csi.learnworlds.com.
- ▶ Model the lifecycle cost of both architectures with the [CSI ROI Calculator](#).
- ▶ For the full treatment of architecture, migration and procurement, including the RFP, ICD and CRS templates referred to in section 7, read *Open Process Automation: Architecture, Execution, and Transformation* by Trevor Cusworth, available on Amazon.

References

Primary sources

- ▶ National Security Agency. [Hardening Department of War \(DoW\) Critical Operational Technology \(OT\) Environments with Zero Trust \(ZT\) Principles](#). Cybersecurity Information Sheet U/OO/6070841-26, version 1.0, October 2026. All quotations and activity numbers in this paper come from this document.
- ▶ Cusworth, T. *Open Process Automation: Architecture, Execution, and Transformation*. The O-PAS descriptions in sections 3, 5 and 7 are drawn from it.

Cited in the NSA guidance

- ▶ NIST. [SP 800-207, Zero Trust Architecture](#). 2020.
- ▶ NIST. [SP 800-82r3, Guide to Operational Technology \(OT\) Security](#). 2023.
- ▶ Department of Defense. [Zero Trust for Operational Technology Activities and Outcomes](#). 2025.
- ▶ CISA et al. [Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure \(AA26-097A\)](#). 2026.
- ▶ CISA et al. [Adapting Zero Trust Principles to Operational Technology](#). 2026.
- ▶ National Security Agency. [Operational Technology Assurance Partnership: Smart Controller Security within National Security Systems](#). 2025.