OT Supply Chain Visibility at the Field Level

INFCIRC/908: Regional Workshop on Addressing Evolving OT Impacts for ITM and Supply Chain Security

Helsinki, Finland, 16-18 June 2026

Presented By: Shannon Eggers, Idaho National Laboratory

INL/CON-26-92870

U.S. DEPARTMENT of ENERGY

National Nuclear Security Administration

Visibility Assumed. Verification Absent.

A new vulnerability is disclosed in a widely used embedded OS component. It affects devices running version 4.x firmware. Do you know which of your field devices are running that version — right now?

Procurement	Engineering	Cybersecurity
Sees Knows what was ordered	Sees Knows what was designed	Sees Monitors OT network traffic
Blind spot Not what was installed or updated in the field	Blind spot Not what changed during maintenance or outages	Blind spot Rarely has component-level firmware visibility

End users often lack visibility and understanding of how acquired technology is developed, integrated, deployed, and maintained.

The OT Visibility Challenge: Why traditional tracking fails in OT

20 to 40-year lifecycles
The original supply chain context — vendors, software versions, component sourcing — is often lost long before a vulnerability is discovered.

Multi-tier opacity
A nuclear digital I&C system may pass through a prime contractor, multiple subcontractors, an integrator, and an OEM — each adding firmware, libraries, or configuration.

Procurement ≠ installation
Procurement records capture the contract. They rarely capture what firmware version was installed during a scheduled outage three years later.

OT/IT convergence risk
As OT systems connect to IT networks for monitoring and remote diagnostics, the supply chain attack surface expands into territory that traditional OT security does not address.

Update mechanisms as vectors
Firmware updates, vendor patches, and maintenance laptops are all legitimate — and all represent unverified supply chain touchpoints at the field level.

The Human Factor: Who has access in the OT supply chain?

Insiders are individuals with authorized access who could commit or facilitate malicious acts — or be unwittingly exploited. In OT environments, the insider population is wider than most programs assume.

OEM vendors

Access type

Firmware delivery, remote diagnostics, patch deployment

Visibility concern

Trusted but component-level changes rarely verified at receipt

System integrators

Access type

Installation, configuration, commissioning

Visibility concern

Often have deep knowledge of protection and control architecture

Maintenance personnel

Access type

Replacement parts, calibration, outage work

Visibility concern

Physical access to field devices; changes may be undocumented

Managed service / remote access

Access type

Ongoing monitoring, vendor diagnostics, patch mgmt

Visibility concern

Persistent privileged access; may not be subject to full trustworthiness review

Contractors & inspectors

Access type

Construction, assessments, regulatory visits

Visibility concern

Periodic access; may have sensitive system or layout knowledge

Unwitting insiders

Access type

Any staff targeted via phishing or social engineering

Visibility concern

No intent — but access, authority, or knowledge can be exploited

Everyone who has authorized access — vendors, contractors, inspectors — are potential insider threats.

U.S. DEPARTMENT of ENERGY
NNSA National Nuclear Security Administration

Practical Tools: From procurement records to field-level traceability

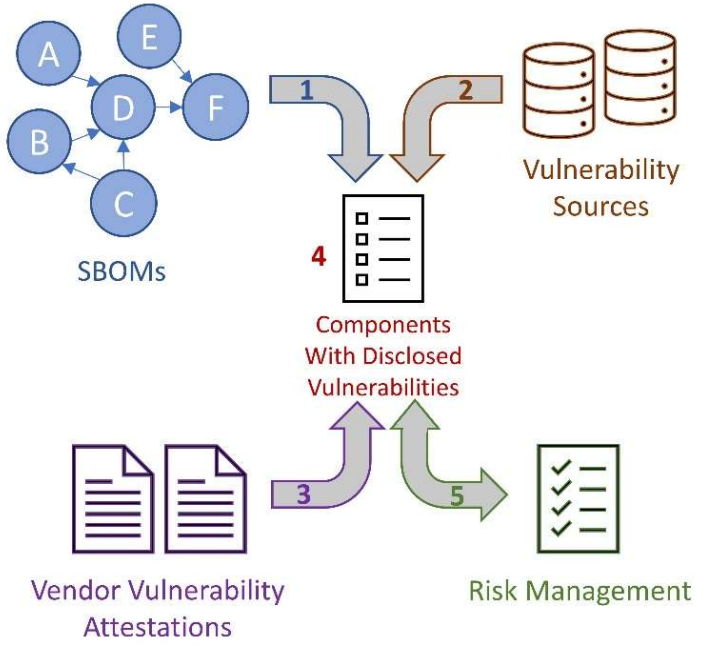
SBOM	**Software Bill of Materials** Machine-readable inventory of software components, versions, dependencies, and supply chain relationships in a system or device. Rapid impact analysis on CVE disclosure. Connects a vulnerability advisory to specific installed assets.
HBOM	**Hardware Bill of Materials** Component-level record of hardware provenance: part numbers, revision history, manufacturer, supplier, country of origin. Counterfeit detection, lifecycle tracking, identification of components from high-risk sources.
Passport STAMP	**Software Trace of a Manufacturing Process/Product** A complete trace of all software that touched the function or structure of a manufactured physical artifact, including design tools, compilers, machine firmware, process control software. Answers not just "what software is in this device" but "what software shaped this physical component."
Lifecycle tracking	**End-to-end digital asset records** Continuity from procurement through installation, modification, maintenance, and decommission; linked to specific physical devices. Closes the gap between design intent and field reality. Enables response to field-level vulnerability queries.

SBOMs & vulnerability tracking

Best Practices:

- SBOM program with extended Passport STAMPS generated through the manufacturing cycle
- Equipment database with detailed configuration management information for all digital assets

Enables improved vulnerability and risk management.



Vulnerability Management: From disclosure to your field devices — can you close the loop?

1 — Disclosure
ICS-CERT or NVD advisory published for a component version

2 — Component Search
Is that component installed in your facility?

3 — Version Mapping
Are you running the affected firmware or software version?

4 — Location
Which specific devices, in which systems, at which sites?

5 — Risk evaluation
Is it safety-significant? Where is it in the DCSA? What security controls protect it?

6 — Response
Patch or mitigate? Accept and document as is?

Without field-level inventory and SBOMs, steps 2–4 become manual investigations lasting weeks — during which vulnerable devices remain in service.

Vulnerability Disclosure Reports (VDRs) paired with SBOMs allow operators to rapidly determine whether a disclosed CVE affects their installed base — the "find all affected assets" problem.

U.S. DEPARTMENT of ENERGY
National Nuclear Security Administration

Case Study: Supply chain as the delivery mechanism

Discovered in 2010, Stuxnet was a sophisticated malware designed to physically destroy uranium enrichment centrifuges at Iran's Natanz facility by manipulating Siemens S7 PLCs. No witting insider has been confirmed. The attack succeeded by weaponizing the supply chain and exploiting the trust extended to contractors and their equipment.

Supply Chain Attack TTPs

Delivery via infected USB drives

Stuxnet spread through USB media introduced by contractors and equipment suppliers servicing the air-gapped facility — the supply chain physically bridged the air gap.

Targeted Siemens Step 7 software supply chain

Stuxnet intercepted and modified Siemens' own engineering software, so infected project files were silently passed from supplier workstations to field PLCs during routine programming and maintenance.

OT / Insider Threat Aspects

Unwitting insiders as the delivery vector

Contractors carrying infected laptops and USB drives had no knowledge they were delivering a weapon. This is the IAEA NSS 8-G §2.9 unwitting insider scenario operationalized at national-infrastructure scale.

Insider-level OT knowledge, externally acquired

Attackers knew specific PLC models, centrifuge cascade configuration, and safe RPM tolerances — knowledge that would normally exist only inside the facility. Likely sourced through supply chain intelligence, procurement documents, and vendor relationships.

Case Study: Supply chain as the delivery mechanism

Discovered in 2010, Stuxnet was a sophisticated malware designed to physically destroy uranium enrichment centrifuges at Iran's Natanz facility by manipulating Siemens S7 PLCs. No witting insider has been confirmed. The attack succeeded by weaponizing the supply chain and exploiting the trust extended to contractors and their equipment.

Supply Chain Attack TTPs

Stolen digital certificates from trusted OEM vendors

Stuxnet's drivers were signed with legitimate digital certificates stolen from Realtek Semiconductor and JMicron Technology — both trusted hardware vendors. Operating systems accepted the malware as verified, legitimate software.

Compromised software trust chain

By signing malicious code with stolen OEM certificates, Stuxnet bypassed every host-based security control that relied on code signing as proof of integrity. The trust model itself became the attack surface.

OT / Insider Threat Aspects

Why certificate theft matters for OT supply chains

OT environments routinely trust vendor-signed firmware and software updates without secondary verification. If an attacker controls a signing certificate — or the vendor's build environment — digitally signed does not mean trustworthy.

No asset inventory = no anomaly baseline

The absence of a precise field-level inventory of PLC types, configurations, and expected behaviors meant there was no baseline against which to detect the manipulation. Operators relied on the SCADA display — which Stuxnet had compromised.

Case Study: Supply chain as the delivery mechanism

Discovered in 2010, Stuxnet was a sophisticated malware designed to physically destroy uranium enrichment centrifuges at Iran's Natanz facility by manipulating Siemens S7 PLCs. No witting insider has been confirmed. The attack succeeded by weaponizing the supply chain and exploiting the trust extended to contractors and their equipment.

Supply chain = insider access

No witting insider needed. Contractors, vendors, and their software are trusted by default. That trust is the vulnerability.

Digital signatures are not sufficient alone

Stuxnet was signed with legitimate stolen certificates from Realtek and JMicron. Signed ≠ safe. OT patch and update workflows that rely solely on code signing as the integrity check are exposed to this exact vector.

Field inventory enables anomaly detection

Knowing exactly what is installed, in what configuration, with what expected behavior is the precondition for detecting manipulation.

Cyber supply chain guidance

Domain	Publication
Nuclear	IAEA TDL-011, Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain
	IAEA NSS 8-G, Preventive & Protective Measures against Insider Threats
	IAEA NSS 17-T, Computer Security of Instrumentation & Control Systems
	UK NSCS/DSIT, Cyber Assessment Framework; OT Supply Chain Guidance
	NEI 08-09 rev 7 Add. 3, Cyber Security Plan for Nuclear Power Reactors, Systems and Services Acquisition
	EPRI Cyber Security in the Supply Chain: Cyber Security Procurement Methodology
	EPRI Secure Development, Integration, and Delivery (SDID) Audit Topical Guide
ICS/OT	EU NIS2 Directive, Art. 21 — Supply chain security obligations (2023
	ENISA, Threat Landscape for OT/ICS (2023); Supply Chain Guidelines
	ANSSI, ICS Cybersecurity Guide; EBIOS RM method
	DHS Cyber Security Vendor Procurement Language for Control Systems
	IEC 62443-2-4, Security Program Requirements for IACS Solution Suppliers
	IEC 62443-4-1, Secure Product Development Lifecycle Requirements
	UL 2900-2-2, Part 2-2, Particular Requirements for Industrial Control Systems
Energy	DOE Cybersecurity Capability Maturity Model (C2M2)
	EPRI Cyber Security Procurement Methodology for Power Delivery Systems
	ESCSWG, Cybersecurity Procurement Language for Energy Delivery Systems
	NERC CIP-013-1, Cyber Security-Supply Chain Risk Management

Cyber supply chain guidance

Domain	Publication
ICT	CISA, https://www.cisa.gov/topics/information-communications-technology-supply-chain-security
	CISA, Vendor Supply Chain Risk Management (SCRM) Template
	CISA, Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists
	ENISA Threat Landscape for Supply Chain Attacks
	ISO/IEC 27036-3, Information Security for Supplier Relationships, Part 3, Guidelines for ICT Supply Chain Security
	ISO/IEC 20243-1, Information Technology-O-TTPS-Mitigating maliciously tainted and counterfeit products
	NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems
	NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security
	NIST SP 800-147, BIOS Protection Guidelines
	NIST SP 800-147b, BIOS Protection Guidelines for Servers
	NIST SP 800-161 R1, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
	NIST SP 800-218, Secure Software Development Framework (SSDF)
	UL 2900-1, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
Software	SAFECode, Fundamental Practices for Secure Software Development
	SAFECode, The Framework for Software Supply Chain Integrity
	Center for Internet Security, CIS Software Supply Chain Security Guide
	SAFECode, Managing Security Risk Inherent in the use of Third-Party Components
	CISA, Defending Against Software Supply Chain Attacks

Guidance Example: A three-level approach applied to nuclear OT

NIST SP 800-161r1 describes a multilevel risk management hierarchy. The model is designed so that enterprise-level strategy shapes operational-level controls — and operational findings feed back upward to refine the strategy.

Level 1 Enterprise	CSCRM strategy and policy; risk appetite; governance structure; supplier inventory (SR-13); enterprise-wide SBOM/HBOM requirements embedded in procurement policy and contract language.
Level 2 Mission / Program	Program-specific CSCRM plans; CDA identification; vendor assessment processes; trustworthiness determinations for personnel with OT access; information sharing with ISACs and CISA.
Level 3 Operational (Field)	Component-level asset inventory (CM-8); installed firmware/software tracking; access records for every party touching a field device including remote access; vulnerability monitoring tied to specific installed versions; C-SCRM plan per system.

Key controls mapped to field-level OT (NIST 800-161r1):

SR-13

Supplier inventory — know every tier-1 supplier and their criticality to specific systems

CM-8

Component inventory — track every installed component, version, and firmware revision

RA-5

Vulnerability monitoring — scan across the supply chain, including sub-suppliers

MA-4

Nonlocal maintenance — control and audit all vendor remote access to OT systems

Key Takeaways: What field-level supply chain visibility requires

✓ **Asset inventory to the component level**	Not just system names. Include firmware versions, software revisions, and hardware provenance for every field device.
✓ **SBOMs and HBOMs at procurement and maintenance.**	Requested contractually, maintained through modifications — not a one-time document.
✓ **Access records that capture every human touchpoint**	Every vendor, contractor, and integrator who accesses a field device — including remote access — logged and retained.
✓ **Vulnerability response that traces from advisory to device**	A process that answers "which of our installed devices run the affected version?" in hours, not weeks.
✓ **Insider threat integrated into supply chain risk**	Vendors, integrators, and maintenance personnel are part of the insider threat picture.

Visibility is not a one-time audit. It is a capability — built through procurement requirements, maintained through lifecycle discipline, and tested through vulnerability exercises.

Thank You!