OPERATIONAL TECHNOLOGY CYBERSECURITY COALITION

A Unified Approach to OT Cybersecurity

ISA / IEC 62443 Position Paper

OTCC supports harmonization of cybersecurity standards for industrial and operational technology (OT) systems

Operational Technology Cybersecurity Coalition

Table of Contents

Operational Technology Cybersecurity Coalition

Executive Summary

To combat regulatory fragmentation, the Operational Technology Cybersecurity Coalition (OTCC) advocates for a single, horizontal standard to govern industrial and operational technology (OT) cybersecurity. Policy should prioritize one globally interoperable framework over a patchwork of sector-specific mandates. Established frameworks such as ISA/IEC 62443, a globally recognized set of standards for securing industrial control systems, are leading options for this type of formal recognition and adoption. This approach reduces regulatory sprawl, simplifies compliance for critical infrastructure owners and operators, and strengthens national resilience through a unified defensive baseline.

- OTCC supports cybersecurity policies that are cohesive, adaptable, risk-based, and interoperable at a global level. We advocate for the creation and use of consensus-based technical standards, guidelines, practices, processes, and definitions that facilitate the management of cyber risks.

- OTCC supports legislation and regulations that recommend and recognize the use of leading global standards. These standards provide consistency and promote fair competition and international trade.

Today, many countries and governments are developing their own unique standards and regulations for their country or industries. This has led to an influx of regulations with which an organization must comply, creating an acute burden for global companies.

Governments should focus on adopting requirements aligned to standards that take a holistic approach and are developed by global experts in industrial automation cybersecurity. Such an approach aligns with the last two Administrations' National Cyber Strategies, which advocated for the harmonization and elimination of duplicative regulations.

ISA/IEC 62443 is uniquely positioned as the only global consensus-based standard currently developed, tailored, and in use for the physics-based requirements of OT. A policy grounded in interoperable, consensus-based standards offers the dual benefits of securing critical infrastructure and industrial operations while ensuring consistent application across the globe.

This paper outlines the following OTCC recommendations to harmonize OT cybersecurity standards and regulations:

1. Recognize ISA/IEC as the Global OT Security Standard
2. Shift from Compliance to Interoperability
3. Catalyze Market Maturation through Lead-User Adoption
4. Enhance Sector-Specific Technical Guidance and Capacity Building; and
5. Fund Workforce Development for OT Security Competency

The Value of Standards in Reducing the Burden of Regulatory Sprawl

The global cybersecurity landscape is currently experiencing a significant shift as new regulations and standards emerge across different regions and sectors. While well-intentioned, the proliferation of unique, sector-specific mandates creates an acute burden for organizations that operate across multiple jurisdictions and industries. This fragmentation often leads to "compliance for compliance's sake" rather than improved operational resilience. Recent government initiatives risk creating duplicative regulations when new standards and guidelines recreate controls and processes already defined in existing frameworks.

The Transportation Sector: A Case Study in Duplication

The Transportation Security Administration (TSA) developed the TSA Pipeline Security Directives (e.g., SD Pipeline-2021-02 series and the 2024 NPRM) introducing cybersecurity requirements for incident response and network segmentation for pipeline operators. The initial rollout forced operators to map these new SDs against existing ISA/IEC 62443 programs, creating potential operational burdens.

The Energy Sector: NERC CIP and Double-Reporting Burden

The transportation sector is not alone. In the U.S. Energy Sector, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards provide a mandatory regulatory framework for the bulk power system. Recent efforts to introduce additional, layer-on requirements often mirror the controls already established within ISA/IEC 62443 and NIST SP 800-82 and the Cybersecurity Framework 2.0 (NIST CSF 2.0), creating at times duplicative requirements that must be deconflicted by the private sector.

Forcing utilities to cross-map these new, redundant mandates against their established NERC CIP compliance programs creates a "double-reporting" burden. Instead of enhancing security, this administrative overlap diverts limited engineering resources away from active threat mitigation and toward reconciling minor technical discrepancies between two nearly identical regulatory masters.

European Union: Regulatory Multiplicity

This trend is mirrored internationally by the European Union’s regulatory multiplicity, where the NIS2 Directive, the CER Directive, and the Cyber Resilience Act (CRA) create overlapping entity-level and product-level requirements. Without a unifying, horizontal standard, navigating these fragmented rules is a massive undertaking for any manufacturer or operator.

The solution lies in grounding policy in interoperable, consensus-based standards. By formally recognizing standards like ISA/IEC 62443, governments can provide a common technical language that works across pipelines, power grids, and factories alike, reducing the need for agencies to "reinvent the wheel" for every new technology or sector.

Key Standards OTCC Supports

Current U.S. frameworks for critical infrastructure demonstrate a high degree of technical alignment. Key pillars such as asset identification, security zones, access control, and supply chain integrity now map directly across both frameworks, allowing organizations to streamline compliance and reduce administrative friction.

A common "better together" approach involves using NIST 800-82 to establish an overarching security posture and satisfy regulatory audit requirements, while simultaneously embedding ISA/IEC 62443 technical benchmarks into Requests for Proposal (RFPs). This dual-track strategy bridges the gap between high-level policy and the engineering realities of the shop floor. In practice, leading utility providers do not choose a single standard in isolation; instead, they leverage the complementary strengths of multiple frameworks to build a comprehensive defense.

ISA/IEC 62443

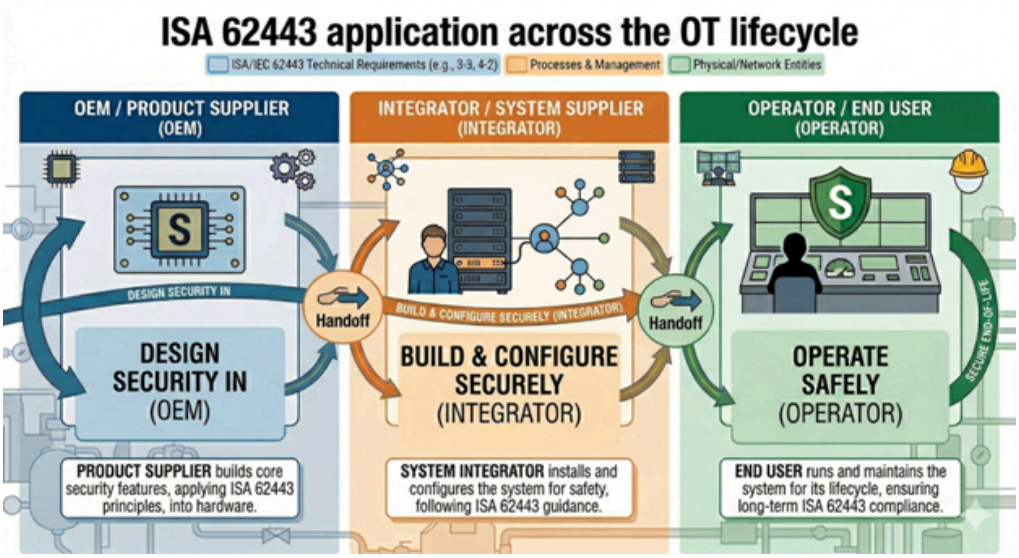
ISA/IEC 62443 is a set of cybersecurity standards specifically tailored for industrial automation and control systems (IACS) and operational technology. It is widely adopted by the world's leading suppliers and integrators.

ISA/IEC 62443 provides detailed requirements and methods for addressing the unique security challenges in industrial environments.

The OTCC also strongly supports the NIST CSF 2.0 and NIST 800-82 as the essential governance and risk management layer for critical infrastructure. While NIST 800-82 and the NIST CSF 2.0 provide the high-level taxonomy: Identify, Protect, Detect, Respond, and Recover, necessary for executive communication and organizational risk strategy, ISA/IEC 62443 provides the technical how-to required for implementation in physical environments. By mapping the prescriptive controls of 62443 to the outcomes defined by NIST, organizations can achieve a holistic security posture that satisfies both board-level governance and shop-floor engineering requirements. This synergy ensures that security is not only strategically managed through NIST 800-82 and the NIST CSF 2.0 but also technically enforced through the site-specific rigor of the ISA/IEC 62443 series.

Challenges addressed by ISA/IEC 62443 include:

- Protecting data confidentiality
- Preventing cyber-physical failures
- Safeguarding legacy systems
- Maintaining productivity in the face of potential incidents



Initially developed by the International Society of Automation (ISA) ISA-99 standards committee and later adopted by the International Electrotechnical Commission (IEC), these consensus-based standards are regularly updated with input from experts in IACS security.

The Horizontal Reach of ISA/IEC 62443

ISA/IEC 62443 is applicable across various industry sectors and critical infrastructure. The versatility of ISA/IEC 62443 lies in its "horizontal" design, providing a flexible security framework that addresses the shared physics and operational constraints of industrial control systems across diverse sectors.

Battery Energy Storage Systems (BESS)
ISA/IEC 62443 is instrumental in ensuring remote management interfaces do not become entry points for disruptive cyber-attacks in Power Conversion Systems (PCS) and site controllers.

Water & Wastewater
The technical rigor of ISA/IEC 62443 standards protect Programmable Logic Controllers governing chemical dosing and pump stations, where a compromised logic sequence could directly impact public safety.

Manufacturing
ISA/IEC 62443 standards govern the lifecycle of automation equipment, from robotic arms on an assembly line to sensors in pharmaceutical cleanrooms.

The standard outlines a defense-in-depth model that uses “zones” (logical groupings of assets) and “conduits,” (communication paths). It provides guidance on building cybersecurity management systems (CSMS), and offers instructions for conducting risk assessments in IACS/OT environments.

By focusing on the fundamental relationship between zones and conduits, ISA/IEC 62443 allows these varied industries to implement a consistent, defense-in-depth posture that protects the integrity of the physical process, regardless of the specific end product. It helps organizations define security maturity, choose security products and service providers, and supplement core guidance with technical reports tailored to specific situations. That being said, it is important to note that the standard recognizes that not all OT is the same, that risk differs across sectors, and addresses this variance. Accepting this industry standard should naturally incorporate all associated standards, thus helping to harmonize regulations across all levels.

This standard provides unique holistic guidance not only to the owner and operator of the equipment but also provides detailed requirements and guidance to the installer or integrator (e.g., secure install) and the Original Equipment Manufacturers (OEMs) or vendor (e. g., secure development lifecycle) to provide a complete secure solution from development to install to operation, making it one of the most comprehensive and robust industrial cybersecurity standards available. Industry experts are collaborating to drive improvements with OEMs, across design and deployment, and operations. Government policy can make real and immediate impact by trusting their hard work.

Aligning NIST Frameworks with the Unique Needs of Operational Technology

NIST SP 800-82 is the primary NIST document addressing OT security, providing detailed guidelines for managing risks and securing OT systems. NIST standards, particularly NIST SP 800-82, provide comprehensive guidance on securing OT systems by offering specific recommendations tailored to the unique characteristics of OT environments, including considerations for safety, reliability and performance, while addressing the need to integrate OT security with broader IT security practices. Essentially, NIST helps organizations design and implement cybersecurity strategies for OT systems that prioritize operational continuity and safety alongside data protection.

- **Unique OT considerations:** Unlike typical IT systems, OT systems often have unique safety and operational requirements that NIST standards acknowledge and address with specific security controls.
- **Integration with IT security:** While focusing on OT specifics, NIST emphasizes the importance of integrating OT security practices with existing IT security strategies to achieve a holistic approach.
- **Target audience:** NIST OT guidance is relevant to various stakeholders including control engineers, system administrators, security consultants and OT system operators.

How NIST standards are applied to OT:

- **Risk assessment:** Conducting thorough risk assessments to identify vulnerabilities in OT systems and prioritize mitigation efforts.
- **Segmentation and isolation:** Implementing network segmentation to separate OT networks from IT networks and minimize potential attack pathways.
- **Access control:** Restricting access controls to OT systems including user authentication and authorization procedures.
- **Patch management:** Developing a robust patch management process for OT devices, accounting for potential operational impacts.
- **Incident response planning:** Create incident response plans tailored to OT incidents, including procedures for containment and recovery.

NIST SP 800-82 and ISA/IEC 62443 play distinct but complementary roles. Both are essential because they bridge the gap between policy and practice: NIST 800-82 helps leadership define the security strategy, while ISA/IEC 62443 provides technical teams with the exact standards needed to make that strategy a reality on the factory floor or in the power plant.

Challenges to Adoption

One significant barrier to the widespread adoption of ISA/IEC 62443 is that it remains a proprietary, paid standard. Unlike many open-source frameworks, the cost associated with accessing the full suite of documents can create a financial hurdle for smaller companies, municipalities and budget-constrained operators, limiting the reach of these critical security blueprints.

Updating Existing Frameworks for Emerging Technology

Although emerging technologies like Artificial Intelligence (AI) and Quantum Computing introduce fresh challenges, they do not necessitate entirely new, disconnected regulatory frameworks. The 62443 standard is designed to be extensible to these advancements.

- **Artificial Intelligence:** AI components, including autonomous Agentic AI or AI-generated code, should be treated as high-risk software entities within the existing ISA/IEC 62443 framework. This ensures that even the most advanced tools remain subject to validation and strict access controls. This aligns with the U.S. Cybersecurity Infrastructure Security Agency's (CISA) philosophical approach of treating AI as software.

- **Post-Quantum Cryptography (PQC):** The framework allows for a pragmatic, risk-based prioritization of PQC. Rather than blanket mandates, policies should focus on sectors where data integrity and long-term safety are most critical, particularly in brownfield environments where upgrading legacy devices is technically prohibitive.

International Adoption of ISA/IEC 62443

ISA/IEC 62443 has earned formal recognition across multiple nations and regions, demonstrating its viability as the global baseline for OT cybersecurity.

United States	The NSA's OT Cybersecurity Assurance Partnership drew heavily on 62443 controls as the backbone of its security baseline for product development of national security systems.
Australia	Standards Australia has formally adopted 62443 as a national standard (AS IEC 62443), integrating it into the country's critical infrastructure protection framework. This is a clean example of a nation-state choosing not to reinvent the wheel and instead anchoring its domestic requirements to the international consensus baseline.
European Union	The Cyber Resilience Act's (CRA) essential cybersecurity requirements for connected products align strongly with 62443-4-1 and 62443-4-2, particularly regarding the secure development lifecycle and component hardening. Standards bodies developing harmonized standards under the CRA are explicitly looking to 62443 as the technical baseline. This means any OT product supplier selling into Europe will effectively be operating under 62443-aligned requirements.
Saudi Arabia	Saudi Arabia's national OT cybersecurity framework, developed through the National Cybersecurity Authority, uses 62443 as a foundational reference.
Singapore	Cyber Security Agency of Singapore (CSA) recently updated its OT Cybersecurity Masterplan in 2024. A key pillar of this plan is the promotion of "Secure-by-Deployment" principles. The Masterplan explicitly references the ISA/IEC 62443 lifecycle—covering OEMs, Integrators, and Operators—to ensure that security is not just a feature of a product but is maintained during installation and long-term operation.

Critical Recommendations for U.S. Policy Makers

The OTCC offers the following five policy recommendations to drive adoption of a unified, interoperable OT cybersecurity standard.

1

Recognize ISA/IEC 62443 as the Global OT Security Standard

Policy makers should avoid developing bespoke national standards. Instead, they should formally adopt ISA/IEC 62443 as the foundational framework for OT security. By establishing legal and regulatory reciprocity for organizations that achieve compliance with these standards, governments can drive the adoption of robust security controls. This approach replaces fragmented local requirements with a unified, international benchmark, effectively strengthening the security posture of critical infrastructure and enhancing national security.

2

Shift from "Compliance" to "Interoperability"

Current policy often treats OT security as a checklist. Policy should instead prioritize interoperable security. By mandating that new critical infrastructure projects use components that support open, ISA/IEC 62443-aligned security protocols, policy makers ensure all vendors' systems can communicate securely, preventing silos that occur with proprietary, non-standardized equipment.

3

Catalyze Market Maturation through Lead-User Adoption

To support the vast majority of infrastructure operators, most of whom are below the cyber poverty line, policy must focus on the government's power as a lead market user. By mandating ISA/IEC 62443 standards in major public works, the government can drive economies of scale for secure components. This reduces the cost of entry for the private sector and fosters a standardized supply chain where secure-by-design technology is the default, rather than a luxury, for every operator.

4

Enhance Sector-Specific Technical Guidance and Capacity Building

To bridge the gap between high-level policy and shop-floor reality, CISA should support Sector Risk Management Agencies (SRMAs) in helping critical infrastructure owners and operators to adopt common cross-sector standards such as ISA/IEC 62443. CISA and SRMAs should encourage these organizations to develop translation layers that map broad national directives to the specific engineering rigor of the ISA/IEC 62443 series, working in coordination with ISA/IEC and the private sector.

5

Fund Workforce Development for ISA/IEC 62443 Competency

A significant barrier to ISA/IEC 62443 adoption is a lack of qualified personnel who understand both industrial engineering and cybersecurity. Policy should include dedicated funding for Professional Certification programs and expanded training in cyber informed engineering (CIE) to ensure that the OT workforce is technically equipped to craft policy and support these environments.

Operational Technology Cybersecurity Coalition

About the OT Cyber Coalition

The Operational Technology Cybersecurity Coalition (OTCC) is dedicated to advancing cohesive, risk-based, and globally interoperable cybersecurity policy for industrial and operational technology environments. OTCC brings together leading experts to advocate for consensus-based standards that reduce regulatory fragmentation and strengthen critical infrastructure resilience worldwide.

www.otcybercoalition.com