SECURING OPERATIONAL TECHNOLOGY

WITH TRUST AND COLLABORATION

Contents

Executive Summary

Operational Technology (OT) environments underpin critical infrastructure across the globe—from energy and utilities to manufacturing, transportation, financial services, and public services. As these environments become increasingly digitalized and interconnected through technologies like the Industrial Internet of Things (IIoT), artificial intelligence (AI), and cloud-based systems, the risks posed by cyber threats grow exponentially.

Unlike information technology (IT), OT environments prioritize availability, reliability, and safety over confidentiality. Cyberattacks on OT systems can lead to physical damage, environmental hazards, financial loss, and even threats to human life. That's why, a one-size-fits-all approach using IT cybersecurity frameworks often results in ineffective or even harmful outcomes when applied to OT.

At the heart of effective OT cybersecurity is the Trusted Advisor—a cross-disciplinary expert who blends deep industrial knowledge with cybersecurity acumen. This paper defines the core competencies required to succeed in this role and emphasize the need for ecosystem-wide collaboration involving vendors, engineers, regulators, and cybersecurity professionals.

This paper also underscores the importance of advocating for cybersecurity by design throughout the Engineering, Procurement, and Construction (EPC) lifecycle. By embedding security requirements early, organizations can avoid costly retrofits, align with global standards such as IEC 62443, and ensure safer, more resilient industrial systems from the ground up.

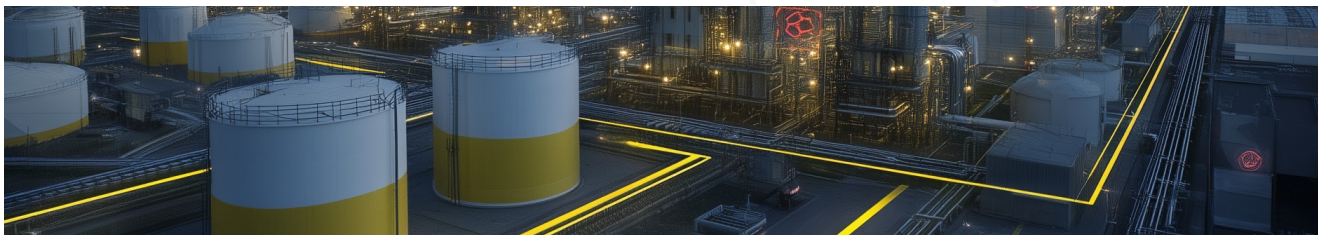
Ultimately, securing OT environments requires more than tools—it demands trust, context, and a shared understanding of what's at stake. This paper offers a roadmap for organizations seeking to modernize securely, protect critical infrastructure, and navigate the complex realities of cyber risk in the industrial age.

Introduction

The rising stakes of OT cybersecurity

As industrial operations grow increasingly interconnected through digital transformation initiatives, the cybersecurity threat landscape facing operational technology (OT) environments has reached unprecedented complexity. No longer isolated or air-gapped, today's OT systems are being integrated with IT networks, connected to cloud services, and enhanced with the Internet of Things (IoT) and Industrial Internet of Things (IIoT) technologies. While this shift has delivered operational efficiency and innovation, it has also introduced a wide range of cyber risks that traditional approaches cannot mitigate.

OT cybersecurity poses unique challenges due to the nature of physical systems and their real-time demands. Disruption, latency, or malfunctions in these environments can cause production halts, equipment damage, environmental spills, or even threatening lives. Unlike IT systems—where downtime can often be tolerated for maintenance—OT systems demand high availability and deterministic behavior at all times.



Real-world examples that redefined OT security

In the rapidly evolving landscape of OT, IoT, and IIoT cybersecurity, the past decade has witnessed a series of landmark cyberattacks that have reshaped global understanding of cyber risk in industrial environments. These attacks were not just disruptive, they were transformational, exposing systemic vulnerabilities, the fragility of interconnected systems, and the real-world consequences of poor cybersecurity practices.

Saudi Aramco (2012): One of the most disruptive cyber attacks in history, the Shamoon malware wiped data from over 30,000 workstations, severely disrupting operations at the world's largest oil producer. The attack exposed the vulnerabilities of critical infrastructure and underscored the need for robust cyber hygiene and response capabilities.

Triton/Trisis (2017): One of the most dangerous OT-targeted attacks to date, this malware was designed to disable safety instrumented systems at a petrochemical plant, putting lives at risk and proving that cyber attacks can move from digital disruption to physical destruction.

3CX (2023): Infiltration of a popular VoIP provider used by industrial clients enabled attackers to pivot into downstream environments, highlighting the latent risk in even peripheral third-party software.

Schneider Electric (2024): Threat actors breached the company's infrastructure and exfiltrated over 40GB of sensitive OT-related data, exposing vulnerabilities across global energy and automation systems.

Matrix Botnet (2024): A widespread botnet campaign that hijacked smart industrial devices, weaponizing them to launch massive distributed denial-of-service (DDoS) attacks, disrupting OT networks across sectors.

Change Healthcare (2024): This targeted campaign paralyzed healthcare operations across the U.S., affecting critical OT systems such as medical device networks and patient care delivery platforms.

Norwegian Dam (2025): Attackers exploited weak authentication on a remote control system, manipulating valves to release excess water flow. Though no damage occurred, the four-hour undetected breach revealed how overlooked exposures in OT environments can threaten infrastructure stability.

From nation-state campaigns to supply chain intrusions and targeted attacks on safety systems, these incidents have forced a reassessment of how critical infrastructure must be defended. They underscore a central truth: OT environments cannot be secured with IT mindsets or generic frameworks. Moreover, the threat landscape continues to escalate, with attacks becoming more frequent, more sophisticated, and more destructive in the last five years.

These incidents reveal the urgent need for tailored cybersecurity frameworks, a well-developed ecosystem of collaboration, and Trusted Advisors capable of navigating the unique complexities of industrial systems.

Challenges with traditional practices

Despite increasing threats, many organizations continue to apply conventional/parameter IT cybersecurity strategies to OT systems—an approach that often fails due to key differences in priorities, architectures, and constraints.

Patching

Frequent updates are routine in IT but often impractical or dangerous in OT, where unplanned reboots can halt critical production lines.

Scanning and pen testing

Automated scans that flood network devices may crash legacy OT systems.

Endpoint security

Many OT systems lack the resources to run antivirus or EDR tools common in IT environments.

These practices not only risk damaging sensitive industrial processes but can also erode trust between cybersecurity teams and plant operators, making future collaboration harder.

The need for a trust-based, tailored approach

What's needed is a fundamental shift: from one-size-fits-all frameworks to **actionable, risk-based, context-driven cybersecurity** rooted in operational reality. This transformation must begin with **Trusted Advisors**—professionals who deeply understand both OT and cybersecurity, and who can translate business goals into pragmatic security strategies without compromising safety or uptime.

Furthermore, this shift cannot happen in isolation. It requires a collaborative OT cybersecurity ecosystem that includes OT cybersecurity service providers, engineers, vendors, integrators, regulators, and cybersecurity experts working together to co-create resilient industrial defenses.

Core competencies of a Trusted Advisor

The OT cybersecurity domain is a nuanced and high-stakes field. Advisors working in this space must not only possess technical capabilities but also exhibit cross-disciplinary fluency across industrial operations, systems engineering, cybersecurity, and risk management. The most valuable advisors are to whom plant engineers, automation vendors, and CISOs alike turn with confidence—**Trusted Advisors.**

The following eight competencies represent the **foundation of credibility, capability, and impact** for any advisor operating in critical infrastructure and industrial environments.

Deep operational and process expertise: Trusted Advisor must understand how industrial processes work, not just how they are controlled. This includes mechanical, chemical, electrical, and process automation fundamentals that define the industrial context.

Secure digital transformation enablement: Digital transformation introduces IIoT, cloud analytics, remote maintenance, and AI into OT environments. A Trusted Advisor must balance innovation with security, ensuring cybersecurity doesn't hinder progress.

Mastery of Industrial Control Systems (ICS): Understanding ICS hardware and software—including DCS, SCADA, PLCs, MES, RTUs, and SIS—is non-negotiable. An advisor must know the **protocols, vendor ecosystems, lifecycle stages, and fail-safes** that make up ICS environments.

Understanding differences between OT, IoT, and IIoT: These three domains differ in their connectivity, reliability expectations, and attack surface. A Trusted Advisor must tailor strategies based on device class, network behavior, and operational criticality.

OT cybersecurity ≠ IT cybersecurity: This competency is about cultural, technical, and operational humility. OT cybersecurity decisions can literally affect physical safety. IT-centric mindsets—like "patch everything now" or "install antivirus everywhere"—can do more harm than good.

Dispelling the "IT systems in OT" myth: Labeling Level 2 or 3 devices as "just IT" leads to the application of unfit controls. These systems are embedded in industrial contexts and operate with different uptime, safety, and access constraints. All systems that manage a process including workstations, engineering workstations systems and OT servers are core OT systems, not IT ones.

Risk-based, realistic approach to security: Trusted Advisors focus on what's achievable and most impactful, not on unrealistic or checkbox-style compliance. Every plant, system, and business context is different—so is every security journey.

Validation and oversight of AI and automated tools: AI tools can provide early detection, behavior modeling, and even autonomous response. However, without context, they can block critical processes or raise false alarms.

A trusted OT cybersecurity advisor is more than a consultant or engineer—they are a **strategic, technical, and operational partner.** These eight competencies empower them to navigate the unique challenges of industrial environments with authority, empathy, and credibility.

Each competency is strengthened through real-world experience, cross-functional collaboration, and a commitment to pragmatism over perfection. As we'll see in the next section, ignoring these principles often results in misapplied controls and broken trust—a risk no industrial operator can afford.

The high cost of misapplied IT controls

The hidden risks of inappropriate controls

One of the most common—and costly—mistakes in OT cybersecurity is applying controls, frameworks, or policies developed for IT environments directly to OT environments without adaptation. While the intent may be noble, the results are often harmful.

Unlike IT, OT environments prioritize availability, deterministic behavior, and safety. A firewall rule, scan, or policy that works in IT may cause a production line to freeze, a turbine to trip, or a power relay to misfire.

Why IT controls fail in OT environments

The failure often stems from five systemic misunderstandings:

- **Confusing OT systems with IT endpoints:** Just because an HMI runs on Windows, it doesn't mean it can be treated like a workstation in a corporate domain.
- **Assuming patching schedules are transferable:** IT expects patching within days. OT may only allow changes once per year during planned outages.
- **Running aggressive vulnerability scans on fragile systems:** OT devices often crash or reboot when scanned with IT tools.
- **Over-reliance on endpoint agents and antivirus:** Many ICS components lack the capacity or compatibility to run these tools without affecting real-time performance.
- **Forcing policy-driven compliance without context:** Applying blanket control lists (e.g., NIST 800-53 or ISO 27001) without interpreting operational realities leads to misalignment and distrust.

How IT-based standards can misguide OT security strategy

Many security programs are built on standards like:

- **ISO/IEC 27001 –** Designed for general information security management
- **NIST SP 800-53 –** Comprehensive, but heavily IT-focused
- **CIS Top 18 –** Developed from IT threat models with minimal OT relevance

While these frameworks have value, applying them without adaptation can lead to controls that are technically correct but operationally infeasible or unsafe.

Why OT-specific standards are essential

Instead, organizations should use or align with standards specifically built for OT:

- **IEC 62443 (ISA99) –** A multi-part framework for securing industrial automation and control systems (IACS), it introduces zoning, system-level security levels, and lifecycle integration.
- **NIST SP 800-82 –** Focused on ICS security and best practices tailored to OT environments
- **ISO/IEC 30141 –** Addresses IoT system architecture and introduces security principles for connected environments
- **IEEE 1686 –** Defines cybersecurity capabilities for IEDs (Intelligent Electronic Devices) in the energy sector

These standards consider the operational context, real-time constraints, and lifecycle of control systems. They guide decision-making not just based on threats, but on industrial consequences.

Consequences of misapplied controls

Operational consequences

- Unplanned downtime
- Loss of production
- Equipment damage or failure
- Safety system malfunction

Strategic consequences

- Loss of trust in cybersecurity teams
- Rejection of security initiatives by operations
- Wasted investment on incompatible tools
- Delays in digital transformation due to misalignment

Best practices to avoid these pitfalls

- **Perform contextual, OT-specific risk assessments** before applying controls.
- **Involve plant operations and engineering** in cybersecurity design and governance.
- **Use IEC 62443 zoning and SL-based approaches** to align technical controls with business and process risk.
- **Test all controls in non-production environments** before deployment.
- **Build a tailored OT cybersecurity policy** separate from IT, with aligned but distinct processes.

Cybersecurity by design: Embedding security into the EPC lifecycle

Why cybersecurity can't be an afterthought

In traditional project execution, cybersecurity is often addressed **after systems are procured or deployed,** leaving critical security gaps that are expensive and risky to fix later. This reactive approach doesn't work in OT environments where **availability, safety, and physical system behavior** are paramount.

The solution is to integrate **cybersecurity by design—**embedding security controls early in the **Engineering, Procurement, and Construction (EPC)** lifecycle of industrial projects. Doing so ensures that new control systems are born secure, aligned with operational requirements, and resistant to cyber threats from day one.

Cybersecurity by design: A proactive strategy

Cybersecurity by design means embedding security requirements, assessments, and validations throughout the EPC lifecycle. It turns security into a design constraint, just like safety, availability, and performance.

Key goals

- Anticipate and mitigate threats **before deployment**
- Align system design with **IEC 62443 security levels**
- Reduce the cost of late-stage rework
- Improve acceptance by operators and regulators

Cybersecurity activities in the EPC lifecycle

During the Engineering phase

- Perform OT risk assessments and threat modeling.
- Define security zoning and conduits in line with IEC 62443-3-2.
- Establish cybersecurity specifications for control systems and networks.
- Integrate security into functional design documents and cause-and-effect matrices.

During the Procurement phase

- Ensure cybersecurity clauses are included in vendor RFPs.
- Select vendors whose products meet IEC 62443-4-2 or equivalent.
- Require third-party validation or certifications of system hardening.
- Define security test plans for factory and site acceptance.

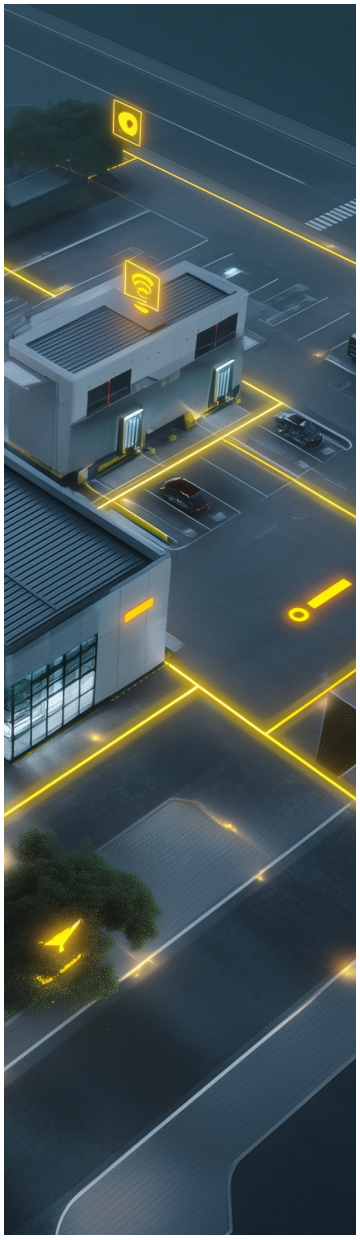
During the Construction & Commissioning phase

- Validate configurations and rule sets during Factory Acceptance Testing (FAT).
- Simulate integrated use cases during Integrated FAT (iFAT).
- Conduct full cybersecurity tests during Site Acceptance Testing (SAT), including network segmentation, authentication controls, and failover behavior.
- Document final security configurations in operational handover packages.

Standards supporting secure-by-design practices

Several OT-specific standards provide detailed guidance on integrating cybersecurity during the lifecycle:

- **IEC 62443-3-3:** Defines foundational security requirements (e.g., access control, data integrity) applicable during system design
- **IEC 62443-3-2:** Introduces the concept of zones and conduits, providing a structure for architectural segmentation
- **IEC 62443-2-4:** Specifies security requirements for system integrators, ensuring secure practices during project execution
- **IEC 62443-4-1 & 4-2:** Define secure product development lifecycles and technical security requirements for components
- **NIST SP 800-82 (Rev. 2):** Offers lifecycle guidance for ICS cybersecurity and mapping to risk management frameworks



Best practices for EPC-aligned cybersecurity

- **Start early:** Integrate cybersecurity at the conceptual design stage.
- **Involve all parties:** Include OT, engineering, operations, and IT teams in risk workshops and FAT planning.
- **Use security test cases in FAT/iFAT/SAT:** Validate SL-based controls in the exact configuration that will run in production.
- **Specify security outcomes, not just features:** For example, “only authenticated devices may access this zone,” rather than “install a firewall.”
- **Maintain traceability:** Link security requirements to compliance documentation and vendor deliverables.

Cybersecurity by design is a necessity. Incorporating cybersecurity into the EPC lifecycle ensures that industrial control systems are deployed securely and efficiently, with minimal disruption and maximum resilience.

By treating cybersecurity as an engineering discipline from the very beginning, organizations can lower lifecycle costs, increase compliance, and improve stakeholder confidence—all while securing the operational integrity of critical infrastructure.

Partnership as a strategic enabler

Why no one can do it alone

Securing OT environments is a team effort. The complexity, interdependence, and cross-domain nature of industrial systems make it impossible for any single organization—be it an asset owner, a cybersecurity vendor, or a regulator—to tackle all cyber risks alone.

The answer lies in strategic partnerships. When industrial stakeholders work together—sharing knowledge, responsibilities, and capabilities—they form an OT cybersecurity ecosystem that is greater than the sum of its parts.

In this section, we examine why partnership is not just beneficial, but essential, and how organizations can build collaborative relationships that yield measurable security and operational outcomes.

The strategic value of collaboration

Collaborative efforts create a force multiplier effect by enabling:

- **Faster threat identification and response**

Shared threat intelligence, indicators of compromise (IOCs), and incident response plans can reduce detection and mitigation timelines dramatically.

- **Unified standards adoption**

Coordinated alignment with IEC 62443, NIST SP 800-82, and sector-specific regulations ensures consistent implementation across systems and vendors.

- **Shared innovation and R&D**

Pooling expertise accelerates the development of OT-tailored cybersecurity tools and analytics.

- **Operational and contextual awareness**

OT security is not just a technical issue—it's also a cultural, safety, and operational concern. Strong partnerships bridge these gaps.

Key stakeholders in OT cybersecurity partnerships

1. **Asset owners and operators:** Bring critical operational knowledge and are ultimately responsible for securing their infrastructure.

2. **Automation and control system vendors:** Design and supply core technologies (PLCs, SCADA, DCS) and must integrate cybersecurity by design.

3. **OT cybersecurity technology vendors:** Provide specialized tools such as anomaly detection, secure remote access, and network segmentation designed specifically for OT environments

4. **System integrators:** Connect components and ensure interoperability. Their design decisions heavily influence network segmentation and architecture.

5. **Cybersecurity service providers and consultants:** Conduct risk assessments, design security architectures, respond to incidents, and offer third-party validation.

6. **Regulators and government agencies:** Develop the legal and policy framework, facilitate information sharing, and often fund sector-wide cyber resilience programs.

7. **Standardization bodies (e.g., ISA, IEC, NIST):** Ensure consensus-driven security guidelines and protocols applicable across industries and geographies.

8. **Academic and research institutions:** Advance knowledge, develop the talent pipeline, and contribute to innovation in cybersecurity solutions and methods.

Best practices for building strategic partnerships

- **Start with shared objectives:** Focus on outcomes like improved safety, uptime, and resilience—not just compliance.
- **Formalize collaboration:** Use contracts, joint governance models, and service level agreements to clarify roles and responsibilities.
- **Promote information sharing:** Use platforms like ISACs or internal community-of-practice meetings to share insights, indicators, and experiences.
- **Build joint training and response capabilities:** Cross-train teams across disciplines and run tabletop exercises with all stakeholders represented.
- **Adopt a common language:** Use frameworks like IEC 62443 to establish shared terminology and threat models across the ecosystem.

IEC 62443 as a common partnership framework

The IEC 62443 series is uniquely suited to support collaborative security efforts, as it:

- Defines zones and conduits that align security boundaries across multiple stakeholders.
- Introduces Security Levels (SLs) that help organizations agree on the necessary strength of controls.
- Provides clear roles and responsibilities for asset owners, integrators, and vendors.
- Supports integration in procurement processes, ensuring security from the outset.

It creates a shared foundation that all parties—technical and non-technical—can reference, reducing ambiguity and enabling better alignment.

Key principles and proactive steps

Securing OT environments demands a collective approach grounded in trust, transparency, and shared accountability. At the foundation of this effort are key principles and proactive measures:

Know your environment: Establish full visibility into all connected assets, their configurations, communication pathways, and associated risks. This foundational step helps uncover blind spots and potential vulnerabilities that could be exploited by adversaries.

Adopt an attacker's mindset: Continuously assess your defenses by simulating real-world threats. Stress-test systems to identify vulnerabilities, understand how attackers might infiltrate, and uncover gaps in detection and response mechanisms.

Build the capability to respond and recover: Invest in robust incident response and recovery plans. These should include clearly defined roles, automated response procedures, communication playbooks, and the ability to maintain critical functions during and after a cyber incident.

Follow a maturity roadmap: Develop and execute a roadmap that moves your organization from reactive to proactive cybersecurity maturity. This includes adopting industry standards, continuous improvement programs, and periodic benchmarking to measure progress.

Stakeholder-specific actions

To achieve resilient OT security, every stakeholder in the ecosystem has a distinct and essential role to play:

Asset owners and operators must elevate cybersecurity to a strategic function—integrating governance across engineering and operations, investing in internal Trusted Advisors, and prioritizing security from the design phase through the full lifecycle of their systems.

Vendors and integrators must adopt secure-by-design principles and offer transparency around vulnerabilities, patches, and protocols. Aligning solutions with recognized standards like IEC 62443 or NIST SP 800-82 is vital for building and maintaining client trust.

Cybersecurity service providers should tailor offerings to the OT context, moving beyond generic controls toward contextual, risk-based programs. Their role must evolve from technical implementers to transformation enablers, helping clients manage digital risk while driving operational innovation.

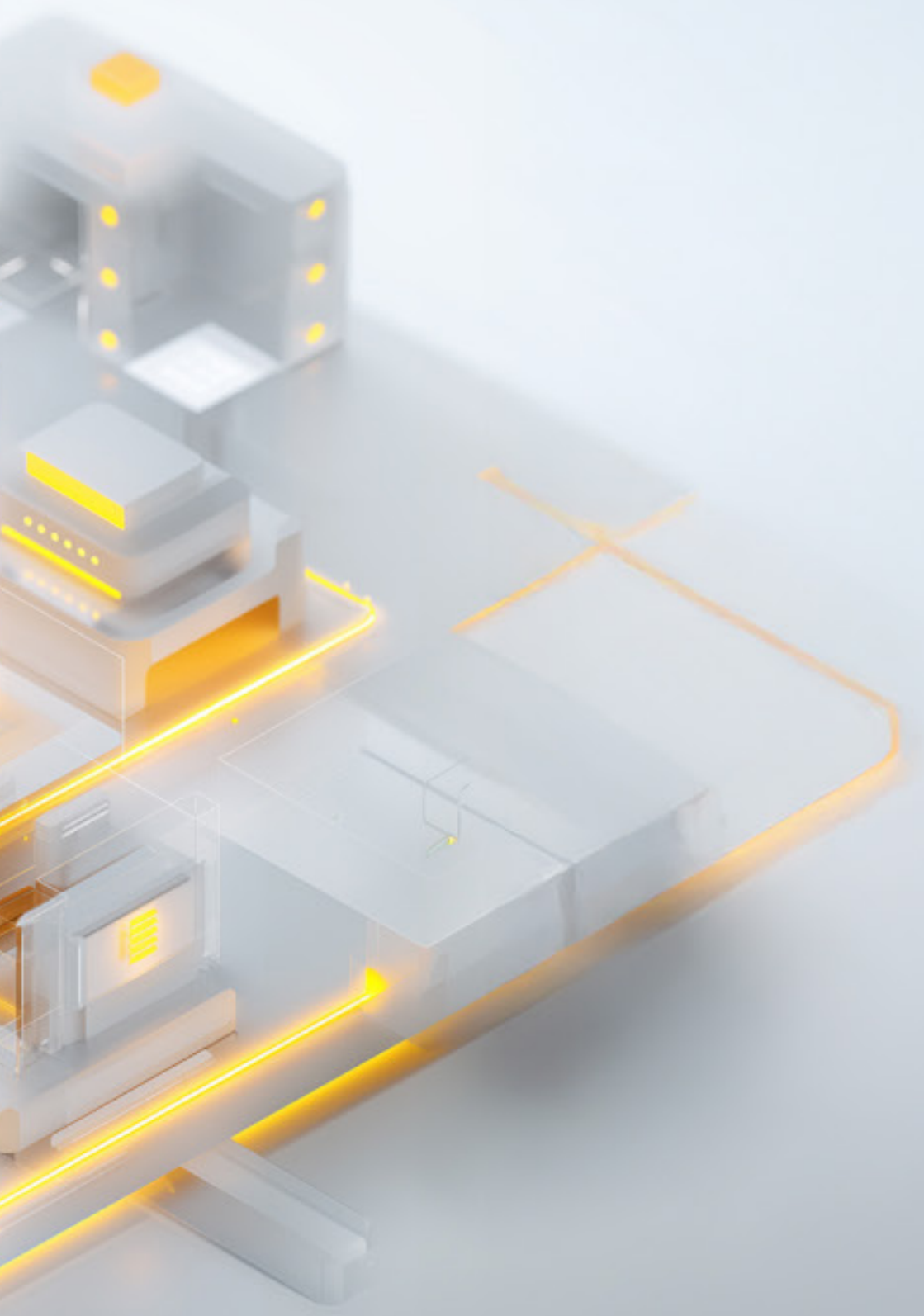
Governments and regulators must foster alignment through clear standards, national CERT collaboration, and funding for OT-specific research and workforce development. Regulation should drive maturity without impeding innovation.

Looking ahead: Cybersecurity a shared responsibility

The advancement of OT cybersecurity is not only a technological challenge, it is a human organizational, and strategic challenge. It requires building bridges between people and departments, between industries and governments, and between innovation and regulation.

To make progress, we must shift from fear-based reactions to trust-driven strategies. We must stop securing OT like IT, and start securing it like the mission-critical, real-world infrastructure it is.

Let this whitepaper be a starting point for conversations, collaboration, and decisive action. Together, through trust, collaboration, and competency, we can safeguard the future of industrial operations and critical infrastructure across the globe.



About Us

CPX, a G42 company, is a leading provider of end-to-end cyber and physical security solutions and services. Founded in 2022 and headquartered in Abu Dhabi, CPX employs over 600 cyber and physical security specialists serving enterprises, governments, and critical infrastructure sectors in the UAE and beyond. With a strong focus on delivering transformative security across the AI ecosystem, CPX empowers organizations to assess risks, protect assets, and operate with unwavering confidence.

Discover more at **www.cpx.net.**

Reach out to us at **contactus@cpx.net.**