How IGEL Helps OT Across Critical Industries

ISA/IEC 62443 and the Endpoint Trust Gap: Strengthening OT Cybersecurity, Operational Resilience, and Critical Infrastructure Protection

May 2026

Table of Contents

Executive Summary

Operational Technology (OT) environments are under growing pressure to change how they integrate with the enterprise systems. As industrial organizations modernize, connect and interconnect more systems, and converge IT and OT operations, the cybersecurity risks increase. In pharmaceutical manufacturing, energy, healthcare, and other critical industries, cybersecurity incidents are not only data problems, they are uptime problems, safety problems, continuity problems, and resilience issues.

ISA/IEC 62443 was developed specifically for Industrial Automation and Control Systems (IACS), to provide a structured framework for improving OT cybersecurity across the lifecycle of systems, components, and operations. It is widely used as a consensus-based cybersecurity standards family for industrial automation and control system environments, and it is used by asset owners, system integrators, and suppliers to reduce risk in ways that reflect the realities of OT.

However, while security architectures have advanced across identity, network access, segmentation, browser isolation, and cloud-delivered controls, there are still risks exposed by the endpoint trust gap. Security policy can be well designed upstream yet undermined by a hardware device layer that can be variable, difficult to verify, inconsistently governed, and slow to recover. In OT and critical infrastructure, where operators, engineers, third parties, and supervisors rely on secure access to systems that must remain available, that trust gap becomes an operational resilience issue.

This is where IGEL IT for OT, built on the IGEL Adaptive Secure Endpoint Platform, provides an important layer of risk reduction. Through a read-only operating foundation, centralized governance, attested workload delivery, contextual policy enforcement, and recovery-oriented design, IGEL helps organizations support ISA/IEC 62443-aligned objectives for integrity, controlled access, operational oversight, and resilience. The result is IGEL Adaptive Secure Endpoint Platform: a more trusted, governed, and resilient endpoint and workspace model for OT and OT-adjacent operations.

ISA/IEC 62443 helps define what stronger OT cybersecurity should look like. IGEL helps organizations operationalize important parts of that framework by making endpoint participation more trustworthy, governable, and resilient.

Defining the Endpoint Trust Gap in OT Cybersecurity

OT security strategies increasingly rely on layered controls involving segmentation, privileged access controls, identity governance, monitoring, and remote access security as part of **Zero Trust** principles. While these improvements are essential, they rely on an assumption that does not always hold true in practice: that the endpoint, whether requesting access, executing workflows, or presenting operational interfaces, can be inherently trusted.

Endpoints in industrial operations are often distributed, exposed, heterogeneous, and long-lived. They may support human-machine interface access, plant-floor workstations, warehouse devices, control-room operations, engineering sessions, third-party maintenance workflows, digital signage, or OT-adjacent business processes. Some are modernized, but many are not and still depend on legacy applications or Windows-bound workflows. Others sit at the boundary between IT controls and OT production. This inconsistent endpoint model can weaken policy confidence, complicate compliance, and make secure access harder to enforce across the entire environment.

OT security goes beyond preventing unauthorized access; it ensures endpoints participate reliably within governed environments. When endpoints drift from a known-good state, whether through configuration sprawl, ungoverned software, or delayed recovery, other controls are forced to compensate.

That is why the endpoint trust gap deserves more attention. The issue is that network controls or identity controls are only as dependable as the device layer beneath them. In critical industries, where downtime has direct business and operational and safety consequences, endpoint trust becomes inseparable from operational resilience.

What ISA/IEC 62443 Is and Why It Matters for IACS

ISA/IEC 62443 is a family of standards focused specifically on securing industrial automation and control systems. Unlike general IT cybersecurity frameworks, it was created to address the realities of industrial environments, where safety, availability, lifecycle longevity, operational continuity, and engineering constraints all shape how security must be implemented.

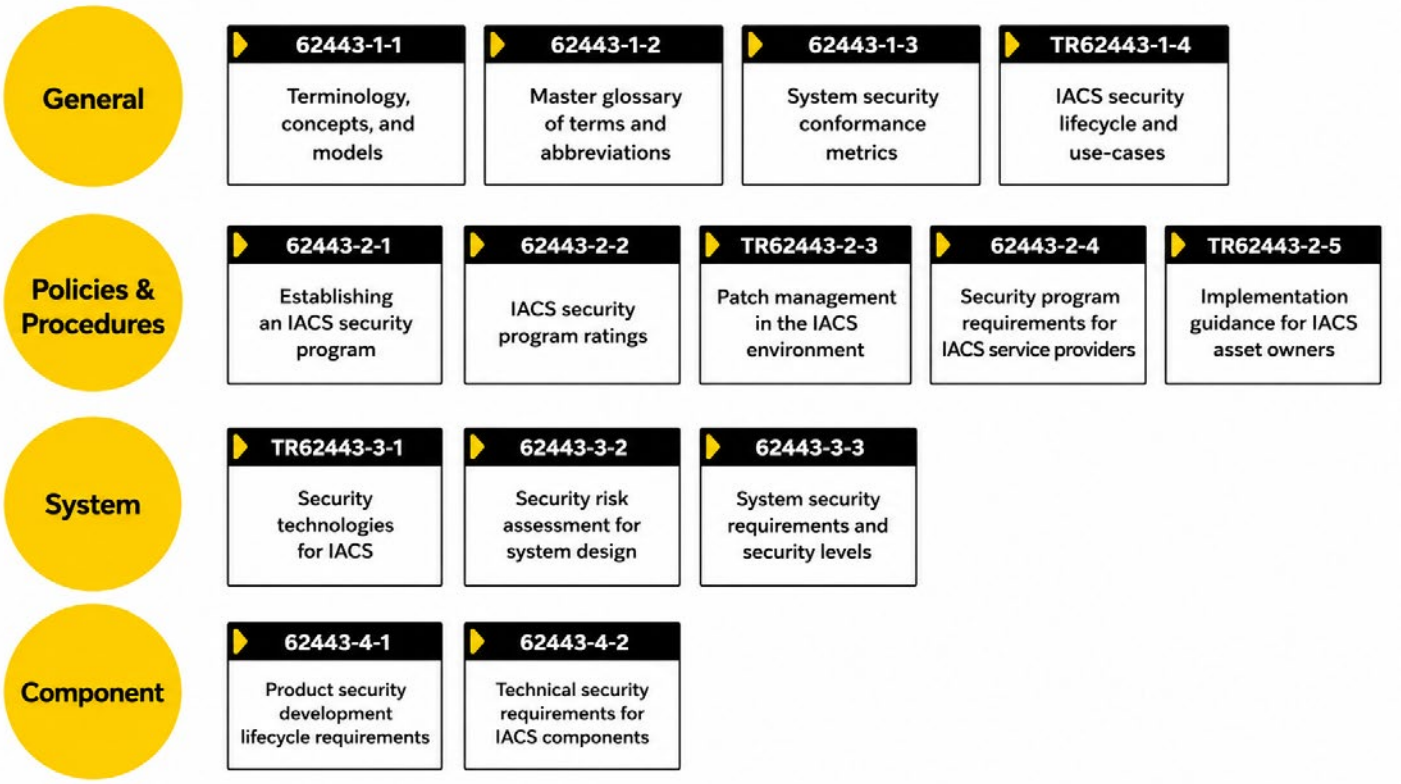
The standard is broad in scope and distributes responsibility across multiple stakeholders, including asset owners and operators, system integrators, service providers, and product suppliers. IGEL observes this shared responsibility model frequently in converged IT/OT environments, where risk is rarely managed through a single control point or by a single organizational role.

Industrial organizations are under pressure to connect more assets, enable more remote and third-party access, digitize workflows, improve visibility, and modernize aging infrastructure. At the same time, they must preserve uptime and avoid security measures that create operational friction or force disruptive redesigns. ISA/IEC 62443 provides a common structure for managing those trade-offs in a disciplined way.

In practical terms, the standard helps OT leaders answer a set of essential questions:

- How should risk be assessed in an industrial environment?
- How should systems be segmented?
- How should access and network / application communications be controlled?
- What responsibilities belong to operators, integrators, and vendors?
- How can security be improved without impacting operations?
- How to quickly recover from an endpoint failure on the production line?

IEC 62443 is comprehensive because it addresses policies, processes, system-level protections, and component-level requirements rather than treating industrial cybersecurity as a purely network-centric problem. The table below shows the framework hierarchy.



Core ISA/IEC 62443 Concepts

For many executives and practitioners, ISA/IEC 62443 can appear more complex than other frameworks because it is a comprehensive multi-part series rather than a single checklist. However, five familiar concepts are of particular importance for OT decision-makers:

1. The standard is risk-based. It does not impose uniform controls on every asset or workflow. Instead, it helps organizations determine the level of protection required based on risk, function, and consequence. This includes the concept of security levels, which express the degree of resistance required against different threat categories and scenarios.
2. The series emphasizes zones and conduits. Zones group assets with similar security needs, while conduits govern and secure communications between them. This supports segmentation, restricted data flow, policy consistency, and defense in depth.
3. ISA/IEC 62443 reinforces least privilege and controlled access. In OT, secure access is appropriate, constrained, observable, and aligned to operational need.
4. The standard prioritizes system integrity and availability. In industrial environments, confidentiality is only one part of the security equation. Systems must continue to operate, changes must be controlled, and recovery must be achievable.
5. IEC 62443 reflects a shared responsibility model. Asset owners, integrators, and suppliers all influence industrial risk in different ways. One of the standard's strengths is that it creates a common language across those stakeholders.

ISA/IEC 62443 Positions Security as Part of the OT Architecture

An OT environment can be segmented correctly on paper and still be exposed through weak endpoint participation. For example:

- How should risk be assessed in an industrial environment?
- A privileged remote session may be wrapped in strong identity controls and still originate from a device that has drifted from policy.
- A recovery plan may exist and still fail to restore operations quickly if endpoint rebuilds are slow, manual, or inconsistent.

Endpoint trust is not separate from OT architecture; it is a critical component to ensure that architecture works under pressure.

How IGEL Supports ISA/IEC 62443 as the Trusted and Governed Endpoint Layer for OT

IGEL supports the system-level requirements of ISA/IEC 62443 by helping organizations strengthen the endpoint layer that supports secure access, system integrity, controlled participation, and operational resilience.

At the system level, ISA/IEC 62443-3-2 requires organizations to define zones and conduits, assess risk, and establish target security levels. ISA/IEC 62443-3-3 then defines the system security requirements needed to achieve those targets, including identification and authentication control, use control, system integrity, restricted data flow, timely response to events, and resource availability.

IGEL operationalizes these requirements at the endpoint by enforcing a secure, read-only endpoint OS, centralized policy control through Universal Management Suite (UMS), and governed application access via the IGEL App Portal, supporting identity and authentication, use control, system integrity, restricted data flow, and rapid response to disruption.

Within that broader architecture, IGEL helps create a trusted and governed endpoint layer. Its prevention-first, centrally governed model makes the device participating in OT workflows more predictable, better controlled, and easier to recover. That, in turn, strengthens how segmentation, identity, policy enforcement, and secure access decisions are applied across manufacturing plants, critical infrastructure, and industrial control environments.

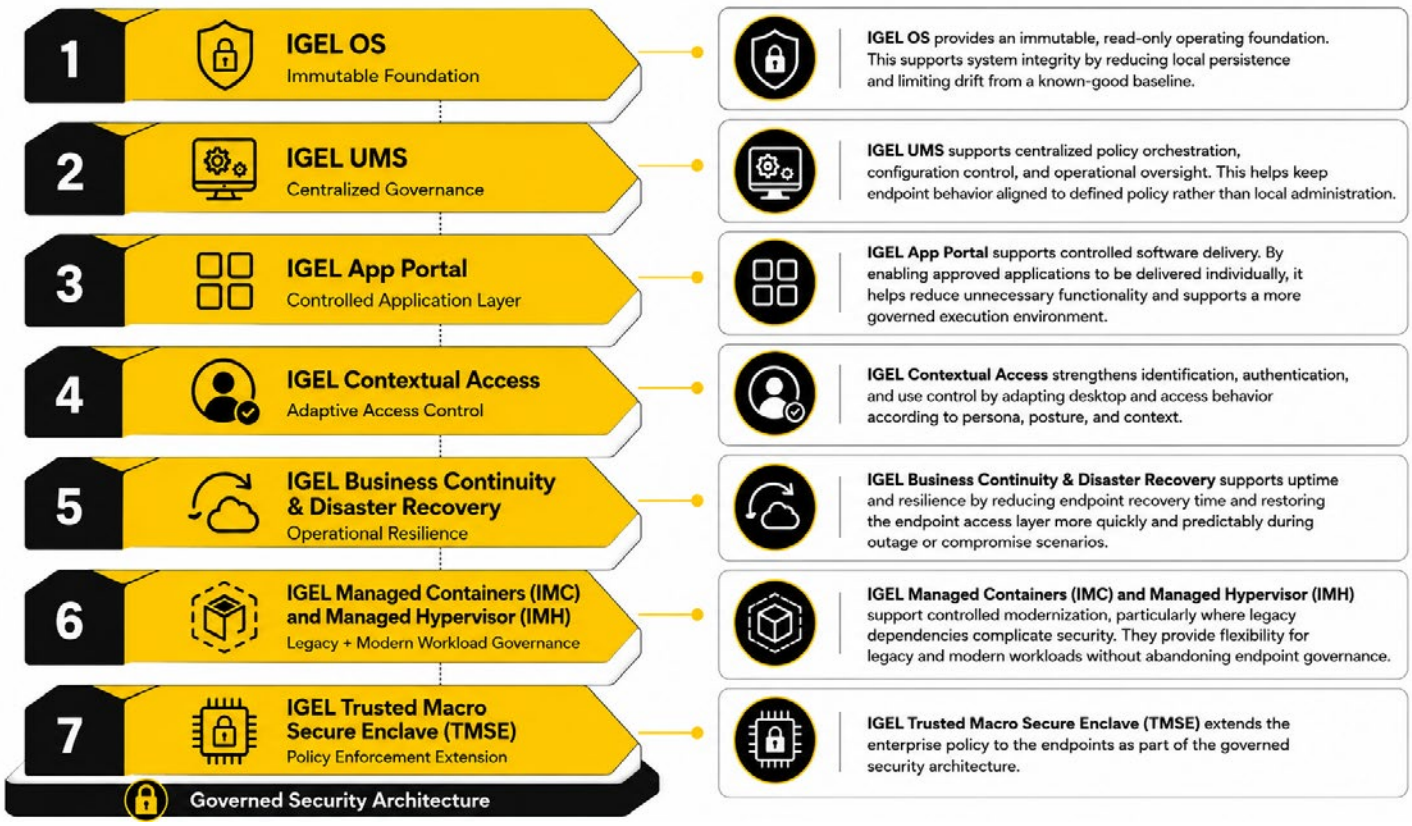
The IGEL Preventative Security Model as the Endpoint Trust Foundation

ISA/IEC 62443 is fundamentally concerned with reducing risk through defined controls and controlled system behavior. For endpoints, that means minimizing unauthorized change, limiting unnecessary functionality, preserving integrity, and ensuring devices participate in industrial workflows under governance rather than by exception.

The IGEL Preventative Security Model aligns to that logic through immutable operation, reduced attack surface, policy control, and trusted participation in access decisions, rather than assuming compromise and relying primarily on remediation.

The IGEL Platform as the Operational Model for Endpoint Control

Within an ISA/IEC 62443-aligned architecture, the IGEL platform contributes directly at the system level where endpoint behavior affects the security objectives of the system.



IGEL Trusted Macro Secure Enclave and ISA/IEC 62443 Zones and Conduits

ISA/IEC 62443-3-2 requires organizations to define zones and conduits, establish target security levels, and apply cybersecurity requirements according to risk and trust boundaries. In practice, that means segmentation is more than separating networks, it governs how users, devices, applications, and communications move across those boundaries.

IGEL Trusted Macro Secure Enclave (TMSE) builds a policy extension model on the trusted foundation. Where the IGEL Preventative Security Model establishes the endpoint as a verifiable trust anchor, TMSE extends enterprise policy to that endpoint through the IGEL control plane, shaping how it is configured, what it can access, and how it is allowed to participate across the environment.

Zones and conduits are only effective when participation across trust boundaries is controlled, policy-aligned, and continuously governed. TMSE strengthens that model by extending enterprise governance to the endpoint layer, helping ensure that endpoints entering OT workflows do so with known posture, controlled behavior, and alignment to broader security, segmentation, and compliance requirements.

TMSE makes zones and conduits more enforceable by ensuring that the endpoint is not treated as an assumed point of trust, but as a governed participant in the broader OT security architecture.

Mapping IGEL to ISA/IEC 62443-3-3

ISA/IEC 62443-3-3 defines system-level security requirements for IACS. IGEL can support selected objectives as follows:

ISA/IEC 62443-3-3 REQUIREMENT	DESCRIPTION	HOW IGEL SUPPORTS IT	PRIMARY IGEL CAPABILITIES
Identification and Authentication Control (IAC)	Users, devices, and system components must be appropriately identified and authenticated before access is granted.	IGEL helps ensure the endpoint is a governed, enrolled, policy-controlled device rather than an unmanaged client. UMS and contextual policy strengthen the endpoint's role in trust decisions.	IGEL UMS IGEL Contextual Access IGEL OS
Use Control (UC)	Authenticated users and systems should only be able to perform actions appropriate to their role and context.	IGEL supports least-privilege access through persona-aware and context-aware policy enforcement, controlled application access, and tightly governed workspaces.	IGEL Contextual Access IGEL UMS IGEL App Portal IGEL TMSE
System Integrity (SI)	Systems must be protected against unauthorized modification, malicious code, and configuration drift.	IGEL's read-only, immutable OS, reduced local persistence, controlled application delivery, and Secure Boot support help preserve a known-good endpoint state.	IGEL OS IGEL App Portal IGEL UMS
Data Confidentiality (DC)	Information must be protected from unauthorized disclosure.	IGEL reduces endpoint-side data exposure by limiting local data persistence and supporting controlled workspaces, though it does not replace encryption, DLP, or broader data protection controls.	IGEL OS IGEL Contextual Access IGEL UMS
Restricted Data Flow (RDF)	Communications must be limited according to zones, conduits, and policy.	IGEL strengthens endpoint participation within segmented architectures by ensuring devices are governed and policy controlled.	IGEL TMSE IGEL UMS IGEL Contextual Access
Timely Response to Events (TRE)	Systems should support detection, reporting, and response to cybersecurity events.	IGEL improves endpoint visibility through telemetry, centralized monitoring, and policy-state awareness, supporting faster investigation and response.	IGEL Insights IGEL UMS
Resource Availability (RA)	Systems must continue to perform required functions and recover appropriately from disruption.	IGEL reduces endpoint fragility and supports faster restoration of secure access after compromise, misconfiguration, or device failure.	IGEL Business Continuity & Disaster Recovery IGEL OS IGEL UMS

While IGEL aligns most directly with the system-level requirements of ISA/IEC 62443, its relevance extends across the broader framework. At the system level, IGEL helps strengthen secure access, endpoint integrity, controlled participation, and recovery readiness within OT environments. At the same time, it supports the wider goals of the standard by reflecting the core principles described in the general section, helping organizations operationalize policy and governance through centralized control, and contributing component-level security value through its secure endpoint platform and controlled software delivery model.

IGEL Adaptive Endpoint Solution Platform for OT as the Outcome

For organizations modernizing OT environments, IGEL Adaptive Endpoint Solution Platform for OT represents a shift away from conventional, mutable endpoint models and toward a more controlled operating state. It enables secure participation in industrial workflows without losing sight of uptime, operational continuity, and the realities of legacy dependencies.

The three-plane architecture of the IGEL Adaptive Secure Endpoint Platform:

1. Execution — IGEL OS
Provides the immutable endpoint OS and known-good runtime state. This is where trust begins and where PSM is most directly anchored.

2. Control — Universal Management Suite (UMS)
Applies real-time policy, configuration control, and device governance. This is where TMSE is anchored and where policy is orchestrated and enforced.

3. Data — App Portal
Delivers attested and validated applications and workloads via the IGEL App Portal, supporting validated & trusted workload delivery and policy-aligned software access.

Operational Resilience and Critical Infrastructure Protection

In critical industries, cybersecurity and resilience are inseparable. Manufacturing organizations depend on production continuity. Healthcare environments depend on reliable access to clinical and operational systems. Energy, utilities, and other infrastructure sectors depend on the continuity of services where disruption can have consequences far beyond the IT environment. In each of these cases, the endpoint is more than simply a user device, it is often a point of operational participation that must remain secure, governed, and recoverable under pressure where every minute of downtime can be critical.

This is why the endpoint trust gap has broader implications in OT than it does in many traditional IT environments. A device that is difficult to verify, difficult to control, or slow to restore can create operational drag even when upstream controls are sound. Recovery is also different in OT. The challenge is how to secure access to critical processes that can be restored quickly enough to support continuity of operations. In high-consequence environments, that difference matters.

IGEL's value in this context is that it helps reduce endpoint fragility. By combining immutable operation, centralized governance, controlled application delivery, and recovery-oriented design, IGEL supports a more resilient access layer for industrial operations. That does not replace broader OT resilience planning, but it does strengthen one of the most exposed and operationally significant parts of the architecture: the endpoint through which users, devices, and workflows connect into critical environments.

Secure Remote and Vendor Access for OT and IACS Environments

The IEC standard requires controlled access, authenticated participation, and restricted communications across trust boundaries. In practice, however, OEM technicians, contractors, integrators, and remote engineers often connect from inconsistent or weakly governed devices.

IGEL helps reduce that risk by providing a controlled endpoint workspace for remote access into OT-adjacent or OT-supporting workflows. The IGEL device used for remote participation is more predictable, more tightly governed, less exposed to local persistence, and more consistent across sites. This governance directly supports the ISA/IEC 62443 objectives of use control, system integrity, and restricted data flow.

Endpoint Security Use Cases in OT, IACS, and Critical Infrastructure

This approach is most compelling when tied to specific OT use cases where ISA/IEC 62443 requirements meet endpoint reality: production-line terminals, HMI access points, control-room workstations, plant-floor operator devices, warehouse and logistics terminals, SCADA-adjacent access clients, and legacy Windows-dependent operational workloads.

In each case, the user has to be authorized, and the endpoint itself must be sufficiently controlled to participate in a segmented, policy-driven industrial architecture. IGEL's immutable OS, centralized policy management, contextual enforcement, and legacy workload support make it relevant at exactly these access points.

A Practical Path Forward for OT Leaders

For CIOs, CISOs, and CTOs responsible for IT and OT environments, the practical path forward begins by identifying where endpoint trust has the greatest operational impact. That typically includes shared workstations, plant-floor devices, HMI terminals, engineering access points, control-room systems, and remote or third-party access workflows.

From there, organizations should prioritize high-consequence access points where a compromised or poorly governed endpoint could undermine segmentation, delay recovery, or weaken confidence in policy enforcement. In many cases, improving the endpoint layer can deliver immediate benefits by reducing configuration drift, strengthening access control, and making operational recovery more predictable. The next step is to align endpoint state with broader OT cybersecurity strategy. That means supporting zones and conduits with endpoints that are trusted, governed, and policy-aware; enabling workload flexibility without reverting to unmanaged device models; and improving resilience by ensuring secure access can be restored quickly after disruption. For OT leaders, the goal is to reduce the gap between security architecture on paper and enforceable control in day-to-day operations.

Summary: Strengthening OT Cybersecurity and Operational Resilience

ISA/IEC 62443 gives OT leaders a practical framework for strengthening cybersecurity across industrial environments without losing sight of uptime, safety, and operational continuity. ISA/IEC 62443 recognizes that OT security failures are not caused only by the absence of a network control. They can also result from a device layer that is difficult to authenticate reliably, difficult to configure consistently, difficult to keep in a known-good state, or difficult to restore quickly after disruption.

Many organizations modernize upstream controls while continuing to rely on conventional endpoint models that were not designed for high-trust, high-consequence, policy-sensitive operations. This creates friction between the security architecture they want and the endpoint behavior they can enforce.

A preventative endpoint model supports the practical intent of the standard by reducing the opportunity for drift, unauthorized software execution, and uncontrolled local change.

By strengthening the endpoint layer beneath modern access and segmentation strategies, IGEL IT for OT can reduce the endpoint trust gap and move toward a more trusted, resilient, and governed endpoint foundation for secure access, controlled participation, and continuity of operations across critical industries.