STONESIGHT / EXECUTIVE WHITEPAPER

IT/OT CONVERGENCE

When the security boundary moves before anyone notices



STONESIGHT ADVISORY SERVICES

INDEPENDENT JUDGMENT. INFORMED ACTION.

01 / THE FRONT ARRIVES

The change begins beneath the surface.

The sea is calm. Along the horizon, a dark shelf of clouds begins to advance. Colder, denser air moves beneath warmer air, forcing it upward. The boundary becomes visible as the atmosphere reorganizes. By the time the front dominates the sky, the movement that created it is already well underway.

Something similar happens on the factory floor. A robot continues lifting, welding, or assembling exactly as it did yesterday. Its enclosure looks familiar. Production continues. Yet behind the machine, the tools used to program and maintain it have changed.

A dedicated teaching pendant once connected through specialized hardware and protocols. Now an engineering laptop, tablet, or networked workstation performs some of those tasks. Commercial software and TCP/IP networking enter the supporting environment. The production manager sees the same robot. The IT manager may never see the computer behind it.

That is the convergence front. The most consequential change can arrive below the visible operation, through infrastructure, maintenance, and access. The machine's appearance provides no reliable indication of how its security boundary has moved.

The distinction matters. A programmable logic controller or robot controller may still run specialized firmware. Windows or Linux may reside on the engineering workstation, operator interface, or gateway instead. The exposure comes from the complete chain of systems able to influence the process, wherever the general-purpose computing sits.

A computer used for maintenance may connect to the internet elsewhere, download an update, or support a vendor session before reconnecting to industrial equipment. The machine does not need its own direct internet connection to inherit exposure from that pathway.

For leadership, the question is immediate: does our security model describe how this equipment is operated and maintained today? A design built around isolation can become outdated without a dramatic equipment replacement. The business may approve a useful enhancement while unknowingly accepting a different set of dependencies. As with the front on the horizon, understanding the movement beneath the surface is what makes preparation possible.

Same machine. Different exposure.

DEDICATED CONTROL

Teaching pendant / specialized connection

THE SHIFT

CONNECTED MAINTENANCE

Engineering laptop / TCP/IP / remote services

The maintenance pathway becomes part of the security boundary.

02 / THE MAINTENANCE PATHWAY

Convenience creates a new connection.

Remote support solves real operational problems. It brings expertise to a factory quickly, reduces travel, and shortens downtime. Standard computing platforms can make systems easier to integrate and maintain. Those benefits are substantial. They also require explicit decisions about who can reach equipment, what they can change, and how that access ends.

In my experience, technicians have connected a mobile phone to an otherwise isolated network so that a colleague elsewhere could perform maintenance. I have also seen remote desktop access enabled and credentials shared for a support task, with the access left available afterward. These were practical shortcuts taken to finish necessary work.

The individuals involved did not necessarily think they were redesigning the security architecture. They were restoring service, avoiding another site visit, or completing an overdue adjustment. But the result was a new route into an operational environment, sometimes without the awareness of its accountable managers.

The maintenance pathway must therefore be treated as part of the system. An asset inventory should identify engineering workstations, gateways, support accounts, update mechanisms, and temporary connections alongside the production equipment. A diagram showing separation is incomplete if everyday work routinely bridges it.

Proprietary technology and physical isolation never guaranteed immunity. They could restrict particular access routes. Their value depended on how the environment actually operated. Once laptops, removable media, shared credentials, or remote services cross that boundary, the organization must understand and govern those crossings.

A workable support process should provide named accounts, appropriate authentication, approved connection paths, task-specific authorization, and time-limited access. Someone must verify that the session has ended and that any temporary exception has been closed. Urgent work needs a clear escalation route.

Leadership also has to examine why people bypass the approved process. If the schedule demands an immediate repair but the authorized route takes days, the workaround becomes predictable. Policies alone cannot resolve that conflict. Make the safe method practical, resource it adequately, and measure whether people can use it under real operating pressure. Otherwise, the documented environment and the actual environment will continue to diverge.



IT/OT CONVERGENCE / CONSEQUENCES

The connection was temporary. The consequences may not be.

03 / THE BUSINESS CONSEQUENCE

Protect what keeps the enterprise moving.

A company can operate a sophisticated corporate security program and still misunderstand its operational exposure. Office endpoints may be monitored, identities governed, and audits completed while engineering workstations or supplier connections remain outside the same visibility. The reassuring dashboard may describe only part of the business.

Start with a different question: where does revenue flow? For a manufacturer, it may depend on production cells, process controls, and material handling. For a logistics company, it may depend on warehouse automation and routing. Identify the physical capabilities the enterprise must preserve, then trace the technology and maintenance dependencies supporting them.

The consequences extend beyond stolen information. An interruption can stop production. An unauthorized change can affect equipment behavior. Corrupted process data can leave operators making decisions from an inaccurate picture. A process that appears to be running may be producing output that cannot be trusted.

None of this means that access to a laptop automatically gives an intruder control of a factory. Permissions, segmentation, controller design, safety systems, and other safeguards matter. The point is to examine the actual path and its possible consequences, rather than infer protection from the equipment's familiar appearance.

Operational security also requires operational judgment. NIST's guidance recognizes the distinctive performance, reliability, and safety requirements of OT.[1] A change that is routine in an office environment may require engineering review, vendor coordination, testing, and a maintenance window in production.

Recovery deserves the same discipline. Restoring a server is not equivalent to restoring a safe, reliable process. The organization may need validated control logic, equipment configurations, specialist knowledge, replacement components, and an agreed sequence for restarting operations.

Executives should ask for evidence that these dependencies are understood and that recovery assumptions have been exercised. Which failure could stop a critical process? Who can authorize its restoration? How will operators know that its output is trustworthy? Answering those questions connects cybersecurity to the business outcomes it is meant to protect. The cost of a missed dependency may remain invisible until the moment the enterprise needs it most.

04 / THE LEADERSHIP RESPONSE

Keep the protection as the environment changes.

The response begins with a shared operating picture. Operations, engineering, technology, and security leaders should examine critical processes together. Each brings knowledge the others need. The objective is to identify where connectivity has changed, which assumptions no longer hold, and who is accountable for the resulting exposure.

Validate the boundary. Review actual network paths, maintenance practices, vendor arrangements, and update methods. Confirm whether supposedly isolated equipment has indirect connections. Repeat the review when equipment, supporting software, or service agreements change. An old architecture diagram is a starting point, not proof of present conditions.

Assign ownership across the whole chain. Someone must own the controller, the engineering workstation, the support account, the gateway, and the recovery process. Responsibilities can be shared, but decisions cannot be left in the gap between departments. Define who approves access and who accepts an unresolved operational risk.

Limit access according to the work. Separate environments where appropriate, restrict the ability to change critical systems, and make vendor access visible and revocable. Evaluate controls with the people responsible for safe operation. Protection should support the process without introducing an unexamined operational hazard.

Prepare for exceptions before an outage creates urgency. Establish how emergency support is authorized, how activity is recorded, and when temporary arrangements expire. Review recurring exceptions as evidence that the normal process may need redesign. A repeated workaround is an operating practice, even if the policy calls it exceptional.

Give leadership a concise view of material gaps: unknown dependencies, persistent access, unsupported components, unclear ownership, and untested recovery. Track corrective actions through completion. Report what the evidence establishes and where uncertainty remains, rather than treating policy coverage as proof that a process is protected.

Convergence will continue wherever connectivity creates value. The leadership task is to ensure that protection evolves with it. At StoneSight, that means connecting independent judgment to operating reality: what management believes is protected, what people actually do, and what evidence supports that belief. The front cannot be managed from yesterday's weather report. Neither can the enterprise be secured from yesterday's assumptions.

05 / AFTER THE FRONT

Clearer conditions.
A different environment.

After a cold front passes, the air often becomes cooler and clearer. Visibility improves, but the conditions have changed. The sensible response is to navigate using the environment now in front of us.

IT/OT convergence calls for the same adjustment. Once common computing platforms and new maintenance paths enter the operation, the old assumptions do not return simply because the installation is complete or the immediate disruption has passed.

The opportunity is clarity: a current view of dependencies, deliberate access decisions, accountable ownership, and recovery plans grounded in the physical process. The goal is an enterprise that can use connectivity with confidence because it understands what has changed and has adapted its protection accordingly.

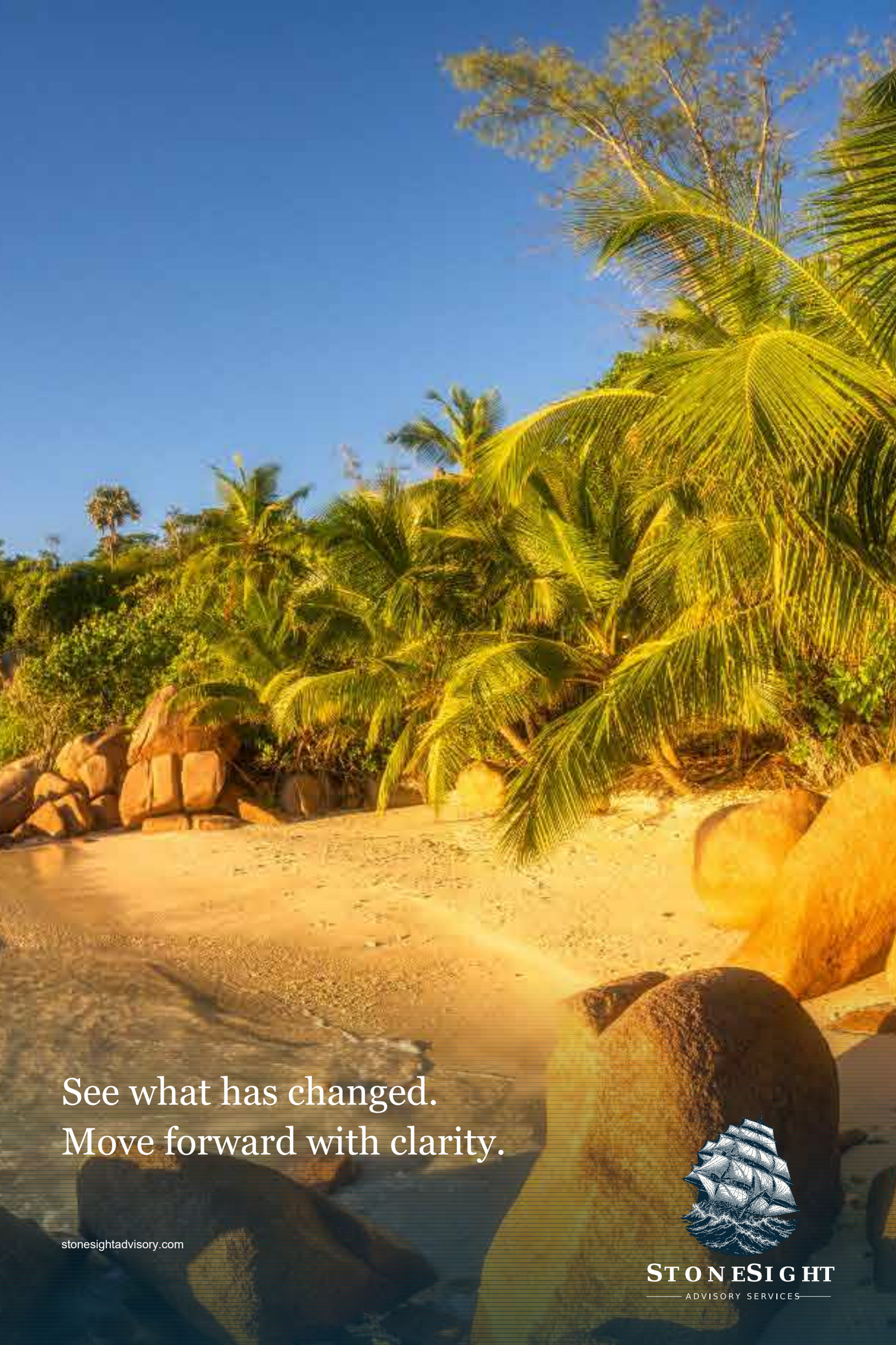
ABOUT THIS PERSPECTIVE

Joe Marroquin | CEO & Principal Advisor, StoneSight Advisory Services

Adapted and updated from the author's LinkedIn article, "IT OT Convergence: Is Your Security Paradigm Valid?" (July 13, 2022).

[1] NIST, Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3, September 2023. Supporting guidance on OT performance, reliability, and safety.

doi.org/10.6028/NIST.SP.800-82r3


See what has changed.
Move forward with clarity.
stonesightadvisory.com
STONESIGHT
ADVISORY SERVICES