W H I T E P A P E R

Why Is IT/OT Convergence So Hard To Accomplish?

Martin van der Linden, 2026

Executive Summary

Regulatory accountability is tightening. Cyber incidents are producing physical consequences. Critical infrastructure has become a matter of strategic concern. Across these pressures, leaders are increasingly answerable for a category of risk that used to be managed inside a plant, by people who do not report to them, on systems they do not see.

Beneath all of it sits a question the enterprise has not answered: who governs the space where corporate IT, industrial operations, and external vendors meet?

That space – where systems connect, data moves, and external parties gain access – has become central to both value creation and risk. It is not formally owned. It is not consistently governed. The result is a persistent gap between responsibility and authority: a **governance void** at the heart of the cyber-physical enterprise.

Programmes scoped to controls, compliance, or incremental integration will continue to produce activity without resolving the underlying issue. The question convergence ultimately forces is not technical. It is structural: who governs the cyber-physical domain, and on what authority?

A Problem That Has Already Reached the Boardroom

For most of the last decade, the risks that emerge where enterprise IT meets industrial systems were handled at a technical level, inside specialist functions, well below executive sightlines.

That has changed.

Cyber incidents have demonstrated that digital compromise can have direct physical consequences – stopped production, damaged equipment, environmental exposure, public safety events. Regulatory regimes have moved past guidance toward enforceable accountability. NIS2 attaches to the Operator's cyber risk and CER to the resilience of the essential service; parallel regimes in other jurisdictions are converging on the same ground. Several extend personal liability to executive leadership. Geopolitical conditions have elevated industrial capability and critical infrastructure to matters of national strategic concern.

These pressures arrive on the same desk. They cannot be discharged by writing a security policy, certifying against a control framework, or producing audit evidence. They demand that the organisation can demonstrate, coherently and over time, that it governs cyber-physical risk – not merely that it controls it.

That is a different requirement, and most enterprises are not yet structured to meet it.

Why This Is Not the Convergence Problem You Were Briefed On

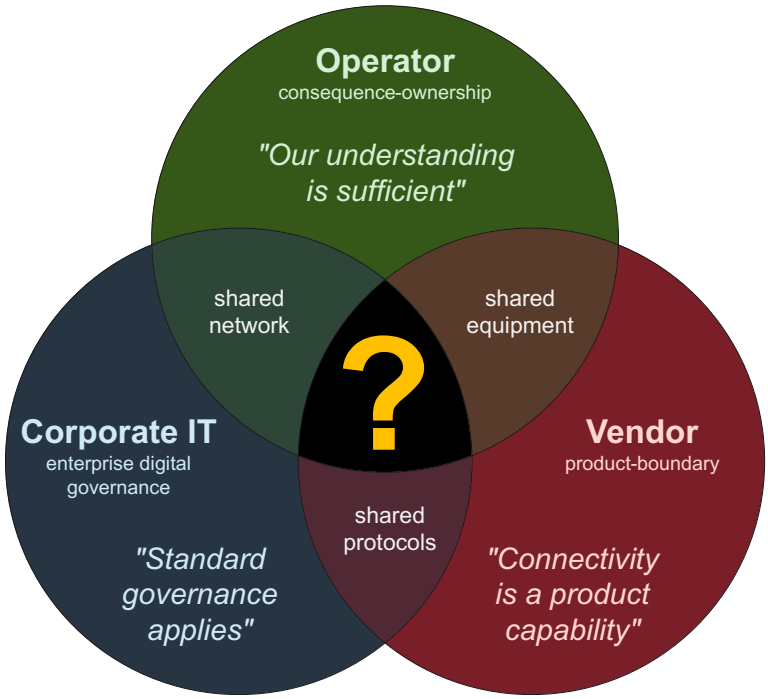
IT/OT convergence has been on enterprise agendas for years. It has been framed as a technology problem, a security problem, an integration problem – pick the brief that fits the function presenting it.

Each of these framings is partially true. Each leads to programmes that produce activity without producing resolution.

The reason is that convergence is not, at its core, any of those things. It is the meeting of three actors who do not share an authority structure.

First, the *Operator* – the operations leadership who carry the consequences of industrial systems: production, safety, environmental performance, and standing in front of an industrial regulator. Second, *Corporate IT* – the CIOs and CISOs who carry responsibility for the integrity of the enterprise digital environment. Third, the *Vendor* – the equipment and software companies whose products run inside the plant, and whose remote connectivity, support contracts, and lifecycle decisions increasingly shape what is possible inside it.

Each operates on a different timescale. Each optimises for a different outcome. Each defines risk in different terms. None has the authority to define the whole.



Three actors, three logics, three assumptions –
and no shared authority for the space between them.

Where these three actors intersect, a new operational space has formed. It is visible in remote access pathways from vendor environments into plant systems, in the replication of process data into cloud platforms, in the systems that bridge production and enterprise planning, and in the engineering environments that sit between control networks and corporate identity services.

This space is now central to value creation. It is also where risk concentrates. And it is not recognised as a domain in its own right. It is treated, depending on who is asked, as an extension of IT, a dependency of operations, or a feature of vendor products. Decisions taken within it – about trust, access, connectivity, and data – are consequential, but they are rarely treated as matters of governance. They are handled as matters of implementation.

The assumption that someone, somewhere, must be in control persists. The operating model to support that assumption does not.

This is the **governance void**.

Why Current Programmes Do Not Close It

Once the void is named, the limits of the dominant response become clear.

Programmes are initiated under security or IT leadership. Frameworks are applied. Gaps are assessed. Controls are implemented. Evidence is produced. Progress is reported.

These activities are necessary. They are not sufficient.

They work within the boundaries of the existing organisation, and in doing so they avoid the need to redefine those boundaries. They produce outputs that can be audited, but they do not resolve the question of who has the authority to make decisions that cross domains, organisations, and lifecycles.

As long as convergence is approached this way, it will tend to stabilise at the point where it becomes manageable within current structures. The harder questions – of ownership, accountability, and architectural intent – are deferred.

This is why convergence programmes can appear active while the underlying problem remains unchanged. The void is not a gap that closes once enough technical work has been done. It is a gap in the operating model. It closes only when the enterprise decides to govern the space, not merely to operate inside it.

What Closing the Void Actually Requires

If the governance void is structural, its resolution is structural.

It begins with ownership. Not ownership in the sense of system responsibility, but ownership in the sense of authority – the ability to define how, and under what conditions, IT systems, operational systems, and external parties interact. Without this, coordination replaces control, and accountability remains diffuse.

From ownership follows the need for clear decision rights. Who approves connectivity that crosses domains. Who governs identity and access that spans organisational boundaries. Who determines what data leaves the operational environment. Who leads when a cyber event has physical consequences. These questions cannot be left to emerge informally. They have to be assigned deliberately, and they have to hold across projects, leadership changes, and contract cycles.

Architecture, in this context, becomes less about connectivity and more about constraint. It defines where separation must be maintained, where integration is permitted, and what conditions must be met for that integration to occur. It establishes boundaries that persist beyond individual projects and technologies.

The role of the vendor has to be reframed. Vendors are not external to the problem; they are embedded within it. Their design choices, support models, and access pathways shape the cyber-physical domain as much as internal decisions do. Treating vendor interaction as a procurement or support concern rather than a governance concern leaves a critical part of the domain unmanaged.

Finally, convergence has to be understood over the lifecycle of industrial systems. Decisions made during design and procurement persist for decades. Governance that operates only at the level of projects or programmes is insufficient for assets that outlast organisational structures and leadership tenures.

Implications

The implications are not confined to any single function.

For boards and executive leadership, the governance void introduces a category of risk that cannot be delegated without clarity on how it is governed. For CIOs and CISOs, it extends responsibility beyond the enterprise perimeter into environments where traditional models do not directly apply – and gives them a structural reason to engage operations leadership as peers, not as internal customers. For operations, it requires engagement in decisions that have historically been externalised to IT or to vendors. For architects, it demands a focus on operating models as much as on systems.

Most significantly, it challenges the assumption that convergence can be achieved without changing how the enterprise itself is structured to make decisions.

Conclusion

IT/OT convergence has been framed as a technical challenge for long enough to make partial progress feel like success. The problem it represents is not the connection of systems. It is the governance of what those connections create.

As long as the cyber-physical domain remains unowned, convergence will continue to fragment into manageable pieces, each of which makes sense locally and none of which resolves the whole. The question that remains is not how to connect IT and OT more effectively.

It is whether the enterprise is prepared to define, explicitly, who governs the space between them.

The framework that addresses this question – its governance logics, its decision rights, and its architectural form – is developed in the three-book series Governance and Architecture for the Cyber-Physical Enterprise. The series, companion white papers, and engagement tracks are available at thegovernedboundary.com.