http://www.diva-portal.org

Postprint

This is the accepted version of a paper presented at *45th IFIP WG 5.7 International Conference on Advances in Production Management Systems, APMS 2026, Bergamo, Sept 13-17, 2026*.

Citation for the original published paper:

Anderson, M., West, S., Larsson, T. (2027)
Jurisdictional Contestation in Emergent Digital Manufacturing Domains: Top-Down DevOps Vertical Ownership as Double Loop Learning
In: Pezzotta G., Gaiardelli P., Cimini C., Sala R., Romero D., Baalsrud-Hauge J. (ed.), *Advances in Production Management Systems: Shaping the Future of Industry Through Sustainable, Data-Driven, and Human-Centric Production Systems: 45th IFIP WG 5.7 International Conference, APMS 2026, Bergamo, Italy, September 13–17, 2026, Proceedings, Part IV* (pp. 166-180). Springer Science+Business Media B.V.
IFIP Advances in Information and Communication Technology
https://doi.org/10.1007/978-3-032-38606-9_12

N.B. When citing this work, cite the original published paper.

©IFIP, 2027. This is the author's version of the work. It is posted here by permission of IFIP for your personal use. Not for redistribution.

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:bth-30623

Jurisdictional Contestation in Emergent Digital Manufacturing Domains: Top-Down DevOps Vertical Ownership as Double Loop Learning

Matthew Anderson[1][0000-0001-5214-4477], Shaun West[2][0000-0002-8042-1459] and Tobias Larsson[1][0000-0002-9662-4576]

[1] Department of Mechanical Engineering, Blekinge Institute of Technology (BTH), Karlskrona, Sweden
[2] School of Engineering and Architecture, Hochschule Luzern, Horw, Switzerland

matthew.anderson@bth.se

Abstract. Emergent digital manufacturing capabilities often stall despite technical readiness because established organisational functions contest ownership of newly visible technology domains. This paper characterises this mechanism as diagnostic reductionism: the reduction of a multi-dimensional digital capability to the single aspect that an incumbent function can recognise and govern. Drawing on jurisdictional theory, organisational learning, Conway's Law, team topologies, and digital waste, the paper argues that diagnostic reductionism produces waste through non-use, in which technically available capabilities are organisationally foreclosed. An illustrative edge computing vignette shows how distributed approval authority fragments ownership and prevents platform-level outcomes. The paper proposes executive-sponsored DevOps vertical ownership, supported by platform-team governance, as a double loop intervention that shifts ownership from functional control to end-to-end accountability for manufacturing outcomes. The contribution is threefold: extending jurisdictional theory to intra-organisational technology domains, identifying governance as a source of digital waste, and theorising the conditions under which top-down DevOps can resolve jurisdictional contestation in digital manufacturing.

Keywords: digital manufacturing; diagnostic reductionism; jurisdictional contestation; digital waste; DevOps vertical ownership; platform teams.

1 Introduction

When manufacturers add new digital capabilities (e.g., edge devices, digital twins, connected worker platforms, or analytics systems), an organisational pattern repeats. Existing teams see only what they recognise: infrastructure teams spot network endpoints, quality teams see instruments, maintenance sees monitors, and automation sees PLC-adjacent devices. This recognition sparks jurisdictional claims as each team asserts ownership, comparing the new technology to what it already manages. The proposing team, usually closest to production, sees the technology's value reduced to the

narrow view of the claiming function; key process data and operational context are sidelined. As a result, progress stalls, not due to technical failure, but organisational disagreement over ownership and purpose. Prior research shows that firms adopt digital tools without the necessary organisational foundations [1], but how governance shapes this process is less well understood.

This pattern extends beyond operational technology, wherever new digital manufacturing tools meet established governance. Jurisdictional contestation emerges: teams claim ownership by partially recognising aspects within their domain, narrowing the technology to what they understand. The opportunity for a broader, data-driven manufacturing ecosystem, combining machine telemetry, process context, quality data, and operational intelligence, is lost before technical evaluation. We term this diagnostic reductionism: the reduction of a multi-dimensional digital capability to the single aspect that an established function can diagnose. Drawing on Abbott's [2] framework of diagnosis, inference, and treatment, the narrowing occurs at diagnosis. Infrastructure teams focusing solely on network endpoints are the most common form, but the mechanism is widespread.

The paper makes three contributions. First, it applies Abbott's [2] jurisdictional theory to explain why established organisational functions rationally pursue claims over emergent digital domains, introducing diagnostic reductionism as a construct for this mechanism. Second, drawing on Romero et al.'s [3] digital waste taxonomy, it argues that the organisational consequence is waste through non-use: technically available digital capabilities that are organisationally foreclosed. Third, it proposes that in large manufacturers with entrenched distributed governance, executive-sponsored DevOps vertical ownership can provide a more reliable mechanism than the available alternatives for breaking through jurisdictional paralysis.

The paper proceeds as follows. Section 2 establishes theoretical foundations across four complementary lenses. Section 3 characterises the phenomenon of jurisdictional contestation, including an illustrative vignette from an edge computing deployment. Section 4 develops the argument for top-down DevOps vertical ownership as the solution mechanism. Section 5 examines the governance paradox. Section 6 discusses implications. Section 7 concludes.

2 Theoretical Foundations

This section draws on four complementary lenses. Abbott's [2] system of professions provides the vocabulary for jurisdictional claims. Argyris and Schön's [4, 5] learning theory explains how governance assumptions become self-reinforcing through defensive routines. Skelton and Pais's [6] team topologies, grounded in Conway's Law [7], offer a prescriptive organisational design vocabulary for the proposed remedy. Romero et al.'s [3] digital waste taxonomy provides the consequence framework, grounding the cost of jurisdictional contestation in manufacturing-native vocabulary.

2.1 Jurisdictional Claims and the System of Professions

Abbott [2] theorises professions as occupational groups competing for jurisdiction over solvable problems. Jurisdictional claims advance through three phases: diagnosis

(framing a problem in the profession's domain), inference (the uncertain space where tacit knowledge resides), and treatment (applying the profession's toolkit). Competition arises when social or technical changes weaken an existing profession's jurisdiction or create entirely new niches [2, 8]. Outcomes range from full jurisdictional seizure to negotiated settlements, including subordination, division of labour, and advisory relationships [2].

Sako et al. [9] extend this to digital technology domains, distinguishing 'protective' jurisdictional control (full or subordinate jurisdiction, delegating tasks to subordinates) from 'connective' jurisdictional control (division of labour between equal-status groups). This distinction becomes material when infrastructure teams claim emergent digital domains: they exercise protective control by treating new capabilities as subordinate to infrastructure governance, rather than recognising the need for connective control between infrastructure and process engineering knowledge domains [10].

2.2 Double Loop Learning and Defensive Routines

Argyris and Schön [4, 5] distinguish single loop learning (correcting actions without questioning assumptions) from double loop learning (examining and potentially changing the governing variables: beliefs, norms, policies, and incentives that shaped actions). Argyris [11] identifies 'defensive routines' as organisational practices that prevent embarrassment or threat while simultaneously preventing learning. These routines persist regardless of personnel changes because they are embedded in structures, policies, and incentive systems. Critically, formal governance processes can function as defensive routines when they protect existing power arrangements while appearing to enable change [5, 12].

2.3 Team Topologies and Conway's Law

Skelton and Pais [6] build on Conway's Law [7], the observation that organisations produce systems that mirror their communication structures, to propose four fundamental team types: stream-aligned, enabling, complicated-subsystem, and platform teams. The 'inverse Conway manoeuvre' involves deliberately designing organisational structures to produce the desired technical architecture. If the desired outcome is an integrated digital manufacturing platform, then the organisational structure must support end-to-end ownership rather than fragmenting it across functional silos.

The converse is equally significant: if the decision architecture is distributed across multiple approval points, Conway's Law predicts that the resulting technical architecture will mirror that fragmentation. An emergent digital capability governed by five separate approval authorities will not become a platform; it will become five individually approved point capabilities. This mechanism links organisational governance directly to technical outcomes and explains why distributed jurisdictional settlements systematically prevent platform-level digital manufacturing capability.

2.4 Digital Waste Through Non-Use

Romero et al. [3] introduce the concept of 'digital waste' in the context of cyber-physical production systems. They distinguish waste from overuse (abused digital capabilities, unnecessary complexity) from waste due to non-use (lost digital opportunities, failure to exploit available capabilities). This taxonomy, grounded in the lean manufacturing tradition, provides a consequence framework for jurisdictional contestation.

When infrastructure teams claim emergent digital domains and govern them through narrow infrastructure categories, the organisational consequence is digital waste through non-use. The technology is present, the capability is technically available, but the governance structure ensures it is never fully activated. This is not a technology gap; it is waste generated by organisational design. Critically, because it is waste in the lean sense, it is identifiable, measurable, and eliminable using the same thinking that manufacturing organisations already apply to physical processes. This reframing gives jurisdictional contestation practical urgency: it is not an abstract governance debate but a source of waste that directly affects manufacturing performance.

3 Jurisdictional Contestation in Emergent Digital Domains

This section develops the paper's central mechanism: jurisdictional contestation in emergent digital manufacturing domains. The argument is that contestation begins when established organisational functions recognise familiar artefacts within a new digital capability and use that recognition to claim ownership. This recognition is not irrational; it reflects each function's existing responsibilities, incentives, and risk models. However, because the recognition is partial, it narrows the capability before its broader manufacturing value can be realised. The section first defines this narrowing as diagnostic reductionism, then explains why such claims are rational within existing governance assumptions, examines bi-modal IT as an institutionalised form of handover failure, and finally illustrates the mechanism through an edge computing vignette.

3.1 Diagnostic Reductionism

Diagnostic reductionism occurs whenever an established organisational function encounters an emergent digital capability and diagnoses it through the lens of its own expertise, reducing a multi-dimensional technology to the single dimension it recognises (Fig. 1). The most prevalent form is infrastructural reductionism, where IT infrastructure teams encounter emergent digital manufacturing assets and recognise the familiar: network switches, Ethernet-connected controllers, servers, firewalls, industrial PCs, and edge devices. This recognition triggers a jurisdictional claim grounded in hardware management expertise. The infrastructure team's diagnosis frames the technology as a networking and endpoint-management problem; its treatment applies existing governance practices (patching, change advisory boards, ITIL service management, ticket queues). If the digital capability is reducible to its hardware components, then infrastructure governance is the appropriate regime.

However, this framing constitutes a category error. The organisational value of emergent digital manufacturing capabilities resides not in hardware but in process application data, control logic, recipe management, quality parameters, and production context. A SCADA server is not a file server; a Historian database is not an ERP database; an edge device running quality analytics is not a network switch. The infrastructure team's claim succeeds at diagnosis (identifying hardware) but fails at inference (understanding what the hardware does within the industrial process). In Abbott's [2] terms, the claim lacks the abstraction necessary to adapt infrastructure knowledge to the emergent digital domain. This reduction is fundamentally at odds with the sociotechnical understanding of manufacturing systems that the APMS community has developed through research on human cyber-physical systems and the Operator 4.0 [13], which emphasises that the value of digital manufacturing technology lies in the cooperation between humans, machines, and software systems, not in hardware alone.

This pattern is not confined to infrastructure teams or to OT. Quality, maintenance, and safety functions each perform diagnostic reductionism in their own register: partial recognition at the diagnostic stage triggers protective jurisdiction where connective jurisdiction is required.

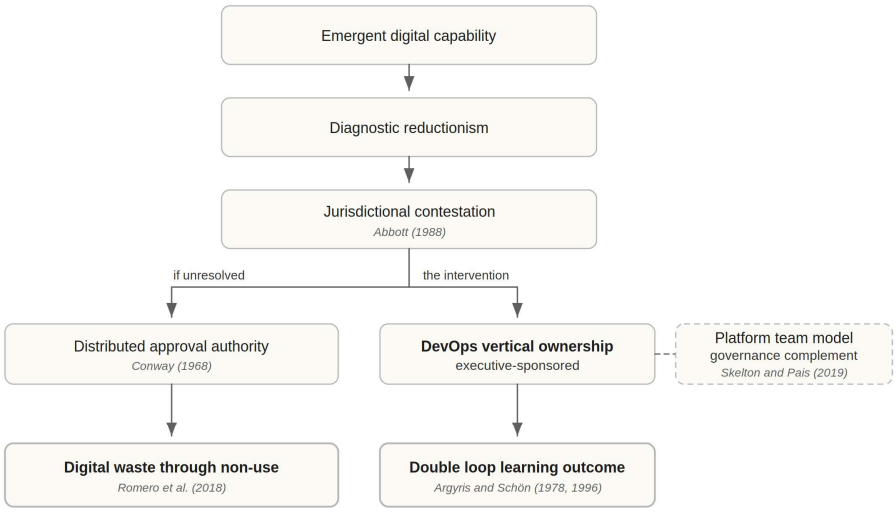

Fig. 1. Jurisdictional contestation and the double loop intervention through DevOps vertical ownership.

3.2 The Rationality of the Claim

The infrastructure team's claim is rational within its governing variables. Infrastructure teams are measured on availability, security posture, compliance, and cost efficiency. Unmanaged digital assets represent genuine risk, particularly given the 87% increase in

ransomware incidents targeting industrial organisations in 2024 [14]. The claim is, in part, a legitimate response to a real governance gap [15].

The problem is not the identification of risk but the assumption that infrastructure governance is the sole response. When emergent digital capabilities are subsumed under infrastructure governance, the industrial process context is subordinated to IT operational stability. In Sako et al.'s [9] terms, building on Abbott's [2] jurisdictional framework, infrastructure teams exercise 'protective' jurisdictional control, incorporating new domains as subordinate to existing governance, rather than 'connective' control, which recognises the need for equal-status collaboration. The same rationality applies to every species of diagnostic reductionism: quality teams imposing calibration governance on vision systems, maintenance teams imposing CMMS workflows on predictive platforms, and safety teams imposing audit regimes on connected worker systems are each acting rationally within their governing variables. The problem in every case is that rational action within one set of governing variables forecloses an outcome that requires a different set of governing variables.

3.3 Bi-modal IT as Institutionalised Handover Failure

A common organisational response to the tension between innovation and operational stability is bi-modal IT: structurally separating a Mode 1 (stability) function from a Mode 2 (agility) function [16]. While this aims to balance exploitation and exploration [17], it institutionalises the handover problem. Mode 2 teams develop capabilities and demonstrate value. When solutions must transition to Mode 1, the model depends on a capability that does not exist reliably anywhere: effective handover between organisationally separate groups [18]. Handover between separated units is inherently lossy; tacit knowledge resists transfer by definition. The receiving team must acquire context that was not present, and this context cannot be captured in documentation.

Three failure modes emerge. First, governance mismatch: Mode 1's operating model (ITIL, change advisory boards, scheduled maintenance) may be structurally incompatible with the requirements of digital manufacturing (continuous availability, safety-critical change management, production-synchronised maintenance). Second, innovation death by friction: each initiative must navigate the same handover and face the same mismatch. Third, shadow operations: when handover fails (as it must), the innovation team does not walk away clean.

This third mode describes how bi-modal IT collapses into uni-modal exploitation. When Mode 1 cannot absorb a solution, Mode 2 accumulates a shadow operations burden: supporting what they built because no one else can. Each cycle adds to this backlog. Innovators progressively become operators of their back-catalogue, capacity for new work shrinks, and eventually they do exactly what Mode 1 does, without the governance, staffing, or mandate. The innovation function cannibalises itself. The 'same person doing all tasks' pathology, widely observed in industrial IT, is a direct symptom: the builder becomes permanent custodian, closed to new ideas not by choice but by accumulated obligation. While Romero et al.'s [3] taxonomy focuses on digital waste through non-use (capabilities that are never activated), the shadow operations burden represents a related but distinct organisational effect: innovation capacity consumed by underfunded operational support rather than applied to new capability devel-

opment. Both are consequences of governance structures that separate innovation from operation.

3.4 Vignette: The Edge Device as Jurisdictional Microcosm

This vignette is drawn from the first author's direct involvement in digital manufacturing transformation at the case firm, an anonymised global producer of bespoke engineered-to-order industrial assets for heavy industries, operating across 160 sites with a distributed IT function and an emerging digital manufacturing capability. It is presented as an illustrative account, not as empirical evidence. At one plant, a machining line producing high-value components experienced intermittent quality issues and avoidable rework. Data relevant to the problem existed, but in fragmented form: PLC states, historian trends, inspection results, spreadsheets, and operator knowledge all contributed to the explanation. The organisation could see that variation was occurring, but could not easily identify the cause or intervene early enough to prevent recurrence.

A cross-functional team proposed adding an industrial edge computing device between OT and IT. The device did much more than serve as a hardware node: it could stream machine telemetry for visibility and analytics, buffer time-series data for root cause analysis, transfer files between network zones, bridge old and new protocols, connect with MES, ERP, CMMS, and quality systems, and run analytics close to the process. For the team, this device was the basis for a data-centric manufacturing system, assembling process context, quality data, and machine signals into an ecosystem of operational intelligence locally and eventually across sites.

Layer 1: The jurisdictional claim. Following formal review, the infrastructure team asserted jurisdiction. They observed a device at a network boundary transferring data and diagnosed it using familiar terms: server hardening, firewall rules, file movement, patching, and change control. In their view, the edge device was merely a tool for file transfer. This was not technically incorrect, but it was incomplete. Abbott's [2] terms apply: the diagnosis recognised hardware, but not the broader manufacturing data ecosystem it enabled. Governance followed this limited view, reducing the platform for digital capability to a single function of moving files.

This narrow framing did not merely exclude 'other tasks': it excluded a new paradigm. A data-driven approach would integrate machine telemetry, process context, quality data, and operator knowledge, supporting streaming dashboards, local root-cause analysis, predictive insights, and closed-loop intervention. This platform could enable benchmarking, pattern recognition, and learning across sites, and improve planning and continuous improvement through real-time operational data. Governance, as Romero et al. [3] note, created digital waste through non-use: technical capabilities were available but organisationally blocked. The broader vision was not rejected, just made unlikely.

Layer 2: Alignment negotiation. Despite constraints, the pilot progressed and demonstrated broader value. Working with plant engineers, operators, and quality staff, the team linked machine states, cycle data, inspection results, and operator input. The device buffered local data for rapid root-cause analysis and translated telemetry into real-time visibility, revealing patterns across tooling, recipes, and inspections. The pilot succeeded because those shaping the solution were also testing it; operators trusted the

outputs, which reflected their experience. The device became not just an analytical tool but a shared object around which process learning occurred.

Layer 3: Decision-point paralysis. Because the device was approved primarily as a file-transfer tool, every additional feature required new negotiation through governance designed for a different model. Adding telemetry, MES integration, maintenance signals, comparisons, and analytics was not forbidden, but each was costly in terms of consultation and approval. Multiple groups (cybersecurity, infrastructure, enterprise architecture, plant engineering, quality, and digital) were involved initially. Over time, consultation became distributed approval authority. Each group expected further development to pass through them. No one blocked progress, but no extension advanced smoothly. As Abbott [2] notes, jurisdictional settlements never fully settled: each party regarded its earlier input as ongoing authority, creating shared but fragmented control where no one owned the outcome.

Layer 4: Conway's Law consequence. This fragmented decision-making process led to a fragmented technical outcome, as Conway's Law [7] predicts. Without a single authority to approve the device as a multi-capability platform, it was approved only for file transfer. The broader ecosystem, operational visibility, cross-site learning, integrated planning, and closed-loop improvement remained unrealised. Ownership of parts became clearer, while ownership of outcomes grew murkier. At handover, technical custody was clear, but contextual understanding was lost. The device functioned, but only for its narrowest purpose. What could have been a learning system became a supported device. This case shows how governance intended to manage digital innovation can create the very fragmentation and waste it aims to prevent.

4 Top-Down DevOps Vertical Ownership as the Solution Mechanism

The vignette shows a failure not of execution but of the governing variable itself. Responses that accept that variable and improve execution within it operate in single loop mode and cannot resolve contestation that is structural in origin; what follows therefore develops a double loop intervention and the conditions under which it is required.

4.1 Single Loop: Correcting Within Existing Governance

Most responses to jurisdictional contestation in emergent digital domains operate in single loop mode. They accept the governing variable that technology domains should be owned by the organisational layer whose existing expertise most closely resembles the technology's physical characteristics, and improve execution within that assumption. Examples include improving communication between teams, creating liaison roles (Skelton and Pais's [6] Anti-Type B), establishing joint working groups, and adding domain-specific runbooks to existing ITIL processes. These interventions may reduce immediate friction but do not address the governing variable itself.

4.2 Double Loop: Questioning the Ownership Model

DevOps, understood not as a toolchain but as an organisational design principle, constitutes a double loop intervention [19]. Its core proposition, 'you build it, you run it',

directly challenges the governing variable of layer-based ownership. The team that designs a digital manufacturing data architecture is also responsible for its operational health. There is no handover because there is no organisational boundary between creation and operation. Infrastructure capabilities are consumed as platform services rather than governed through a separate hierarchy. This changes the governing variable from 'technology is owned by the layer that recognises its hardware' to 'technology is owned by the team accountable for its business outcome'.

4.3 Why Traditional IT Resists the Double Loop

Argyris [20] argued that 'smart people' are often the most resistant to double loop learning because their professional identity is invested in their existing competence. Infrastructure teams have optimised for exploitation: their structures, incentives, and identity are built around operational stability. When emergent digital capabilities arrive, the path of least resistance is to claim jurisdiction and govern with infrastructure processes. Innovation is 'disruptive in the negative sense': it introduces uncertainty that governance is designed to minimise. Digital manufacturing initiatives are not actively blocked but progressively attenuated, dying not from rejection but from the friction of inappropriate governance applied by teams whose incentives reward the elimination of precisely the kind of uncertainty that innovation requires.

4.4 Why Top-Down Authority Is Required

The vignette in Section 3.4 demonstrates why the double loop intervention cannot emerge from consensus. Once multiple stakeholders have been consulted and each interprets their involvement as ongoing decision authority, jurisdiction becomes distributed in a way that will not reconsolidate from the bottom up. No jurisdictional contestant will voluntarily cede their claim, because doing so diminishes their organisational standing. The decision-point paralysis is self-reinforcing: each approval gate is individually reasonable, but the cumulative effect is that nothing progresses.

This connects directly to Argyris's [11] analysis of defensive routines. Defensive routines persist because nobody has the authority or willingness to make the undiscussable discussable. In the context of emergent digital domains, the undiscussable is: 'your team does not own this, even though you recognise the hardware.' That conversation only happens with an executive mandate. A senior leader must declare: this capability belongs to this vertical team, end-to-end, from problem definition through operation and improvement. Infrastructure provides services. Security provides guardrails. Enterprise architecture provides patterns. But the vertical team owns the outcome.

Building vertical teams and adopting a DevOps approach to owning the solution is therefore not merely a preferred organisational design; in large manufacturers with entrenched distributed governance, it is a more reliable mechanism than the available alternatives for breaking through jurisdictional paralysis. Alternative pathways, including coalition building, gradual cultural change, and crisis-triggered reorganisation, are systematically undermined by the defensive routines described in Section 2.2: each requires the very consensus that distributed veto prevents. Top-down DevOps is not a deployment preference; it is the organisational intervention that makes the double loop possible in contexts where distributed approval authority has calcified. Without execu-

tive authority to assign ownership, the emergent digital capability will remain constrained to its narrowest approved function, generating digital waste through non-use [3], even as the organisation believes it is governing responsibly.

5 The Governance Paradox: From Control Gates to Platform Enablement

Even with top-down DevOps, governance remains essential. The question is how it is provided. Most designs propose horizontal governance layers: enterprise architecture, PMO, business analysis, and security/compliance. This section argues that such layers carry a specific risk: they may function as defensive routines [11], structures that appear to enable learning while protecting existing power dynamics.

5.1 Horizontal Governance as a Defensive Routine

If a digital manufacturing innovation team must 'hand over' to core operations via a PMO with standardised '*build, run, change, replace'* lifecycle stages, the PMO becomes a boundary object through which context is lost, and innovation is subjected to steady-state assumptions. The PMO does not eliminate the handover problem; it relocates it to a higher level of abstraction. In Argyris's [11] terms, this constitutes a defensive routine: it protects the organisation from genuinely integrated accountability by imposing a familiar process that appears rigorous yet prevents the double loop shift.

Abbott [2] identifies 'intellectual jurisdiction' as a settlement in which an incumbent profession controls the cognitive knowledge of an area but allows practice by others. Enterprise architecture functions often exercise precisely this jurisdiction: controlling standards, technology selection, and integration patterns while vertical teams execute within constraints. When positioned horizontally above vertical teams, EA may systematically resist the architectural heterogeneity that digital manufacturing requires, for example, legacy OT protocols integrated with cloud analytics, or edge computing that does not conform to standard data centre models. An EA function that gates innovation through approval operates differently from one that embeds patterns into platform services consumed autonomously. The former is a defensive routine; the latter is double loop-consistent governance.

5.2 The Platform Team as Double Loop-Consistent Governance

Skelton and Pais's [6] platform team model resolves this paradox. Rather than positioning governance above vertical teams (gating), the platform team embeds governance into services (enabling) [21]. Standards are enforced through platform design: a self-service deployment pipeline with embedded security scanning achieves compliance through use rather than approval. In the digital manufacturing context, a platform team provides self-service infrastructure (network segmentation templates, secure remote access, edge computing environments, data integration patterns) that vertical teams consume autonomously. This changes the governing variable of governance itself: from 'governance means controlling what teams do' to 'governance means shaping the environment in which teams operate'.

6 From Jurisdictional Contestation to Governable Digital Manufacturing Capability

The preceding analysis shows that emergent digital manufacturing capabilities do not fail only because of technical immaturity, weak business cases, or poor implementation. They also fail because existing governance structures interpret them through familiar organisational categories, thereby restricting their potential use. This discussion draws together the practical and theoretical implications of that argument. It first examines what the analysis means for practitioners attempting to build digital manufacturing capability in environments shaped by distributed authority, functional silos, and inherited IT governance models. It then clarifies how diagnostic reductionism extends jurisdictional theory into intra-organisational technology domains. Finally, it identifies limitations and future research directions, particularly regarding empirical validation, measuring digital waste through non-use, and the cybersecurity implications of vertical ownership.

6.1 Mechanism and Boundary Conditions

The paper's central claim is that diagnostic reductionism produces digital waste through non-use when three conditions coincide. First, an emergent digital manufacturing capability must include artefacts that are recognisable to established functions, such as infrastructure, quality, maintenance, safety, or automation. Second, that function must possess enough formal or informal authority to convert recognition into a jurisdictional claim. Third, the organisation must lack a countervailing ownership model capable of preserving the capability's end-to-end manufacturing purpose. Under these conditions, governance intended to reduce risk can unintentionally reduce capability. The result is not failed adoption in the usual sense, but constrained adoption: the technology is implemented, yet only in its narrowest authorised form.

6.2 Practical Implications

For practitioners navigating emergent digital domains, the analysis suggests that diagnostic reductionism should be treated as a predictable governance response rather than as individual resistance. Established functions claim new digital capabilities because their responsibilities, incentives, and risk models make those claims rational. Changing the outcome therefore requires changing the governing variables, not blaming the actors. Table 1 summarises the practical implications that follow from this argument.

Several implications are especially important. Bi-modal structures should explicitly acknowledge and fund the shadow-operations burden carried by innovation teams when Mode 1 functions cannot absorb new capabilities. Governance structures should also be assessed by whether they enable teams to move faster or require them to wait for approval. Platform-based governance supports movement; gating functions reproduce defensive routines. Vertical teams should be composed transdisciplinarily, combining OT, data engineering, process improvement, lean, and business domain expertise. Measurement systems must support the same ownership logic, assessing vertical teams on operational health, adoption, benefits realisation, and repeatability, and plat-

form teams on service consumption, developer experience, and time-to-capability. Finally, digital waste through non-use should be made visible through the gap between technically available capability and governance-authorised use.

Table 1. Practical implications for emergent digital domains.

Implication	Rationale	Implementation indicator
Expect diagnostic reductionism.	Functions act rationally within their governing variables.	Change the governing variables, not the actors.
Adopt bi-modal structures with shadow-operations awareness.	Mode 2 teams carry operational continuity that Mode 1 cannot absorb.	Operational continuity is acknowledged and funded in the operating model.
Evaluate governance for defensive-routine potential.	Governance can protect power arrangements while appearing to enable change.	Platform model (teams move faster) versus gating model (teams wait for approval).
Compose vertical teams transdisciplinarily.	Multidisciplinary consulting cannot transfer situated knowledge; siloed organisations duplicate solutions (Conway's Law [7] in reverse).	OT, data engineering, process improvement, lean, and domain expertise on one team.
Align measurement with ownership.	Misaligned measurement undermines structural change by rewarding the old model.	Vertical teams on operational health, adoption, benefits, repeatability; platform teams on service consumption, developer experience, time-to-capability.
Make digital waste through non-use visible and measurable.	The gap between technical capability and authorised use is measurable and actionable.	Foreclosed-capability gap: the difference between technically available and governance-authorised capability sets, per asset or per site.

6.3 Theoretical Implications

This paper extends Abbott's [2] jurisdictional theory from its traditional domain (professions in society) to intra-organisational technology domains, demonstrating that emergent digital manufacturing capabilities are subject to the same dynamics of reductive diagnosis, protective jurisdiction, and failed settlement that Abbott describes in inter-professional contestation. The central construct, diagnostic reductionism, names the mechanism by which any established function narrows an emergent digital capability to the single dimension it can diagnose from existing expertise; infrastructural reductionism (hardware reduction) is the most prevalent species, but the mechanism generalises to quality, maintenance, safety, and automation functions. The identification of horizontal governance layers as potential defensive routines [11] extends Argyris's framework to IT governance design. The characterisation of diagnostic reductionism as a source of digital waste through non-use [3] bridges organisational theory and lean manufacturing, offering a consequence framework grounded in the manufacturing systems literature. The proposition that executive-sponsored DevOps vertical ownership offers a more reliable intervention than the available alternatives in contexts of entrenched distributed governance addresses a gap in the existing DevOps literature,

which emphasises cultural transformation but rarely confronts the power dynamics that prevent it.

6.4 Limitations and Further Research

This paper is conceptual and does not present empirical validation. The edge computing vignette reflects the first author's insider position within the case firm and is offered illustratively rather than as validation. Longitudinal case studies tracking the evolution of governance from bi-modal to top-down DevOps to platform team structures would be valuable. Developing and validating an instrument to quantify the foreclosed-capability gap is left to future work. The cybersecurity dimension warrants dedicated investigation: any alternative governance model must demonstrate equivalent or superior security outcomes. The interaction between vertical ownership, platform security services, and industrial control system requirements (safety integrity levels, network segmentation, secure remote access) is a productive area for further research. Finally, the paper assumes a primarily Western industrial context; the dynamics may differ in organisational cultures with different power distance or uncertainty avoidance orientations.

7 Conclusion

Digital manufacturing transformation is fundamentally a sociotechnical challenge, one in which persistent socio-cultural barriers, including siloed communication and resistance to change, constrain progress as powerfully as any technology gap [22]. The organisational structures within which emergent digital capabilities are pursued shape outcomes as powerfully as the technologies themselves. This paper has argued that diagnostic reductionism, the narrowing of emergent digital capabilities to the single dimension that an established function can diagnose, is a predictable consequence of structures optimised for exploitation, and that bi-modal IT institutionalises handover points that systematically degrade digital manufacturing initiatives through governance mismatch, shadow operations burden, and the progressive accumulation of digital waste through non-use [3].

In large manufacturers where distributed approval authority has calcified into jurisdictional paralysis, executive-sponsored DevOps vertical ownership offers a more reliable mechanism for breaking through than the alternatives considered here. This proposition is contingent, not universal: it applies most strongly where emergent digital domains present recognisable infrastructure artefacts, where multiple governance functions have acquired implicit approval authority, and where alternative change mechanisms (coalition building, gradual cultural shift) are systematically undermined by the defensive routines that distributed governance produces. The platform team model provides the governance complement: embedding standards in self-service infrastructure rather than approval processes, preserving security, architectural coherence, and compliance while removing the gating functions that generate waste.

The broader implication is that digital manufacturing transformation is constrained not primarily by technology but by organisational structures, jurisdictional claims, and learning systems that reproduce existing power arrangements. Overcoming these con-

straints requires genuine double loop learning: the willingness to question whether organisational models inherited from a previous era of IT governance remain appropriate for the emerging era of digital manufacturing. The cost of not doing so is measurable: it is digital waste, and it accumulates with every emergent capability that is reduced to its narrowest approved function.

Disclosure of Interests. The lead author's practitioner experience at an industrial firm informs this study. The authors have no other competing interests to declare that are relevant to the content of this article.

8 References

1. Anderson, M., West, S., Harrison, D.: Exploring accidental digital servitization in an industrial context. In: Dolgui, A., Bernard, A., Lemoine, D., von Cieminski, G., Romero, D. (eds.) APMS 2021. IFIP AICT, vol. 632, pp. 126–135. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-85906-0_15
2. Abbott, A.: The System of Professions: An Essay on the Division of Expert Labor. University of Chicago Press, Chicago (1988). https://doi.org/10.7208/chicago/9780226189666.001.0001
3. Romero, D., Gaiardelli, P., Powell, D., Wuest, T., Thürer, M.: Digital lean cyber-physical production systems: the emergence of digital lean manufacturing and the significance of digital waste. In: Moon, I., Lee, G.M., Park, J., Kiritsis, D., von Cieminski, G. (eds.) APMS 2018. IFIP AICT, vol. 535, pp. 11–20. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99704-9_2
4. Argyris, C., Schön, D.: Organizational Learning: A Theory of Action Perspective. Addison-Wesley, Reading (1978)
5. Argyris, C., Schön, D.: Organizational Learning II: Theory, Method, and Practice. Addison-Wesley, Reading (1996)
6. Skelton, M., Pais, M.: Team Topologies: Organizing Business and Technology Teams for Fast Flow. IT Revolution Press, Portland (2019)
7. Conway, M.E.: How do committees invent? Datamation 14(4), 28–31 (1968)
8. Furness, C.: The system of professions. Education for Information 35(3), 353–356 (2019). https://doi.org/10.3233/EFI-190271
9. Sako, M., Qian, M., Attolini, J.: Future of professional work: evidence from legal jobs in Britain and the United States. Journal of Professions and Organization 9(2), 143–169 (2022). https://doi.org/10.1093/jpo/joac011
10. Hantsch, C., Westner, M., Matschi, M.: IT/OT-Konvergenz: Status-Quo und Umsetzungsempfehlungen. HMD Praxis der Wirtschaftsinformatik 62(2), 402–418 (2025). https://doi.org/10.1365/s40702-024-01111-1
11. Argyris, C.: Overcoming Organizational Defenses: Facilitating Organizational Learning. Allyn and Bacon, Boston (1990)
12. Argyris, C.: Strategy, Change and Defensive Routines. Pitman, Boston (1985)
13. Romero, D., Bernus, P., Noran, O., Stahre, J., Fast-Berglund, Å.: The operator 4.0: human cyber-physical systems and adaptive automation towards human-automation symbiosis

work systems. In: Nääs, I., et al. (eds.) APMS 2016. IFIP AICT, vol. 488, pp. 677–686. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-51133-7_80

14. Dragos: 2025 OT Cybersecurity Year in Review. Dragos, Inc. (2025)
15. Abbatemarco, N., Brechbühl, H.: Identifying and filling gaps in operational technology cybersecurity. MIS Q. Exec. 23(4), Article 6 (2024). https://doi.org/10.17705/2msqe.00105
16. Tushman, M.L., O'Reilly, C.A.: Ambidextrous organizations: managing evolutionary and revolutionary change. California Management Review 38(4), 8–30 (1996). https://doi.org/10.2307/41165852
17. Kusanke, K., Winkler, T.J.: Structural ambidexterity through bimodal IT: a literature review and research agenda. In: Proceedings of the 17th International Conference on Wirtschaftsinformatik (2022)
18. Toutaoui, J., Benlian, A., Hess, T.: Managing paradoxes in bi-modal information technology functions: a multi-case study. Information Systems Journal 32(6), 1177–1202 (2022). https://doi.org/10.1111/isj.12396
19. Blüher, T., Maelzer, D., Harrendorf, J., Stark, R.: DevOps for manufacturing systems: speeding up software development. Proc. Des. Soc. 3, 1475–1484 (2023). https://doi.org/10.1017/pds.2023.148
20. Argyris, C.: Teaching smart people how to learn. Harvard Business Review 69(3), 99–109 (1991)
21. Pauli, T., Marx, E., Fielt, E., Marheine, C., Matzner, M.: Inhibitors and enablers of leverage in digital industrial platform ecosystems. Bus. Inf. Syst. Eng. 67(5), 711–731 (2025). https://doi.org/10.1007/s12599-024-00896-1
22. Anderson, M., Dober, P., West, S., Gaiardelli, P.: Human-centric smart factory transformation: a roadmap integrating lean, digitalization, and organizational learning. In: Mizuyama, H., et al. (eds.) APMS 2025. IFIP AICT, vol. 767, pp. 518–531. Springer, Cham (2026). https://doi.org/10.1007/978-3-032-03542-4_36