From Traditional Supply Chains to Smart Networks Exploring the Impact of Industry 4.0 Transformation

Mohammad Salman
Research Scholar, Ph.D. in Management, Shubham University, Bhopal.

Prof. S.D Sharma
Research Supervisor, Department of Management, Shubham University, Bhopal.

ABSTRACT

Industry 4.0 is changing supply chains from sequential, firm-centred pipelines into data-rich networks capable of sensing, reasoning, coordinating and learning. Yet technology acquisition alone does not create a smart network. This paper develops an integrative conceptual framework explaining how connected sensing, interoperable data, analytics and digital twins become operational and strategic capability through governance, partner alignment and human competence. Drawing on the supply chain, operations, information systems and resilience literature, the paper distinguishes four maturity stages: visibility, integration, prediction and bounded autonomy. It argues that performance effects are mediated by decision latency, cross-enterprise orchestration and the quality of data semantics; they are moderated by cybersecurity, data rights, absorptive capacity and power asymmetry. The resulting smart network framework reconnects Industry 4.0 research with supply-chain theory and offers testable propositions, a measurement architecture and a staged implementation roadmap. The contribution is deliberately conceptual rather than empirical: the proposed relationships should be evaluated through longitudinal, multi-tier and event-based research designs. The analysis concludes that the central transformation is not digitisation of isolated tasks but the creation of a governed, adaptive network in which physical flows and digital representations continuously inform one another.

Keywords: *Industry 4.0; Smart Supply Networks; Digital Twins; Supply Chain Resilience; Artificial Intelligence; Interoperability; Sustainability.*

1. Introduction

For much of the twentieth century, supply chain management was organized around planned handoffs: forecast demand, schedule production, procure materials, move inventory and reconcile exceptions after they occurred. Information technology improved the speed of these handoffs, but it did not necessarily alter their underlying logic. The emerging Industry 4.0 configuration is different. Internet-connected assets, cyber-physical systems, cloud platforms, artificial intelligence (AI), advanced analytics, blockchain-enabled traceability and digital twins can render events visible while they are unfolding and can connect sensing to decision and execution (Lasi et al., 2014; Lee et al., 2015; Zhong et al., 2017). The practical promise is compelling: lower decision latency, earlier disruption detection, more precise allocation of scarce capacity and transparent environmental and social accountability.

However, the language of "smart supply chains" often conflates a technology list with a network capability. A warehouse may use robots while suppliers still exchange delayed spreadsheets; a digital twin may simulate one plant but not capture supplier capacity, transport constraints or customer commitments. Such local optimisation can increase rather than reduce network fragility. Reviews consistently identify data quality, interoperability, skills, investment uncertainty and cyber risk as material obstacles to Industry 4.0 adoption (Büyüközkan & Göçer, 2018; Kamble et al., 2018; Rad et al., 2022). The scholarly challenge is therefore explanatory: through which mechanisms do digital technologies transform a chain of transactions into a smart, adaptive network?

This paper addresses that question through a structured conceptual synthesis. It has three objectives: first, to distinguish traditional supply chains from smart networks; second, to propose a multi-layer framework linking technologies, organisational enablers and outcomes; and third, to present propositions and a research agenda suitable for rigorous empirical assessment. Rather than claiming a universal positive effect of digitalisation, the paper treats Industry 4.0 as a contingent socio-technical transformation. This framing is essential because benefits arise only when technological signals are trusted, shareable, interpretable and actionable across organisational boundaries.

2. From Linear Chains to Smart Networks

Traditional supply chains are not literally linear; they contain multiple suppliers, facilities, carriers and markets. "Linear" here describes the dominant managerial architecture: information is fragmented, planning cycles are periodic, and coordination is predominantly bilateral. Visibility is retrospective, forecasts aggregate uncertainty, and managers intervene after thresholds are breached. Enterprise resource planning and electronic data interchange reduced transaction costs, but their emphasis remained recordkeeping and planned integration. By contrast, a smart network combines continuous event capture with shared data models, predictive and prescriptive analytics, and digitally supported execution. It is a network because value depends on reciprocal information and material dependencies among actors rather than on the digitisation of one focal firm.

The distinction has theoretical consequences. Resource-based arguments suggest that technology itself is imitable, whereas the ability to integrate, reconfigure and govern complementary resources can become a dynamic capability (Teece, 2007; Warner & Wäger, 2019). Information processing theory similarly predicts that the richer and more uncertain the environment, the greater the need for information-processing capacity. Industry 4.0 expands that capacity, but also increases coordination demands because decision rights, data ownership and algorithmic accountability must be agreed across firms. Supply-chain digital transformation should therefore be understood as the co-evolution of technical architecture, relational governance and operating routines (Vial, 2019; Frederico et al., 2020).

Table 1. Conceptual Contrast Between Traditional Supply Chains and Smart Networks

Dimension	Traditional Supply Chain	Smart Network
Information	Periodic, siloed and largely retrospective	Event-driven, contextual and selectively shared
Planning	Forecast and schedule centred	Sense, simulate, decide and replan continuously
Control	Functional and firm-specific	End-to-end orchestration with local autonomy
Risk response	Detect after disruption and expedite	Predict exposure, test scenarios and contain impacts
Value logic	Efficiency and unit-cost optimisation	Efficiency, resilience, service and sustainability jointly
Human role	Manual reconciliation and escalation	Exception design, model oversight and partner governance

Source: Developed by the Author from The Reviewed Literature

3. Industry 4.0 Technologies and Transformation Mechanisms

The first mechanism is sensing. Internet of Things devices, RFID, machine telemetry, geolocation, computer vision and mobile interfaces convert physical states into digital events. At their best, these technologies expose location, condition, capacity utilisation, energy use and quality status at a useful temporal granularity. The value is not the volume of data but its fitness for a decision: accurate time stamps, common identifiers and event provenance. Cyber-physical systems make this connection bidirectional by allowing analytical insights to influence equipment and process settings (Monostori, 2014; Xu et al., 2014).

The second mechanism is integration. Cloud and edge architectures allow distributed data to be made discoverable and processed close to operations when latency matters. Integration is not equivalent to centralisation. A network can retain local control and protect sensitive information while sharing governed events, commitments and exceptions. Interoperability requires common semantics for products, orders, assets, locations and emissions; otherwise, the same "inventory" signal can mean incompatible things to different partners. Studies of big data in supply chains show that analytical value depends heavily on data governance and organisational capability, not simply data availability (Kache & Seuring, 2017; Brinch, 2018).

The third mechanism is intelligence. Machine-learning models detect patterns in demand, quality, maintenance and risk; optimisation models prescribe allocations, routes, schedules and inventories. AI should not be treated as a substitute for managerial judgment. Training data can encode past bias, models can fail under structural breaks, and automated recommendations can shift risk toward less powerful suppliers. Effective use therefore requires human-in-the-loop controls, model monitoring, explanations appropriate to the decision and escalation paths. In this sense, the important outcome is augmented coordination rather than automation for its own sake (Baryannis et al., 2019; Toorajipour et al., 2021).

The fourth mechanism is simulation. A digital twin is a dynamic digital representation connected to a physical entity or process and used to monitor, analyse or predict its behaviour. At supply-chain level, a twin should represent material, information and decision dependencies across nodes, not merely a 3D model of a factory. It enables managers to test demand shocks, supplier outages, transport failures and carbon constraints before committing actions. Its credibility, however, depends on validated assumptions, refresh frequency and traceable data lineage. A polished dashboard without these properties is a digital shadow, not a decision-grade twin (Kritzinger et al., 2018; van der Valk et al., 2022; Wang et al., 2022).

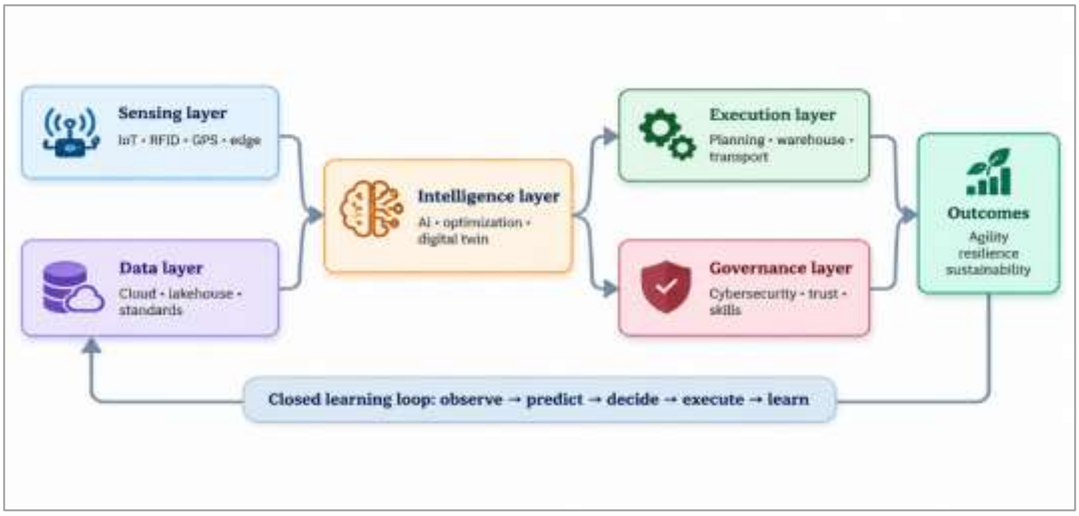

Figure 1. Smart Network Transformation Framework

Source: Developed By the Author

4. An Integrative Smart Network Framework

Figure 1 proposes five connected layers. The sensing layer creates trustworthy representations of physical events. The data layer standardises, protects and makes those representations available through fit-for-purpose architecture. The intelligence layer turns observations into forecasts, risk signals, optimisation choices and simulations. The execution layer embeds these choices in planning, procurement, production, warehousing and transport routines. Governance, shown as a parallel layer, establishes data rights, cybersecurity, partner incentives, ethical controls and skills. The framework is intentionally circular: execution generates new observations, allowing models and rules to learn from outcomes.

Three mediating capabilities link these layers to performance. First, decision latency is the time between a material event and a coordinated response. Shorter latency is valuable only when the response is accurate and authorised. Second, orchestration capability is the ability to reconcile local objectives with network-level service, resilience and sustainability objectives. Third, learning capability converts exception histories into changed policies, models and process designs. These capabilities explain why equivalent investments can yield different outcomes. A firm with excellent sensors but poor exception ownership may simply observe problems earlier; a network with shared decision protocols can act earlier and prevent propagation.

The framework also incorporates boundary conditions. Data-sharing benefits decline when partners cannot trust data use, when contractual power is asymmetric or when participation costs are unequally distributed. Cybersecurity is not a residual technical issue because greater connectivity expands attack surfaces and operational dependencies. Finally, sustainability should be measured rather than assumed. Route optimisation may lower fuel use but increase delivery frequency; real-time inventory visibility may reduce waste but raise energy demand from digital infrastructure. Smart networks are sustainable only where design objectives explicitly include environmental and social constraints (Saberi et al., 2019; Ghobakhloo, 2020).

5. Propositions for Empirical Research

The framework supports a set of propositions that can be tested using multi-respondent, multi-tier and longitudinal data. P1: The effect of Industry 4.0 technology deployment on supply-chain performance is mediated by data interoperability and decision latency. P2: Cross-enterprise data governance positively moderates the relationship between interoperability and network resilience. P3: Digital-twin capability improves disruption response only when twin models incorporate partner capacity, logistics constraints and validated data lineage. P4: AI-enabled decision support improves operational performance when model transparency and human override mechanisms are high; the relationship weakens under severe distributional shifts. P5: The positive effect of smart-network maturity on sustainability performance is stronger when carbon, waste and labour indicators are embedded in planning objectives. P6: The relationship between digital investment and performance is inverted U-shaped when connectivity outpaces cybersecurity, change capacity and partner readiness.

These propositions move beyond simple adoption-performance correlations. A survey can measure adoption, but it cannot adequately establish whether a smart network changed response quality during a disruption. Stronger designs combine archival event data, system logs, partner surveys and post-event analysis. Difference-in-differences designs can compare facilities or supplier tiers before and after staged deployment. Configuration methods can identify alternative paths, such as high data governance plus moderate automation versus high automation plus strong central orchestration. Such designs will also help separate the effect of digital tools from concurrent lean, resilience and procurement initiatives.

6. Maturity Pathway and Managerial Implications

Transformation should not begin with an enterprise-wide technology catalogue. It should begin with a defined network decision that is currently slow, unreliable or high-risk: for example, allocating constrained components, detecting cold-chain excursions or responding to a port closure. The maturity pathway in Figure 2 provides a practical sequencing logic. Visibility creates reliable event capture and a common operational picture. Integration connects those events to planning and partner systems. Prediction uses historical and real-time signals to anticipate risk and demand. Bounded autonomy automates only decisions with explicit objectives, confidence thresholds and human override. Each stage should earn the right to progress by demonstrating data quality, adoption and decision value.

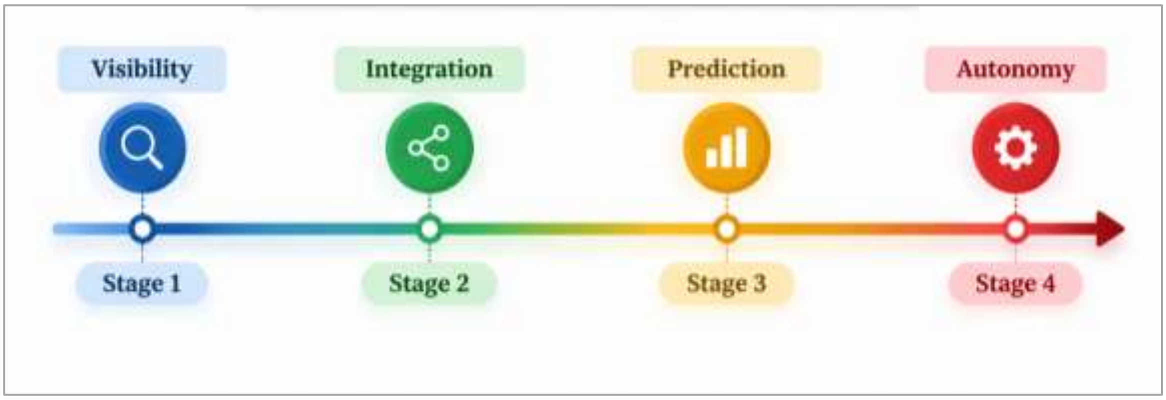

Figure 2. Smart Network Maturity Pathway

Source: Developed by the Author

Table 2. Staged Implementation Architecture and Non-Financial Leading Indicators

Stage	Primary Capability	Evidence of Readiness	Illustrative KPI
1 Visibility	Trusted event capture	Common IDs; completeness and timeliness measured	Event completeness; traceability lead time
2 Integration	Cross-functional and partner data flow	Data contracts; exception ownership; access controls	Decision latency; forecast data latency
3 Prediction	Risk and scenario intelligence	Back-testing; monitored models; documented assumptions	Alert precision; recovery-time forecast error
4 Bounded autonomy	Controlled execution of routine decisions	Confidence thresholds; audit trail; override and rollback	Touchless-resolution rate; service recovery time

Source: Developed by the Author

Managers should govern a portfolio of use cases, each with a clear baseline, owner, data contract and outcome hypothesis. A "control tower" should not become another reporting layer; it should have decision rights and links to execution. Contracting should specify data purpose, retention, quality accountability, intellectual-property boundaries and incident response. Workforce investment is equally central. Planners need not become data scientists, but they must understand model limitations, confidence levels and how to challenge outputs. Suppliers, particularly smaller firms, may need shared standards, onboarding support and cost-sharing to prevent a digital divide. These practices translate technology adoption into relational capability and protect the legitimacy of the transformation.

7. Resilience, Sustainability and Risk

Resilience is often described as the ability to resist, recover and adapt. Industry 4.0 can support all three phases: visibility may reveal emerging exposure, simulation may prepare contingencies, and digital coordination may speed recovery. Nevertheless, digital dependency creates new single points of failure, such as a compromised cloud service, faulty master data or an opaque optimisation engine. The appropriate objective is not maximal automation but graceful degradation: processes should be able to operate safely when connections, data feeds or models are unavailable. Cyber resilience, backup modes and tested manual fallbacks must be designed into the operating model (Ivanov & Dolgui, 2020; Spieske & Birkel, 2021).

Sustainability can become a first-class decision variable in smart networks. Product passports, sensor-enabled condition monitoring and traceable chain-of-custody records can support circular flows, food safety and responsible sourcing. Yet blockchain or other distributed ledgers should be adopted only where their assurance value exceeds their governance and energy cost. Similarly, AI can reduce waste through better matching of supply and demand, but it can also optimise away buffers that protect workers and communities during volatility. Managers should report a balanced set of service, resilience, carbon, material-waste, data-security and supplier-inclusion outcomes. This broader measurement prevents a narrow efficiency narrative from masking transferred risk.

8. Research Agenda

Four research priorities follow. First, researchers should develop validated measures for smart-network capability that distinguish installed technology from interoperable, governed and routinely used capability. Second, studies should investigate data rights and power asymmetry in multi-tier ecosystems, particularly where focal firms impose standards on small suppliers. Third, more evidence is needed on algorithmic governance: which explanation, override and accountability arrangements produce calibrated reliance rather than blind acceptance or avoidance? Fourth, digital-twin research should test predictive validity under rare disruptions rather than evaluating only attractive visualisation or normal-condition optimisation.

Methodologically, the field needs research that joins technical and organisational levels of analysis. Event logs can capture latency and response; surveys can measure trust and absorptive capacity; interviews can explain how decision rights are negotiated. Cross-country work is also necessary because regulation, digital infrastructure and labour institutions shape adoption. Finally, 2025 and 2026 research should examine generative AI carefully. Large language models may lower the cost of retrieving documents, translating supplier communications and summarising exceptions, but they should not be positioned as authoritative operational decision-makers without grounding, access controls, testing and auditability. Their contribution is likely to be strongest as an interface to governed network knowledge rather than as a replacement for validated optimisation or domain expertise.

9. Measurement and Evaluation Architecture

A rigorous evaluation architecture is necessary because investment proposals often present a single, attractive performance number while overlooking spillovers and implementation cost. The unit of analysis should be the decision episode, such as a stock-out risk, quality excursion, capacity shortfall or transport disruption. For each episode, organisations can record the moment at which a signal became available, the time at which it was interpreted, the decision made, the execution time and the realised outcome. This produces a traceable chain from digital capability to operating result. It also avoids the mistaken inference that a new dashboard created value merely because it was used during a period in which market conditions improved.

Metrics should be organised across four domains. Operational metrics include order-cycle time, perfect-order rate, inventory record accuracy, schedule adherence, fill rate and total landed cost. Resilience metrics include time to detect, time to decide, time to recover, exposure coverage, alternative-source feasibility and the magnitude of service loss under a defined scenario. Sustainability metrics include product-level greenhouse-gas intensity, energy per unit, waste, returns, reuse and supplier participation. Finally, digital-governance metrics include data completeness, semantic conformance, model drift, access-control exceptions, cyber incidents and the proportion of automated decisions that are successfully overridden when required. A balanced scorecard makes trade-offs visible; it prevents an apparent efficiency gain from being achieved by transferring inventory, labour burden or cyber risk to another partner.

Causal attribution deserves special attention. Before deployment, teams should specify the decision hypothesis, baseline period, expected mechanism and plausible confounders. For example, an AI demand-sensing pilot may claim to reduce emergency freight by improving forecast responsiveness. Its evaluation should therefore compare error and response time against a matched baseline, control for promotions and supply constraints, and report both accuracy and economic consequences. Simulated benefits should remain labelled as simulations; they should not be reported as realised savings. Digital twin projects require a separate validation protocol that compares simulated states and predicted outcomes with observed events, reports model error, and documents the range of conditions for which the model is credible.

Network-level evaluation further requires a distributional lens. A focal buyer may shorten its own lead time by requiring suppliers to update portals more frequently, but the burden of data entry or system integration may fall disproportionately on smaller firms. Therefore, measures should be disaggregated by tier, geography and firm size where feasible. Researchers should ask whose visibility has improved, whose decisions have become more constrained and which actors can contest a recommendation. These questions are not peripheral ethics issues; they determine the quality and durability of collaboration. A smart network that creates information rents for one actor while reducing the adaptive capacity of others is unlikely to remain resilient over time.

10. Implementation Governance and Design Principles

The implementation sequence should be governed as an operating-model change, not as a stand-alone IT programme. A senior business owner needs accountability for the network decision, whereas technology leaders own architecture, integration and security. Legal, procurement, finance, operations and sustainability teams should jointly define data purpose and success measures. This cross-functional design avoids a common failure mode: deploying a technically elegant platform that has no authority to change purchase orders, production priorities or transportation bookings. Clear decision rights are especially important during disruptions, when rapid action can otherwise conflict with contractual obligations or local performance targets.

Data governance should specify five practical elements. First, a data contract defines events, identifiers, quality rules, refresh frequency and permitted uses. Second, a rights model defines who can view, correct, aggregate, export and retain data. Third, provenance records how data were generated or transformed, including model version and source system. Fourth, a stewardship process assigns responsibility for resolving master-data and semantic conflicts. Fifth, an incident protocol defines how partners communicate a suspected cyber breach, a corrupted feed or a material modelling error. These elements may seem administrative, but they enable the trust that makes inter-firm automation feasible.

Architecture choices should reflect decision criticality. High-frequency machine safety or cold-chain control may require edge processing because an external connection cannot be assumed. Long-horizon network design may benefit from cloud-scale modelling. Application programming interfaces and event-driven integration are usually preferable to brittle point-to-point interfaces, but standardisation must be proportionate to the use case. A small supplier should not be excluded because it cannot afford a sophisticated platform; lightweight interfaces, shared hubs and phased onboarding can preserve participation. The relevant criterion is not technological sophistication but whether the architecture delivers trustworthy, timely and economically feasible coordination.

Organisational learning is the final design principle. Each exception should leave an auditable learning trace: what signal was available, what decision rule was applied, what human judgment changed, what happened and what must be revised. This trace supports model retraining, process improvement and accountability. It also protects against automation bias by making it legitimate for users to challenge a recommendation. Periodic "decision reviews" can examine false alerts, missed disruptions, unintended supplier effects and model drift. In mature smart networks, learning is not a post-project retrospective; it is part of daily operations.

11. Discussion

The central contribution of this paper is to recast Industry 4.0 as network transformation rather than technology adoption. This reframing brings together three literature streams that are too often treated separately: digital technologies create the ability to sense and analyse; supply-chain management explains interdependence and flow coordination; and dynamic capability theory explains how organisations reconfigure routines under change. A smart network exists only when these streams are connected. Sensors without common data semantics create isolated visibility. Analytics without decision rights create advisory outputs. Automation without governance creates unmanaged operational and ethical exposure.

The framework also qualifies the assumption that more data always improves supply-chain decisions. More data can raise noise, increase surveillance concerns and lead managers to focus on what is measurable rather than what is material. Smartness is therefore selective. It requires purposeful data collection, calibrated algorithms and explicit trade-offs. In a volatile setting, a simple but trusted alert that reaches an authorised planner may be more valuable than a complex model that cannot be interpreted or integrated with operations. This insight has implications for emerging economies and small and medium enterprises, where scalable adoption can be based on interoperable basics rather than on costly, all-at-once automation.

A final implication concerns the future relationship between resilience and efficiency. Traditional optimisation frequently treats inventory, capacity and supplier redundancy as costs to be minimised. Smart-network capability can improve the information available for such choices, but it does not eliminate the underlying strategic decision about where to place buffers. A resilient network uses data and simulation to hold the right buffer, at the right place and for the right risk, while preserving the ability to adapt. The aim is not a frictionless chain; it is a transparent, governable and recoverable network.

The framework has limitations that should discipline its use. It is a conceptual synthesis and does not estimate effect sizes, establish causality or imply that every technology is appropriate for every sector. Industries differ in product complexity, regulation, asset intensity, data availability and partner concentration. The framework also uses "network" as an analytical ideal; real supply chains retain contractual boundaries, competitive interests and uneven bargaining power. These limitations are productive because they point to boundary-condition research rather than to universal prescriptions. Future empirical work should identify the minimum viable combinations of sensing, integration, governance and human competence for specific decisions and contexts.

For policy makers and industry associations, the implication is to complement investment incentives with shared infrastructure and assurance mechanisms. Open yet secure data standards, supplier capability programmes, trustworthy digital identity, cyber-response exercises and guidance on carbon-data interoperability can lower collective adoption barriers. Public policy should not equate digitalisation with deregulation or surveillance. The durability of smart networks depends on confidence that operational data are used for legitimate, transparent and proportionate purposes. Such institutional foundations are especially important where supply networks span jurisdictions with different privacy rules, digital readiness and enforcement capacity.

This perspective also changes how executives should sponsor transformation. The most persuasive business case is not a speculative promise of a fully autonomous supply chain. It is a portfolio of measurable decisions in which better sensing, interpretation and coordination have identifiable consequences. A pilot should be designed to scale only when its information definitions, cyber controls, training materials and partner agreements can travel with it. Conversely, a use case should be stopped when its signal quality, economic value or governance legitimacy cannot be demonstrated. This discipline prevents technology theatre and concentrates scarce change capacity on decisions that improve the network.

12. Conclusion

Industry 4.0 can transform supply chains into smart networks, but the transformation is neither automatic nor primarily technological. The decisive shift is the establishment of a closed, governed learning loop between physical events, shared data, analytical judgment and execution. The smart network framework explains this shift through five layers and three mediating capabilities, while recognising cybersecurity, power asymmetry, data rights and sustainability as boundary conditions. Its practical implication is clear: build from high-value decisions, demonstrate trustworthy visibility, integrate partners through data governance, and automate only within explicit safeguards. Its scholarly implication is equally clear: future research should test capability mechanisms and outcomes over time rather than infer transformation from technology adoption alone. In this way, the field can move from celebratory narratives of digitalisation to defensible knowledge about how networks become genuinely smart.

References

1. Abdirad, M., & Krishnan, K. (2021). Industry 4.0 in logistics and supply chain management: A systematic literature review. IISE Transactions, 53(12), 1343-1359. https://doi.org/10.1080/10429247.2020.1783935
2. Baryannis, G., Dani, S., & Antoniou, G. (2019). Predictive analytics and artificial intelligence in supply chain management. Computers & Industrial Engineering, 137, 106024. https://doi.org/10.1016/j.cie.2019.106024
3. Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: A literature review. International Journal of Production Research, 57(15-16), 4719-4742. https://doi.org/10.1080/00207543.2017.1402140
4. Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy. MIS Quarterly, 37(2), 471-482. https://doi.org/10.25300/MISQ/2013/37:2.3
5. Brinch, M. (2018). Understanding the value of big data in supply chain management. International Journal of Production Economics, 195, 234-249. https://doi.org/10.1016/j.ijpe.2017.10.007

6. Büyüközkan, G., & Göçer, F. (2018). Digital supply chain: Literature review and a proposed framework for future research. Computers in Industry, 97, 157-177. https://doi.org/10.1016/j.compind.2018.02.010
7. Choi, T.-M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. Production and Operations Management, 27(10), 1868-1883. https://doi.org/10.1111/poms.12838
8. Dolgui, A., Ivanov, D., & Sokolov, B. (2020). Reconfigurable supply chain: The X-network. International Journal of Production Research, 58(13), 4138-4163. https://doi.org/10.1080/00207543.2020.1774673
9. Fatorachian, H., & Kazemi, H. (2018). A critical investigation of Industry 4.0 in manufacturing. International Journal of Production Economics, 204, 107-117. https://doi.org/10.1016/j.ijpe.2018.02.012
10. Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. International Journal of Production Economics, 210, 15-26. https://doi.org/10.1016/j.ijpe.2019.01.004
11. Frederico, G. F., Garza-Reyes, J. A., Anosike, A., & Kumar, V. (2020). Supply Chain 4.0: Concepts, maturity and research agenda. Supply Chain Management, 25(2), 262-282. https://doi.org/10.1108/SCM-09-2018-0339
12. Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for sustainability. Journal of Cleaner Production, 252, 119869. https://doi.org/10.1016/j.jclepro.2019.119869
13. Gunasekaran, A., Papadopoulos, T., Dubey, R., Fosso Wamba, S., Childe, S. J., Hazen, B., & Akter, S. (2017). Big data and predictive analytics for supply chain and organizational performance. Journal of Business Research, 70, 308-317. https://doi.org/10.1016/j.jbusres.2016.08.004
14. Hofmann, E., & Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. Computers in Industry, 89, 23-34. https://doi.org/10.1016/j.compind.2017.04.002
15. Ivanov, D. (2020). Predicting the impacts of epidemic outbreaks on global supply chains. Transportation Research Part E, 136, 101922. https://doi.org/10.1016/j.tre.2020.101922
16. Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks. International Journal of Production Research, 58(10), 2904-2915. https://doi.org/10.1080/00207543.2020.1750727
17. Kache, F., & Seuring, S. (2017). Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management. International Journal of Operations & Production Management, 37(1), 10-36. https://doi.org/10.1108/IJOPM-02-2015-0078
18. Kamble, S. S., Gunasekaran, A., & Sharma, R. (2018). Analysis of the driving and dependence power of barriers to adopt Industry 4.0. Computers in Industry, 101, 107-119. https://doi.org/10.1016/j.compind.2018.06.004
19. Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital twin in manufacturing: A categorical literature review. IFAC-PapersOnLine, 51(11), 1016-1022. https://doi.org/10.1016/j.ifacol.2018.08.474
20. Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. Business & Information Systems Engineering, 6, 239-242. https://doi.org/10.1007/s12599-014-0334-4
21. Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23. https://doi.org/10.1016/j.mfglet.2014.12.001

22. Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005
23. Mithas, S., Tafti, A., & Mitchell, W. (2013). How a firm's competitive environment and digital strategic posture influence digital business strategy. MIS Quarterly, 37(2), 511-536. https://doi.org/10.25300/MISQ/2013/37.2.07
24. Monostori, L. (2014). Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia CIRP, 17, 9-13. https://doi.org/10.1016/j.procir.2014.03.115
25. Negri, E., Fumagalli, L., & Macchi, M. (2017). A review of the roles of digital twin in CPS-based production systems. Procedia Manufacturing, 11, 939-948. https://doi.org/10.1016/j.promfg.2017.07.198
26. Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain. International Journal of Information Management, 48, 70-78. https://doi.org/10.1016/j.ijinfomgt.2019.02.004
27. Rad, F. F., Oghazi, P., & Palmié, M. (2022). Industry 4.0 and supply chain performance: A systematic literature review. Industrial Marketing Management, 105, 268-293. https://doi.org/10.1016/j.indmarman.2022.06.009
28. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261
29. Spieske, A., & Birkel, H. (2021). Improving supply chain resilience through Industry 4.0. International Journal of Physical Distribution & Logistics Management, 51(8), 821-847. https://doi.org/10.1108/IJPDLM-12-2019-0348
30. Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. Journal of Manufacturing Systems, 48, 157-169. https://doi.org/10.1016/j.jmsy.2018.01.006
31. Teece, D. J. (2007). Explicating dynamic capabilities. Strategic Management Journal, 28(13), 1319-1350. https://doi.org/10.1002/smj.640
32. Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management. Journal of Business Research, 122, 502-517. https://doi.org/10.1016/j.jbusres.2020.09.009
33. Tortorella, G. L., & Fettermann, D. (2018). Implementation of Industry 4.0 and lean production in Brazilian manufacturing companies. International Journal of Production Research, 56(8), 2975-2987. https://doi.org/10.1080/00207543.2017.1391420
34. van der Valk, H., Haße, H., Möller, F., Arbter, R., Henning, J. L., & Otto, B. (2022). Supply chains in the era of digital twins: A review. Computers in Industry, 142, 103755. https://doi.org/10.1016/j.compind.2022.103755
35. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003
36. Wamba, S. F., Queiroz, M. M., Trinchera, L., & Wright, R. (2020). Dynamics between blockchain adoption determinants and supply chain performance. International Journal of Production Economics, 229, 107791. https://doi.org/10.1016/j.ijpe.2020.107791
37. Wang, L., Wang, Y., & Liu, H. (2022). Digital twin-driven smart supply chain. Frontiers of Engineering Management, 9, 56-70. https://doi.org/10.1007/s42524-021-0186-0
38. Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation. Long Range Planning, 52(3), 326-349. https://doi.org/10.1016/j.lrp.2018.12.001

39. Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243. https://doi.org/10.1109/TII.2014.2300753
40. Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of Industry 4.0. Engineering, 3(5), 616-630. https://doi.org/10.1016/J.ENG.2017.05.015
41. Addo-Tenkorang, R., & Helo, P. T. (2016). Big data applications in operations/supply-chain management. Computers & Industrial Engineering, 101, 528-543. https://doi.org/10.1016/j.cie.2016.09.023
42. Ardolino, M., Saccani, N., Gaiardelli, P., Rapaccini, M., & Crespi, G. (2018). The role of digital technologies for the service transformation of industrial companies. International Journal of Production Research, 56(6), 2116-2132. https://doi.org/10.1080/00207543.2017.1324224
43. Bag, S., Gupta, S., & Foropon, C. (2019). Examining the role of dynamic remanufacturing capability. International Journal of Production Research, 57(16), 5211-5228. https://doi.org/10.1080/00207543.2019.1589620
44. Dubey, R., Gunasekaran, A., Childe, S. J., Wamba, S. F., & Papadopoulos, T. (2016). The impact of big data on world-class sustainable manufacturing. International Journal of Advanced Manufacturing Technology, 84, 631-645. https://doi.org/10.1007/s00170-015-7674-1
45. Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect. International Journal of Production Research, 57(3), 829-846. https://doi.org/10.1080/00207543.2018.1488086
46. Jagtap, S., Garcia-Garcia, G., Rahimifard, S., & Duong, L. (2021). Optimisation of the food supply chain using digital technologies. International Journal of Production Research, 59(1), 292-308. https://doi.org/10.1080/00207543.2020.1771450
47. Moeuf, A., Pellerin, R., Lamouri, S., Tamayo-Giraldo, S., & Barbaray, R. (2018). The industrial management of SMEs in the era of Industry 4.0. International Journal of Production Research, 56(3), 1118-1136. https://doi.org/10.1080/00207543.2017.1372647
48. Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration. Supply Chain Management, 24(2), 235-253. https://doi.org/10.1108/SCM-03-2018-0143
49. Sahin, F., & Robinson, E. P. (2002). Flow coordination and information sharing in supply chains. Journal of Operations Management, 20(5), 505-521. https://doi.org/10.1016/S0272-6963(02)00055-3
50. Tiwari, S. (2021). Supply chain integration and Industry 4.0: A systematic literature review. Benchmarking, 28(3), 990-1030. https://doi.org/10.1108/BIJ-08-2020-0428
51. Winkelhaus, S., & Grosse, E. H. (2020). Logistics 4.0: A systematic review. International Journal of Production Research, 58(1), 18-43. https://doi.org/10.1080/00207543.2019.1612960