International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(Review Article)

Check for updates

Balancing technology deployment with operational control in high-volume supply chains

Chukwuebuka Okenna Umeh * and Akachukwu Leslie Nnonyelu

Kogod School of Business, Master's in business administration, American University USA.

International Journal of Science and Research Archive, 2026, 19(03), 1003-1011

Publication history: Received on 15 May 2026; revised on 25 June 2026; accepted on 27 June 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.19.3.1405

Abstract

Digital technologies like robotics, the Internet of Things (IoT), artificial intelligence (AI) and centralized control towers are becoming essential to high-volume supply chains, such as e-commerce fulfillment networks, large-scale warehousing and global logistics networks, to keep up with the growing demands for speed, accuracy and scale. The rapid deployment of these technologies, however, frequently outstrips the governance structures required to maintain operational control, which is defined here as the ability of managers and operators to monitor, audit and intervene in automated processes. This article explores the challenge of technology deployment and operational control in high volume supply chain environments, using secondary literature and documented industry case studies. The discussion is structured around the principles that underline operational control, the technological elements that facilitate it, and the processes by which operational control is achieved in practice. Four documented case studies show how successful and problematic it is to balance the two: United Parcel Service's route optimization system, Ocado's automated grocery warehouses, Maersk's logistics network operations center, and Target Canada's automated inventory and replenishment system. The results show that technology deployment has a measurable impact on visibility, resilience and efficiency, but only when organizations plan for human intervention points, decision rights and workforce capability in addition to technology. Without such design, automation adds inflexibility, friction in the workforce, and single points of failure. The article ends with the conclusion that balance is not the result of the amount of technology used, but rather the result of deliberate governance design.

Keywords: High-Volume Supply Chains; Technology Deployment; Operational Control; Automation; Algorithmic Management; Sociotechnical Systems

1. Introduction

Large transaction volumes, short delivery times, and high stock-keeping unit (SKU) variability are hallmarks of high-volume supply chains, which are found in e-commerce fulfillment centers, third-party logistics networks, and global shipping operations. The need to move goods faster, more accurately and at lower marginal cost has driven many of these operations to increasingly adopt technology, such as robotic picking and sorting systems, autonomous mobile robots, Internet of Things (IoT) sensors, AI-based forecasting and centralized control towers [1]. According to industry analyses, global investment in supply chain robotics will continue to increase at double-digit rates per year, and documented automated order-processing implementations have reduced the amount of manual intervention required significantly and in some cases by more than half, processing time [1,2].

In parallel to this discrete automation expansion, organizations have also embraced a wider approach to supply chain digitalization, such as big data analytics, blockchain and AI, to enhance the performance of the supply chain network. The results of the firm-level network analysis suggest that digitalization programs are positively related to information-

* Corresponding author: Chukwuebuka Okenna Umeh
Kogod School of Business, Master's in business administration, American University USA.

processing capacity, recovery capacity, and inventory turnover efficiency, and that these effects amplify overall supply chain resilience [3]. Complementary survey-based evidence from manufacturing companies also revealed that digitalization enhances supply chain visibility, which in turn partially mediates the improvements in supply chain performance [4].

However, the same literature that celebrates the advantages of technology deployment also recognizes a related and understudied problem: the more supply chains become automated, the more control traditionally held by direct human supervision, manual checks, and local decision-making is lost. In this article, operational control is defined as the ability of managers and operators to monitor, audit, understand and take control of supply chain processes in a manner that maintains accountability, flexibility and the ability to override automated decisions when necessary.

This tension is not new. Organizational research over the past few decades has demonstrated that the implementation of new technology in a work system can alter social structures, team autonomy and morale in ways that are not always predicted by the designer of the technical system alone [5]. The extent and pace of automation in logistics and fulfilment environments is relatively new, as is the need to design governance structures that can keep up with that deployment.

This article tackles the question: How can organizations with high-volume supply chains implement technology on a scale to perform competitively, without losing control of their operations to manage risk, accountability and disruption? The rest of the article is structured based on secondary literature and documented industry case studies. Section 2 provides an overview of the key concepts of operational control. Section 3 describes the key technological components that enable it. In Section 4, the integration of technology deployment and operational control in practice is explored. Four documented case studies are included in Section 5. The ethical issues and challenges of this integration are discussed in Section 6. Section 7 covers emerging trends and Section 8 ends with implications for practice..

2. Operational Control in High-Volume Supply Chains

Operational control in high-volume supply chains is the ability of managers and operators to manage, interpret, audit and intervene in the technical systems that operate day-to-day. Operational control in technology-intensive supply chains is organized around five interrelated principles, while lean manufacturing is organized around the elimination of waste.

2.1. Visibility

The degree of visibility of the relevant actors to what is happening in the supply chain, from inventory to shipment to equipment condition. If you can't see it, you can't control it, because managers can't intervene in conditions they can't see. The delivery of visibility is becoming more and more through centralized control towers, which integrate data from planning, warehousing and transportation systems into one operational view [6,7].

2.2. Decision Rights

Decision rights are who or what is allowed to make decisions based on the information that visibility gives. As supply chains become automated, decision rights shift from individual workers and managers to algorithms and centralized platforms; maintaining operational control will involve a conscious shift of decision rights, including the development of new roles that will coordinate across functions and balance the trade-offs [8].

2.3. Intervenability

The extent to which a human actor can stop, change, or alter an automated process before the impact of that process becomes irreversible. Human-in-the-loop architectures formalize intervenability by defining the locations in a decision pipeline where automated outputs are reviewed or escalated, but not automatically executed, for example, pre-emptive review, confidence-based routing, or exception handling [9].

2.4. Accountability

Accountability relates to the ability to assign responsibility for an automated decision to a person, role or process. Practitioner analysis of control tower implementations reveals that effectiveness is not just about digital tooling but also about the organization's design, competent staff, and decision rights [10]. If there is no accountability, then organizations are unable to identify who is responsible when an automated system makes a mistake and what should be done to rectify it.

2.5. Adaptability

The ability of a sociotechnical system to be reconfigured when conditions change, not just at the time of deployment. The study of the introduction of new technology into an existing work system, which was a classic study of mechanized coal mining, showed that the social structure, team autonomy, and morale of the work system are not always the same as those that the technologist had envisioned when designing the technical system in isolation [5].

These five principles, when combined, help to differentiate technology deployment (the installation of digital tools and automated systems) from operational control (the institutional capacity to govern what those tools and systems do once installed).

3. Key Components of Technology-Enabled Operational Control

The literature on the challenges of organizations trying to maintain operational control when implementing advanced technology on a large scale contains several technological and organizational elements that are repeated.

Control Towers: Control towers are digital centralized systems that bring together data from planning, warehousing, transportation and partner systems into one operational view [7,11]. Control tower implementations can be divided into systems that only present data to the human for interpretation and systems that go beyond that and automatically calculate corrective actions, reassign resources and notify stakeholders without requiring human sign-off [6]. Industry estimates have been able to attribute meaningful performance gains to advanced control tower capabilities, such as modest revenue gains, logistics cost reductions in the low single digits and labor efficiency improvements of up to 10 to 20 percent.

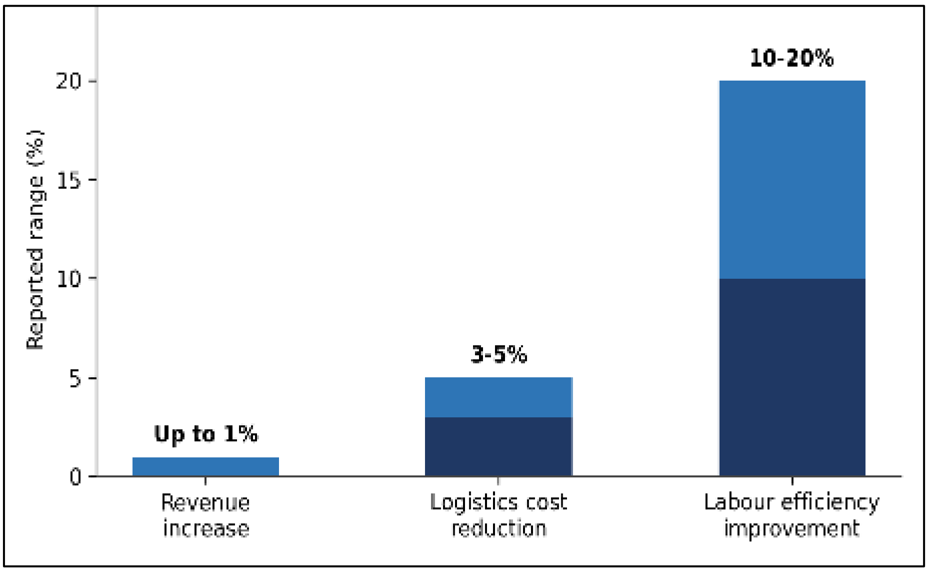

Figure 1 Reported operational gains from advanced supply chain control tower deployment, based on industry estimates [11]

3.1.1. *Human-in-the-Loop Systems*

Human-in-the-loop (HITL) systems formalize the points at which automated decisions are reviewed or escalated to a human actor. Analysis of automated decision systems in enterprise operations reveals four common patterns of intervention: pre-emptive review of decisions before execution, confidence-based routing of decisions to human reviewers for low confidence decisions, asynchronous audit of completed decisions, and exception handling for decisions outside normal parameters [9]. This taxonomy does not view operational control as a binary decision between automation and manual control, but rather a series of intervention points that can be configured.

3.1.2. *Sociotechnical Design*

Sociotechnical design considers decision rights, job roles, incentive structures, and feedback channels as components of the system being designed, not as changes made after technology has been implemented [5]. This approach is based on the historical observation that the social and technical aspects of a work system are interdependent and that changes in one will influence the other.

3.1.3. Cybersecurity and Data Governance

Supply chain systems are increasingly interconnected, and therefore more vulnerable to cyber risk, as well as being more reliant on the people who can understand and manage the data they produce. In logistics and supply chain environments, the lack of workers with the analytical and technical skills required to operate and maintain automated systems and the increased cybersecurity risk due to the growing interconnectedness of systems are recurring challenges in adoption studies of Industry 4.0 technologies [12,13]. If these capacity gaps remain, organizations can implement systems whose outputs are not sufficiently understood, audited, or corrected by the people who are supposed to be responsible for them.

4. Integration of Technology Deployment and Operational Control

4.1. Real-Time Visibility and Control Tower Orchestration

In addition to discrete automation solutions, a more comprehensive supply chain digitalization, which includes IoT sensing, big data analytics, AI-based forecasting, and blockchain traceability, has been correlated with tangible improvements in visibility, resilience, and performance. A national supply chain digitalization pilot program was used to conduct firm-level network analysis, which revealed that digitalization raised measures of network resilience by about one-fifth, based on difference-in-differences estimation, and by about one-third, after correcting for endogeneity, with the effects mainly attributable to better information-processing capacity, recovery ability and inventory turnover efficiency [3].

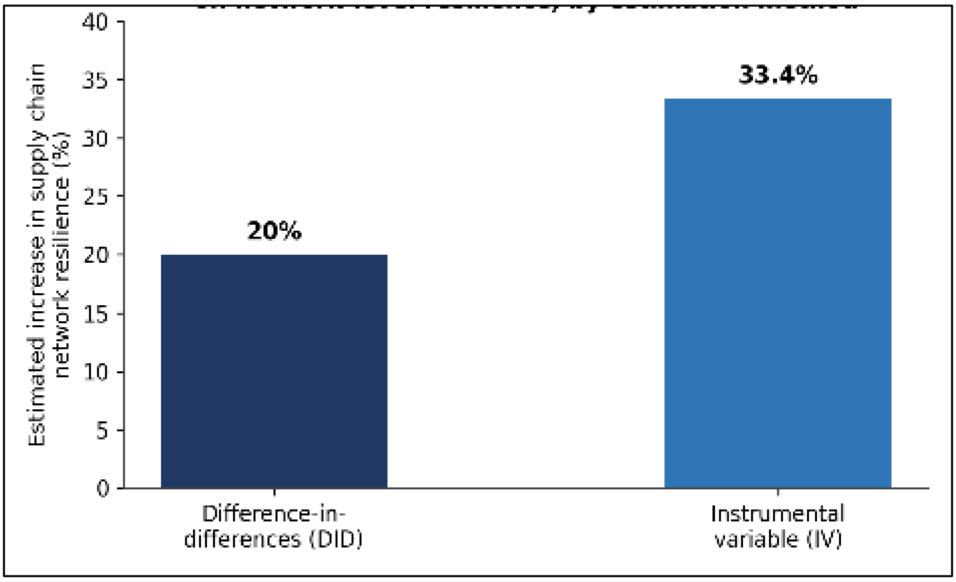

Figure 2 Estimated effect of supply chain digitalization on network-level resilience, by estimation method [3]

Investment in robotics, such as autonomous mobile robots, robotic picking arms, and automated sorting systems, is projected to continue to double-digit growth in supply chains through the end of the decade and is increasingly being used to compress cycle times and reduce manual handling [1]. The gains are documented by vendors: one implementation of order automation reportedly handled over a third of orders without any human involvement and cut the average order processing time from seven hours to less than three [2].

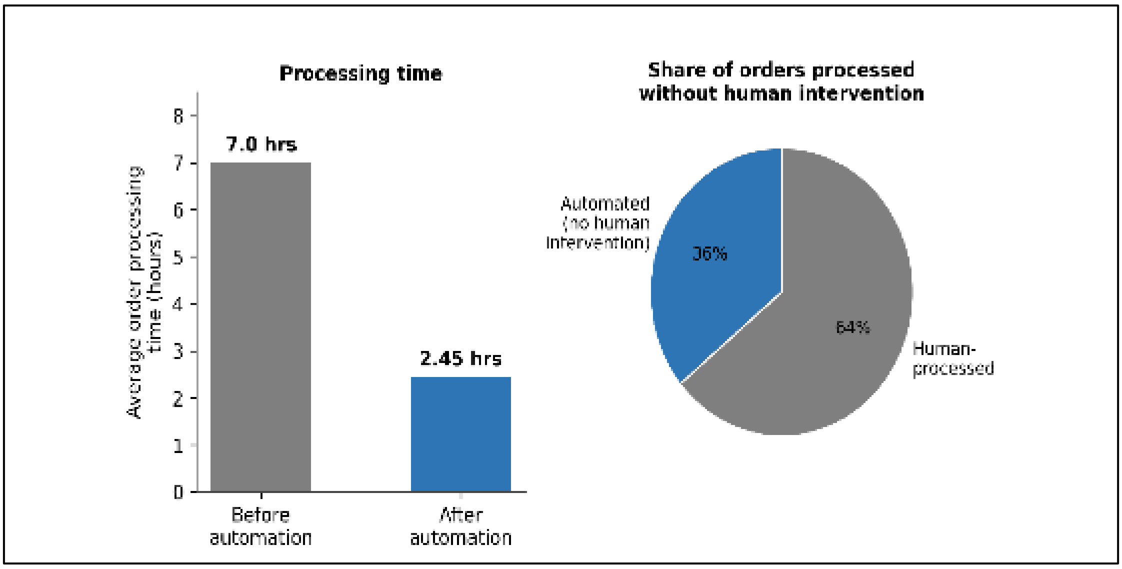

Figure 3 Documented effect of order-automation deployment on processing time and the share of orders requiring human intervention [2]

4.2. Human-in-the-Loop Decision Architecture

By carefully selecting human-in-the-loop intervention points, such as confidence-based routing and exception handling, most routine, low-risk decisions can be made automatically, while human judgment is reserved for situations with greater uncertainty, higher stakes, or conditions that fall outside the system's design parameters [9]. This selective approach to oversight is neither inefficient nor brittle, as universal manual review nor universal automation. Organizations that establish formal feedback mechanisms between humans and machines, instead of assuming that automation is a one-way street, are more likely to maintain control of the process as automation becomes more prevalent in their decision-making processes, as the case studies in Section 5 demonstrate.

4.3. Sociotechnical Design and Workforce Considerations

Operational control is not something that can be added to a technical system after it is deployed; it must be built into the system along with the technology, including decision rights, job design, and feedback loops between people and systems [5]. If this design work is not done, technology can undermine the trust and discretionary judgment that employees may bring to handling operational exceptions. Over two years of ethnographic research in large-scale e-commerce fulfilment centers revealed that algorithmic management systems that monitor, score, and assess workers' performance by collecting data continuously can create a sense of objectification among workers and encourage covert resistance practices, as workers find informal ways to manage how they are treated within the metrics-driven system [14]. This case, discussed in more detail in Section 5, is an example of the expense of implementing a technology that requires a lot of measurements to be taken but not much control or voice at the worker level.

4.4. Risk Management and Resilience

Once automated workflows are set up, they may not be able to handle unexpected events that fall outside their programmed parameters, and a single misconfigured rule can cause errors to cascade through a process instead of just one transaction [15]. At a higher level of systems, the growing interdependence of parts of the digital supply chain can lead to cascading failure: a vulnerability, software bug or disruption in one part of the chain can quickly spread through tightly coupled networks, and the benefits of automation are balanced by a proportionate decrease in resilience to failure at the component level [16]. To mitigate this risk, organizations need to have orchestration-capable control towers, not just visibility towers, with clear organizational decision rights, meaning the same platform that identifies an operational exception should also be given the authority, within limits, to take action on the exception or escalate it to a human decision maker [6,10].

5. Case studies

5.1. United Parcel Service: Human-in-the-Loop Route Optimization with ORION

ORION (On-Road Integrated Optimization and Navigation) is an algorithmic route-planning system developed by United Parcel Service (UPS) to minimize the distance, time and fuel used to complete a driver's delivery sequence [17]. Initial implementations produced routes that were hard for drivers to follow, due to the lack of local road conditions and established customer relationships in the underlying rules, and the system needed to be significantly redesigned before it could be adopted [17]. Instead of eliminating driver judgment from the process, UPS kept the driver intervenability by letting drivers go off the suggested sequence and, when they did, documenting a reason for the deviation; this feedback was then used to improve the algorithm's future recommendations [17]. UPS claimed that removing just one mile per driver per day would save them tens of millions of dollars annually across the entire company, making even marginal routing improvements a priority that warranted this amount of design effort [18]. The ORION case is an example of a deliberate sociotechnical design decision: UPS did not try to eliminate the role of the driver as a constraint to be optimized away, but instead created a structured channel for driver judgement to shape and correct the automated system after deployment.

5.2. Ocado: Exception-Based Human Intervention in Automated Grocery Warehouses

Ocado's grocery fulfilment centers are highly automated with a dense grid of mobile robots that retrieve storage bins and transport them to either further automated handling or to pick stations staffed by humans [19,20]. Robots are also being fitted with robotic picking arms that can use machine learning to pick a wide range of grocery products, including fragile and irregularly shaped items, and that can learn by watching human pickers perform the same tasks [19]. Importantly, the system is designed to have an explicit intervenability mechanism: if an anomaly occurs, for example, damaged packaging, the robotic arm can be directly controlled by a human operator, and the exception can be handled manually by the human operator [19]. This design focuses human attention specifically on the area of greatest uncertainty – the handling of irregular or unexpected items – while routine retrieval and sorting proceed automatically at scale over a grid spanning several football fields [20]. Ocado's approach is an example of how one of the four patterns of human-in-the-loop intervention described in Section 3 can be integrated into automated material handling, instead of being considered as a governance layer after deployment.

5.3. Maersk: Network Operations Centre and Orchestrated Control Towers

Maersk's warehousing and distribution business has a network operations center (NOC) that brings together data from the warehouse control systems, equipment sensors and facility cameras in one set of monitoring displays [21]. This integrated data is not used to make decisions automatically but instead is sent to a specific manager who then makes decisions on resource allocation for the monitored facilities [21]. This design is based on the difference between visibility and orchestration that was introduced in Section 3: the NOC provides full situational awareness, but the authority to act on that awareness is clearly delegated to an accountable human role, not spread across automated subsystems. The NOC model shows how a control tower can provide a wide range of technological deployment, with many data feeds being integrated in real time, but not necessarily spread the decision authority needed for operational control.

5.4. Target Canada: Automated Replenishment Without Reliable Data Governance

Target's 2013 Canadian launch was based on a fast and extensive deployment of SAP-based inventory management software and JDA forecasting and replenishment software in three new distribution centers and 133 stores [21]. The system needed to be populated with a lot of item-level data, including dimensions, weight, and case-pack quantities, and the initial data load was rushed, with many errors found in the data fed into the automated replenishment system from the start [21,22]. The effects of these errors were not stopped before they reached the replenishment system, so products did not fit on store shelves, paperwork mismatches delayed overseas shipments, and merchandise accumulated undisturbed in distribution centers while stores reported empty shelves [21,22]. Strikingly, an internal review later revealed that the automated feature, which was supposed to trigger replenishment shipments when a store's stock was running low, a built-in mechanism for sustaining flow without manual intervention, had in some cases been manually disabled by analysts who distrusted the system's own data, removing the very automation the supply chain relied on without replacing any other form of human oversight [21]. This case is the opposite of the UPS and Ocado examples: decision rights were not clearly defined at Target Canada, accountability for data quality was spread across vendors, merchandisers, and contracted data-entry personnel, and validation checks were not implemented, leading to an otherwise standard ERP and replenishment deployment that spiraled into a supply chain failure that helped close all 133 Canadian stores in 2015 [21,22].

6. Ethical Considerations and Challenges

In high-volume supply chains, the use of advanced technology and operational control presents ethical and practical issues that go beyond the technical issue of system design.

One of the initial concerns is data security and the protection of sensitive operational data. The more data that control towers, sensors, and algorithmic management systems generate about shipments, equipment, and individual worker performance, the more it becomes an operational asset and a security liability, and interconnected supply chain systems are exposed to a greater risk of cyberattacks, software defects, and cascading failures as described in Section 4 [12,16].

The second is the differential distributional effect of technology deployment. The technology needed for sophisticated control towers, sensor networks and predictive analytics is a significant investment that larger companies can make more easily than smaller companies, which is driving a divide between those that can afford to invest in these systems and those that can't [12,13].

A third, and arguably the most consequential, concern is the erosion of data governance and accountability as deployment outpaces an organization's ability to validate what it has deployed. As the Target Canada case in Section 5 illustrates, when item-level data feeding an automated replenishment system is inaccurate and no validation or escalation mechanism exists to catch the errors, responsibility for the resulting failures becomes difficult to locate, spread across vendors, merchandisers, and contracted data-entry staff, and frontline employees may disable automated functions altogether rather than work within a system they no longer trust [21,22]. The UPS and Ocado cases, on the other hand, show that structured channels for human judgment, such as deviation logging or exception handling by a remote pilot, can maintain some of the discretion and accountability that would be lost in fully automated systems.

To overcome these challenges, organizations must consider data governance, equitable access to enabling infrastructure, and workforce voice as part of the technology deployment process, not as an afterthought once systems are up and running.

7. Trends and Advancements

Over the next few years, several developments are emerging that will influence the way organizations manage technology deployment and operational control in high-volume supply chains.

AI and machine learning are being integrated into the current control tower and human-in-the-loop systems, enhancing the confidence-based routing and exception-handling processes outlined in Section 3, and allowing for a growing proportion of routine decisions to be made automatically with greater safety, while more complex or high-stakes cases are still referred to human reviewers [9]. This is not a replacement for human oversight but will focus it even more on cases that truly need judgment.

Edge computing, which processes data near where it is created instead of sending it to a centralized server, is likely to help lower the latency between the time an operational exception occurs and the time it is brought to the attention of a human decision-maker, as in Ocado's remote-pilot system [19]. Edge architecture also helps to minimize the amount of data flowing over networks, which can help mitigate some of the cybersecurity risks mentioned in Section 6.

Combined, these trends indicate that the future of technology deployment in high-volume supply chains will not be just an increase in automation, but an increase in "calibrated automation," in which a growing number of digital tools will be matched by a growing number of human oversight mechanisms to control them.

8. Conclusion

In high-volume supply chains, there is a structural decision that is frequently presented as automation versus control. The evidence and case studies presented in this article indicate that the more productive approach is automation with designed control: organizations that can scale the use of technology without relinquishing control of operations, as demonstrated in the examples of UPS' deviation logging feedback loop, Ocado's remote-pilot exception handling, and Maersk's network operations center, do so by considering governance as a parallel design problem, not an afterthought. By contrast, the Target Canada case illustrates what happens when a large-scale automated system is deployed faster than the organization can validate the data and decision rights it depends on.

In all of these cases, three patterns emerge: decision rights and feedback loops are not added on after the automated systems are implemented, but are designed in parallel; human oversight is focused on areas of highest uncertainty or consequence, rather than distributed or nonexistent; and visibility platforms are accompanied by clear accountability for who is authorized to act on what they reveal.

The takeaway for organisations with high volume supply chains is that the rate of technology uptake should be matched, intentionally, with governance structures, workforce voice and clarity of decision rights. This secondary-data synthesis was not designed to answer the empirical question of which combinations of human-in-the-loop design and control tower architecture are best suited to which categories of operational risk; future research based on primary data across other sectors and firm sizes would help answer this question.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed No conflict of interest to be disclosed.

Statement of ethical approval

The study was based solely on secondary data from peer-reviewed journal articles, industry reports and documented case material from recognized organizations, which are publicly available. This research did not involve the collection or analysis of primary data from human participants, animals or proprietary organizational records, so there was no need for ethical approval.

References

[1] RTS Labs. Supply chain automation guide 2026: benefits, use cases and implementation [Internet]. 2026 [cited 2026 Jun 17]. Available from: https://rtslabs.com/supply-chain-automation/

[2] Conexiom. Supply chain automation: what it is and how to implement it [Internet]. 2024 [cited 2026 Jun 17]. Available from: https://conexiom.com/blog/supply-chain-automation-what-it-is-and-how-to-implement-it

[3] Tian Y, Cui L. Supply chain resilience and digital transformation: perspectives from a supply chain network. Humanit Soc Sci Commun. 2025;12:1738.

[4] Al Tera A, Alzubi A, Iyiola K. Supply chain digitalization and performance: a moderated mediation of supply chain visibility and supply chain survivability. Heliyon. 2024;10(4):e25584.

[5] Trist EL, Bamforth KW. Some social and psychological consequences of the longwall method of coal-getting. Hum Relat. 1951;4(1):3-38.

[6] Locus. Control towers in supply chain decision-making: a framework [Internet]. 2026 [cited 2026 Jun 17]. Available from: https://locus.sh/blogs/control-towers-supply-chain-decision-making/

[7] NetSuite. What is a supply chain control tower? [Internet]. 2025 [cited 2026 Jun 17]. Available from: https://www.netsuite.com/portal/resource/articles/inventory-management/supply-chain-control-tower.shtml

[8] Accenture. From visibility to value: applying a supply chain control tower to achieve end-to-end visibility [Internet]. [cited 2026 Jun 17]. Available from: https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-additional-pages-1/pdf/pdf-177/accenture-supply-chain-control-tower-from-visibility-to-value.pdf

[9] Daruna S. Human-in-the-loop frameworks in automated decision systems: a systematic analysis of design patterns, performance characteristics, and deployment considerations. Am J Eng Technol. 2026;8(2):17-25.

[10] Supply Chain Management Review. What it really means: supply chain control towers [Internet]. 2026 [cited 2026 Jun 17]. Available from: https://www.scmr.com/article/what-it-really-means-supply-chain-control-towers

[11] Kinaxis. What is a supply chain control tower? [Internet]. 2026 [cited 2026 Jun 17]. Available from: https://www.kinaxis.com/en/supply-chain-control-tower

[12] Mexico Business News. Industry 4.0 adoption faces cost, talent, cybersecurity barriers [Internet]. 2025 [cited 2026 Jun 17]. Available from: https://mexicobusiness.news/cloudanddata/news/industry-40-adoption-faces-cost-talent-cybersecurity-barriers

[13] Journal of e-Science Letters. The digital supply chain: challenges and opportunities in Industry 4.0 [Internet]. 2025 [cited 2026 Jun 17]. Available from: https://scienceletters.researchfloor.org/the-digital-supply-chain-challenges-and-opportunities-in-industry-4-0/

[14] Cheon E, Erickson I. Fulfillment of the work games: warehouse workers' experiences with algorithmic management. Proc ACM Hum-Comput Interact. 2025;9(CSCW2):Article CSCW228.

[15] MakeForms. What are the risks of over-automation? [Internet]. 2024 [cited 2026 Jun 17]. Available from: https://makeforms.io/blog/workflow-automation-risks

[16] Sustainability Directory. What are the potential risks of over-reliance on technology? [Internet]. 2025 [cited 2026 Jun 17]. Available from: https://sustainability-directory.com/question/what-are-the-potential-risks-of-over-reliance-on-technology/

[17] Harvard Business School Digital Initiative. UPS: driving performance by optimizing driver behavior [Internet]. 2017 [cited 2026 Jun 17]. Available from: https://d3.harvard.edu/platform-digit/submission/ups-driving-performance-by-optimizing-driver-behavior/

[18] Transport Topics. UPS routing program ORION helps drivers trim miles, reduce costs [Internet]. 2022 [cited 2026 Jun 17]. Available from: https://www.ttnews.com/articles/ups-routing-program-orion-helps-drivers-trim-miles-reduce-costs

[19] Ocado Intelligent Automation. OCADEX/Pick: on-grid robotic pick [Internet]. [cited 2026 Jun 17]. Available from: https://ocadointelligentautomation.com/systems/on-grid-robotic-pick

[20] Harvard Business Review. How online grocer Ocado is automating warehouses using swarms of robots [Internet]. 2018 [cited 2026 Jun 17]. Available from: https://hbr.org/sponsored/2018/05/how-online-grocer-ocado-is-automating-warehouses-using-swarms-of-robots

[21] Haivision. Case study: Maersk Network Ops Center (NOC) [Internet]. 2025 [cited 2026 Jun 17]. Available from: https://www.haivision.com/case-studies/maersk/

[22] Castaldo J. The last days of Target Canada. Canadian Business [Internet]. 2016 Jan [cited 2026 Jun 17]. Available from: https://canadianbusiness.com/ideas/the-last-days-of-target-canada/

[23] Panorama Consulting Group. 6 lessons learned from the Target Canada supply chain failure [Internet]. 2021 [cited 2026 Jun 17]. Available from: https://www.panorama-consulting.com/target-canada-supply-chain-failure/