

How Technology Is Used As A Tool In Supply Chain Management?

Posted on September 29, 2018

View this essay online:

<https://academic-master.com/how-technology-is-used-as-a-tool-in-supply-chain-management/>

Introduction

Technology has transformed supply chain management from a largely administrative function into a coordinated information system linking demand, purchasing, production, inventory, transport, delivery, returns, and risk. Every movement of goods now creates data that can be used to plan replenishment, verify location, manage quality, and respond to disruption. A customer order can update inventory, trigger procurement, reserve production capacity, create transport requirements, and affect financial forecasts. The value comes from connecting these events accurately, not from installing one fashionable device. Radio-frequency identification, barcodes, enterprise software, sensors, transport platforms, analytics, and secure data exchange all serve different purposes. An [enterprise resource planning](#) system can coordinate internal records, while standards such as GS1 identifiers and EPCIS help trading partners exchange event information consistently (GS1, n.d.-a). Technology therefore improves supply chains when physical movements and digital records correspond, organizations agree on data definitions, and staff can act on the information produced. Without those conditions, automation can accelerate the same errors that previously occurred manually.

Planning, Procurement, and Data Discipline

Planning and procurement systems improve coordination by combining demand history, lead times, supplier performance, capacity, inventory, and financial information. Enterprise resource planning platforms can connect sales orders with purchasing, production, accounts, and warehouse records, while supplier portals and electronic orders reduce repeated data entry. Advanced analytics may improve forecasts by identifying patterns that are difficult to see manually, but models remain dependent on the quality and relevance of their data. A forecast trained during stable conditions may perform badly during a strike, pandemic, product launch, geopolitical disruption, or rapid change in consumer demand. Human judgment therefore remains necessary for unusual conditions and for decisions involving risk tolerance. Technology also creates a governance problem: if product descriptions, units of measure, locations, or supplier identities are inconsistent across systems, apparently precise dashboards can still be wrong. Organizations need clear ownership of master data, validation at entry, documented corrections, and rules identifying which system is authoritative for

each field. Better software cannot compensate for unclear processes or poor information discipline.

Warehouses, Transport, and Real-Time Visibility

Warehouses and transport networks benefit from technologies that make physical movement visible. Warehouse-management systems direct receiving, put-away, picking, packing, counting, and shipping, while barcode scans confirm that the intended item and quantity moved. Transport-management systems compare routes, capacity, carriers, service levels, and freight costs. GPS, telematics, and connected sensors can report location, temperature, door openings, or equipment conditions, which is especially valuable for food, pharmaceuticals, chemicals, and other sensitive products. These systems allow earlier response to delay or quality risk, but “real time” does not mean perfect knowledge. Devices can fail, communications can drop, and a location message does not prove that the correct product is inside a vehicle. Useful systems therefore emphasize exception management rather than displaying every possible event. Alerts should correspond to meaningful thresholds, have a clearly assigned owner, and lead to physical investigation when necessary. Technology is most effective when it helps managers recognize deviations early and correct the underlying process instead of merely editing the digital record.

RFID, Barcodes, and Traceability Standards

RFID is one of the technologies most closely associated with supply-chain visibility. Radio-frequency tags can identify objects without the direct line of sight usually required by barcodes, and multiple items may be read rapidly depending on tag type, frequency, reader placement, packaging, and material. GS1 notes that RAIN RFID can support identification and visibility, while EPCIS provides a standardized way to record what object moved, when it moved, where the event occurred, and why it happened (GS1, n.d.-a; GS1, n.d.-b). RFID does not automatically eliminate inventory anomalies. Tags and readers add cost, and metals, liquids, dense packing, or interference can reduce performance. A low-value product may be more economical to track at case or pallet level, while inexpensive barcodes remain appropriate for many operations. The correct technology depends on value, risk, speed, environment, and partner capability. The wider lesson of GS1 traceability guidance is that identifiers, event records, and interoperable processes matter as much as the physical data carrier itself (GS1, n.d.-c).

Analytics, Artificial Intelligence, and Organizational Change

Analytics and artificial intelligence can turn supply-chain data into predictions and recommended actions. Companies use them to identify slow-moving inventory, forecast demand, estimate delays, optimize routes, detect quality patterns, and test alternative network designs. Digital twins may

represent factories, warehouses, or transport networks so managers can simulate disruptions before changing physical operations. These tools are useful, but optimization models only evaluate the objectives and constraints included in them. A model designed to minimize cost may overlook worker fatigue, community effects, contractual restrictions, or resilience unless those factors are explicitly represented. Organizations should document model assumptions, validate recommendations against actual outcomes, monitor performance when conditions change, and maintain human accountability for consequential decisions. Technology should also be judged by its effects on smaller suppliers and employees. Requirements that demand expensive systems can exclude otherwise capable partners, while constant monitoring may create inappropriate workplace surveillance. A sound implementation begins with a specific operational problem, tests the proposed solution through pilots, and includes users who understand practical exceptions that software designers may miss.

Cybersecurity, Privacy, and Resilience

Connectivity increases efficiency but also expands cybersecurity and privacy risk. A compromised supplier account, stolen credential, malicious software update, exposed sensor, or ransomware incident can interrupt operations or corrupt the information on which planning depends. NIST's Cybersecurity Framework 2.0 supply-chain guidance emphasizes managing the risks associated with acquired products, services, and suppliers across the technology lifecycle (National Institute of Standards and Technology [NIST], 2024). Practical controls include least-privilege access, multifactor authentication, network segmentation, secure configuration, software inventories, logging, tested backups, incident-response procedures, and contractual requirements for vulnerability reporting. Tracking technology can also raise privacy concerns when tags remain active after sale or when employee locations are monitored continuously. Resilience therefore requires both cyber controls and operational alternatives: critical suppliers should be identified, manual workarounds practiced, recovery priorities defined, and substitute routes or sources considered. A highly digital supply chain can become fragile if every process depends on one platform, vendor, or communications channel, so redundancy and recovery planning must accompany integration.

Conclusion

Technology is most valuable in supply chain management when it improves decisions, traceability, coordination, and resilience rather than simply increasing the volume of collected data. RFID can improve item identification, but it works within a broader architecture that includes barcodes, enterprise systems, warehouse and transport platforms, sensors, analytics, standards, and cybersecurity. GS1 traceability standards show the importance of consistent identifiers and shared event data across organizations, while NIST guidance demonstrates that digital integration must be accompanied by supplier and technology risk management (GS1, n.d.-c; NIST, 2024). Successful organizations choose tools according to the problem being solved, product value, environmental conditions, partner capability, and measurable benefit. They also involve workers, validate data and

models, protect privacy, and prepare for system failure. A strong digital supply chain is therefore not one in which every object is monitored continuously. It is one in which accurate, appropriately shared information helps people deliver products safely, efficiently, transparently, and reliably while retaining the ability to operate when technology is disrupted.

References

GS1. (n.d.-a). *RFID*.

GS1. (n.d.-b). *EPCIS and Core Business Vocabulary*.

GS1. (n.d.-c). *Global Traceability Standard*.

National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management*.