Augmented Logistics and Smart Supply Chains

A. Combined Scope

Leveraging IoT technology for global supply chain logistics focused on tracking goods from design, production, distribution, delivery, and end use. The logistics process will consider varied levels of automation relative to the capability maturity of enterprises all the way up to digitalization of logistics workflows.

Logistics for tracking scope will extend to include provenance and traceability of physical objects and data linked to identifiers to deliver assets with trusted information and security for the benefit of suppliers, consumers, distributors, operators, logistics companies, businesses, and all stakeholders (personas) in the value chain and industry ecosystems.

Varied levels of security and trust for traceability will be considered for enterprises and global markets, in ways that maximize national security and economic prosperity. Traceability scope will be extended with digital threads to regulate market preference, access, and usage of goods, enable TRUSTED data producers/consumers, marketplaces and AI applications to fuel growth.

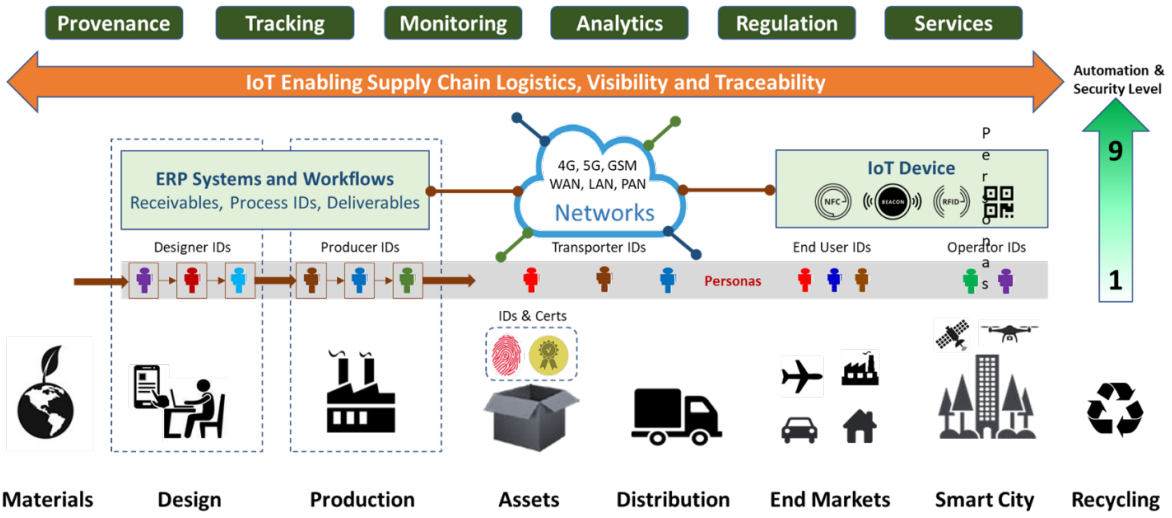


Figure 1. Scope of Supply Chain Covers Enterprise IT Connectivity with In-field IoT Technology

Definition and Objectives of Augmented Supply Chain (Logistics & Tracking)
Augmented supply chain refers to the integration and use of emerging technologies such as IoT, AI, 5G, blockchain, and other digital technologies into traditional supply chain processes. This integration aims to enhance visibility, improve operational efficiency, reduce costs, and provide greater transparency throughout the supply chain. Augmented supply chains use real-time data and analytics to monitor and track goods from suppliers to end customers, making it easier to

identify bottlenecks, optimize operations, and improve overall performance. They adapt quickly to customer needs by anticipating demand, inventory levels, and logistics for assured supply.

Key objectives for Supply Chain Logistics and Tracking include:

- Track goods from design, production, distribution, delivery, and end use (using IDs)
- Allow logistics process to consider various levels of automation in the enterprise.
- Digitalize processes and workflows to establish provenance with trusted sources.
- Maximize efficiency and supply chain resilience for a variety of sectors and asset types.

Supply Chain Logistics and Risk Management (SCRM) is focused on ensuring **AVAILABILITY** of any asset, such as: are there enough sources of supply or lines on communication/transport; can we ensure users will have "parts" available to perform their mission in the supply chain; and how to maximize supply chain resilience to ensure supply for JIT manufacturing.

B. Definitions and Objectives

Definition and Objectives of Smart Supply Chains (Provenance & Traceability)

Augmented Supply Chains evolve to smart supply chains, a network of interconnected enterprises in a value chain that use digital and IoT technologies to exchange information deliver products or services to end-users. Smart-connected value chains leverage advanced technologies and digitalization infrastructure to make intelligent decisions by establishing provenance, traceability and market preference through trusted digital thread and data analytics. They enable marketplaces by leveraging the digital thread of data to manage vulnerabilities, establish market preference and create data-driven ML/AI applications and IoT services to maximize security and economic growth.

Key objectives covering Provenance & Traceability include:

- Establish provenance of digital & physical workflows assets and data linked to identifiers.
- Deliver trusted traceability metadata linked to cybersecurity labels for supply chain.
- Support varied levels of trust across enterprises in the value chain and global markets.
- Create digital threads to regulate market preference/access/usage compliant to policies.

Cyber-SCRM Provenance & Traceability extends beyond **AVAILABILITY** by adding the aspects of **CONFIDENTIALITY & INTEGRITY** of any asset such as: Is my information and supply chain partners' data protected; does the product moved functions as intended (mainly electronics products); Is the product received trusted, secure and not tampered (more than track & trace needed); and Is the product delivered not ending up in adversaries (IP theft and electronics in enemy weapons).

We distinguish between **IoT Devices** and **IoT System**, denoting a complex system in IIoT consisting of IT (servers, routers, switches) and OT (SCADA, IPC, PLC, I/O) plus sensors which are used in IoT Devices. IoT Devices and IoT Systems must consider Classic Log-SCRM and Cyber-SCRM in their lifecycle. IoT devices/systems can be compromised during development creating vulnerabilities in manufacturing or transport process. So, **traceability capabilities** can be augmented **underneath the logistics layer.**

C. Augmented Supply Chain Logistics and Tracking

1. **Definition of IoT devices and systems supporting augmented logistics and supply chain management operations**

    a. Types of devices and systems
        i. RFID antennas and readers
        ii. RFID gateways
        iii. GPS related components
        iv. Discuss and add others here.

2. **Background and history of IoT use in logistics and supply chain.**

    a. Current state of IoT in supply chain
        i. Devices – most common IoT devices for most common use cases
        ii. Implementation and Adoption Across Industry
            1. Logistics and Distribution including Trucking and Warehousing
            2. Manufacturing
            3. Others – decide on common supply chain components or try to map to SCOR model (Plan, Order, Source, Transform, Fulfill, Return) (graphic?)
        iii. Connectivity specific to supply chain use cases (Wi-Fi, BLE, 5G, Lora WAN, others)
        iv. Global implications due to nature of supply chains

    b. Representative examples of use cases
        i. Track and Trace
        ii. Inventory Management
        iii. Medical cold chain (vaccine distribution)
        iv. Others for discussion and to add here.

    c. Documented benefits – reference to existing implementations if possible

    d. Documented barriers and challenges on previous implementations (if possible and can be referenced)

3. **Drivers and Opportunities for Supply Chain Logistics and Tracking**

Insert some write-up with industry drivers/trends and cut-paste Robbie's write-up

strategic/business opportunities - Real-time monitoring and tracking, Predictive maintenance,

inventory management, demand forecasting, visibility & transparency, Automation and robotics, Energy and resource efficiency, Collaboration, etc.

4. The Future State of IoT in Supply Shain

a. Significant and transformative potential use cases (examples)
   i. Artificial Intelligence of Things (AIoT) – impact on supply chain
   ii. Increase in Machine to Machine (M2M) communication.
   iii. Predictive Maintenance impact on asset management and parts supply
   iv. Perpetual Inventory Management – all inventory across enterprise tracked all the time.
   v. Advanced data analytics based on ubiquitous IoT data.
   vi. Interoperability
   vii. Others for discussion and to add here.

b. Anticipated benefits based on advances in IoT.

Are these barriers different than the recommendation section? Should we delete them?

c. Barriers to future adoption and advances
   i. Equipment specific barriers
   ii. Persona specific barriers (change management at enterprise level)
   iii. Applicable broad overall barriers (to be identified elsewhere in report and can be tied to supply chain here)

5. Summary of Recommendations for augmented supply chain logistics and tracking.
Here we insert a title with short summary 3-4 lines. Need to combine a few general ones on standards and workforce development. Consider combining all recommendations into one list at the end instead of separating them for both ***Logistics & Traceability***

a. R01 - National IoT Strategy for adoption of IoT in supply chain logistics ***[Removed]***
b. R02 - Promote standards and protocols for IoT in supply chain logistics. ***[Use Combined}***
c. R03 - Provide financial incentives to encourage adoption of IoT in supply chain logistics.
d. R04 - Foster PPPs focused on adoption of IoT in supply chain logistics

   R05 - Invest in workforce development for IoT Logistics, Tracking, etc. ***[Use Combined}***
e. R06 - Strengthen cybersecurity measures focused on IoT in supply chain logistics.
f. R07 - Promote international collaboration on adoption of IoT in supply chain logistics.
g. R08 - Monitor and evaluate progress of adoption of IoT in supply chain logistics.
h. R09 - Select mix of policies, incentives, and requirements to support sustainable, scalable growth in domestic IoT manufacturing supply chain.

6. **Detailed Recommendations for augmented supply chain logistics and tracking.**
   Here we cut paste one-by one our written recommendations.

    a. Title
    b. Description
    c. Justification
    d. Implementation Considerations
    e. Potential Barriers
    f. Participating Agencies
    g. Federal Considerations

TBD – The bullets below are mostly covered in the recommendation section. Should we have a commentary/conclusion about benefits and investment needed?

    h. Investment or other action by federal government
        i. Infrastructure
        ii. Standards definition and compliance enforcement (if needed)
        iii. Incentives to speed adoption
        iv. Education and act as convener of stakeholders

    i. Investment by industry vertical
        i. Device or system implementation where applicable (this may be overreach for this report – for discussion)
        ii. Incentives to speed adoption
        iii. Monetization – discuss and research methodology; could be derived from data availability, data sharing, ability to differentiate product or service.
        iv. ROI based.

    j. Other recommendations related to implementation or deployment and not related to investment.

7. **References Including Speaker Presentations**

    a. Supply Chain Logistics https://www.accenture.com/us-en/blogs/business-functions-blog/resilient-supply-chain
    b. Supply Chain Operational Reference Model https://scor.ascm.org/processes/introduction
    c. Speaker: Angela Fernandez, GS1 global standards and GLN
    d. Speaker: Mike Hineline, Establishment of Vaccine management transport and storage and refrigeration - https://www.linkedin.com/in/mike-hineline-069ba143/
    e. Speaker: Aruna Anand, Continental – Addressed Automotive challenges with best practices https://www.linkedin.com/in/aruna-anand-3566ba28/

D. Smart Supply Chains Provenance & Traceability

1. **Definition of IoT Devices and Systems supporting global supply chain traceability**

- Types of IoT Devices (any connected device and sub-components used in IoT Systems)
    i. Industrial – IPCs, PLCs, I/O Modules, Sensors, SCADA, etc.
    ii. Automotive – ECUs, CAMs, Alarms, ADAS, Infotainment, Telematics, etc.
    iii. Aerospace – Avionics, Flight Control, GPS, Radar, Guidance, etc.
    iv. Medical – Wearables, Monitors (EKG, Blood, Glycose), Pacemakers, etc.
    v. Agriculture – Sensors (Crop, Soil), Drones, Systems (Irrigation, Weather, etc.)
    vi. Consumer – Smart Home (Locks, Appliances, Meters), Trackers, etc.
    vii. Communications – Phones, modems, radios, 5G, gear, routers, switches, etc.
    viii. Computing – Servers, Routers, Storage, GPU/AI Accelerators, etc. *to the extent that they support traceability as part of a broad IoT system or IIoT solution*
    ix. Discuss and add others here.

2. **Background and history of supply chain traceability for assets including IoT Devices**

- Limited on no supply chain provenance and global traceability of device assets and data
    i. Supply chain disaggregation drives vast attack surface threats and vulnerabilities.
    ii. Security vulnerabilities in Design, manufacturing, packaging, delivery, field use
    iii. IoT Device security pervasive in only a few verticals (DRM, Smartcards, etc.)
    iv. Untrusted devices produce untrusted data (risks, plus untrusted AI applications)
    v. No linkage among process and asset IDs creating end-to-end digital thread.
    vi. Digitalization of Design & Production functions lagging vs. HR, Finance, Sales
    vii. Lack of awareness on security of IoT Devices, Electronics and IoT supply chain
    viii. Limited investments to incentivize policies and market behavior on traceability.
    ix. Discuss and add others here.

- Representative Use Cases on Threats and Vulnerabilities
    i. Tampering and Cloning
    ii. Counterfeiting ($3 trillion in 2022)
    iii. Security and Traceability (linked to manage supply chain attacks)
    "Refer to this article, how supply chain security & traceability are tightly coupled
    Vulnerabilities in the supply chain mean that Cybercriminals can target any IoT markets via the contractors, sub-contractors, and suppliers at all tiers of the supply chain. Compounding the complexity of securing the supply chain is that vulnerabilities may be introduced at any phase of the product life cycle: design, production, distribution, acquisition, deployment, maintenance, and disposal.
    iv. Mirai Botnet *(Security and traceability)*
    v. Supermicro Hack (*Disputed, concept on traceability)*
    vi. BLU Third Party Collection of Data (*Security and traceability article link)*
    vii. Western Chips in Drones (*Ukraine article link* and *Iran article link*)
    viii. The Kojima-Toyota Incident Supply Chain Attack (*article link*)

ix. Colonial Pipeline Operations (*Security related to SBOM traceability*)
x. Stuxnet (*Security related to HBOM and traceability related to SBOM*)
xi. Add other threats (non-electronics related) here.

- Global implications due to nature of Electronics / IoT supply chains
  i. 65% of device assemblies are done in Asia.
  ii. No customs control, no identifiers for components
  iii. Vast attack surface enables major nation state attacks.

- Representative Use Case Examples and Benefits of Traceability (Any assets)
  i. Food & Drug Safety
  ii. Counterfeit Prevention
  iii. Sustainability (sourcing, monitoring)
  iv. Product Recalls
  v. Logistics Optimization
  vi. Trusted Materials Sourcing
  vii. Discuss and add others here.

3. Drivers and Opportunities for Supply Chain Provenance and Traceability

Insert some write-up with industry drivers/market trends and cut-paste TomKat's write-up on strategic/business opportunities - Increased demand for IoT devices, Accelerated digital transformation, Reshoring and diversification of supply chains, Geopolitical tensions, (Inter) National Cybersecurity Strategy, Mitigating supply chain risks, Ensuring the security and integrity of critical systems, etc.

4. The Future State of IoT, IT, OT Enabled Supply Chain Traceability.

- Barriers to future adoption and advances needed.
  i. Interoperability across a complex, diverse supply chain network
  ii. Data assurance (via a continuous, verifiable, traceable digital thread)
  iii. Security of processes, technology, and stakeholders across the supply chain
  iv. Market preference for assured supply from domestic and allied suppliers
  v. Certificate Authority linked to physical products and traceability data.
  vi. Enterprise change management and Persona-specific barriers
  vii. Others for discussion and to add here.

- Significant and transformative potential use cases (examples)
  i. Enterprise-level digitalization of People, Processes, Assets (incl. Technology)
  ii. Cryptographic linking of receivables, process, deliverables in all value chains
  iii. Process & asset IDs plus Trust Scores related to provenance, chain of custody.
  iv. Platform identities, certificates, attestation for tracking, tracing, and servicing
  v. Linking physical & digital assets (HBOM, SBOM, DBOM) with product lifecycles
     1. Digital paper trail relation to US Cybersecurity labeling and EU Digital Passports
     2. Digital thread for traceability of all materials and data that can create value.

vi. Others for discussion and to add here.

- Anticipated benefits based on advances enabled by IoT Solutions
  i. Product-as-a-Service, subscription-based business models, new revenue streams
  ii. Product optimization, predictive maintenance, digital twins, data-driven services
  iii. Data marketplaces, data availability, data licensing, audit, and rights
  iv. Data access by enterprises in the value chain including by Personas with PII
  v. Digitalized market access (deliverables tied to monetization practices)
  vi. Business models for IoT Services and data-enabled ML/AI applications
  vii. Others for discussion and to add here.

8. **Summary of Recommendations for Supply Chain Provenance & Traceability**

Here we insert a title with short summary 3-4 lines. Need to combine a few general ones on standards and workforce development. Consider combining all recommendations into one list at the end instead of separating them for both ***Logistics & Traceability***

R01 - Encourage Global Identifier Standards for Supply Chain Traceability ***[Use Combined}***

R02 - Promote Trusted Architectures for Provenance & Traceability

R03 - Incentivize IoT Systems Supply Chains to Adopt Trusted Traceability

R04 - Promote Creation of Traceable and Trusted IoT Network Ecosystems

R05 - Accelerate Evolution of Trusted Digital Threads Across Value Chains

R06 - Incentivize the Creation & Growth of Trusted Data Marketplaces

R07 - Subsidize Digitalization of Enterprises in the IoT Value Chain

R08 - Promote Creation and Orchestration of Trusted Value Chains

R09 - Subsidize Orchestrated Public-Private Partnerships Across Value Chains

R10 - Establish Data Policies that Stimulate Economic Growth

R11 - Facilitate Creation of Data-driven Business Ecosystems

R12 - Evaluate Opportunities, Risks of Using AI in Supply Chains

5. **Specific Recommendations for Supply Chain Provenance & Traceability**

Here we insert a title with short summary 3-4 lines.

- Title
- Description
- Justification
- Implementation Considerations
- Potential Barriers
- Participating Agencies
- Federal Considerations

TBD – The bullets below are mostly covered in the recommendation section. Should we have a commentary/conclusion about benefits and investment needed?

- Investments needed for traceability of the electronics IoT vertical.
    i. Traceability Infrastructure for electronics and chips used in IoT (incl. recycling)
    ii. Standards harmonization, compliance enforcement (prescriptive vs. restrictive)
    iii. Incentives to speed adoption (e.g., security labels, digital passports, digitalization subsidies, market preferences, restrictions, market access/usage of products)
    iv. International collaboration with allies on traceability and customs controls
    v. Orchestration & massive collaboration to digitalize supply chains "piecemeal."
- Investment needed for traceability on any verticals (stated above)
    i. Vary by IoT market based on education, adoption rate, and specific use cases.
    ii. Vary by IoT device or system, market-specific applications, and use cases.
    iii. Monetization – discuss and research methodology; could be derived from data availability, data sharing, ability to differentiate product or service.
    iv. Business Ecosystems – monetization and rev-share of partner-based platforms
    v. Benefits & ROI among participating stakeholders (platform open to all, not few)
- Other recommendations related to implementation or deployment at scale.

6. References Including Speaker Presentations

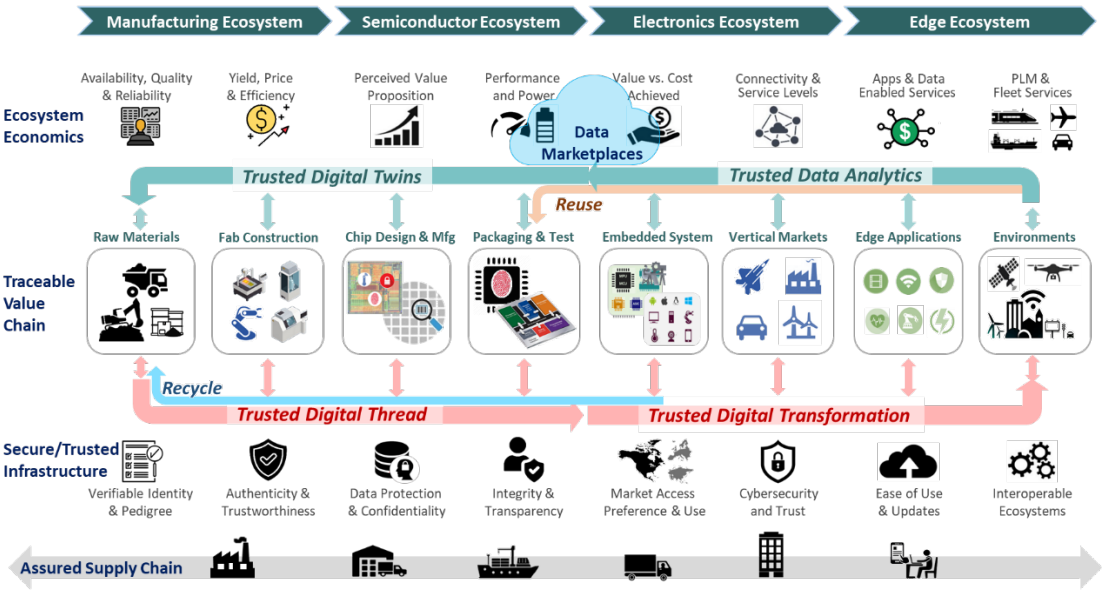
Some references may be moved in the recommendation section (check with Benson)

- **Don Davidson:** (Synopsys), Cyber-SCRM, DBOM, HBOM, SBOM
- **Harvey Reed:** (MITRE) MVP on Data Trust
- **Joe Weiss:** Industrial IoT Infrastructure
- TBD on Enterprise Data Access Control (secure workflows)
- TBD Suppliers of PLM on enterprise digitalization (digital thread)
- TBD Luminary on supply chain open source HW (e.g., Rick Switzer)
- MITRE MVP reference on supply chain data trust (post & share)
- NIST IR 8419 Blockchain for Manufacturing Traceability
- NIST Enterprise-level Cybersecurity Framework (CSF)
- NIST Rick Management Framework (RMF)
- NIST Cybersecurity White Paper on Consumer IoT Products
- NIST SP 800-160 on Systems Security Engineering (SSE)
- NIST SP 800-161 on Supply Chain Risk Management (SCRM)
- NDAA 2023 section 5949 on supply traceability and prohibitions https://www.congress.gov/bill/117th-congress/house-bill/7776/text
- NIST SP 800-171 / 172 on Controlled Unclassified Information (CUI)
- NIST 800.175 Cryptographic Standards Guide
- NIST SP 1800-34 on Validating the Integrity of Computing Devices
- HBR – How smart connected products are transforming competition
- MIT Sloan – Platform strategy and the Internet of Things

- MIT Sloan – The Future of Platforms
- MIT Sloan – New strategies for the platform economy
- BCG – How do you design a business ecosystem
- IBM - The new age of ecosystems

E. Example Use Cases

1. **Electronics & Semiconductor Supply Chain**
   TomKat – [IN PROGRESS] Insert End-to-End operations like Robby (Chip-to-Edge Use Case]



2. **Automotive Supply Chain**
   Robby Moss – [DONE] Cut-Paste End-to-End Use Case
   - *Tracking and tracing of raw materials:*
   - *Supplier performance monitoring:*
   - *Dynamic pricing and demand forecasting:*
   - *Production line optimization:*
   - *Quality control and assurance:*
   - *Energy and resource management:*
   - *Etc. Etc.*

3. **Industrial IoT Supply Chain**
   Steve Griffith – [FUTURE] Insert End-to-End Use Case

4. **Bonus – Agriculture Supply Chain**
   Ranveer Chandra – [FUTURE] End-to-End Use Case

5. **Bonus – Medical Supply Chain**
   Ann Mehra – [FUTURE] Insert End-to-End Use Case

F. Combine Recommendations on Both Logistics & Traceability ***here???***

Instead of having them separate?