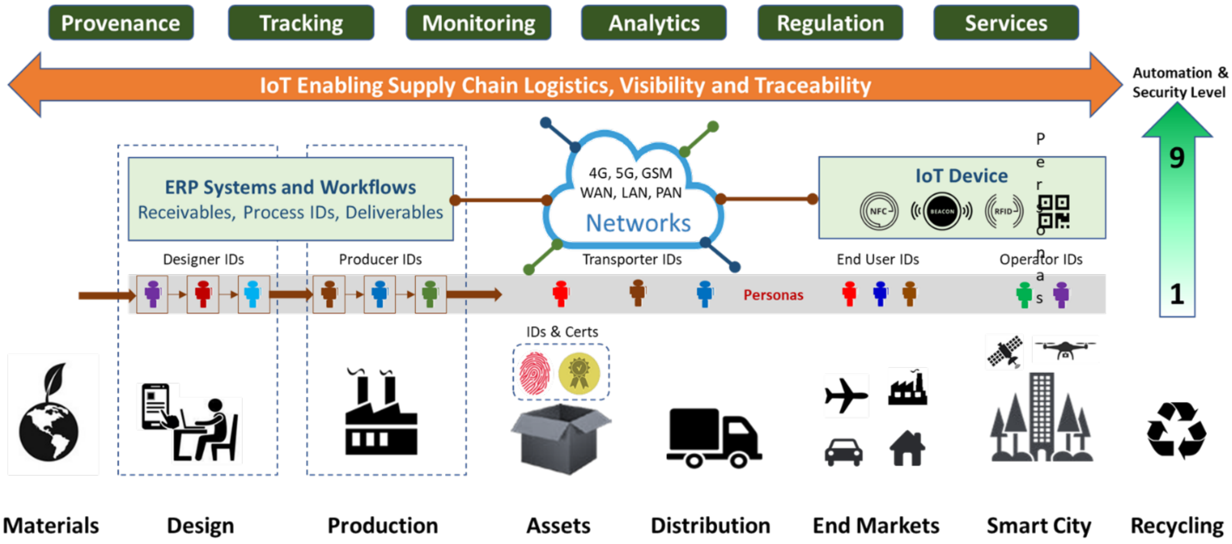
Old Title: Augmented Logistics and Supply Chains

Proposed New Title: Augmented Logistics and Smart Supply Chains

Scope: Leveraging IoT for global supply chain logistics focused on tracking goods from design, production, distribution, delivery, and end use. The logistics process will consider various levels of automation relative to the capability maturity of enterprises all the way up to digitalization of logistics workflows. These will 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, as well as digital threads to regulate market preference, access, and usage compliant to new regulations, in ways that maximize national security and economic prosperity.

The purpose of the diagram is to illustrate a concept of the scope and is subject to change



SUPPLY CHAIN LOGISTICS SECTION

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 (WiFi, BLE, 5G, LoRaWAN, 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. Future state of IoT in supply chain
    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
    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)

4. Recommendations specific to augmented supply chain
    a. 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
    b. 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

    c. Other recommendations related to implementation or deployment and not related to investment
5. Proposed Speakers
    a. Establishment of Vaccine management transport and storage and refrigeration - Mike Hineline https://www.linkedin.com/in/mike-hineline-069ba143/
    b. Speakers: Aruna Anand, Continental – Addressed Automotive challenges with best practices https://www.linkedin.com/in/aruna-anand-3566ba28/
    c. Angela Fernandez, GS1 global standards and GLN
6. References
    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. GS1 global standards presentation

SUPPLY CHAIN TRACEABILITY SECTION

Linking Global Supply Chain Topics on Logistics with Supply Chain Traceability

Classic Logistics and Supply Chain Risk Management (SCRM) is focused on **AVAILABILITY** of any asset

- Do I have enough sources of supply,
- Are there enough lines on communication/transport…
- Can I ensure users will have “parts” available to perform his mission / role in the supply chain…
- How to maximize supply chain resilience (ensure adequate supply for JIT manufacturing)

Cyber-SCRM and traceability adds the aspects of **CONFIDENTIALITY & INTEGRITY** of any asset:

- 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)
- Is the product delivered not ending up in adversaries (IP theft and chips in enemy weapons)

IoT Devices/Systems can be involved in these processes and are themselves products which must consider Classic Log-SCRM and Cyber-SCRM in their own development. IoT devices/systems can be compromised in their development lifecycle, which in-turn is a vulnerability in the manufacturing or transport process. So, **traceability capabilities** can be augmented **underneath the logistics layer**

How to distinguish between **IoT Device** into **IoT System** (or something like that denoting a complex system in IIoT consisting of IT (servers, routers, switches) and OT (SCADA, IPC, PLC, I/O) plus sensors.

1. Definition of IoT devices or IoT Systems supporting **global supply chain traceability**
    a. 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

a. 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

b. 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

c. 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

d. 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. Future state of IoT enabled supply chain traceability
    a. 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
    b. 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
    c. 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 market places, 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
4. Recommendations related to GLOBAL supply chain traceability
    a. 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”
    b. 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)

c. Other recommendations related to implementation or deployment at scale

5. Proposed Speakers (confirmed)

a. Don Davidson, (Synopsys), Cyber-SCRM, DBOM, HBOM, SBOM

b. Methods for Distributed Trust and Traceability

c. Harvey Reed (MITRE) MVP on Data Trust

d. TBD on Enterprise Data Access Control (secure workflows)

e. TBD Suppliers of PLM on enterprise digitalization (digital thread)

f. TBD Luminary on supply chain open source HW (e.g. Rick Switzer)

6. References

a. MITRE MVP reference on supply chain data trust (post & share)

b. NIST IR 8419 Blockchain for Manufacturing Traceability

c. NIST Enterprise-level Cybersecurity Framework (CSF)

d. NIST Rick Management Framework (RMF)

e. NIST Cybersecurity White Paper on Consumer IoT Products

f. NIST SP 800-160 on Systems Security Engineering (SSE)

g. NIST SP 800-161 on Supply Chain Risk Management (SCRM)

h. NDAA 2023 section 5949 on supply traceability and prohibitions https://www.congress.gov/bill/117th-congress/house-bill/7776/text

i. NIST SP 800-171 / 172 on Controlled Unclassified Information (CUI)

j. NIST 800.175 Cryptographic Standards Guide

k. NIST SP 1800-34 on Validating the Integrity of Computing Devices

l. The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime

m. The truth about counterfeits (Customs and Border Protection)

n. CISA Supply Chain Risks Infographic

o. Trust Issues in Microelectronics: The Concerns and the Countermeasures

p. New and Innovative Supply Chain Threats Emerging

q. Uniquely Identifying PCBs, Subassemblies, And Packaging

r. Blockchain Attempts to Secure the Supply Chain

s. The Next Pandemic Could Be Digital: Open Source Hardware Cybersecurity Risks

t. Why DDoS Attacks Use IoT Devices as Weapons?

u. McKinsey - IoT value set to accelerate through 2030: Where and how to capture it

v. HBR – How smart connected products are transforming competition

w. MIT Sloan – Platform strategy and the Internet of Things

x. MIT Sloan – The Future of Platforms

y. MIT Sloan – New strategies for the platform economy

z. BCG – How do you design a business ecosystem

aa. IBM - The new age of ecosystems

bb. Others to be added later