NIST Internal Report
NIST IR 8536 ipd

Supply Chain Traceability:

Manufacturing Meta-Framework

Initial Public Draft

Michael Pease
Evan Wallace
Harvey Reed
Dr. Vivian L. Martin
Steve Granata

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8536.ipd

NIST Internal Report
NIST IR 8536 ipd

Supply Chain Traceability:

Manufacturing Meta-Framework

Initial Public Draft

Michael Pease
Smart Connected Systems Division
Communications Technology Laboratory

Evan Wallace
System Integration Division
Engineering Laboratory

Harvey Reed
Dr. Vivian L. Martin
Steve Granata
MITRE

September 2024

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8536.ipd

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

How to Cite this NIST Technical Series Publication
Pease M, Wallace E, Reed H, Martin VL, Granata S (2024) Supply Chain Traceability: Manufacturing Meta-Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR (Internal Report) NIST IR 8536 ipd. https://doi.org/10.6028/NIST.IR.8536.ipd

Author ORCID iDs
Michael Pease: 0000-0002-6489-2621
Evan Wallace: 0000-0001-9368-5616
Harvey Reed: 0000-0002-4589-2677
Vivian L. Martin: 0009-0000-8698-4730

Contact Information
blockchain_nccoe@nist.gov

National Institute of Standards and Technology
Attn: Smart Connected System Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8200) Gaithersburg, MD 20899-8200

Public Comment Period
September 27, 2024 – November 15, 2024

Submit Comments
blockchain_nccoe@nist.gov

National Institute of Standards and Technology
Attn: Smart Connected System Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8200) Gaithersburg, MD 20899-8200

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8536/ipd, including related content, potential updates, and document history.

Abstract

National manufacturing and critical infrastructure (CI) supply chains are essential to maintaining the overall health, security, and the economic strength of the United States (U.S.). As global supply chains become more complex, tracing the origins of products and materials becomes increasingly challenging. Recent events and current economic conditions have exposed the significant risks posed by disruptions in the security and continuity of the U.S. manufacturing supply chain, highlighting the need for greater visibility and security to safeguard against various hazards and threats. Additionally, the U.S. manufacturing supply chain has proven vulnerable to logistical disruptions and the actions of nefarious actors seeking to commit fraud, sabotage, or corrupt manufactured products.

Improving the traceability of goods and materials throughout the supply chain is critical to identifying disruptions and mitigating these risks. This report introduces a Meta-Framework designed to organize, link, and query traceability data across manufacturing supply chains. The goal of the framework is to enhance end-to-end traceability, providing stakeholders with the tools needed to trace product provenance, ensure regulatory compliance, and bolster the resilience of the U.S. manufacturing supply chain.

Keywords

pedigree; provenance; supply chain traceability; traceability chain.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Note to Reviewers

NIST welcomes feedback and input on any aspect of NIST IR 8536 and additionally proposes a list of non-exhaustive questions and topics for consideration:

1. How well does the Meta-Framework data model relate to existing supply chain practices and your organization? Are there significant gaps between your current practices and the Meta-Framework that this paper should address?

2. How do you expect this white paper to influence your future supply chain traceability practices and processes?
3. How do you envision using this white paper? What changes would you like to see to increase/improve that use?
4. What suggestions do you have on changing the format of the information provided?
5. Is the guidance here sufficient to identify and address supply chain traceability? Are there changes or additional guidance that the authors should consider?

All comments are subject to release under the Freedom of Information Act.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:
    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: blockchain_nccoe@nist.gov

Table of Contents

List of Tables

List of Figures

Executive Summary

Ensuring supply chain traceability is critical for maintaining product authenticity, compliance, and security in today's complex, globalized manufacturing ecosystems. As manufactured goods such as microelectronic components move through the supply chain to employment of a final product in critical infrastructure--stakeholders face increasing challenges in maintaining visibility into the history and provenance of these products. The framework enables end-to-end traceability by linking records from different ecosystems. The Massachusetts Institute of Technology (MIT) Sustainable Supply Chain Lab notes that "While the urgency to act is high [to increasing traceability & transparency], most companies currently lack the capability to understand what is happening in their supply chains. At the same time, suppliers and producers are limited in their access to technologies that connect them with supply chain partners." [1]. This lack of traceability presents significant risks, including the potential introduction of counterfeit goods, non-compliance with regulatory requirements, and threats to the integrity of critical infrastructure systems.

This paper presents a Meta-Framework designed to address these challenges by providing a structured, industry-tailorable approach to capturing, linking, and retrieving traceability data across diverse supply chains. The Meta-Framework enables stakeholders to record and access traceability information securely through trusted data repositories, or ecosystems, facilitating the creation of Traceability Chains—verifiable, chronological records of product-related events throughout the supply chain.

The Meta-Framework uses several key components designed to enhance the visibility, reliability, and integrity of supply chain event data, ensuring stakeholders can discover, understand, and trust the traceability information. The following key principles support a secure and adaptable approach to supply chain traceability.

- **Data Model and Ontologies:** The Meta-Framework supports a flexible data model that allows industry-specific stakeholders to define their syntax and semantics of traceability data for use in their Traceability Records. By enabling industry-specific stakeholders to enforce consistent data definitions across their ecosystems, the Meta-Framework ensures that traceability data is consistent within industry sectors, understandable, and exchanged seamlessly, regardless of the industry or regulatory environment.
- **Traceability Records:** These are the core units of supply chain event data captured throughout the supply chain. Each traceability record documents a supply chain event, such as manufacturing, shipping, or receiving, and is securely stored in a trusted data repository. This allows stakeholders to fully discover the sequence of relevant supply chain events, creating a detailed and reliable record of the product's history.
- **Traceability Links:** To create a Traceability Chain, individual traceability records are linked through verifiable traceability links. These links allow stakeholders to trace a product's history in reverse chronological order, ensuring the integrity and authenticity of the entire supply chain process.

- **Trusted Data Repositories and Ecosystems:** Each industry defined and operated ecosystem serves as a secure data repository, responsible for storing and managing their industry-specific Traceability Records. These ecosystems are governed by industry-specific manufacturing supply chain stakeholders who define their supply chain event data to use in traceability records, which can draw from industry and regulatory standards and conventions to ensure that the data remains trustworthy, accessible, and protected from tampering.
- **External Reference Links:** The framework also allows for industry-specific external reference links to point to additional industry-specific data sources such as test data, third-party attestations or certifications that support more specialized use cases. These links can also be used to provide supplementary evidence for verifying product provenance and pedigree.

These elements allow the Meta-Framework to address some of the key challenges facing supply chain stakeholders by:

- **Challenge #1: Information is stored in disjointed and isolated repositories -** The Meta-Framework mitigates this challenge by establishing data repositories accessible by authorized users.
- **Challenge #2: Inconsistent semantic and data definitions -** The Meta-Framework mitigates this challenge by using industry defined data models and ontologies.
- **Challenge #3: Difficulty validating information integrity -** The Meta-Framework mitigates this challenge by using traceability links and hash-based validation to verify the data integrity of traceability data.

A key strength of the Meta-Framework is its application across industry sectors, as illustrated in this National Institute of Standards and Technology Internal Report (NIST IR) through a simplified manufacturing supply chain scenario. As manufactured goods such as microelectronic components move through the supply chain to employment of a final product in critical infrastructure, the framework enables end-to-end traceability by linking records from different ecosystems. Stakeholders can trace products through the supply chain—retrieving records from trusted data repositories—using traceability links that provide an auditable trail of each product's supply chain history.

As manufactured goods such as microelectronic components move through the supply chain to employment of a final product in critical infrastructure, the framework enables end-to-end traceability by linking records from different ecosystems. By capturing and storing traceability data throughout the supply chain, the Meta-Framework empowers stakeholders to address evolving market-driven and regulatory-driven use cases. It supports product validation, risk management, and regulatory compliance, ensuring that products meet the highest standards for authenticity, quality, and ethical sourcing.

Overall, the Meta-Framework provides a flexible and scalable approach for enhancing supply chain traceability across industry sectors. By leveraging trusted data repositories, defined and documented data models, and secure traceability links, the framework ensures that stakeholders can trace the provenance and pedigree of products with confidence. As supply chains become more complex and globalized, the Meta-Framework offers a critical tool for securing the integrity of supply chain operations and safeguarding critical infrastructure systems.

1. Supply Chain Traceability

The security, resilience, and assurance of national manufacturing and critical infrastructure supply chains are vital to maintaining the overall health, security, and economic strength of the United States (U.S.). As global supply chains become more complex, discerning the origins of products becomes increasingly challenging. MIT Sustainable Supply Chain Lab notes that "While the urgency to act is high [to increasing traceability & transparency], most companies currently lack the capability to understand what is happening in their supply chains. At the same time, suppliers and producers are limited in their access to technologies that connect them with supply chain partners." [1]. This lack of traceability presents significant risks, including potential introduction of counterfeit goods, non-compliance with regulatory requirements, and threats to the integrity of critical infrastructure systems.

The collection of traceability and other supply chain data, as discussed in "Cybersecurity supply chain risk management for systems and organizations.", National Institute of Standards and Technology Special Publication (NIST SP) 800-161r1, [2] can inform the pedigree of products and potentially supports continuous monitoring and risk assessment throughout the supply chain. Provenance and pedigree information can help meet growing regulatory requirements such as ethical sourcing, protect consumers against counterfeit or substandard products and materials, and expose and deter other nefarious activity occurring in the supply chain. Specifically, aggregated provenance information can enable supply chain participants to detect early indicators of degraded supply chain resiliency, such as product or material shortage, logistical disruption, and other threats to supply chain continuity. The discoverability, accessibility, and understandability of traceability data allows for effective risk communication and reporting, ensuring that stakeholders are well-informed and can respond promptly to emerging risks.

Supply chain traceability, as part of broader supply chain transparency, is studied from a bibliographic perspective in "Supply chain transparency: A bibliometric review and research agenda" [3]. In this study, the authors found clusters of research, one of which was "Cluster 5: supply chain transparency for traceability," which is directly related to the traceability topic of this NIST IR. However, the authors also found that this cluster's research papers "…are primarily focused on organizational processes to achieve effective traceability of supply chains." Thus, little research is devoted to manufacturing supply chain-wide interoperability where all applicable and authorized stakeholders can discover, retrieve, and understand relevant supply chain event data, and links to predecessor supply chain event data, such as addressed in this NIST IR.

Fundamentally, achieving supply chain traceability objectives requires stakeholders to have access to information. This report describes a Meta-Framework that supports capturing and accessing pedigree and provenance information to support supply chain traceability, ensuring stakeholders can discover, understand, and trust the traceability information.

The rest of this section is organized as:

- **Traceability Activities** – Representative activities for traceability in manufacturing supply chains.

- **Traceability Challenges** – Key challenges that inhibit realization of supply chain traceability activities.
- **Goals** – Project objectives for the Meta-Framework associated with overcoming the traceability challenges and addressing the traceability activities.
- **Approach** – The approach for establishing a Meta-Framework to improve traceability.

1.1. Traceability Activities

In today's increasingly complex and globalized markets, the ability to trace products and components through the supply chain is essential for ensuring product integrity, compliance with regulations, and meeting consumer expectations. The following subsections will delve into representative activities and explore how supply chain traceability can address a broad spectrum of challenges. By examining these common scenarios, organizations can gain a deeper understanding of the value in implementing robust traceability systems.

1.1.1. Market-Driven: Component Verification

In today's competitive marketplace, customers demand greater transparency and assurance regarding the products they purchase, particularly when it comes to the quality and authenticity of components. As supply chains have become increasingly complex, the ability to verify the origins and journey of a product component is critical for maintaining customer trust and satisfaction.

Consider a scenario where an end customer requires verification that a specific component within a final product is genuine and meets all necessary quality standards. This need for verification arises from several market-driven factors, including concerns about counterfeit components, the desire to maintain brand reputation, and the necessity to meet customer expectations for product reliability.

To address these concerns, manufacturers and integrators must provide detailed traceability data that tracks the component from its origin through the entire supply chain. Additionally, this data must be accessible and verifiable by the end customer, allowing them to confirm the authenticity of the component and its compliance with specified standards.

By implementing robust traceability methods, organizations can also enhance their market position by providing the transparency that customers increasingly expect. This not only helps protect against infiltration of counterfeit goods but also reinforces brand trust. Additionally, the ability to verify component authenticity can be a differentiator in the market, enabling companies to demonstrate their commitment to quality and reliability.

1.1.2. Regulatory-Driven: Ethical Sourcing Verification

As global supply chains expand and evolve, regulatory bodies have increasingly emphasized the importance of ethical sourcing, particularly regarding raw materials used in manufacturing. Governments and industry regulators are requiring companies to ensure that the materials they source, especially those used in sensitive products like electric vehicle (EV) batteries, adhere to ethical standards such as ethical sourcing and labor laws. This regulatory-driven traceability is crucial not only for legal compliance but also for maintaining public trust and corporate responsibility.

To comply with these regulations, manufacturers must track the origin of raw materials through the entire supply chain. This involves documenting the kind and location of source materials and ensuring that they come from suppliers who meet the required ethical standards for their country, industry, and intended marketplace. The traceability data must be robust enough to satisfy government agency requirements and enable companies to demonstrate compliance during audits or inspections.

By providing clear and accessible traceability data, companies can not only comply with regulatory demands but also enhance their reputation by showcasing their commitment to ethical practices. This is increasingly important as consumers and investors alike prioritize corporate responsibility and sustainability.

1.2. Traceability Challenges

While traceability can address both market-driven demands for transparency and regulatory requirements for ethical sourcing, achieving traceability across complex supply chains is difficult. Traceability is typically practiced by the acquirer who determines product pedigree and provenance (colloquially described as "supply chain illumination") as documented in NIST SP 800-161r1 [2].

This method requires gathering information from multiple supply chain stakeholders involved in production processes. Gathering this data can be difficult and time consuming, especially for complex supply chains. Stakeholders attempting to retrieve data further back in the production process are particularly impacted.

Figure 1. Challenges to Component or Assembly Verification Across Stakeholder Tiers shows how a component's original manufacturer may be several supply chain stakeholder tiers away from the interested acquirer. As a result, obtaining information on the component or assembly may be difficult and time consuming.

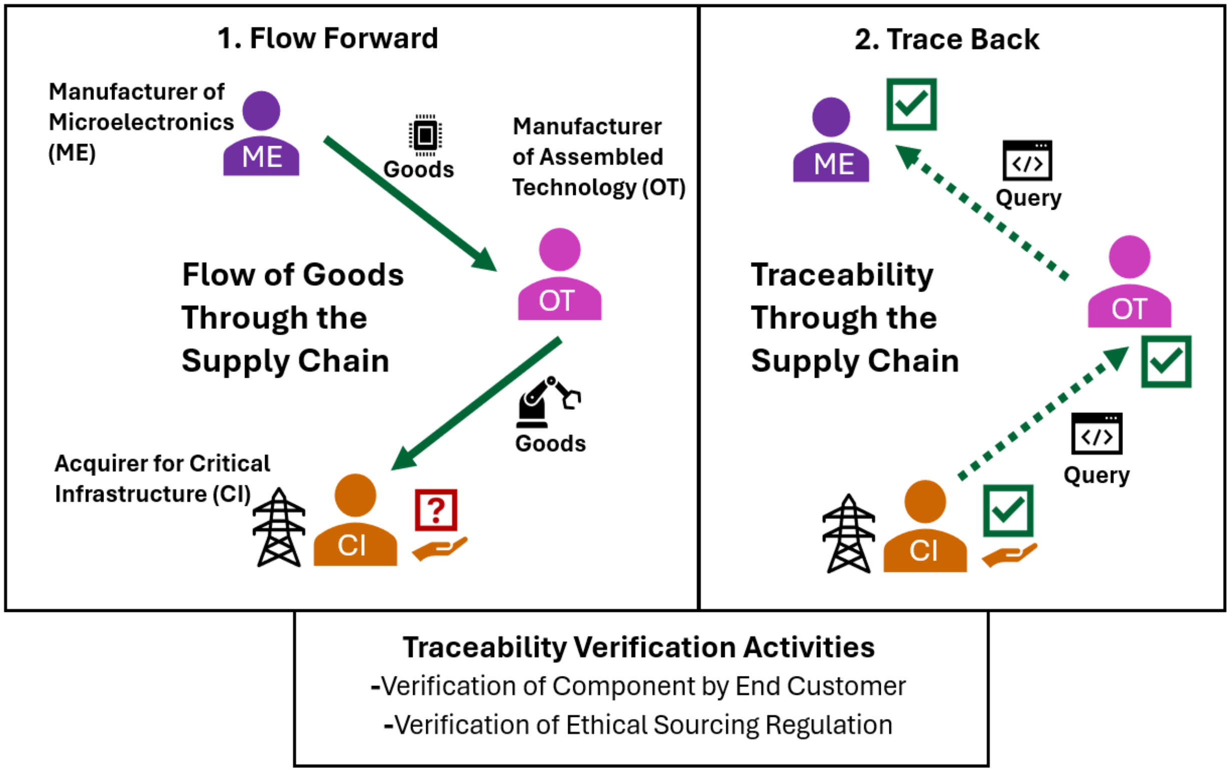

Figure 1. Challenges to Component or Assembly Verification Across Stakeholder Tiers

From this generalization of the path products take and how a stakeholder researches supporting pedigree and provenance information, the following primary challenges associated with establishing supply chain traceability were identified.

1.2.1. Challenge #1: Information is stored in disjointed and isolated repositories.

Situation: Information that can support supply chain pedigree and provenance may only be available in private or otherwise inaccessible data repositories or data stores limiting the ability for manufacturing partners and external stakeholders to obtain this information.

Impact: Without access to provenance and pedigree information, both manufacturers and consumers may be unable to ascertain if the components and products are genuine or conform to regulatory requirements.

Resolving this challenge: Pedigree and provenance information must be accessible to authorized stakeholders. When information spans multiple organizations, the information must also be verifiably linked to allow authorized stakeholders to obtain the manufacturing history of the product and components.

1.2.2. Challenge #2: Inconsistent semantic and data definitions.

Situation: Semantic data gaps occur when supply chain participants write or convey supply chain data in records aligned with stakeholder-internal data semantic rules, which may be inconsistent with, or potentially misunderstood by other supply chain stakeholders.

Impact: Supply chain data fields can be misaligned or mismatched from one manufacturing stakeholder data record to another, since each stakeholder writes its own isolated and sometimes private data. Presently, no consistent means exist to align data across the supply chain.

Resolving this challenge requires: Industry and regulatory bodies must establish information standards that provide the key data elements for their products and components. These standards should ensure the traceability information is sufficient to support pedigree and provenance for the products. As a result, traceability systems that store this information must provide the flexibility to support different industry and regulatory standards and conventions while still providing sufficient consistency to enable automation to validate that records are consistent with industry standards.

1.2.3. Challenge #3: Difficulty validating information integrity

Situation: Ensuring the integrity of pedigree and provenance information presents significant challenges for both end customers and intermediate manufacturers. Data integrity, as defined by the Computer Security Resource Center (CSRC) is:

"The property that data has not been altered in an unauthorized manner.
Data integrity covers data in storage, during processing, and while in transit."

The complexity of modern supply chains means that data is generated, managed, and transmitted by a variety of distinct stakeholders, each potentially using different approaches to securing and documenting their data. Presently, there does not appear to be a consistent method that exists to validate pedigree and provenance integrity across manufacturing supply chains.

Impact: Variation in integrity controls can lead to inconsistent quality and increase the difficulty for stakeholders to validate the authenticity of the pedigree and provenance information.

Resolving this challenge requires: Protocols for information sharing that ensure consistency and reliability across all stages of the supply chain is required. By promoting transparency and alignment in integrity practices, stakeholders can validate the integrity of the pedigree and provenance information on which they will rely to make decisions.

1.3. Goals

The primary goal of this Meta-Framework project is to describe and demonstrate a method for enhancing supply chain traceability across multiple manufacturing supply chain sectors, enabling stakeholders to access information required to trace product provenance and verify the pedigree of products within the supply chain. The specific goals include:

- **Enhancing Accessibility and Visibility:** Improve the accessibility and visibility of supply chain information by enabling stakeholders to record and retrieve data from trusted, accessible data stores. These data stores will link supply chain data, facilitating robust traceability.
- **Establishing a Flexible Data Model:** Develop a flexible data model that supports industry and regulatory efforts in establishing ontologies to provide syntactically and semantically consistent supply chain data for stakeholders.
- **Improving Data Integrity:** Enhance the integrity of traceability information by providing mechanisms that allow stakeholders to validate the data obtained from various organizations.

To achieve these goals, the Meta-Framework will discuss and define several key concepts including construction of traceability chains composed of traceability records that store pedigree and provenance information captured during specific production events. Additionally, the framework will address establishment of trusted data repositories, ecosystems, and methods for creating traceability links that verifiably connect traceability records both within and across these ecosystems.

To demonstrate that the Meta-Framework has achieved these goals, this report will outline its application to the following use cases.

Recording Traceability Records: Enable the recording of traceability records into trusted data repositories with traceability links to applicable predecessor records. This will support construction of a traceability chain that meets traceability use case requirements.

Retrieving Traceability Records: Facilitate the retrieval of traceability records from trusted data repositories. Using traceability links, stakeholders will be able to trace back through a chain of traceability records across one or more trusted data repositories, thereby obtaining comprehensive provenance and pedigree information.

1.4. Approach

This document outlines a Meta-Framework designed to record and retrieve industry-agnostic traceability records from trusted data repositories. The goal is to enable authorized stakeholders to create a traceability chain that supports both market and regulatory-driven traceability use cases.

Recognizing the need to stay focused on the core objective of traceability, this approach prioritizes key traceability activities, such as production, shipment, receiving, and employment, while acknowledging that certain broader supply chain functions (e.g., business-to-business transactions, industry-specific semantics) fall outside the framework’s primary scope. These functions, while important, are considered ancillary to the main goal of ensuring a secure and verifiable traceability chain and have been set aside or accommodated to maintain the clarity and effectiveness of the Meta-Framework.

The approach builds on the foundational work established in NIST IR 8419, "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability" [4], and NIST Project Description "Manufacturing Supply Chain Traceability with Blockchain Related Technology: Reference Implementation" [5]. This approach accommodates both blockchain and legacy data storage technologies to enable wide adoption.

The project emphasizes collaboration and technical exchange with industry groups, standards bodies, academic researchers, and other relevant stakeholders. By engaging with these diverse parties, the project aims to discover, develop, and refine use cases that demonstrate the value of traceability in supply chain data. This collaborative effort will contribute to establishing robust methods for verifying product provenance and pedigree across complex supply chains.

1.5. Audience

The purpose of this report is to describe a framework that facilitates storage and linking of information from manufacturers and integrators, to support supply chain traceability use cases related to product pedigree and provenance. The framework introduces the concept of ecosystems, which serve as trusted, potentially third-party entities that maintain industry-recognized data repositories. These repositories enable manufacturers and integrators to securely record their traceability information, while allowing stakeholders (e.g., customers) to retrieve product-related data. This data supports establishment of a traceability chain, a collection of linked records that provides detailed information on product pedigree and provenance, enhancing transparency, accountability, and security across the supply chain.

The intended audience for this report includes organizations and industry consortia that are considering establishing and operating ecosystems, as well as manufacturers, integrators, and possibly resellers who seek to integrate into these ecosystems and record traceability data. Other stakeholders include policymakers, regulators, academic researchers, and cybersecurity professionals who have an interest in the integrity and security of supply chains.

2. Meta-Framework Overview

The Meta-Framework is designed to enhance supply chain traceability across diverse manufacturing sectors by providing a structured approach to recording, linking, and retrieving traceability information that can inform pedigree and provenance of products. This framework is intended to be industry-agnostic, allowing it to be applied across supply chains, regardless of the specific products or components involved. The overarching goal is to enable stakeholders to establish a comprehensive traceability chain that supports both market-driven and regulatory-driven use cases. Core components of the Meta-Framework include:

- **Data Model and Ontologies:** The Meta-Framework provides a flexible data model that can be adapted to different industries and regulatory environments. This enables ecosystem stakeholders to establish data dictionaries and ontologies that provide syntactic and semantic consistency for data in traceability records, such that any other stakeholder can understand the applicable supply chain event data and make decisions.
- **Traceability Records:** At the heart of the Meta-Framework are traceability records, which capture essential information about product pedigree and provenance at various stages or events within the supply chain. These records are stored in trusted data repositories, ensuring that the information is secure, accessible, and verifiable by authorized stakeholders.
- **Traceability Links:** The Meta-Framework introduces traceability links that link individual traceability records into a traceability chain. These links are designed to be verifiable, ensuring that stakeholders can confidently trace the history of a product or component through various stages of the supply chain, across different repositories, and between different organizations.
- **External Reference Links:** Optional links may include external data sources relevant to the Traceability Record, such as test data, documentation, or third-party attestations that may be too large to include within the traceability record itself. While external reference links can be important and even required by industry or regulatory standards, the Meta-Framework acknowledges that this information may be stored outside the trusted data repository and may not be immediately accessible to all stakeholders without further coordination. For example, the Internet Engineering Task Force (IETF) Supply Chain Integrity, Transparency, and Trust (SCITT) chartered standard [6] provides a description of an HTTP-based Representational State Transfer (REST) API interface that can be implemented to provide 3rd party attestation of claims about software. As such, the Meta-Framework recommends that the data captured within the traceability record, particularly through the variable data block, should be sufficient to address general pedigree and provenance use cases. External reference links, while valuable, should be considered supplemental evidence that may be requested and validated by stakeholders as needed for specialized use cases or risk management purposes.
- **Trusted Data Repositories:** The Meta-Framework advocates for the use of trusted data repositories in ecosystems, where traceability records can be securely stored and accessed. These repositories serve as the backbone of the Traceability Chain, linking

supply chain event data from multiple stakeholders and ensuring that it remains intact and trustworthy throughout its lifecycle.

The Meta-Framework is designed to address key challenges faced by stakeholders including:

- **Challenge #1: Establishing Consolidated Data Repositories and Enhancing Accessibility -** The Meta-Framework describes the use of trusted data repositories, which ecosystems can establish to securely store and manage traceability information. These repositories enable stakeholders to access and retrieve traceability data efficiently, improving transparency and visibility across the supply chain. By outlining best practices for the structure and governance of these repositories, the Meta-Framework ensures that traceability data can be securely shared and accessed across the supply chain.
- **Challenge #2: Enforcing Consistency and Semantic Integrity Through Standardized Data Models -** The Meta-Framework incorporates standardized data models and provides the flexibility to support industry and regulatory ontologies, ensuring that traceability records maintain consistency in both syntax and semantics. This consistency, enforced through ecosystem data dictionaries, ensures that all stakeholders use and interpret traceability data in a uniform way. By addressing the challenge of data consistency, the framework helps industry and regulatory bodies ensure that traceability data is interoperable and meaningful across different sectors and use cases.
- **Challenge #3: Establishing Verifiable Trust in Traceability Data -** The Meta-Framework introduces mechanisms such as traceability links with hash-based validation to ensure data integrity. These mechanisms allow stakeholders to verify the authenticity and accuracy of supply chain traceability records, creating trust points that can be relied upon by both ecosystem stakeholders and non-ecosystem stakeholders (e.g., regulators, customers). Some supply chain integrity efforts are making inroads toward specific types of other trust, such as hardware component verification "...that the internal components of the computing devices they acquire are genuine and have not been unexpectedly altered during manufacturing or distribution processes." [7]. Whereas the focus of this NIST IR is to establish the mechanisms to ensure that recorded supply chain event data across manufacturing sectors maintains data integrity.

By providing these verification tools, the framework helps establish and secure the traceability chain of supply chain event data against tampering and unauthorized modifications, thereby addressing the need for verifiable trust. In summary, the Meta-Framework addresses the key challenges by improving data accessibility and visibility, ensuring consistent and interoperable data across stakeholders, and providing tools to establish and verify the trustworthiness of traceability data. This holistic approach supports a wide range of traceability use cases, whether driven by market demands or regulatory requirements.

2.1. Components of the Meta-Framework

The Meta-Framework is composed of several key components that collectively enable comprehensive supply chain traceability. These components work together to ensure that traceability data is accurately recorded, securely stored, and easily accessible to authorized stakeholders. The Meta-Framework is designed to be flexible and adaptable, allowing it to be applied across diverse industries and regulatory environments.

The Meta-Framework also emphasizes the importance of a flexible data model and ontologies that standardize how traceability data is defined, recorded, and interpreted across different stakeholders. This standardization ensures consistent communication and collaboration among all participants in the supply chain. The following sections provide detailed explanations for the key Meta-Framework components, their roles, and how they interact to support effective supply chain traceability data model and ontologies.

The foundation of the Meta-Framework lies in the stakeholders of the applicable ecosystem developing a flexible and adaptable data model, informed by well-defined industry and regulatory established ontologies. The data model is designed to accommodate the diverse needs of various industries and regulatory environments, ensuring that traceability data is recorded, stored, and interpreted in a consistent and meaningful way across the supply chain.

Additionally, the data model provides constraints and definitions of the data content for supply chain event data records, recorded as traceability records. It provides the necessary guidelines for capturing critical information about products, components, and their movements through the supply chain. The model is designed to be both comprehensive and adaptable, allowing it to meet the unique requirements of different sectors while maintaining a core set of data elements that are consistent across all implementations. This consistency is crucial for ensuring that all stakeholders, regardless of their specific industry or role in the supply chain, can accurately record, retrieve, and interpret the information. The key components of the data model include:

- **Fixed Data Elements:** A standardized set of essential data fields that must be included in every traceability record. These elements provide a consistent baseline of information that is critical for establishing product pedigree and provenance.
- **Variable Data Block:** A customizable section within each traceability record that allows stakeholders to include additional, sector-specific information. This flexibility ensures that the data model can accommodate the varying needs of different industries while still adhering to a common framework. The contents of the variable data block will vary depending on the specific component or event being recorded, allowing for detailed capture of information relevant to each unique context.

Ontologies within the Meta-Framework play a crucial role in defining the information captured in the Variable Data Block. Industry-specific ontologies provide a shared vocabulary and set of definitions for these customizable data elements, ensuring that the data remains meaningful and actionable across different stakeholders and sectors. Ontologies allow for precise definition of information relevant to specific components, events, and use cases, particularly those related to product pedigree and provenance. Specifically, industry and regulatory ontologies for the Meta-Framework are designed to:

- **Standardize Variable Data Elements:** Provide a common set of terms and definitions that can be applied within the variable data block to capture detailed, context-specific information in a consistent manner.

- **Ensure Semantic Consistency:** Align the interpretation of data across different sectors and regulatory environments, particularly in relation to the unique information captured in the Variable Data Block, ensuring that traceability data retains its intended meaning throughout the supply chain.
- **Support Interoperability:** Enable seamless integration and data exchange between different systems, organizations, and industries by ensuring that even the customized data in the variable data block is standardized and interpretable across diverse contexts.

Together, the data model and ontologies provide the structural and semantic foundation necessary for effective traceability. By ensuring that traceability data is both syntactically and semantically consistent—especially in the context of industry-specific details—the Meta-Framework enables stakeholders to communicate and collaborate effectively, ultimately enhancing the visibility, integrity, and reliability of supply chain information.

2.1.1. Traceability Records

Traceability Records are a central component of the Meta-Framework, acting as the foundational units for capturing and documenting supply chain events. Beyond recording data, these records also play a vital role in ensuring the integrity, visibility, and trustworthiness of supply chain information. They represent verifiable evidence of specific supply chain events such as creation, modification, or transfer of products or components. Recording these events can help establish a clear, auditable history of a product's production and support both market-driven and regulatory-driven use cases.

Given the diverse nature of global supply chains, traceability records are designed to be interoperable across multiple systems and organizations. This interoperability is facilitated by the standardized approach to define core data elements along with providing a variable data block for flexibility to accommodate industry- and regulatory-specific needs. Additionally, traceability records are structured to support a wide range of use cases. The flexibility provided by the Variable Data Block allows organizations to adapt their traceability practices as new requirements emerge, without disrupting the overall integrity of the traceability chain. As a result, traceability records can be shared and understood across different platforms and technologies, promoting a more connected and transparent supply chain.

Figure 2. General Construct of Traceability Records shows a Traceability Record being stored in a trusted data repository as part of a larger transaction record or data block. The meta-framework allows transactions to include additional information that maybe required by the trusted data repository such as user authentication or other regulatory requirements beyond the traceability record information. It is important to note that while blockchain is depicted in Figure 2, the Meta-Framework is technology-agnostic. This flexibility allows organizations to implement trusted data stores using the most appropriate technology for their specific needs, ensuring that traceability records are securely stored and accessible to authorized stakeholders.

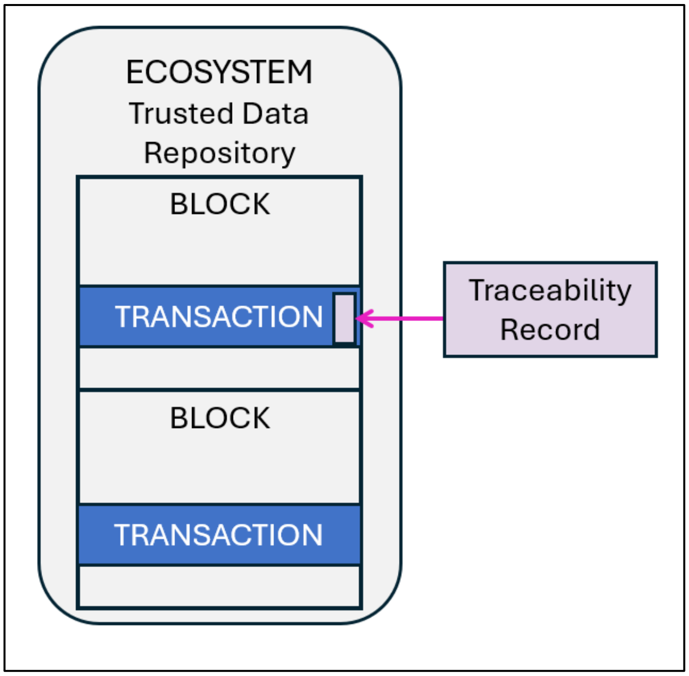

Figure 2. General Construct of Traceability Records

Maintaining the security of traceability records is also important for maintaining trust and reliability. To support trust and reliability, each record is stored in a trusted data repository and protected against unauthorized alterations. The meta-framework emphasizes the importance of validating these records at each stage of the supply chain, providing stakeholders with increased confidence that the data they rely on is accurate and unaltered. This validation process is supported by a combination of the secure environment provided by the trusted data repository and the use of verifiable traceability links that connect records within the traceability chain.

2.1.2. Traceability Links and Chain

A Traceability Chain serves as a critical tool for allowing stakeholders to traceback and obtain supply chain event data, such as product pedigree and provenance information. A Traceability Chain is incrementally constructed as supply chain events occur and new traceability records are recorded and linked to predecessor traceability records. The resulting traceability chain represents the relevant supply chain events, in order of occurrence, as the components and assemblies move through the supply chain, ultimately to the end customer or acquirer. As an example, Figure 3. General Construct of a Traceability Chain depicts one traceability record linking to a predecessor traceability record in a different trusted data store. The traceability record is depicted in more detail, relative to Figure 2. General Construct of Traceability Records to highlight that the Traceability Link is one of the constituent data elements in the Traceability Record.

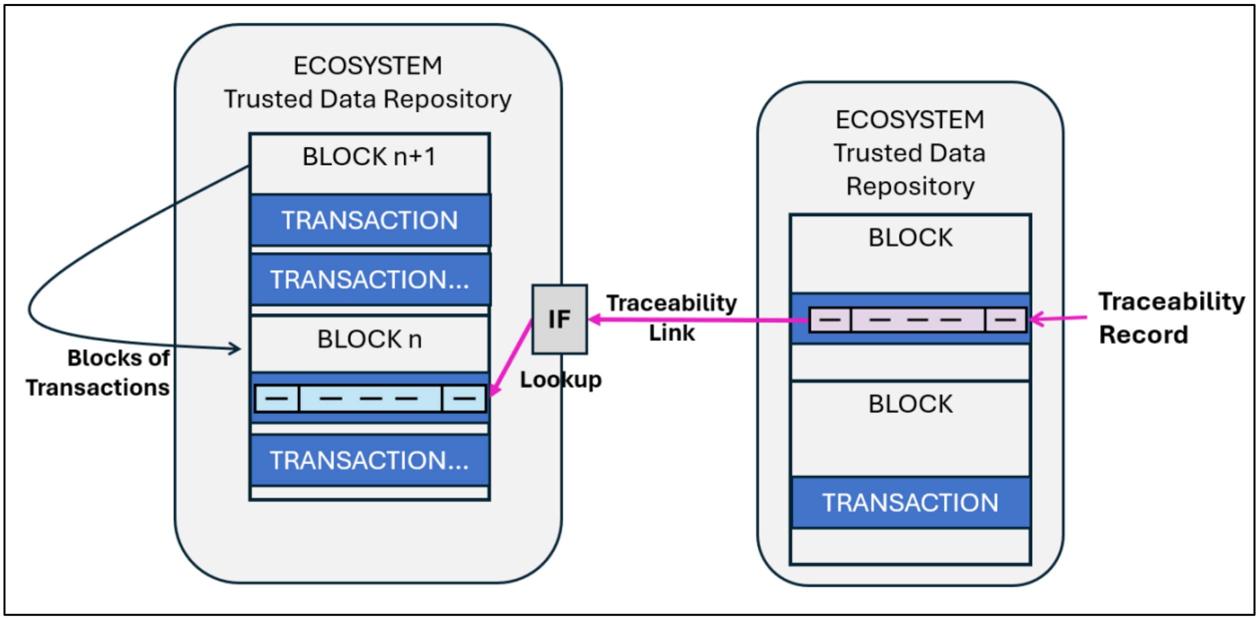

Figure 3. General Construct of a Traceability Chain

The traceability link is a composite data element that facilitates creation of a secure and accessible traceability chain. These links are followed through interfaces provided by the ecosystems in which the records are stored, ensuring that access is controlled, and the integrity of the records is maintained and verifiable. This controlled access is crucial for protection sensitive supply chain data while also allowing authorized stakeholders to verify the authenticity and provenance of products. When tracing back through a traceability chain, the resulting set of retrieved traceability records is a traceability record set.

2.1.3. Trusted Data Repositories and Ecosystems

Ecosystems provide trusted data repositories and the essential technical and governance infrastructure to support one or more manufacturing stakeholders within a specific manufacturing supply chain sector. A foundational purpose of ecosystems is to establish and maintain the trusted data repository to support the data management needs of the ecosystem stakeholders. These repositories enable recording and later retrieval of traceability records by authorized stakeholders using an Internationalized Resource Identifier (IRI), such as a URL, through a secure interface. The trusted data repositories provide the mechanisms required to maintain the integrity, accessibility, and security of the traceability data.

Trusted data repositories can be implemented using either traditional database technologies or blockchain or similar distributed ledger technologies. The Meta-Framework is designed to work seamlessly with both types of technology, ensuring that the method for constructing a traceability chain remains consistent regardless of the underlying infrastructure. To allow validation of traceability records independent of the technology implementation, traceability links include a hash signature of the preceding record. This hash signature serves as a tamper-detection mechanism from the moment the link is established, helping ensure that the data remains intact and unaltered.

Governance of the Trusted Data Repository is a crucial responsibility of the ecosystem to ensure that the data store remains secure, reliable, and aligned with the needs of the participating organizations. Key governance activities for the Trusted Data Repository include:

- **Procurement:** Overseeing the initial setup and deployment of the trusted data store infrastructure.
- **Sustainment:** Managing ongoing maintenance, including patches, updates, and necessary improvements to sustain the desired level of service.
- **Stakeholder Membership:** Managing the organizations, individuals, and entities along with their authenticators and authorizations within the ecosystems.
- **Data Management and Maintenance:** Enforcing data standards, maintaining traceability records, and ensuring data security and availability.

By providing a robust framework for data management, governance, and security, ecosystems ensure that all stakeholders can confidently participate in the supply chain, and record supply chain event data, knowing that the integrity of the supply chain event data is maintained throughout the product lifecycle, and is traceable afterwards. While ecosystem governance is necessary and recognized as a key component supporting the Meta-Framework, detailed governance guidance and specific implementations are outside the scope of this paper.

2.2. Traceability Chain Across Supply Chain Ecosystems

Figure 4. Value and Supply Chain Traceability Events Across Ecosystems illustrates how the Meta-Framework can be used to support the capture, storage, and tracing of traceability records across a supply chain that spans multiple ecosystems, from component production to final product deployment [5].

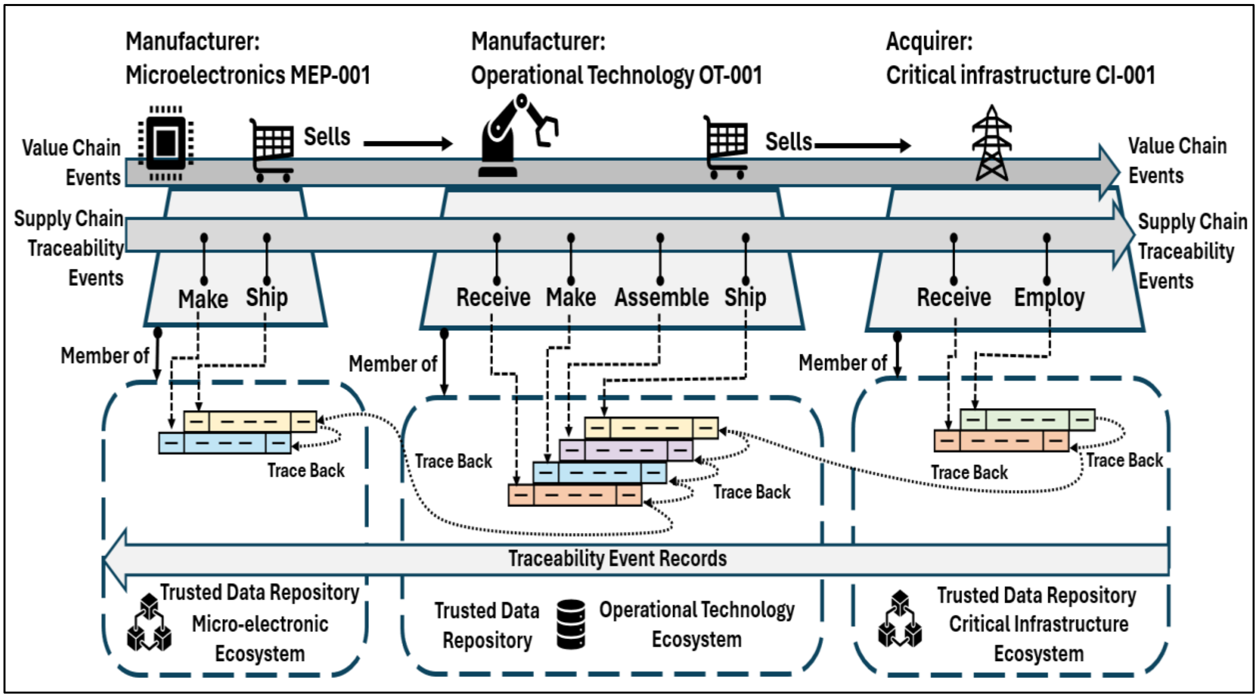

Figure 4. Value and Supply Chain Traceability Events Across Ecosystems

This process involves different stakeholders and trusted data repositories, each responsible for capturing traceability records at various stages of production and product movement. In this example, the manufacturing process involves three key players:

- **Microelectronics Manufacturer (MEP-001):** The process begins with the microelectronics manufacturer, which produces and ships a chip to an industrial controls manufacturer. Each event—make and ship—is captured as a traceability event and recorded in the trusted data repository of the Microelectronics Ecosystem. These events create the initial entries in the Traceability Chain for this product.
- **Operational Technology Manufacturer (OT-001):** The industrial controls manufacturer, upon receiving the chip, logs the receipt event into its Operational Technology Ecosystem. Subsequent activities, including making software and assembly of the control system, as well as shipping of the final assembly to a power plant, are recorded as additional traceability events. Each of these events is recorded in its respective trusted data repository, extending the Traceability Chain.
- **Acquirer: Critical Infrastructure (CI-001):** Finally, the power plant, acting as the acquirer, receives the assembly and logs this event. The final decision to employ the product in the operational environment is captured as a traceability event in the Critical Infrastructure Ecosystem.

As the figure demonstrates, each stakeholder contributes to the growing set of traceability records, incrementally extending the traceability chain as products move through the supply chain. The role of each ecosystem is critical in securely storing these records in trusted data repositories, where the information is available for future retrieval.

The trace-back arrows in the figure represent how traceability data can be accessed in reverse chronological order to verify the product's history. Starting from the critical infrastructure's acquisition of the assembly, stakeholders can trace back through the trusted data repositories of each ecosystem involved in the product's lifecycle. This reverse tracing allows stakeholders to verify the provenance and pedigree of components, ensuring product authenticity and compliance with regulatory or quality standards.

By capturing traceability information at every stage—make, ship, receive, assemble, and employ—the Meta-Framework facilitates end-to-end visibility into the entire supply chain. The traceability chain, constructed by linking traceability records across multiple ecosystems, ensures that complete historical data is available for product verification, risk management, and regulatory compliance long after the product has been delivered.

3. Meta-Framework Data Model

The traceability record concept includes: (a) supply chain event data supporting pedigree and provenance, (b) Traceability Links between traceability records, across trusted data repositories as applicable, incrementally growing a traceability chain, (c) external links to additional manufacturing or event related data that may be too large to be stored with the traceability record or may contain sensitive information the requires additional safeguards and protections. Traceability records are specialized as sub-classes to distinguish major types of manufacturing events, such as Make, Assemble, Ship, Receive, and Employ. Figure 5. Overview Class Model depicts the traceability record subclasses in the context of their Traceability Link relationships. These subclasses represent distinct supply chain events in the progression along manufacturing supply chain activity timelines.

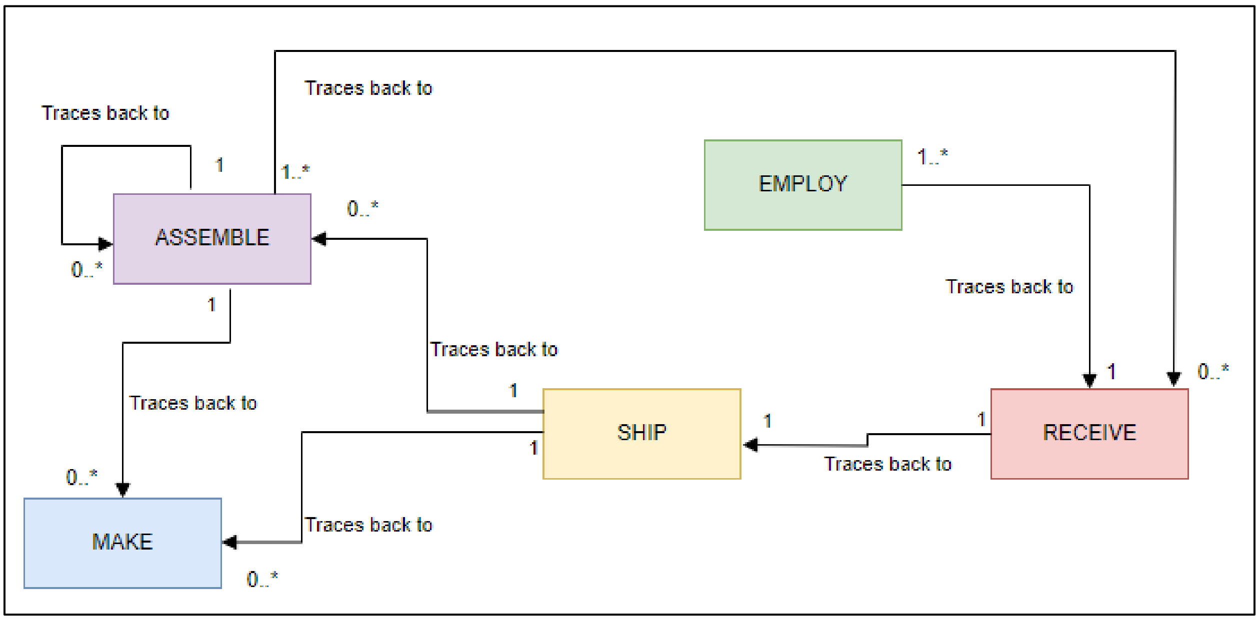

Figure 5. Overview Class Model

The supply chain events represented in the model are Make, Assemble, Ship, Receive, and Employ. Following the data model's traceability records via their traceability links demonstrates end-to-end traceability. For example, an Employ Traceability Record will contain a traceability link to the corresponding Receive Traceability Record. Thus, the end customer captures knowledge of when and by whom the product entered its facility. In turn, a Receive record contains a traceability link to a Ship Traceability Record, such that particulars of the items' transfer are understood. Transitively, the Ship record will then contain a Traceability Link to one or more applicable Assemble or Make Traceability Records. Further, an Assemble Traceability Record will link to each preceding Traceability Record that provided a component used in the assembly during the assemble event. These preceding supply chain events may be Make, Receive, or other Assemble events

There are other business rules needed that are not easily represented in a Class Model. They include:

- A Ship Traceability Record should contain at least 1 traceability link to an Assemble or Make Traceability Record.
- An Assemble Traceability Record should contain at least 2 traceability links. Each traceability link should be to an Assemble, Make, or Receive Traceability Record.
- A Make record will contain no traceability links, so Make records can be thought of as terminal nodes in a traceback graph of a traceability chain.

3.1. Traceability Records

As previously depicted in Figure 5. Overview Class Model, the traceability record subclasses are associated with several supply chain events identified as Make, Assemble, Ship, Receive, and Employ. This is in contrast to the event relationships depicted in Figure 6. Overview Class Diagram for Traceability Record. This section describes the supply chain events as data elements in the respective traceability record subclasses. Collectively, these subsections describe the fixed and variable data elements mentioned previously to support the traceability records and the ability to link these records to form the Traceability Chain. Figure 7. Traceability_Record Attribute depicts the attributes shared by the subclass events.

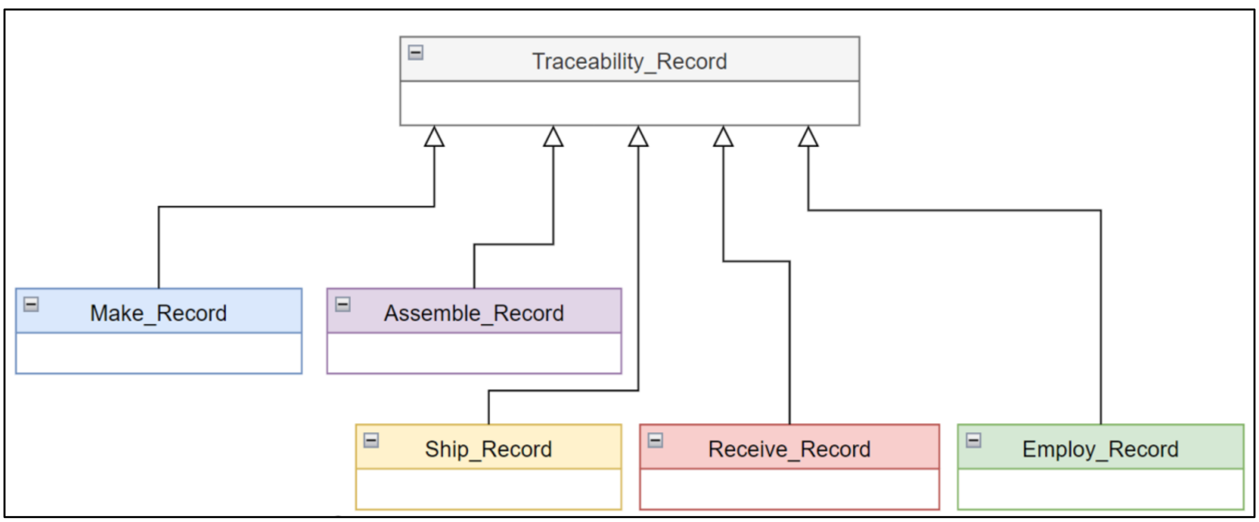

Figure 6. Overview Class Diagram for Traceability Record

The traceability record superclass has minimal attributes: a unique identifier (ID), date/time stamps, organization information, and an Event Type identifier to specify the associated subclass (Make, Assemble, Ship, Receive, and Employ) for the traceability record.

Traceability_Record
Record_ID
Event_Occurrence_Timestamp
Event_Recorded_Timestamp
Organization_ID
Organization_Unit_ID
Event_Type_ID (Make, Assemble, Ship, Receive, Employ)

Figure 7. Traceability_Record Attribute Structure

The attributes of the Traceability_Record superclass are available to each subclass of the traceability event record and are described below in Table 1. Traceability_Record Attribute Definitions.

Table 1. Traceability_Record Attribute Definitions

Data Attribute	Description
Record_ID	Globally unique identifier for each Traceability Record.
Event_Occurrence_Timestamp	Timestamp indicating the date and time of the traceability event occurrence.
Event_Recorded_Timestamp	Timestamp indicating the date and time of the recording of the traceability event within the ecosystem.
Organization_ID	Identifier for the organization responsible for the traceability event (e.g., Company or Business Unit Registered in Ecosystem)
Organization_Unit_ID	Identifier for the sub-unit of the organization where the traceability event occurred (e.g., Business Unit, Factory, or other organizational subunit where event occurred).
Event_Type_ID	Code indicating the subclass of traceability event for this record. This code should be one of Make, Assemble, Ship, Receive, or Employ[1].

3.2. Patterns for Traceability_Record Subclasses

As shown in Figure 6. Overview Class Diagram for Traceability Record above, the Meta-Framework defines subclasses of traceability records for each traceability event type. These subclass models are specialized for the type of event they support but make use of common

[1] This list would likely expand in the future as new traceability use cases require tracking of additional phases of a product life cycle beyond those considered in this paper.

patterns to meet the information needs for each event record subclass. Table 2. Traceability_Record Subclass Attribute Pattern describes the types of attributes that may appear in a subclass, though subclass specific names for these attributes are used within the subclass data definitions.

Table 2. Traceability_Record Subclass Attribute Pattern Description

Pattern Element	Description
Tracked Entity Identifier	Unique identifier for the instance(s) produced by or affected by the event.
Traceability Link Block	Contains zero or more Traceability_Link objects containing the information necessary for linking to precursor trackability records related to this event.
Record Data Schema Specification Identifier	Code or identifier used as a key for defining the data elements required for the contents of the data block and external reference block for the event record including this attribute.
Event Data Block	Variable length data field consisting of one or more key_value_pair objects providing data about the event or products. Requirements for these fields will be specified in the ecosystem data dictionary entry for the record data schema specification schema value given in the event record containing this data block. This would include the minimum set of data needed to verify the authenticity of a product.
External Reference Block	Contains zero or more External_Data_Link data objects containing the information necessary for linking to external data related to this event that may be stored in stakeholder systems or other repositories. This external data supplements data provided within traceability records and does not have the same requirements for persistence as traceability records. These links may not be immediately accessible to the stakeholders (they may have gated access).

To support the data model, the following data object structures are referenced in the subclass models.

3.2.1. Key_Value_Pair Data Objects

To represent a key / value pair, such as those that populate an event data block, the following data object is defined in Figure 8. Key_Value_Pair Attribute Structure and Table 3. Key_Value_Pair Attribute Definitions as:

Key_Value_Pair
Variable_Name
Variable_Value

Figure 8. Key_Value_Pair Attribute Structure

Table 3. Key_Value_Pair Attribute Definitions

Data Attribute	Description
Variable_Name	A label or identifier that describes the type of information being recorded. The variable name helps clarify what specific piece of data is being captured in the record.
Variable_Value	The actual data or information being captured. The variable value provides the specific details associated with the variable name.

3.2.2. External_Data_Link Data Objects

To capture the information for supporting links to external information, the following structure is defined in Figure 9. External_Data_Link Attribute Structure and Table 4. External_Data_Link Attribute Definitions for capturing an individual link:

External_Data_Link
Data_Type_ID
Resource_Link : Internationalized_Resource_Identifier
Parameter_Block : Key_Value_Pair [0..*]
Resource_Hash

Figure 9. External_Data_Link Attribute Structure

Table 4. External_Data_Link Attribute Definitions

Data Attribute	Description
Data_Type_ID	A code indicating the type of data linked.
Resource_Link	An IRI (such as a URL) to access a service to retrieve the data
Parameter_Block	A list of query parameters to submit to the trusted data repository to retrieve the requested traceability record
Resource_Hash	A hash of the record to verify the data integrity of the returned data. This is considered essential for the use cases the meta-framework supports (i.e., where data

Data Attribute	Description
	must be verifiable). If industry cannot determine data integrity, then this data cannot be trusted.

3.2.3. Traceability_Link Data Object

To capture the information for supporting links to precursor traceability records, the following structure is defined in Figure 10. Traceability_Link Attribute Structure and Table 5. Traceability_Link Attribute Definitions for capturing an individual link:

Traceability_Link
Resource_Link : Internationalized_Resource_Identifier
Parameter_Block : Key_Value_Pair [0..*]
Resource_Hash

Figure 10. Traceability_Link Attribute Structure

Table 5. Traceability_Link Attribute Definitions

Data Attribute	Description
Resource_Link	An IRI (such as a URL) to access a service to retrieve the data
Parameter_Block	A list of query parameters to submit to the trusted data repository to retrieve the requested traceability record.
Resource_Hash	A hash of the record to verify the data integrity of the returned data. This is considered essential for the use cases the meta-framework supports (i.e. where data must be verifiable). If industry cannot determine data integrity, then this data cannot be trusted.

The following subsections describe the traceability record subclasses' use of the patterns.

3.3. Make_Record Subclass

A Make event record includes the attributes of a Traceability_Record and extends them with attributes peculiar to the creation of a product where no previously tracked items are used as components. Make record specific attributes are shown in Figure 11. Make_Record Attribute.

Make_Record
Product_ID [1..*]
Make_Type_ID
Make_Data_Block : Key_Value_Pair [0..*]
Make_External_Reference_Links : External_Data_Link [0..*]

Figure 11. Make_Record Attribute Structure

The attributes for Make_Record are defined in Table 6. Make_Record Attribute Definitions below:

Table 6. Make_Record Attribute Definitions

Data Attribute	Description
Product_ID	A list of unique tracked entity identifiers for a physical product(s) resulting from the Make event.
Make_Type_ID	Code or identifier for the type of product resulting from the Make event that serves as the record data schema specification identifier.
Make_Data_Block	List of key_value_pair objects providing data about the Make event and products resulting from it. Requirements for these fields will be specified in the ecosystem data dictionary entry for the Make_Type_ID value.
Make_External_Reference_Links	List of External_Data_Link object for data associated with this Make event that are stored outside of traceability chains.

3.4. Assemble_Record Subclass

An Assemble event record includes the attributes of a Traceability_Record and extends them with attributes peculiar to production in which multiple Make, Assemble, or Receive events are associated. This preserves the traceability for a given assembled product at the event of its fabrication or assembly tasks. Assemble events may provide pointers to data held externally to the blockchain, so that traceability may be complemented by contextual or detailed information. Figure 12. Assemble_Record Attribute Structure depicts attributes of the Assemble event including attributes containing links to externally stored data.

Assemble _Record
Assembly_ID
Assemble_Type_ID
Assembly_Component_Event_Links : Traceability_Link [2..*]
Assemble_Data_Block : Key_Value_Pair [0..*]
Assemble_External_Reference_Links : External_Data_Link [0..*]

Figure 12. Assemble_Record Attribute Structure

The attributes for Assemble Events are defined in Table 7. Assemble_Record Attribute Definitions below:

Table 7. Assemble_Record Attribute Definitions

Data Attribute	Description
Assembly_ID	A unique tracked entity identifier for a physical product resulting from the Assemble event.
Assemble_Type_ID	Code or identifier for the type of product resulting from the Assemble event that serves as the record data schema specification identifier.
Assembly_Component_Event_Links	List of Traceability_Link objects associated with the preceding Traceability Record(s) associated with the Assemble Event.
Assemble_Data_Block	List of key_value_pair objects providing data about the Assemble event and product resulting from it. Requirements for these fields will be specified in the ecosystem data dictionary entry for the Assemble_Type_ID value.
Assemble_External_Reference_Links	List of External_Data_Link object for data associated with this Assemble event that are stored outside of traceability chains.

3.5. Ship_Record Subclass

A Ship event record includes the attributes of a Traceability_Record and extends them with attributes peculiar to the transfer of an item as depicted in Figure 13. Ship_Record Attribute Structure. This transfer is envisioned as the movement of goods from one location and/or responsible party to another location and/or responsible party.

Ship _Record
Shipment_ID
Ship_Type_ID
Ship_Component_Event_Links : Traceability_Link [1..*]
Ship_Data_Block : Key_Value_Pair [0..*]
Ship_External_Reference_Links : External_Data_Link [0..*]

Figure 13. Ship_Record Attribute Structure

The attributes for Ship are defined in Table 8. Ship_Record Attribute Definitions.

Table 8. Ship_Record Attribute Definitions

Data Attribute	Description
Shipment_ID	A single ID for the item or group of items comprising the shipment associated with the Ship event.
Ship_Type_ID	Code or identifier, associated with the type of shipment method and possibly other factors, that serves as the record data schema specification identifier.
Ship_Component_Event_Links	List of Traceability_Link objects associated with the preceding Traceability Record(s) associated with the Ship Event.
Ship_Data_Block	List of key_value_pair objects providing data about the Ship event. Requirements for these fields will be specified in the ecosystem data dictionary entry for the Ship_Type_ID value.
Ship_External_Reference_Links	List of External_Data_Link object for data associated with this Ship event that are stored outside of traceability chains.

3.6. Receive_Record Subclass

A Receive event record includes the attributes of a Traceability_Record and extends them with attributes peculiar to the receipt of items. A Ship event and a Receive event are expected to match up, although, time will elapse between the two events. The Receive event takes place at the place of consumption of the item. That is, where the item represented in the Receive will go on to become part of an extended context. This is envisioned to include target operational environments, such as critical infrastructure, as well as more complex fabrication. Figure 14. Receive_Record Attribute illustrates this subclass.

Receive _Record
Receive_ID
Receive_Type_ID
Source_Ship_Event_Link : Traceability_Link
Receive_Data_Block : Key_Value_Pair [0..*]
Receive_External_Reference_Links : External_Data_Link [0..*]

Figure 14. Receive_Record Attribute Structure

The attributes for Receive are defined in Table 9. Receive_Record Attribute Definitions below:

Table 9. Receive_Record Attribute Definitions

Data Attribute	Description
Receive_ID	A single ID for the item or group of items comprising the shipment received.
Receive_Type_ID	Code or identifier, associated with the type of receive method and possibly other factors, that serves as the record data schema specification identifier.
Receive_Component_Event_Link	List of Traceability_Link object associated with the preceding Ship Record associated with the Receive Event.
Receive_Data_Block	List of key_value_pair objects providing data about the Receive event. Requirements for these fields will be specified in the ecosystem data dictionary entry for the Receive_Type_ID value.
Receive_External_Reference_Links	List of External_Data_Link object for data associated with this Receive event that are stored outside of traceability chains.

3.7. Employ_Record Subclass

In Figure 15. Employ_Record Attribute, an Employ event record includes the attributes of a Traceability_Record and extends them with attributes peculiar to the installation of an item into an operational environment. An Employ event traces back to a Receive event as an initial step into the overall traceability of Pedigree and Provenance of the operational environment's components.

Employ_Record
Employ_ID
Employ_Type_ID
Employed_Product_Event_Reference : Traceability_Link
Employ_Data_Block : Key_Value_Pair [0..*]
Employ_External_Reference_Links : External_Data_Links [0..*]

Figure 15. Employ_Record Attribute Structure

The attributes for Receive are defined in Table 10. Employ_Record Attribute Definitions below:

Table 10. Employ_Record Attribute Definitions

Data Attribute	Description
Employ_ID	A single ID for the item or group of items comprising the shipment received.
Employ_Type_ID	Code or identifier, associated with the type of receive method and possibly other factors, that serves as the record data schema specification identifier.
Employ_Component_Event_Link	List of Traceability_Link object associated with the preceding Receive Record associated with the Employ Event.
Employ_Data_Block	List of key_value_pair objects providing data about the Employ event. Requirements for these fields will be specified in the ecosystem data dictionary entry for the Employ_Type_ID value.
Employ_External_Reference_Links	List of External_Data_Link object for data associated with this Employ event that are stored outside of traceability chains.

4. Meta-Framework Use Cases

The Meta-Framework use cases illustrate how the traceability goals in Section 1.1, Traceability Activities above are satisfied. The use cases are:

- **Recording Supply Chain Event Data:** This involves capturing and storing traceability records, which include supply chain event data, traceability links, and external reference links as applicable. These records are designed to document key events within the supply chain, ensuring that essential information about components, assemblies, or other manufactured goods is securely recorded. A recorded traceability event establishes a traceability link.
- **Tracing and Retrieving Traceability Records:** The Meta-Framework enables stakeholders to trace back through the traceability records to construct a comprehensive traceability picture. This process allows for retrieval of relevant supply chain event data, providing supporting information to verify the pedigree and provenance of components, assemblies, or other manufactured goods.

In this section, sequence diagrams capture the Meta-Framework use cases as the interaction between stakeholders and interfaces, illustrating recording and retrieving traceability records. Figure 16. Ecosystem Example Actions and Interfaces provides examples that aid in interpretation of the sequence diagrams that follow. Those examples include the write actions to an ecosystem, namely, Make, Assemble, Ship, Receive, and Employ, example traceability actions to an ecosystem, namely, Traceability Link, Trace Back, and Trace Back Result. Three example ecosystem interfaces are also depicted for a microelectronics ecosystem, an operational technology ecosystem, and a critical infrastructure ecosystem. The actors are as follows:

- Manufacturer: Microelectronics, designated as ME-001. This actor is a manufacturing concern and a stakeholder in the advantages of supply chain traceability. As a member of a hypothetical Micro-electronics Ecosystem, this manufacturer participates by providing traceability event records to the ecosystem.
- Micro-electronics Ecosystem, designated as ME-E. This actor is responsible for providing an accessible interface to members and non-members of its ecosystem. Membership in an ecosystem implies permission to write and to retrieve traceability event records. Non-members of an ecosystem can access traceability event records utilizing information provided in the traceability link data objects.
- Manufacturer: Operational Technology, designated as OT-001. This actor is a manufacturer specializing in fabrication and assembly of operational technology. As a member of a hypothetical Operational Technology Ecosystem, this manufacturer participates by providing and retrieving traceability event records to the ecosystem.
- Operational Technology Ecosystem, designated as OT-E. This actor, like ME-E, is responsible for providing accessible interfaces to members and non-members of its ecosystem. Likewise, membership implies permission to write and to retrieve

traceability event records. Non-members of an ecosystem can access traceability event records utilizing information provided in the traceability link data objects.

- Acquirer: Critical Infrastructure, designated as CI-001. This actor is a provider and operator of a critical infrastructure service. As a member of a hypothetical Critical Infrastructure Ecosystem, this critical infrastructure actor participates by providing traceability event records to the ecosystem. In the series of sequence diagrams, this actor initiates trace back actions to retrieve traceability event records.
- Critical Infrastructure Ecosystem, designated as CI-E. As with ME-E and OT-E, this actor is responsible for providing accessible interfaces to members and nonmembers of its ecosystem. Similarly, membership implies permission to write and to retrieve traceability event records and non-members may access information on through valid traceability links.

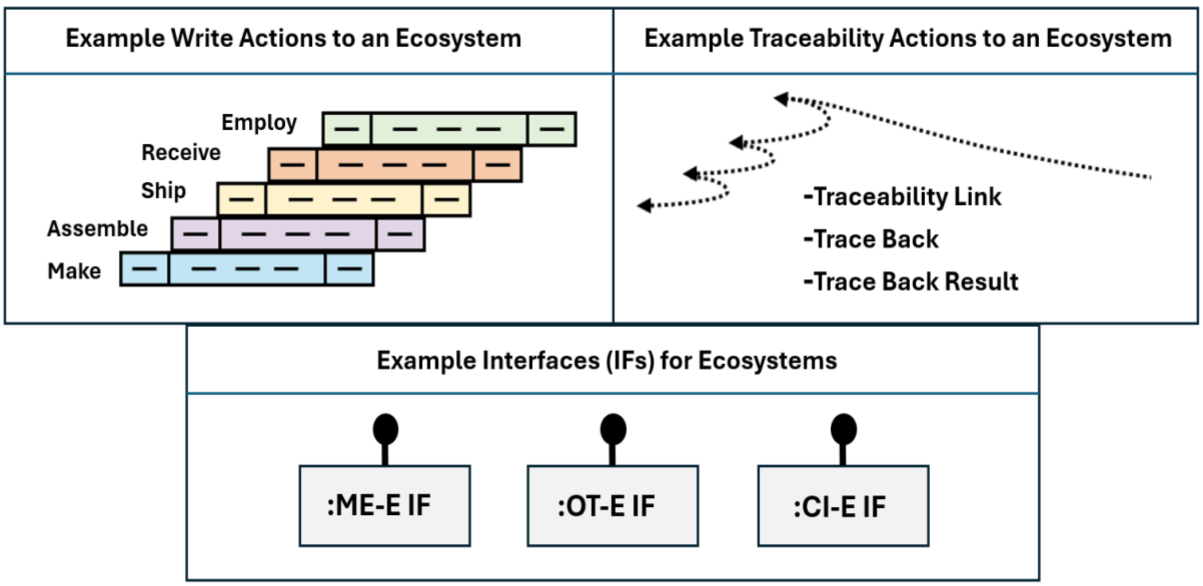

Figure 16. Ecosystem Example Actions and Interfaces

As depicted in the sequence diagrams that follow, an ecosystem's interface minimally addresses:

- write requests for traceability event records from manufacturing and receiving actors, as well as responsibility for these records reaching the trusted data repository and return of a traceability link
- trace back requests from acquiring actors and return of trace back results

Each of the next sections provides a unified modeling language (UML) sequence diagram depicting each of the example actor's interactions with an interface to read or write data in the interoperable ecosystems. The final two sequence diagrams depict the trace back invoked by the acquirer requesting the records that will constitute linked traceability. The diagrams are as follows:

- Sequence Diagram 1 – Manufacturer of Microelectronics Make Traceability Event
- Sequence Diagram 2 – Operational Technology with Receive, Make, Assemble, and Ship Events
- Sequence Diagram 3 – Critical Infrastructure Acquirer with Receive and Employ
- Sequence Diagram 4 – Operational Technology with Trace Back to ME
- Sequence Diagram 5 - Critical Infrastructure Acquirer with Trace Back to ME and OT

For this set of sequence diagrams, ecosystem interfaces provide indirect access to the trusted data repository; therefore, the trusted data repository is not explicitly depicted in the diagrams. Depiction in this way leaves solution and implementation aspects open for trusted data repository providers to consider. Additionally, the Critical Infrastructure Acquirer's position and the Operational Technology Receiver's position are chosen as examples of executing a trace back request. Motivation for the trace back in Sequence Diagrams 4 and 5 can be either of the traceability activities outlined in Section 1.1 Traceability Activities.

4.1. Record Traceability Record Use Case

The following sequence diagrams represent recording supply chain event data via traceability records.

4.1.1. Sequence Diagram 1 – Manufacturer of Microelectronics Make Traceability Events

Figure 17. Manufacturer: Microelectronics ME-001 Writes Make and Ship Event Records illustrates a sequence of traceability events for ME-001. ME-001 is a member of ME-E, the ecosystem pertaining to microelectronics. In this sequence, a Make event record contains the information that characterizes this Make as a unique event. This includes multiple key-value pairs in accordance with the ecosystem's data dictionary and optional external referenced links. At establishment of the Make event in the trusted data repository, the traceability link data is returned to ME-001 depicted by the dashed arrow indicating a return flow.

Likewise, a Ship event is written, and its structure and data comply with the ecosystem data dictionary to describe the event, to include other contents of the shipment, beyond the good written in the Make event depicted. In both cases, the traceability links capture the relationship between the Make and Ship events. This is a pattern present for all writes of traceability event records, allowing trusted data repositories to support the traceability chain for the product.

At the completion of this sequence, ME-001 has submitted a traceability event for having produced a good, submitted a traceability event for having shipped the good, possibly in a shipment along with other goods, and for both events, received corresponding traceability links from the ecosystem interface (ME-E IF). In the next sequence diagram, the Receive event corresponding to the Ship event concluding here begins the next series of writes.

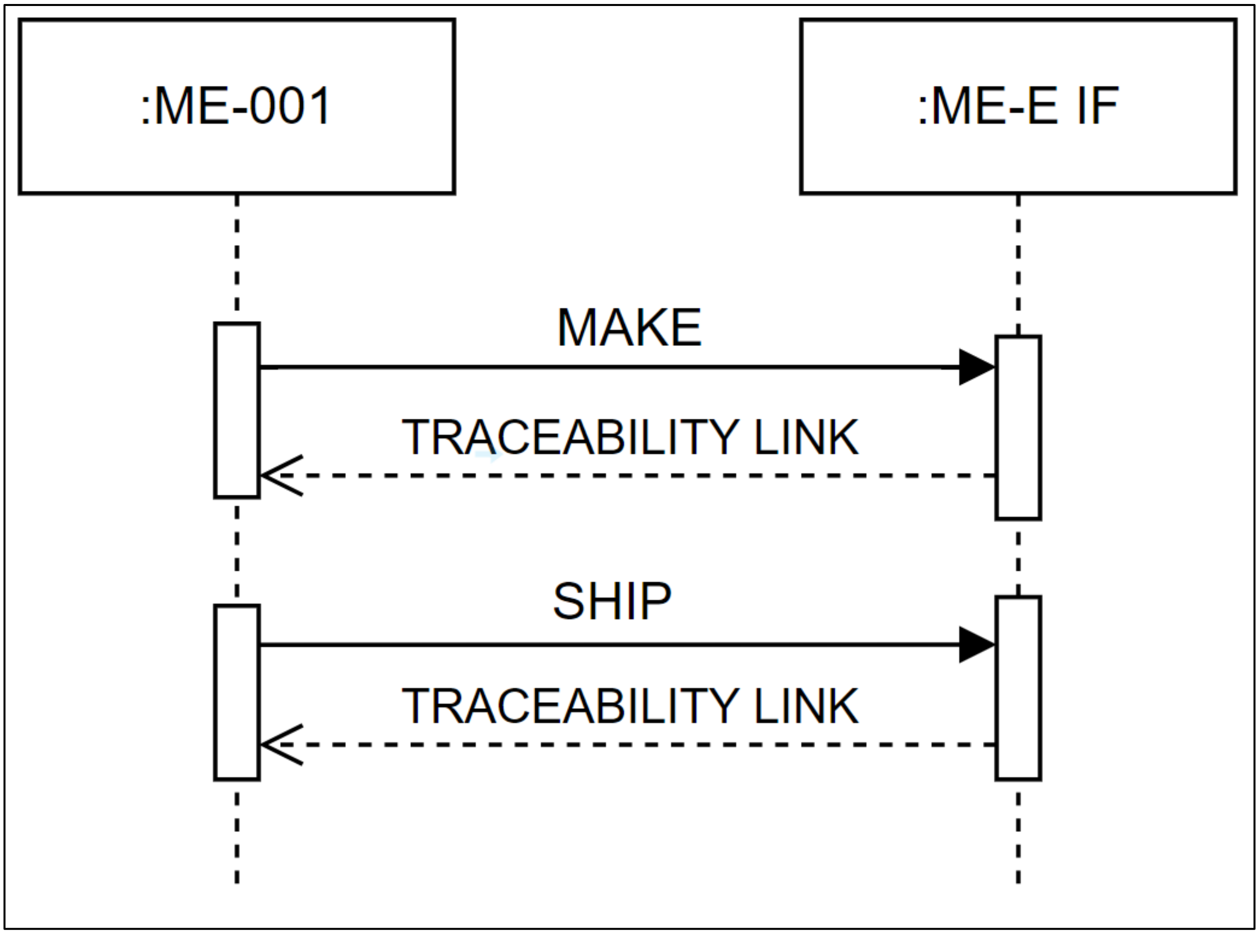

Figure 17. Manufacturer: Microelectronics ME-001 Writes Make and Ship Event Records

4.1.2. Sequence Diagram 2 – Operational Tech with Receive, Make, Assemble, and Ship

Figure 18. Manufacturer: Operational Technology Writes Receive, Make, Assemble, and Ship illustrates a sequence of writes representative of receipt of a good and its incorporation into an assembly, which in this case includes a second good and its corresponding Make event. Note that the ecosystem represented has now switched to Operational Technology – Ecosystem Interface (OT-E IF). The sequence is as follows:

- Receive: a traceability event establishing a link to ME-001's Ship event as well as means to link forward to the Assemble event later in the sequence. Likewise, the traceability link established in Diagram 1 for Ship provides means to tap its relationship (captured in Diagram 4) between the Ship and Receive.
- Make: a traceability event recording the manufacture of a good by OT-001, it has no prior link, as a Make record is an originating event for a good. It will have a traceability link that allows it to be addressed as it moves forward in the supply chain.
- Assemble: a traceability event collecting information that, together, constitutes production of an assembly. Traceability links will reference the Receive which in turn

references the Ship and Make shown in Diagram 1. To conclude this diagram, the built assembly becomes part of a shipment, and the Ship event is written with a traceability link returned. As this sequence is carried forward in time, the traceability links are captured at each event in anticipation of a future request for the events' relationships.

- Ship: a traceability event marking the compilation of the object of the Assemble event into a shipment that possibly includes other goods or assemblies. A Ship event may reference multiple Make and/or Assemble events to capture the shipment's contents. In this case, the diagrammed Assemble, Make, and traceability to ME-001's Make, via the OT-001 Receive and ME-001's Ship settle into the sequence. As with writing the other events in this sequence, the Ship event is concluded with a returned traceability link.

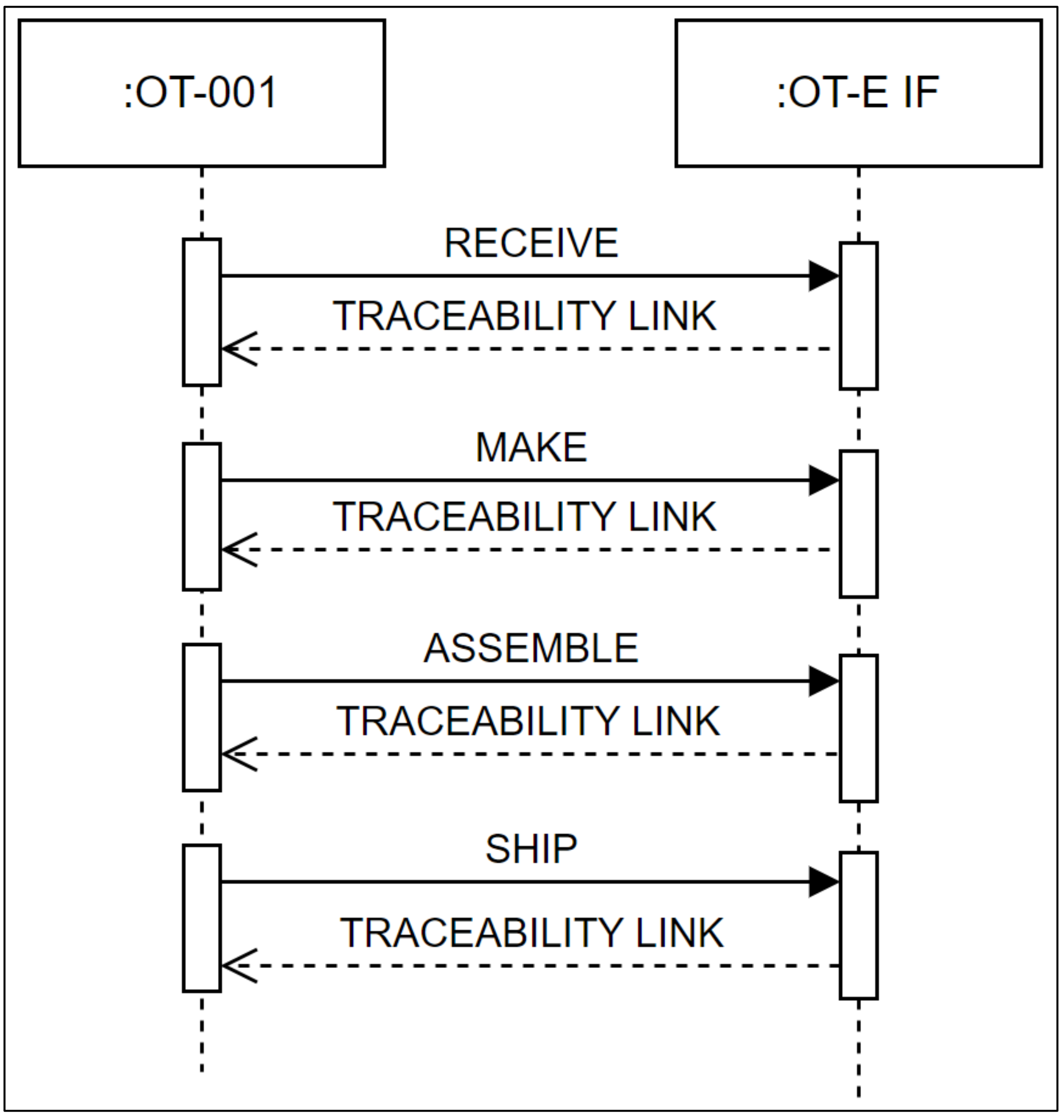

Figure 18. Manufacturer: Operational Technology Writes Receive, Make, Assemble, and Ship Event Records

This concludes Sequence Diagram 2, with a Ship event that will pair with the first traceability link of Sequence Diagram 3, which is a Receive.

4.1.3. Sequence Diagram 3 – Critical Infrastructure Acquirer with Receive and Employ

Sequence Diagram 3 picks up from Diagram 2 with writing a Receive to the ecosystem that CI-001 is a member of. The Critical Infrastructure provider, as an acquiring entity, writes the Receive and upon deciding to install the good received into its service machinery, writes an Employ. As in previous diagrams, each of these writes is followed by a corresponding traceability link returned from their supporting ecosystem. Tapping into the traceability events to support the decision to install the received good is the subject of Sequence Diagram 5.

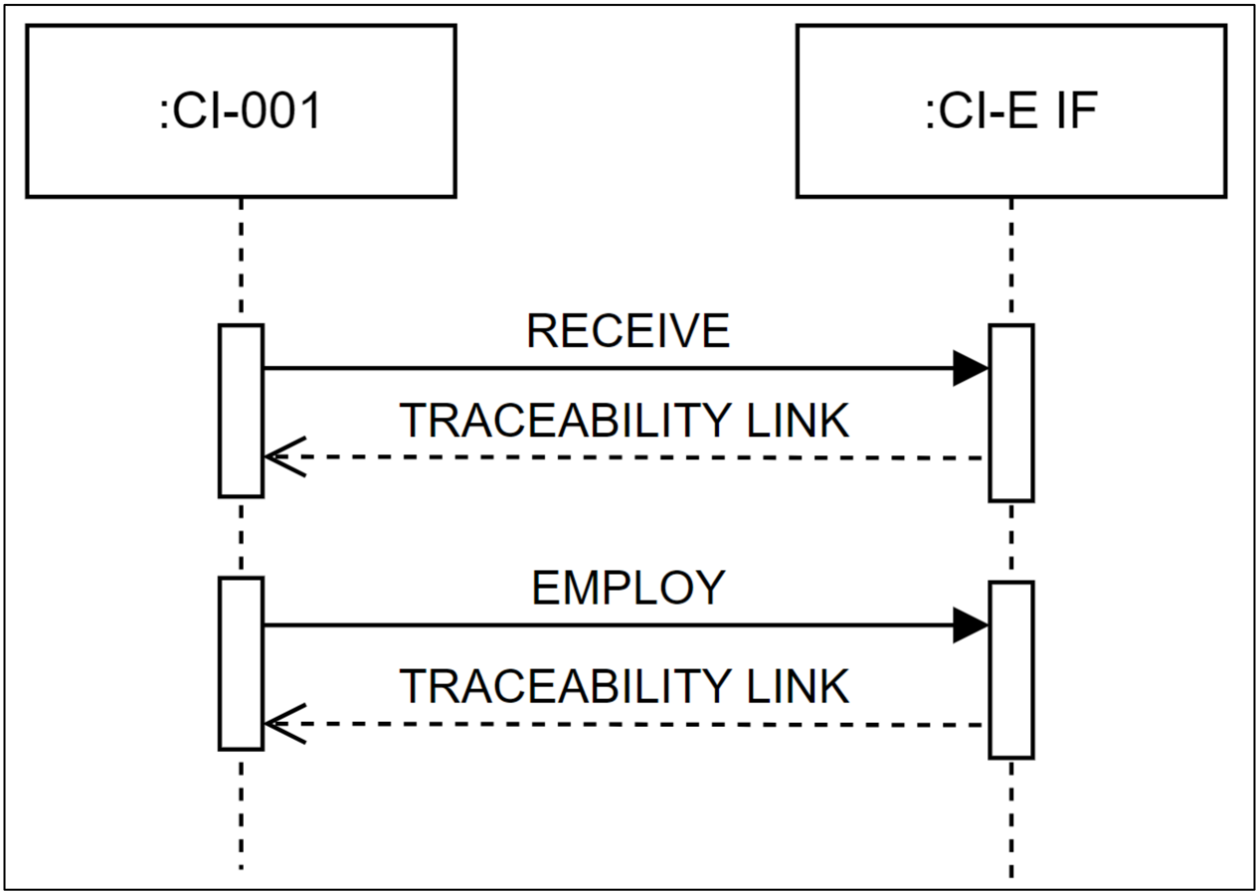

Figure 19. Acquirer: Critical Infrastructure CI-001 Writes Receive and Employ Event Records

4.2. Retrieve Traceability Records Use Case

During retrieval a pattern for usage of the traceability links depicted in the Record Traceability Use Case comes into the sequence. The traceability links are used in the following way to retrieve the corresponding traceability records. These details are omitted from the sequence diagrams:

- An IRI (such as a URL) is used to access the interface used to retrieve the traceability record.

- The traceability link parameters, also stored in the traceability record, are passed to the interface. The parameters uniquely identify the traceability record in the trusted data repository of the destination ecosystem.
- The implementation of the interface locates and passes back the traceability record.
- The retrieved traceability record can then be hashed, and that hash is compared to the stored hash in the traceability record, to assure data integrity from the time of original linking to the present time.
- The retrieved traceability record can then be used to further retrieve the next traceability record(s). A Traceability Record Set is a group of traceability records related through traceability links.

Two sequence diagrams illustrate first, a simple retrieval involving one ecosystem and second, a complicated retrieval involving two ecosystems. The number of ecosystems whose interfaces receive retrieval requests depends on the traceability links referenced and the traceability picture that following the links illuminates. In Sequence Diagram 4, the Operational Technology manufacturer, having received a shipment, inspects the contents and proceeds to initiate a trace back. In Sequence Diagram 5, the critical infrastructure acquirer initiates the trace back at the example time of the decision to employ a received assembly. The trace back results are used in both cases to support decision making about part or assembly integrity.

4.2.1. Sequence Diagram 4 – Operational Technology with Trace Back to ME

Figure 20. Acquirer: Operational Technology Manufacturer Invokes Trace Back illustrates a trace back sequence supporting the acquirer’s decision to accept a received microelectronics good for future use in an assembly, or otherwise. The acquiring operational technology manufacturer may be in the position of either of the two earlier described activities: the need to validate purchased products’ IDs, components, assemblies, including software when needed; or validate that purchased products are ethically sourced.

In this example, the operational technology manufacturer has received a shipment from a microelectronics supplier. Recall in Figure 18. Manufacturer: Operational Technology Writes Receive, Make, Assemble, and Ship Event Records, that the sequence begins with a Receive event and a corresponding traceability link. As a matter of business practice, OT-001 may desire to validate the product’s source as a condition of acceptance of the shipment. OT-001 initiates a trace back via the interface with the Microelectronics Ecosystem, which is followed by review of the trace back result.

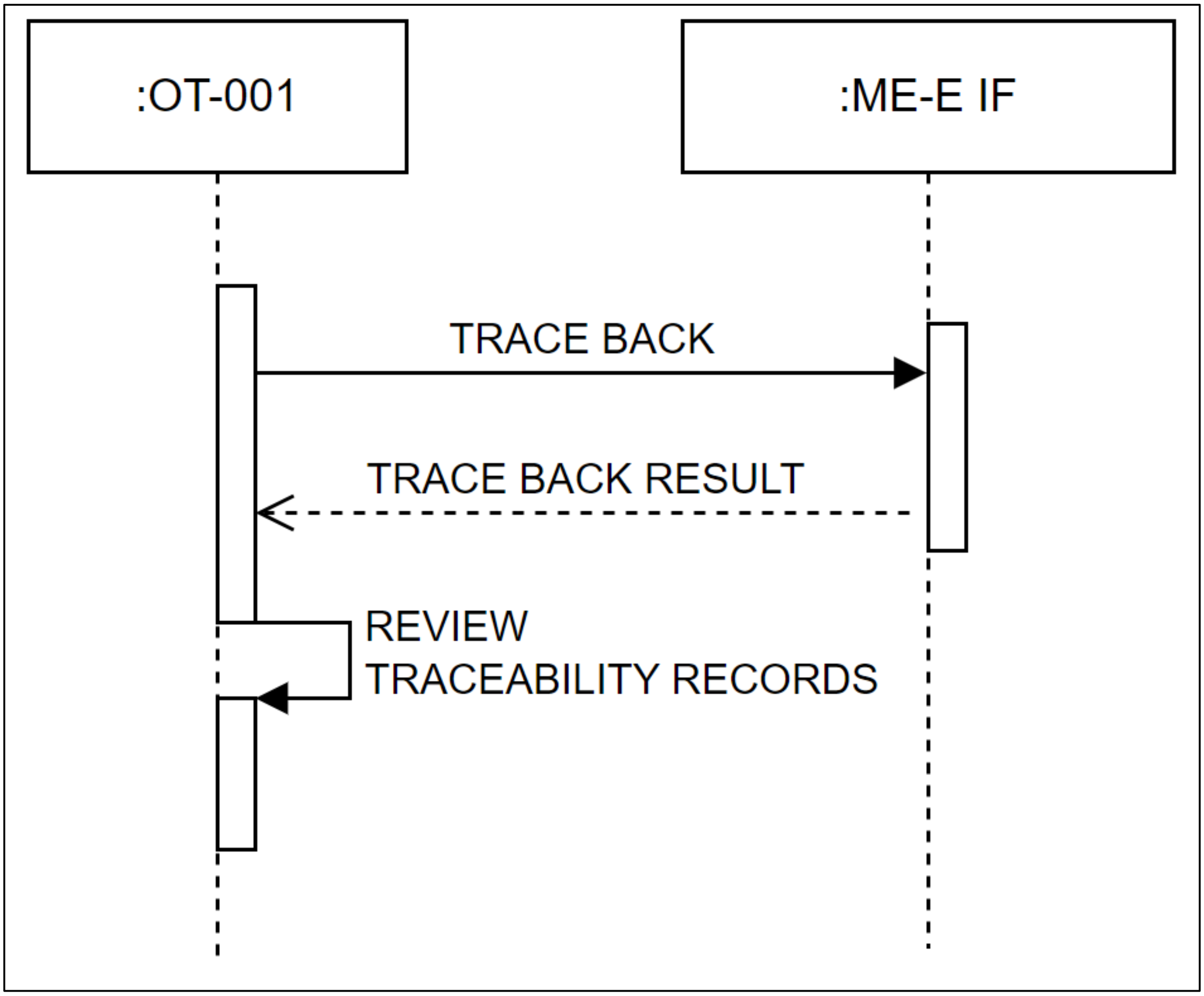

Figure 20. Acquirer: Operational Technology Manufacturer Invokes Trace Back

This unified modeling language sequence diagram depicts trace back request from an Operational Technology manufacturer to its microelectronics supplier via a single ecosystem interface, namely ME-E IF. The trace back results are shown as return transmissions. Additionally, these returned results are shown directed to a review traceability records function.

4.2.2. Sequence Diagram 5 – Critical Infrastructure Acquirer with Trace Back to ME and OT

Figure 21. Acquirer: Critical Infrastructure CI-001 Invokes Trace Back illustrates a trace back sequence supporting the acquirer's decision to put a received good into service. The acquiring critical infrastructure provider may be in the position of either of the two earlier described activities: the need to validate purchased products' IDs, components, assemblies, including software, when needed; or validate that purchased products are ethically sourced.

Actors in this sequence include two interfaces, in recognition that for CI-001 to have a complete set of traceability events; trace back requests must be made to their suppliers. The ecosystem interfaces, OT-E IF and ME-E IF, each will provide a trace back result. The parameters included in the trace back request enable queries of the indirectly accessed trusted data store via each ecosystem interface, in turn. The returned trace back results may be compiled in a linked user presentation to support validation efforts and decision making about supply chain characteristics. Once compiled, the trace back results may be reviewed in a presentation style.

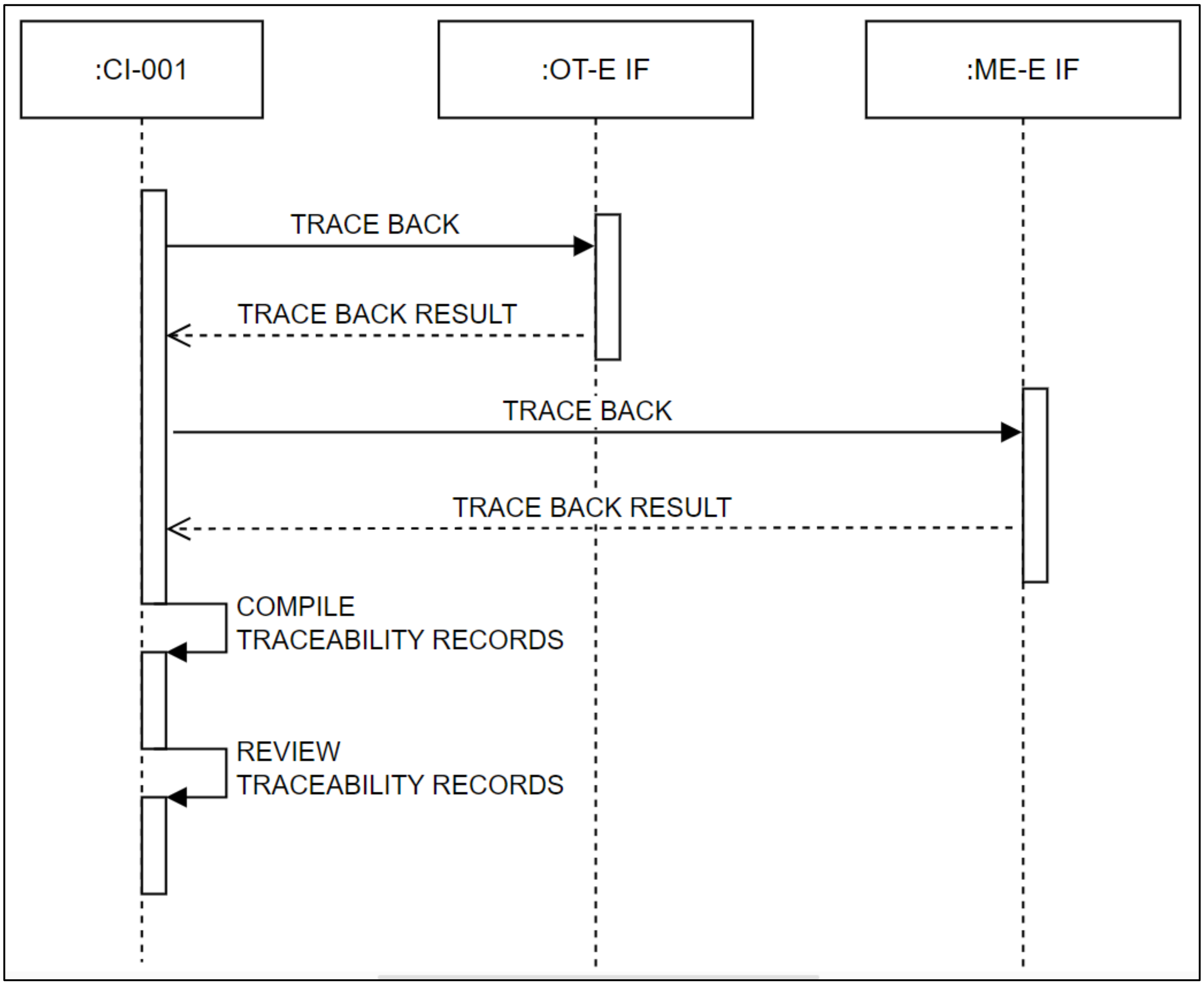

Figure 21. Acquirer: Critical Infrastructure CI-001 Invokes Trace Back

This sequence diagram concludes having shown the work of the successive trace back requests and a compile traceability records function, with a review traceability records function, while leaving open the possibility that ecosystems, either by interface or service offerings, will have a role in the presentation of traceability validation data.

In summary, representative successions of traceability events (Make, Assemble, Ship, Receive, Employ) are illustrated in Diagrams 1-3. Diagram 4 illustrates the requests for the reverse construction of those traceability events such that validation activities may be satisfied. The roles of multiple traceability ecosystems as trusted data repositories are captured in their externally facing and accessible interfaces. As representative works, these five sequence diagrams are not exhaustive. A naturally arising supply chain will most likely be considerably more complex, yet these two scenarios for traceability results have considerable scaling potential due to the patterns they capture.

5. Conclusion

The ability to trace products and components through the supply chain is essential for ensuring product integrity, compliance with regulations, and meeting consumer expectations. However, gathering this data can be difficult and time consuming especially for complex supply chains. The Meta-Framework can enhance supply chain traceability across multiple manufacturing supply chain sectors, enabling stakeholders to access information required to trace product provenance and verify the pedigree of products within the supply chain.

The Meta-Framework improves traceability by providing the ability to:

- **Fully discover** properly sequenced relevant supply chain event data.
- **Understand** discovered supply chain event data.
- **Trust to decide and act** on supply chain activity.

Discovery is enabled by stakeholders recording traceability records, which contain relevant supply chain event data recorded at the time of the event, and later linked, using traceability links, within subsequent traceability records, and incrementally growing a traceability chain. This chain links all relevant supply chain event data, via traceability records, written to trusted data repositories, governed by applicable ecosystems of manufacturing supply chain stakeholders. The chains remain in place after final products are delivered, and later the traceability records can be retrieved by authorized users to verify components, ethical sourcing, and more.

Understanding is enabled by the stakeholders using data dictionaries in their respective ecosystem to constrain the data stored in the traceability record, for example in the data block. Thus, the retrieved traceability record can be understood by using the data dictionary of the corresponding ecosystem.

Trust to decide and act is enabled by stakeholders using the traceability link mechanism to assure that the retrieved traceability record was not subject to tampering from the time of establishing the traceability link to the time of retrieval. This provides a baseline level of data integrity for all traceability chains. Data integrity can be further strengthened by a trusted data repository using blockchain and related technologies. This extends data integrity for the traceability record from the time of initial writing of the record to the time of another stakeholder establishing a traceability link to the record, and beyond.

The baseline level of data integrity for supply chain event data, and the set of links representing provenance of the manufactured goods represented by the Traceability Records, combine to yield high trust in the traceability chain to use for component verification and ethical sourcing.

References

[1] "Supply Chain Traceability," MIT Sustainable Supply Chain Lab, [Online]. Available: https://sustainable.mit.edu/supply-chain-traceability/. [Accessed 6 Sep 2024].

[2] Boyens, Jon M., Angela Smith, Nadya Bartol, Kris Winkler, Alexander Holbrook, and Matthew Fallon. "Cybersecurity supply chain risk management for systems and organizations." (2022). https://csrc.nist.gov/News/2022/c-scrm-guidance-nist-sp-800-161r1 [Accessed 6 Sep 2024]

[3] Montecchi, Matteo, Kirk Plangger, and Douglas C. West. "Supply chain transparency: A bibliometric review and research agenda." International Journal of Production Economics 238 (2021): 108152. Available: https://www.sciencedirect.com/science/article/pii/S0925527321001286. [Accessed 7 September 2024]

[4] K. Stouffer, M. Pease, J. Lubell, E. Wallace, H. Reed, V. Martin, S. Granata, A. Noh and C. Freeberg, "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives," National Institute of Standards and Technology, Gaithersburg, MD, 2022. Available: https://doi.org/10.6028/NIST.IR.8419

[5] "Supply Chain Integrity, Transparency, and Trust (scitt)," Internet Engineering Task Force (IETF), [Online]. Available: https://datatracker.ietf.org/wg/scitt/about/. [Accessed 7 Sep 2024].

[6] "Manufacturing Supply Chain Traceability with Blockchain Related Technology: Reference Implementation," National Institute of Standards and Technology (NIST) Cybersecurity Center of Excellence (NCCoE), [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/2023-08/mfg-sct-blkchn-project-description-final.pdf. [Accessed 12 August 2024].

[7] "Supply Chain Assurance," National Institute of Standards (NIST) National Cybersecurity Center of Excellence (NCCoE), [Online]. Available: https://www.nccoe.nist.gov/supply-chain-assurance. [Accessed 8 March 2023].

Appendix A. List of Symbols, Abbreviations, and Acronyms

API
Application Program Interface

CI
Critical Infrastructure

CI-E
Critical Infrastructure – Ecosystem

CI-E IF
Critical Infrastructure – Ecosystem Interface

CISA
Cybersecurity and Infrastructure Security Agency

CSRC
Computer Security Resource Center

DHS
Department of Homeland Security

EV
Electric Vehicle

HTTP
Hypertext Transfer Protocol

IETF
Internet Engineering Task Force

IRI
Internationalized Resource Identifier

IAM
Identity and Access Management

IT
Information Technology

ME
Microelectronics

ME-E
Microelectronics – Ecosystem

ME-E IF
Microelectronics – Ecosystem Interface

MIT
Massachusetts Institute of Technology

NIST IR
National Institute of Standards and Technology Internal Report

NIST SP
National Institute of Standards and Technology Special Publication

OT
Operational Technology

OT-E
Operational Technology – Ecosystem

OT-E IF
Operational Technology – Ecosystem Interface

REST
Representational State Transfer

SCITT
Supply Chain Integrity, Transparency, and Trust

SCRM
Supply Chain Risk Management

UML
Unified Modeling Language

URL
Uniform Resource Locator

W3C
World Wide Web Consortium

Appendix B. Security and Privacy Considerations

The Meta-Framework introduces several unique cybersecurity and privacy challenges due to the need for trusted data repositories, authenticated access, and the handling of potentially sensitive personal information. This appendix is not intended to be a comprehensive cybersecurity guide and instead, this appendix highlights key considerations. Organizations will need to tailor their cybersecurity and privacy strategies to address their specific operational and regulatory requirements. By proactively addressing these issues, ecosystems can ensure that traceability records remain secure, trusted, and compliant with relevant standards.

B.1. Identity, Authentication, and Access Control

Ecosystems will need robust mechanisms for identity verification, authentication, and access control to ensure that only authorized individuals, entities, and processes can create and modify traceability records. This includes utilizing secure protocols for writing records to trusted data repositories and ensuring that both individuals and automated processes (such as supply chain management systems) are properly authenticated before accessing sensitive supply chain data. Strong identity and access management (IAM) practices will be required to prevent unauthorized access.

Since ecosystems may involve multiple competitive organizations, it is also essential to restrict access to sensitive data. Ecosystems must ensure that organizations can only access the traceability records relevant to their operations, preventing competitors or unauthorized parties from viewing or extracting sensitive production data. However, ecosystems also need to allow external stakeholders (e.g., customers, regulators) to query traceability records. Ecosystems must ensure that queries are limited to specific records without exposing the broader dataset. Preventing enumeration, brute-force parameter guessing, query-based exploitation and other bulk extraction of records will be necessary to safeguard data integrity and confidentiality.

B.2. Privacy Measures

While traceability records are primarily focused on product provenance and pedigree, they may also contain sensitive information related to individuals or entities involved in supply chain activities. Privacy concerns should be addressed at both the recording and retrieval stages. Specifically, traceability records may link to individuals who performed specific production tasks or authorized certain events (e.g., shipping or receiving). Organizations must implement privacy measures to protect personally identifiable information (PII) while ensuring that records can still meet market and regulatory compliance requirements.

Shipping and receiving events could also include sensitive information about individuals or entities (e.g., names, addresses) that must be protected. Ecosystems should ensure that only authorized parties can access this information and that it is redacted or anonymized where appropriate, especially when queried by external stakeholders.

These considerations may require organizations to adopt data minimization principles to collect only the necessary personal information required to support traceability use cases. Similarly, data retention policies should be enforced to ensure that personal data is only stored for as long as necessary for regulatory and operational purposes.

B.3. Other Considerations

In addition to the specific concerns around authentication and privacy, the following general cybersecurity practices should also be considered when implementing ecosystems:

- **Audit and Monitoring:** Ecosystems should maintain a detailed audit trail of all data interactions, including who accessed or modified traceability records and when. Regular monitoring and logging can help detect unauthorized access or suspicious activity.
- **Data Encryption:** Sensitive data, including traceability records and any associated external references, should be encrypted both in transit and at rest. Strong encryption protocols will protect data integrity and confidentiality, especially when records are queried by external stakeholders.
- **Incident Response and Data Breaches:** Ecosystems should be prepared to respond to potential cybersecurity incidents, such as data breaches or unauthorized access. Incident response plans should include procedures for notifying affected stakeholders and mitigating the impact of a breach on the integrity of the traceability records.

Appendix C. Meta-Framework Future Topics

The Meta-Framework outlined in this report provides a foundation for traceability across manufacturing sectors and their supply chains, particularly within manufacturing, assembly, and product delivery. This Meta-Framework represents the beginning of what can become a broader treatment of traceability.

Nonetheless, while this initial version of Meta-Framework, as illustrated in Figure 22 below, focusing primarily on traceability of supply chain event data recorded as linked traceability records, there is a significant opportunity for future research to extend the Meta-Framework traceability record subclasses to the sustainment chain, and add additional Traceability Record subclasses to the supply chain.

By adding new traceability record subclasses into the supply chain and sustainment chain and refining other aspects of the Meta-Framework based on industry input, the Meta-Framework can evolve into a comprehensive tool for lifecycle traceability. This appendix summarizes potential next steps toward this broader vision.

C.1. New Sustainment Chain Traceability Record Subclasses

The Sustainment Chain starts after the manufacturing supply chain and initial Employ event of a product, illustrated in Figure 22. Sustainment Chain Opportunity for Future Research below. In the sustainment chain, additional events such as product returns, recalls, refurbishments, and recycling become important. Future research can explore how to record the sustainment chain event data, to provide a complete lifecycle view of the product.

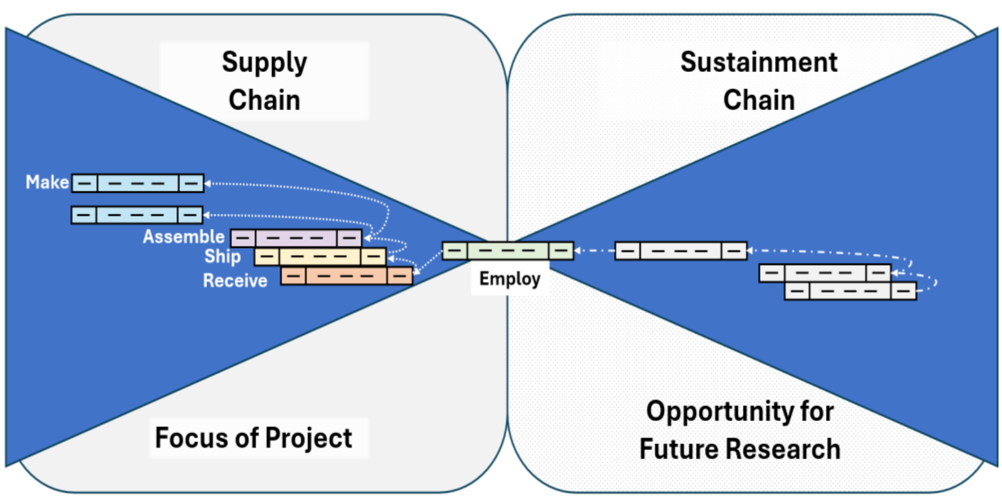

Figure 22. Sustainment Chain Opportunity for Future Research

Future research could explore the introduction of additional sustainment chain traceability record subclasses to record and link regarding sustainment chain event data, described in Table 11. Candidate New Sustainment Chain Traceability Record Subclasses below.

Table 11. Candidate New Sustainment Chain Traceability Record Subclasses

New Traceability Record subclass name for sustainment chain	Description
Returns	When a product is returned by an end customer for any reason, a Return Traceability Record could be created to capture this event. Recording returns as traceability events would provide proof that the product has been removed from service or is no longer in the customer's possession.
Recalls	In the event of a manufacturer-initiated recall, a Recall Traceability Record could trace the product back to the customer. If a customer is also a manufacturer, they could pass along the recall to their customers, enabling a more transparent and efficient recall process throughout the supply chain.
Refurbishment	During a product's sustainment phase, various maintenance actions such as software updates, sensor replacements, or other refurbishments may occur. A Refurbish Traceability Record could capture these modifications, ensuring that all product changes are documented.
Recycling	Some products are decommissioned and recycled at end of life. A Recycle Traceability Record could document the decommissioning process and disconnection from any applicable IT or OT systems, ensuring that the product's lifecycle is fully traceable from creation to disposal.

C.2. Additional Supply Chain Traceability Record Subclasses

Future research could explore the introduction of additional supply chain traceability record subclasses to capture additional supply chain event data, described in Table 12. Candidate New Supply Chain Traceability Record Subclasses.

Table 12. Candidate New Supply Chain Traceability Record Subclasses

New Traceability Record subclass name for supply chain	Description
Precursor	A Precursor Traceability Record could trace raw materials, such as silica used in semiconductor manufacturing, through the production process. This could extend traceability to the origin of the materials used in products, providing a more comprehensive view of the supply chain, and is relevant to ethical sourcing.

New Traceability Record subclass name for supply chain	Description
Continuous Flow and Batch Manufacturing	Future research could include continuous flow and batch manufacturing processes. In these cases, additional traceability records could distinguish between the continuous production of materials and the production of discrete components.
Transportation	Adding Transportation Traceability Records could enhance visibility of logistics and transport phases of the supply chain. These new Traceability Records could document specific steps taken by logistics providers between the shipping and receiving stages, adding deeper transparency and enhanced accountability regarding the product's movement through shipping.