Assured and Preferred Supply of Microelectronics through Provenance, Traceability, and Market Preferences

White Paper

Electronics Division

July 2023

DISCLAIMER: The ideas and findings in this report should not be construed to be official positions of any of the organizations listed as contributors or the membership of NDIA. It is published in the interest of an information exchange between government and industry, pursuant to the mission of NDIA.

© 2023 National Defense Industrial Association. All rights reserved.

[This Page Intentionally Blank]

© 2023 National Defense Industrial Association. All rights reserved.

Executive Summary

This white paper explores the need to develop a preference for assured[1] and traceable microelectronics with initial emphasis on national and economic security, defense, and critical infrastructure. Support of assured and traceable microelectronics by manufacturers will ensure that reliable and secure products are available for supply to Customers in the United States and allied nations. The white paper also explores guaranteed access to trusted assured microelectronics by increasing design and manufacturing in the US and allied nations, as well as by establishing market preferences for assured supply, and actions which are critical for achieving national security and economic growth objectives set forth by congress including through recent Chips and Science Act legislation.

Market preferences for supply chain assurance and traceability can be accomplished though incentives, standards, and legislative requirements. An outcome of these actions will be to build a level, competitive, and secure playing field for microelectronics supply chains along with assuring delivery of secure components and systems to support the US and allied nations with initial emphasis on national security, defense, and critical infrastructure. Additionally, the creation of a trusted digital thread across the supply chain will enable the establishment of marketplaces of data for producers and consumers that can have significant positive impact on supply chain resilience, logistics, innovation, efficiency, security, and ultimately lead to economic prosperity. We can reference this as a "supply value chain".

The Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act funding[2] was a critical first step in providing incentives to advance secure domestic and allied

---

[1] Assurance – "Grounds for justified confidence that a claim has been or will be achieved." SAE International, SAE JA7496, Cyber-Physical Systems Security Engineering Plan (CPSSEP), June 2022. Retrieved from SAE International: https://www.sae.org/standards/content/ja7496_202206/

[2] Hayashi, Y. (2022, December 5). U.S., EU Agree to Coordinate Semiconductor Subsidy Programs. Retrieved from WSJ: https://www.wsj.com/articles/u-s-eu-agree-to-coordinate-semiconductor-subsidy-programs-11670284917

© 2023 National Defense Industrial Association. All rights reserved.

semiconductor supply. However, the Act only addresses the supply side of the ecosystem; for example, it does not create demand for CHIPS. At the same time, other Congressional requirements have been mandated for microelectronics: Fiscal Year 2020 National Defense Authorization Act section 224 "Requiring Defense microelectronics products and services meet trusted supply chain and operational security standards"[3] and Fiscal Year 2023 National Defense Authorization Act section 5949 "Prohibition on certain semiconductor products and services"[4] (including supply chain traceability and assurance aspects). To successfully achieve goals mentioned above, it is imperative that the participants in the global microelectronics supply chain establish an infrastructure for measuring assurance, tracking provenance, enabling supply chain traceability, and establishing a strategy for market preference for assured supply, market access, and end market use.

As we have seen in recent years, the problem of managing demand versus supply imbalance for microelectronic-based products has been exacerbated by supply chain issues caused by natural, pandemic, and geopolitical causes. These issues, combined with the parallel expansion of counterfeiter exploitation, significantly increase the risks for maliciously modified parts or cybersecurity issues to enter the supply chain. Microelectronics have become important elements in growing geopolitical conflicts as microelectronics enable electronic warfare systems, proliferated satellite-based observations, and related systems key to hot and cold warfare to name a few. Warfare, in this context, includes not only traditional methods implemented with armaments, but also increasingly through geopolitical, economic, cyber, trade, attacks to supply chain, communications, and critical infrastructure means.

---

[3] National Defense Authorization Act for Fiscal Year 2020, 10 U.S.C. § 2302 (2020). https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf

[4] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, 41 U.S.C. § 4713 (20220. https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf.

© 2023 National Defense Industrial Association. All rights reserved.

The Value

We must create a system that links evidence of assured supply to end service providers and end users and delivers market value and remuneration for the assurance of the supply chain and services infrastructure.

Today, consumers can scan a code and understand where they get their coffee or chocolate bar, which village, and how it is produced (see Figure 1). This allows the consumer to reward the producer for the quality and eliminate layers of costly supply chain middlemen to deliver better value to the consumer. In the same way, we must create a system that rewards the producers of microelectronics for how and where they produce the goods that deliver our home conveniences, move us around in the world, safegaurd our money, and connect us to our loved ones and the rest of the world.

Figure 1: Traceability and Associated Value, Chocolate Example[5]

[5] Beyond Good. (2023, June). Derived from Beyond Good: https://farmers.beyondgood.com/

© 2023 National Defense Industrial Association. All rights reserved.

This evidence will be delivered through provenance and traceability utilizing a digital thread to provide the framework for trust, as assurance case data becomes verifiable and linked to specific products (see Figure 2). An end-to-end digital thread is thereby created through the digitalization of workflows of enterprises participating in the value chain. Information about data can be provided in entirerty, or via metadata indices, delivered through a data marketplace. Cryptography implemented in digital certificates, communicated through a digital thread through the supply chain, can provide IP protection as needed.

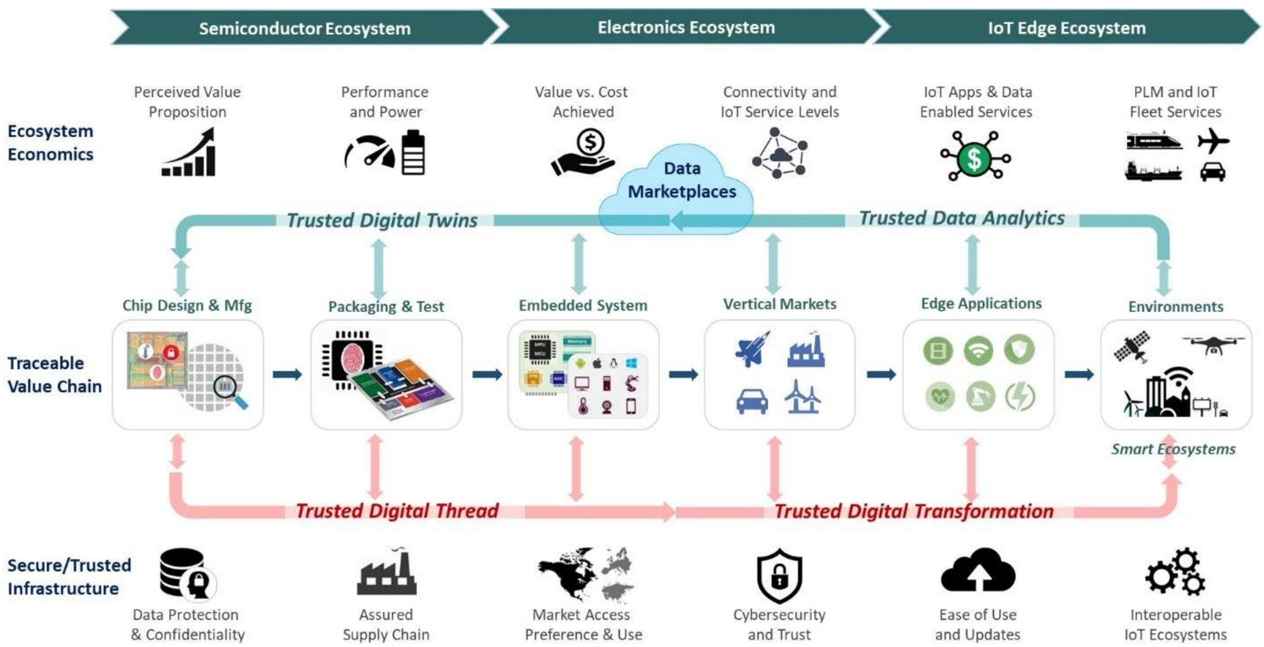


Figure 2: Assurance & Preferred Supply through Provenance & Traceability

A secure and trusted infrastructure provides the foundation to create digital threads across the value chain. A digital thread linking data producers and consumers enables them to establish market preference. Through market access, and through the use of a digital transformed environment, enterprises can become smart-connected suppliers in the value chain. Connected enterprises enable networks of data producers and consumers. As the data available in this value chain expands, analytics and AI-based applications can be leveraged to

© 2023 National Defense Industrial Association. All rights reserved.

enable digital twin models and other derivative works. Increasingly improving virtual models, or digital twins[6], fed with real marketplace data through analytics, can be used to make better, more reliable, higher quality products from the start and to better inform decisions.

All of this enables additional opportunities for producers to improve customer value and to monetize that value. These opportunities include IoT and data enabled services, such as fleet management and control, product lifecycle management through subscription, business models, hardware as a service, and a variety of data-enabled applications.

From a national perspective, supply chain availability can be monitored much faster and more accurately, allowing the ability for more precise risk identification and mitigation. This includes risk such as geopolitically and naturally caused supply chain gaps. Also, the ability to track the illegal distribution of critical and proprietary technologies to prohibited entities or competitors, and the ability to disable them if such distribution occurs, can be realized.

The Approach

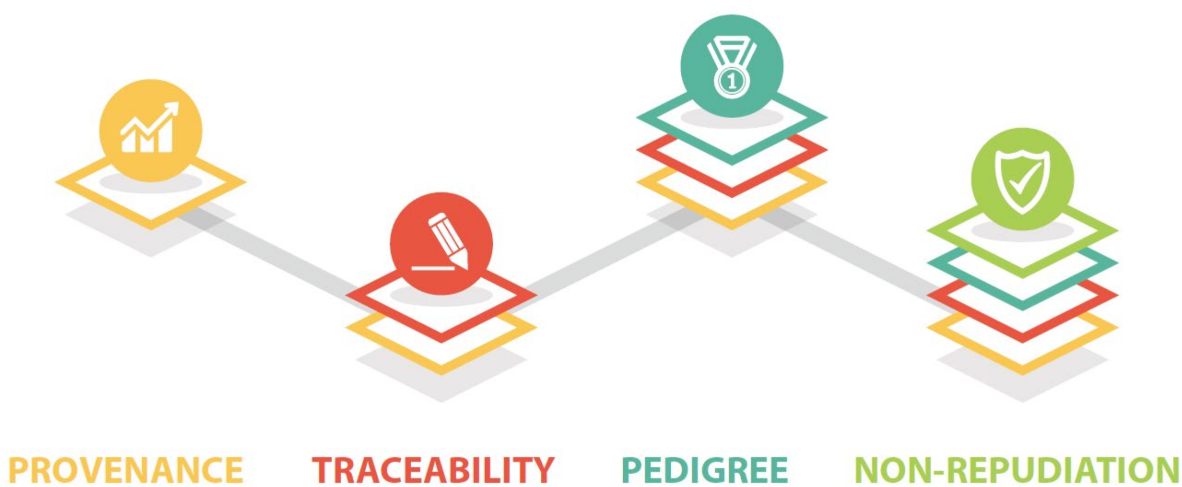
The approach includes three elements: digital solutions, physical traceability, and market behavior. These approaches are all aimed to provide a secure and available supply of microelectronics from a robust and diverse supply chain. This requires the following:

[6] Digital twin – "A set of virtual information constructs that mimics the structure, context and behavior of an individual / unique physical asset, or a group of physical assets, is dynamically updated with data from its physical twin throughout its life cycle and informs decisions that realize value." AIAA Digital Engineering Integration Committee and AIA Technical Operations Council, Digital Twin: Definition & Value, December 2020. Retrieved from AIAA: https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/policy-papers/digital-twin-institute-position-paper-(december-2020).pdf.

© 2023 National Defense Industrial Association. All rights reserved.

Provenance and Supply chain traceability[7]: Utilization of physical identifiers linked to a digital thread that connects devices as they travel through the supply chain. This will include linkages (a relationship) to provenance (includes assurance claims linked to data) while protecting proprietary information. Without supply chain traceability, there is no ability to provide accountability for risk mitigation and assurance, and maximize economic value.

- **Provenance** - The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data at each step. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.
- **Traceability** - A domain of consideration encompassing the process for determining the provenance of an item (also referred to as tracking)
- **Pedigree** - The validation of the composition of technologies, products, and services at each step.
- **Non-repudiation** - The assurance that someone cannot deny the validity of something or refute responsibility.



[7] See Figure 3 for the relationship and definition of these terms.

© 2023 National Defense Industrial Association. All rights reserved.

Figure 3: Provenance and Derivative Terms[8]

Market Preference: Consumer behavior today places an overwhelming value on performance and price with related demand that drives 98% of global semiconductor production (supply). As the scale of commercial demand drives supply investments, altering the commercial buying behavior model to include valuing assured supply will then provide economic incentives, or demand, for industry adoption, truly establishing a dual use demand business case for secure supply compliant with the standard(s)[9,10]. Regulations and requirements applied to both defense and non-defense market segments can also help value the standard(s) and further tip the scales. Market preferences will reduce challenges and favorably influence opportunities to achieve national economic and security objectives.

Market Access and Usage: By developing microelectronics architectures that link securely embedded identifies in the hardware to enable physical asset traceability through trusted digital threads, stakeholders in the microelectronics value chain can use this new tool to regulate market access, usage, and enable new "anything as a service" business models such as pay-as-you-go and chip use leases.

Supply chain traceability of microelectronics components, and the supporting infrastructure of requirements and standards, can create the level of supply chain transparency needed to accelerate the creation of smart value chains and digital marketplaces for microelectronics

[8] SAE International, SAE JA7496, Cyber-Physical Systems Security Engineering Plan (CPSSEP), June 2022. Retrieved from SAE International: https://www.sae.org/standards/content/ja7496_202206/

[9] Adam Hastings & Simha Sethumadhavan, *A New Doctrine for Hardware Security*, 2020. Retrieved from ArXiv.org: https://arxiv.org/pdf/2007.09537.pdf

[10] Simha Sethumadhavan & Tim Sherwood, *Mechanism Design for Improving*, 2022. Retrieved from Computing Community Consortium: https://cra.org/ccc/wp-content/uploads/sites/2/2023/04/01378-Mechanism-Design-Workshop-Report.pdf

© 2023 National Defense Industrial Association. All rights reserved.

and market preference. All this can be jump-started by policy and incentives. Key benefits include enabling new market opportunities, efficiencies, and managing system level risks by mitigating through the assurance of authenticity, and, most importantly, the enablement of U.S. and allied Nations' leadership in microelectronics to ensure supply continues un-interupted.

Recommended Next Steps

Figure 4 shows a high-level overview of the recommendations, beginning with three main works (in block 1) recommended to further detail the primary elements introduced in this whitepaper. Blocks 2-4 contain elements that should be inserted as appropriate into those three work areas to produce the desired result.

© 2023 National Defense Industrial Association. All rights reserved.

1. Further Standards Development	•Established industry consensus standards in three work areas... •1. Physical traceability •2. Assurance standards with market preferences •3. Data marketplaces, including traceability & IP compliance •Use cases & exemplar inillustration for these areas
2. USG Efforts:	•Acquisition regulations requiring electronics supply in accordance with industry consensus standards •USG Funding to facilitate above
3. Drive Market Adoption	•Policy driving market behavior for defense and critical infrastructure (preference for domestic & allied manufacturing)
4. Supporting Recommendations	•Education and workforce development •Scientific work that combines incentives and technology •Make security accountable and explainable •Co-develop emerging technologies •Prioritize human impacts of hardware security

Figure 4: Overview of Recommendations

The three new work areas recommended to further develop matters discussed in this paper are briefly introduced below. Additionally use cases and an exemplar illustration for context are desired.

1. **Physical traceability** of parts across the supply chain tied to digital traceability that enables validation and remediation of quality, reliability, safety, and security concerns across the entire supply chain (to include provenance and assurance).

© 2023 National Defense Industrial Association. All rights reserved.

2. Establish **assurance standards and market preferences** requiring those standards that drive the United States Government/Department of Defense (USG/DoD), critical infrastructure, and consumer demand to U.S. supply to drive capabilities, capacity, and sustainable profitability domestically. Internationally developed standards with allied nations can have a benefit, complementary supply from allied nations. These standards should take into consideration existing standards (such as IPC traceability standards) and programs (such as DMEA Trusted IC Program and RAMP-C) and address gaps where appropriate.
3. Digital/virtual modeling and traceability of the microelectronics supply chain and establishment of **data marketplaces and apps** that drive value to consumers, industry, the USG and their allies.
4. Use Cases – suggestions: 1) Intellectual Property (IP) compliance and traceability 2) physical traceability and provenance.
5. Exemplar or story illustrating at least one use case.

© 2023 National Defense Industrial Association. All rights reserved.

Contributors

Below is a list of the contributors of this paper:

Eustace Asanghanwa, Microsoft

Brett Attaway, Siemens

Bert Clements, Army DEVCOM

Zachary A. Collier, Radford University

Dave Chesebrough, Defined Business Solutions

Donald Davidson, Synopsys

Daniel DiMase, Aerocyonics, Inc.

Tom Katsioulas, Archon Design Solutions, Inc.

Tom Dodson, Intel

Michael Durkan, Siemens

Larry Gurule, I-Infusion

Joel Heebink, Aerocyonics, Inc.

Dave Huntley, PDF Solutions

Kirsten Koepsel, Aerocyonics, Inc.

Cesar Martinez, Intel

Jeremy Muldavin, GlobalFoundries

Eli Munson, Maxar Technologies

Harvey Reed, MITRE

Simha Sethumadhavan, Columbia University

Kevin Sink, TTI, Inc.

Christopher Sundberg, Woodward, Inc.

Ezra Hall, GlobalFoundries

© 2023 National Defense Industrial Association. All rights reserved.

Members of the Electronics Division reviewed this paper prior to its publication. For more information about the Electronics Division, including a list of upcoming events, please visit NDIA.org/Divisions/Electronics

—END—

© 2023 National Defense Industrial Association. All rights reserved.