STAMP Initiative Workshop 2025

Advancing Semiconductor Traceability & Security

Date & Time: March 4, 2025

10:00 AM – 4:00 PM EST

Virtual Host: Sandia National Laboratories

STAMP Initiative Overview:

The Semiconductor Traceability and Market Provenance (STAMP) is a multi-stakeholder effort aimed at implementing robust traceability solutions across the semiconductor industry. By aligning with policies such as the U.S. CHIPS Act and the EU CHIPS Act, this initiative fosters international collaboration to protect critical infrastructure and national interests by creating a market preference for assured supply of semiconductor.

Why This Matters:

The rapid growth of the semiconductor industry and rising geopolitical tensions have highlighted the urgent need for a secure and transparent global supply chain, achievable through traceability, provenance, and marketplace that values and assure supply. Counterfeiting, adversarial exploitation, and supply chain disruptions present critical risks to economic and national security. The STAMP team seeks to support the development of a Global Chip Traceability ID system that ensures supply chain integrity, enhances security, and drives economic resilience.

Key Topics & Agenda

This second workshop, following a successful EU meeting, will cover essential topics shaping the future of semiconductor traceability:

- **Aligning International Priorities:** Building international cooperation on semiconductor security.
- **Traceability Frameworks:** Exploring solutions for a secure and interoperable traceability ecosystem.
- **Industry & Government Collaboration:** Strengthening partnerships and standards.
- **Economics & Policy Strategies:** Identifying financial incentives and policy support.
- **Integration of Traceability & Risk Management:** Linking trust and assurance throughout supply chains.

Global Traceability Framework



Align U.S. - EU Policy

Funding Opportunities & Challenges

Partnerships for Adoption

Workshop Agenda





10:00-10:15 AM – **Welcome & Workshop Overview**
Introduction by Dan DiMase, Jim Gobes, Rick McCormick
Key organizational goals & expected outcomes



10:15-10:45 AM – **Keynote: The Need and Vision for the Future**
Speaker: Jeremy Muldavin
Addressing security challenges in semiconductor supply chains




10:45-11:30 AM – **European Progress and Coordination**
Speakers: Eduard Hoeberichts, Patrick Langlois , Johanna Baehr
Update on Global Chip Traceability initiative Workshop in the EU, Feasibility Study, and Fraunhofer AISEC WG on Velektronik Trusted Microelectronics



11:30 AM-12:15 PM – **Architectural Solutions & Panel Discussion**
Moderator: Don Davidson
Panelists:

- *UT Dallas - **Yiorgos Makris**,*
- *University of Kansas - **Sumaiya Shomaji***
- *Hushmesh - **Manu Fontaine***
- *Micron - **Jeff Shiner***

Panelists from industry and government discussing architectural approaches and solutions



12:30-1:30 PM – **Standards Panel**
Moderator: Dan DiMase
Panelists:

- *SEMI – **Paul Trio**: Director, Standards*
- *SAE – **Rich King:** Director, Government & Industry Affairs, Aerospace*
- *IPC/USPAE – **James Will**: Executive Director*
- *NIST – **Sanjay Rekhi:** Group Leader of the Security Components and Mechanisms Group within the Computer Security Division*
- *Ford Motor Co - **Gloria D'Anna** – SAE G-32 Co-Chair*



1:30-2:30 PM – **Traceability Economics and Business Models**
Moderator: Tom Katsioulas

- *Airbus - **Andreas Schweiger**: System Architect, Defense & Space*
- *Lockheed Martin - **Brian Gabriel**: Critical Materials Senior Manager*
- *Infineon - **Theodore Varelas**: Director Strategic Initiatives, Digital Security & Identity*
- *GlobalFoundries - **Ezra Hall**: GF Worldwide A&D Business leader*
- *Integra Technologies - **Sultan Lilani**: Technical Business Development*
- *Cadence Design Systems - **Steve Carlson**: Technology and Market Strategist*
- *Tartan Silicon Inc. - **Alan Aronoff**: Founder and CEO*
- *Synopsys - **Reed Hinkel**: Director, Strategic Programs*
- *PDF Solutions - **Christophe Begue**: Vice President of Corporate Strategic Marketing*

Driving value from end applications to chip design and manufacturing



2:30-3:00 PM – **Meta-framework for Supply Chain Trustability**
Speaker: Micheal Pease
Update on NIST IR8536 efforts and the meta-framework

Workshop Agenda



3:00-3:30 PM – **Initiative Ecosystem Panel**
Moderator: Jim Gobes
Connecting traceability to adjacent security initiatives
Panelists:

- *DMEA – **Aman Gahoonia**: Director TAPO*
- *Aerospace Corporation – **Christine Rink**: Principal Engineer*
- *Mission Critical Systems – **Don Davidson**: SCRM and Policy Expert*
- *Chip Scan – **Calvin Chu**: COO*
- *MITRE - **Brett Meadows**: System Security Engineer*

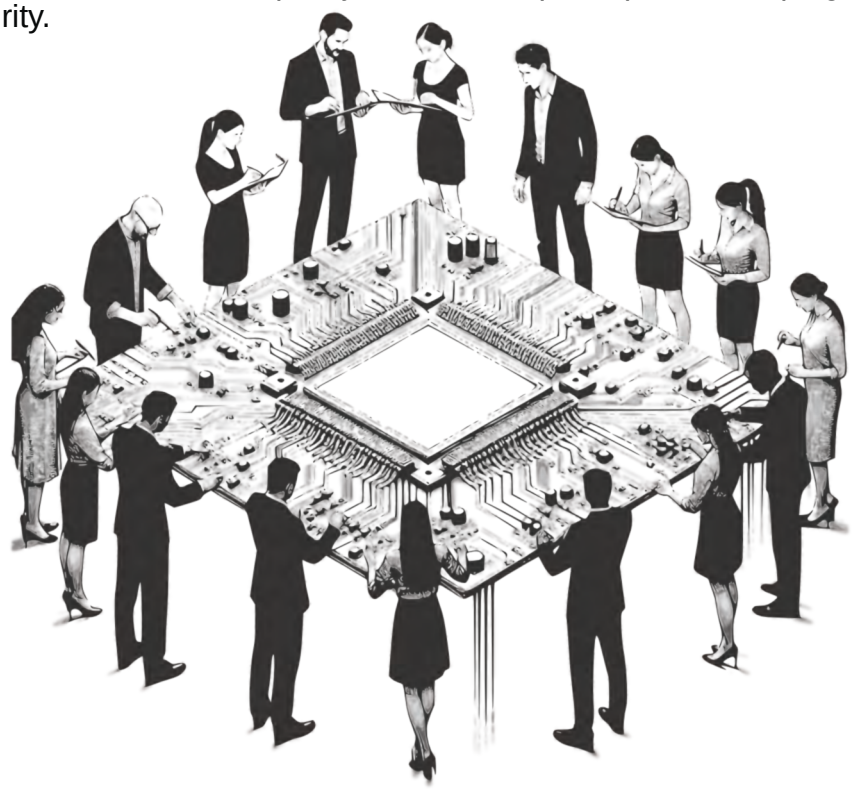
3:30-4:00 PM – **Wrap & Discussion**
Moderator: Jim Gobes
Active discussion and feedback on next steps to build a multi-year campaign.

How to Get Involved

Register for the Workshop:
https://events.gcc.teams.microsoft.com/event/633189c7-7c95-4b2e-85bc-a812b08893d9@7ccb5a20-a303-498c-b0c1-29007381b574

Contribute to Future Events:
Participate in panel discussions and working groups. Join us for the "**Global Chip Traceability: Securing the Semiconductor Supply Chain"** Panel session at GOMAC 2025 and an upcoming NIST Workshop in MD on the15th of April. Your participation in these and future workshops helps build momentum.

Join the STAMP Initiative:
Engage with global leaders on semiconductor security. The STAMP Initiative invites all global stakeholders—government agencies, semiconductor manufacturers, trade organizations, infrastructure providers, end users, and policy leaders—to participate in shaping the future of chip traceability and security.



STAMP Introduction for March 4th Workshop

Welcome to the STAMP Workshop hosted by Sandia National Laboratories. The Semiconductor Traceability and Market Provenance (STAMP) Initiative is a grassroots, cross-border collaboration of thought leaders dedicated to ensuring provenance, security, and traceability in the global microelectronics supply chain. Born from industry and government concerns over supply chain integrity, STAMP has rapidly gained momentum, attracting interest from major corporations, industry groups, and government agencies across the U.S., Europe, and beyond.

STAMP is leading the charge to establish a Global Chip Identifier (GCI) infrastructure and methodologies—one that ensures every semiconductor can be traced from design through manufacturing to deployment. By linking the digital thread of meta-data associated with physical objects, the initiative aims to mitigate supply chain risks, combat counterfeiting, enhance export controls, and enable new business models in semiconductor lifecycle management.

This initiative aligns with the U.S. CHIPS Act, the EU CHIPS Act, and other allied nation investments that include emerging global security policies, fostering a unified approach to trusted and assured microelectronics. Through its ecosystem of semiconductor manufacturers, policymakers, and cybersecurity experts, STAMP is pioneering the standards and infrastructure necessary for assured and preferred semiconductor supply chains—critical for industries such as defense, automotive, IoT, and advanced computing.

With feasibility studies, pilot programs, and industry-wide adoption roadmaps underway, STAMP is not just a vision—it is an actionable framework shaping the future of secure, transparent, and resilient semiconductor supply chains.

Today's workshop brings together key stakeholders to advance this effort—aligning our collective expertise, identifying challenges, and driving concrete next steps toward implementation.

Why This Initiative is Personally Important to Me

Throughout my career, I have worked across multiple areas of the microelectronics supply chain, including microelectronics fabrication, franchise and non-franchised distribution, integration, maintenance, and repair. I have served in several key roles that exposed me to the challenges and risks of supply chain vulnerabilities:

- **President of ERAI**, where I investigated, mediated, and reported **supply chain issues**
- **Industry advisory committee member of GIDEP**, which reports on **counterfeiting and obsolescence issues**
- **Member of the Customs and Border Protection's Intellectual Property Rights subcommittee** in the **Customs Operations Advisory Committee**
- **Director of Compliance and Quality at Honeywell**, where I oversaw critical supply chain investigations

In all of these roles, I have seen firsthand the impact of counterfeit and tampered parts and have been directly involved in investigating supply chain failures. Many of these investigations took years to resolve due to the lack of traceability of the origin and destination of component parts and die.

Today, the microelectronics supply chain lacks upstream and downstream visibility. When quality issues arise, most companies can only provide a statistical analysis of affected parts, rather than pinpointing exactly where and how problematic components were used.

This lack of traceability is particularly concerning for cyber-physical systems security, where new zero-day vulnerabilities are discovered, yet cannot be easily patched or replaced in the field. This was starkly evident with the Spectre and Meltdown vulnerabilities, where:

- Over 20 years of microelectronics production were impacted before the vulnerability was discovered
- Decades of fielded systems were affected, many of which are still in use today
- New variants of the vulnerability continue to emerge, with no clear way to track and mitigate the impact

The Growing Need for Traceability in Advanced Packaging

The need for traceability will be even more critical as the industry moves toward advanced packaging solutions. With multi-die chiplets integrated into a single package, ensuring provenance and security at the die level will be a new challenge. Unlike traditional monolithic chips, chiplets are sourced from multiple manufacturers and assembled into a final product—introducing new risks of counterfeiting, quality issues, and security vulnerabilities.

Without robust traceability mechanisms, it will become increasingly difficult to identify the origin of a compromised or defective die, leading to prolonged investigations, operational disruptions, and security risks. Implementing a standardized approach to traceability—down to the individual chiplet level—is essential to maintaining trust and integrity in next-generation microelectronics.

STAMP represents an opportunity to fundamentally change how we manage risk, ensure trust, and protect critical systems. By working together, we can establish a foundation for microelectronics security that benefits industry, government, and society as a whole.

It is my pleasure to introduce our host, Rick McCormick who is a Senior Scientist at Sandia National Laboratories, where he leads Semiconductor Technology Strategy in the Microsystems Engineering, Science, & Applications (MESA) center. In prior department and senior management roles at Sandia, his departments delivered leading edge research and products spanning silicon and compound semiconductor electronic and photonic technologies for rad-hard electronics and photonics in nuclear weapons and satellites, advanced computing systems, power electronics & photovoltaics, and quantum photonics. He currently leads Sandia's efforts for contributions and partnerships under the recent CHIPS and Science Act legislation, and has program responsibility for over $14M of research in Sandia's Nanodevices and Microsystems Lab-directed R&D foundation. Prior to his current role, Rick led dozens of advanced technology R&D and product

development and manufacturing programs at AT&T Bell Laboratories, R&D startups, Emcore Fiber Optics, and Sandia. He received his BSEE, MSEE, and Ph.D. degrees from the University of Washington, Georgia Institute of Technology, and Heriot-Watt University (Edinburgh), in 1981, 1983, and 1993. He has over 80 publications, 4 book chapters and 16 patents. He served on several NSF center advisory boards and currently serves on the Strategic Advisory Board for the AIM Photonics Manufacturing Institute.

Rick, off to you!

Sandia National Laboratories

Exceptional service in the national interest



STAMP Workshop

Rick McCormick

Senior Scientist, Semiconductor Technology Strategy

Microsystems Engineering, Science, and Applications (MESA)

fbmccor@sandia.gov www.sandia.gov/mesa

Welcome & Thank You!

Mar 2025

MESA

Research | Develop | Produce

NNSA U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

SANDIA'S HISTORY:
THE MANHATTAN PROJECT

SANDIA IS A FFRDC:
FEDERALLY FUNDED R&D CENTER



THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

I am writing a similar note direct to Dr. O. E. Buckley.

Very sincerely yours,

Harry Truman

Mr. Leroy A. Wilson,
President,
American Telephone and Tele
195 Broadway,
New York 7, N. Y.

Government-owned, contractor-operated

FFRDCs are long-term strategic partners to the federal government, operating in the public interest with objectivity and independence and maintaining core competencies in missions of national significance

Sandia: A National Security Laboratory

FIVE MAJOR PROGRAM PORTFOLIOS



Sandia: ~ 17,000 Staff, ~$5.5B costing

- Microelectronics and microsystems are key enablers for all of our missions.
- Current and future products are heterointegrated combinations of different technologies (Si and III-V electronics, MEMS, Photonics, Quantum, etc.).
- Many/most of our missions require operation in challenging extreme environments and high levels of trust & security.
- Key Needs- Production & R&D partners, STEM Staff

Sandia's broad semiconductor capabilities

MESA

Microsystems Engineering, Science, & Applications



- **Only production semi fabs in the DOE: providing what industry cannot, will not, or should not**
- **Trusted source for custom strategically radiation hard (TSRH) microelectronics**
- **Largest government owned 2+ fabs (Silicon, Compound, & Advanced Packaging / HI)**

MESA: ~300,000 parts across 44+ products

Research & Development | Si µSys (CMOS) | III-V µSys (HBT) | MEMS | Photonics (Si, III-V) | Production

Full production flow, from design to fabrication to packaging to product acceptance

Other key Sandia facilities :
CINT and PRF: DOE/SC User facilities
IBL and Rad reactors/accelerators
Counterfeit Detection Center
High Performance Computing Testbeds & SW



- **40 yrs. of Research & Product impact**
- **>300 Patents**
- **69 past CRADAs + 9 currently active**
- **1000+ Tech. Transfer exemplars**
- **1000+ Licenses**
- **45 R&D 100 Awards**

Semiconductor Traceability and Market Provenance (STAMP): US-EU initiative

Jeremy Muldavin

Cadence Design Systems, Inc.

Contact Information

617-710-9784 c, muldavin@cadence.com

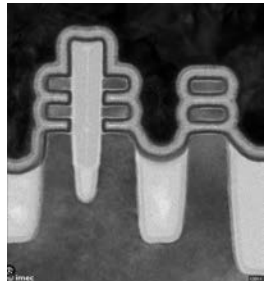


Our Cyber-Physical Infrastructure

Connected



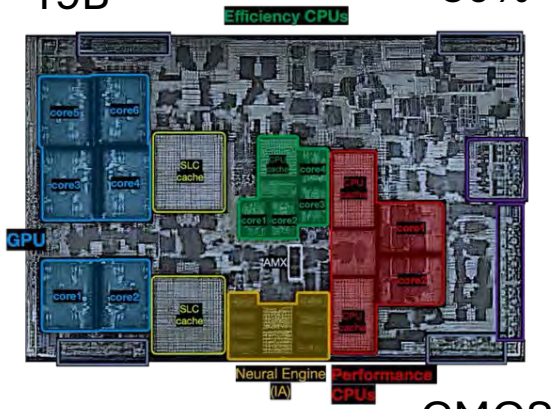
Complex



CPU
GPU
NPU

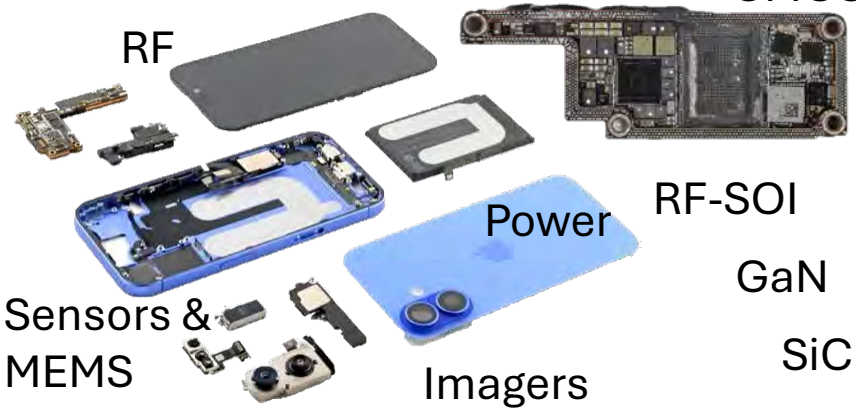
“3nm”
19B

50%



CMOS

RF



RF-SOI

Power

GaN

SiC

Sensors &
MEMS

Imagers

Distributed



Semiconductor Supply Stages

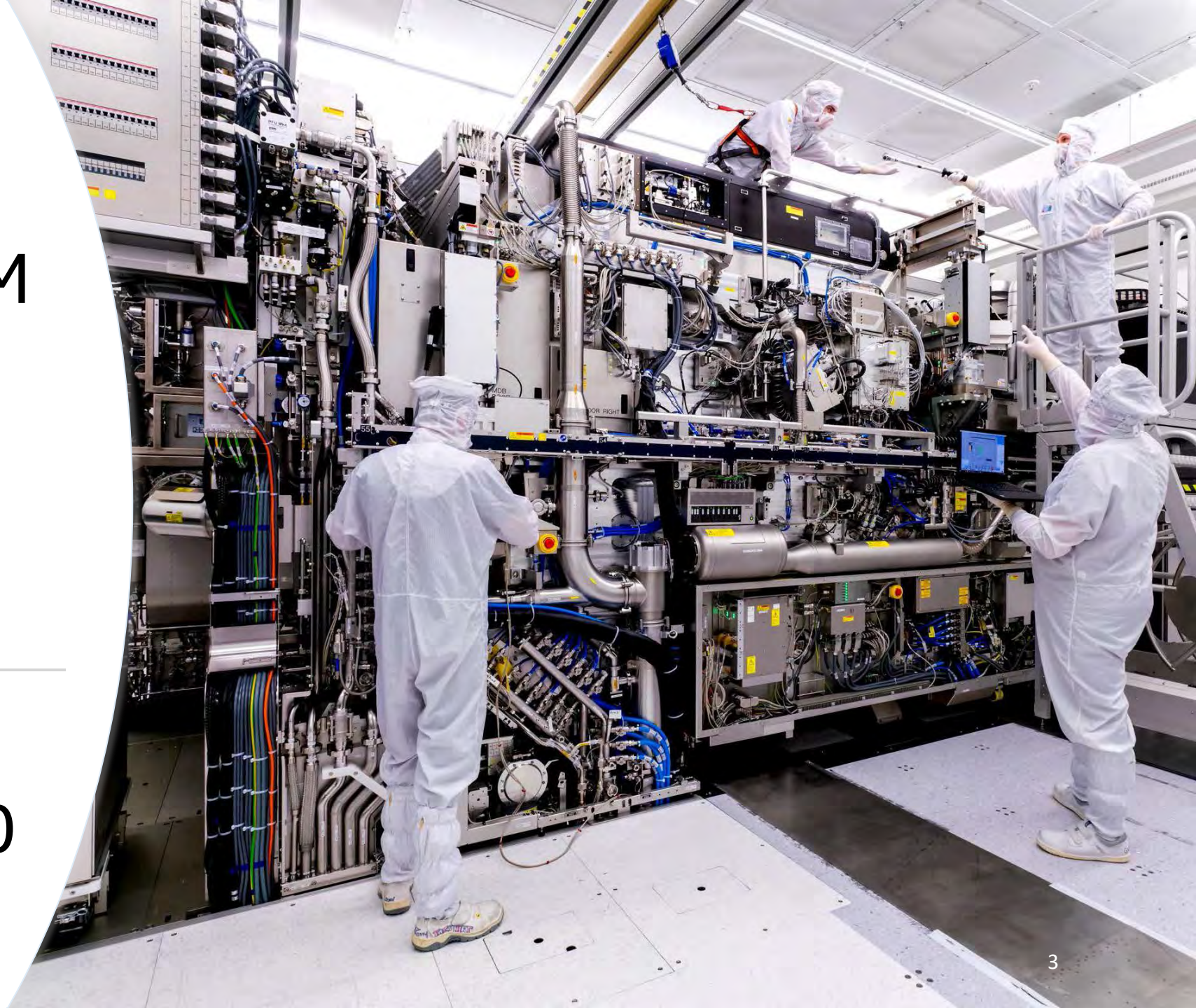


Apple Suppliers 2024

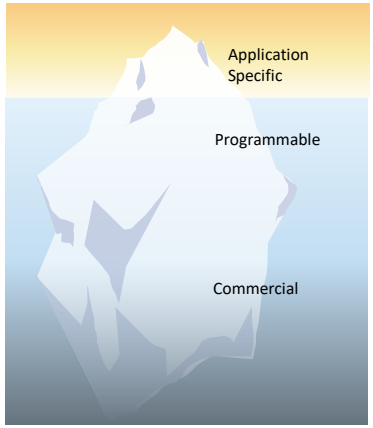
$150M

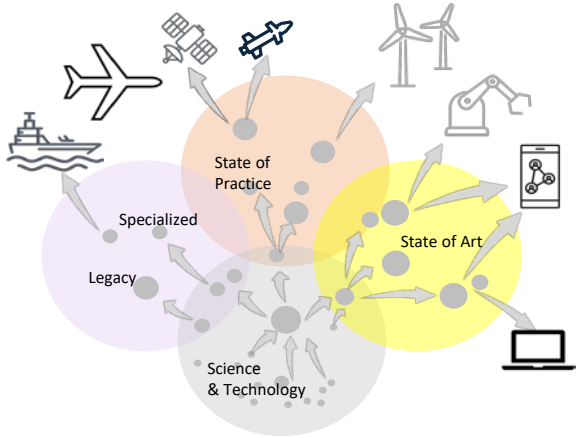
EUV Lithography

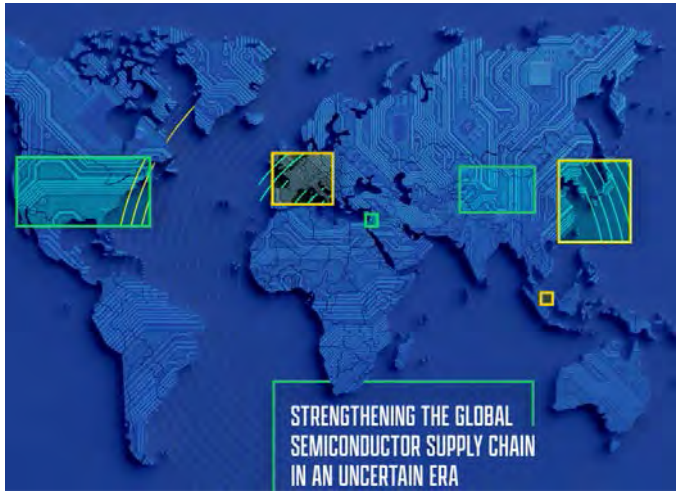
100,000



Overview of Microelectronic Needs







Commercial Foundation

- **Microelectronics enable our Economy**
- **Advanced Technology** is needed across all lithographic nodes for dual use
- **Market incentives and assurance tied to standards** can drive demand to support the business model of at scale fabs, to develop and sustain the IP ecosystems, foundry capacity, and packaging ecosystem

Technology to Capability

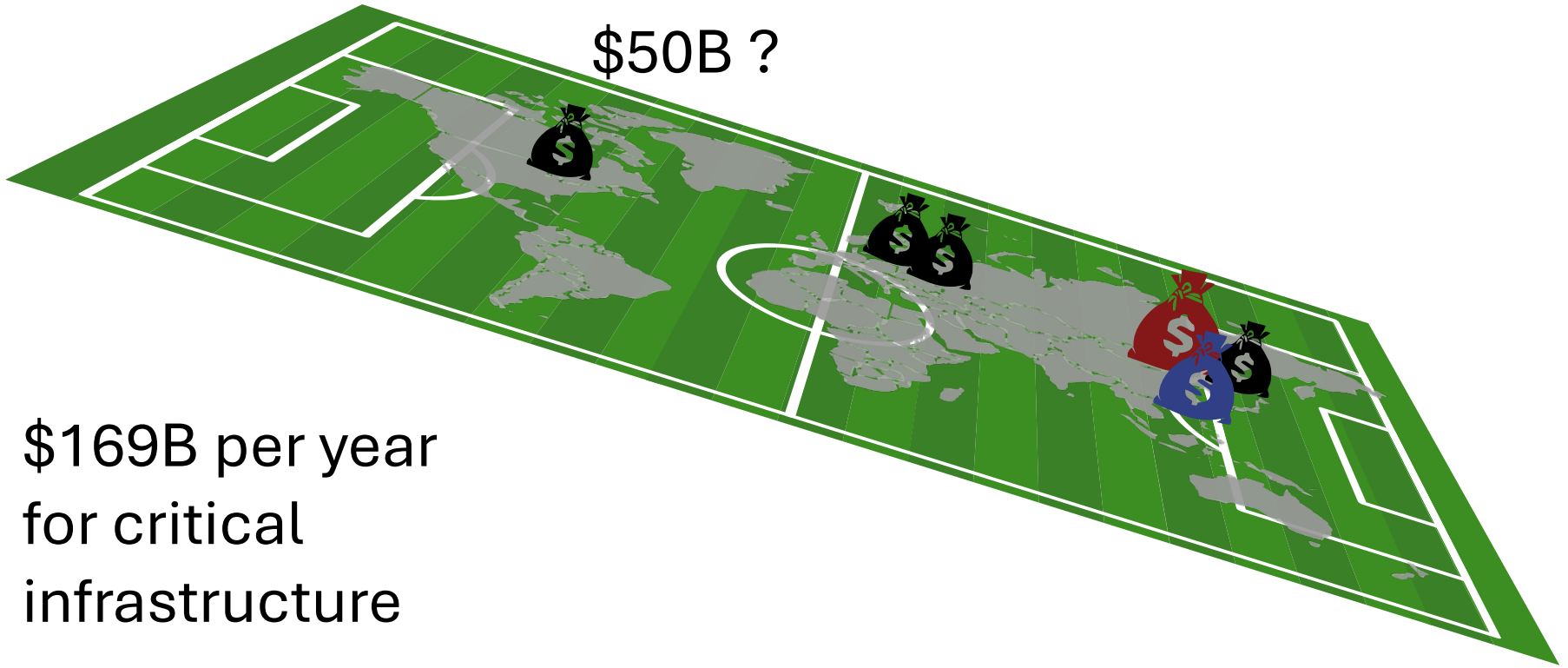
- To address security and economic interests, R&D investments must result in **assured production**
- To accomplish this, **R&D** must be done in **close collaboration with at-scale manufacturing**
- ME assurance processes and data with **end-to-end traceability** can result in technology investments that increase market leadership and security

Building Assured Supply

- **Leverage assured supply** chain partners and geographic locations to expand production
- **Coordinate investments** to accelerate development & technology transition into assured supply chains
- **Strength in standards and market preferences** can drive demand for assured supply and supply chain sustainability

Strength in standards and market preferences can fortify ME Security & Demand

How do we level the playing field?



$169B per year
for critical
infrastructure

Global Traceability Initiative

- **Urgency of Action:** Growing geopolitical tensions and rising dependence on semiconductors make the need for a secure supply chain critical. The initiative focuses on creating a unified system to trace semiconductor chips via Global Chip IDs, ensuring the security and integrity of critical technologies.

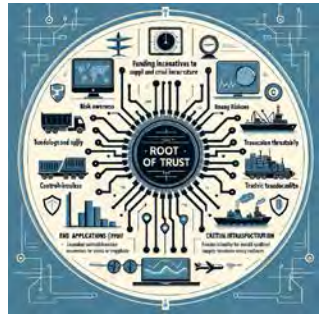


- **Strategic Alignment:** Closely aligned with the U.S. CHIPS Act, EU CHIPS Act, and U.S.-EU Trade and Technology Council. The initiative enhances economic resilience, prevents adversarial threats, and secures global infrastructure.

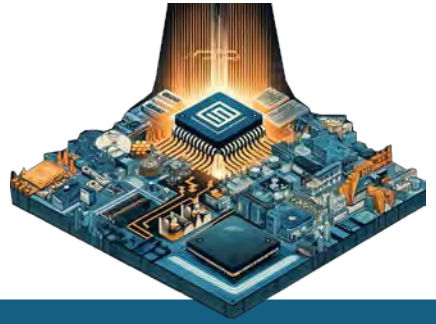


- **Call to Action:** Governments are encouraged to endorse and prioritize chip traceability in defense and key sectors. International collaboration is crucial to establish secure, traceable, and compliant semiconductor supply chains globally.



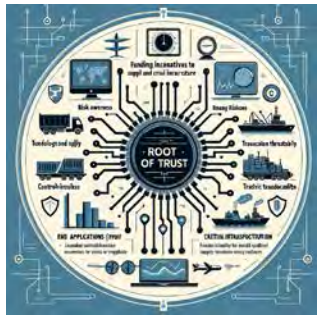


Problems Addressed by Traceability



Economic

- Unlevel playing field & Asia dominance in microelectronics
- Dumping of state of practice semiconductors by China
- No market preference for assured supply to critical infrastructure (lowest cost wins)



Technology

- Lack of awareness of risks to supply & critical infrastructure
- Traceability from R&D into assured supply needs funding incentives
- Control (root of trust) of end technology at risk



Defense

- Limited assured supply of semiconductors
- Defense and critical infrastructure are linked
- Export control and foreign military controls of technology challenging



Policy

- EU/US CHIPS supply side investments can benefit from coordination
- Lack of demand side incentives to sustain supply investments
- Lack of coordinated US/Allied technology policy (Trade and Common Defense)

* Icons generated from CHATGTP4o, don't look too closely....

Supply Chain Attributes



Approach to Assurance and Transparency

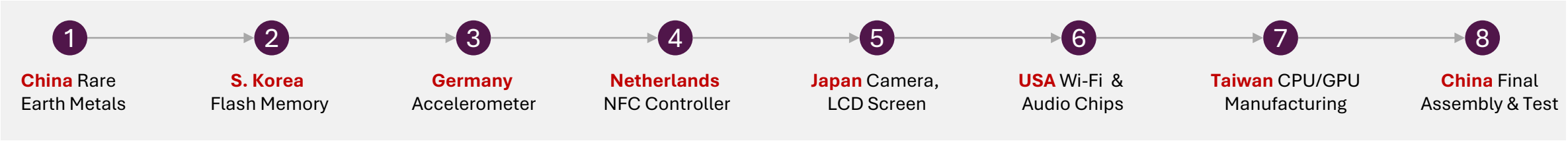


- Physical identifiers
- Digital thread
- Supporting data
- Market preference and incentive

Source: White Paper, *Assured and Preferred Supply of Microelectronics through Provenance, Traceability, and Market Preferences*, Trust and Assurance Committee, 2023

Why Chip Traceability Matters

Journey of chips though untrusted environments assembled with other chips into electronics products



Chip Supply Chain

- Lack of visibility in fragmented supply chain
- Over 65% of electronics assembled in Asia
- Ineffective sanctions and customs controls
- Costly support, liabilities, and loss of value

Critical Infrastructure

- No security in Systems & Process Sensors
- Silos and no visibility in IT/OT convergence
- Nation state attacks infiltrating supply chains*
- Compromised equipment and human safety

https://www.bloomberg.com/news/articles/2024-09-19/exploding-pagers-sound-global-alarm-for-supply-chain-security

Challenges About Chip Traceability

Industry CEO "*Traceability for Security should be our top priority... but many will turn a blind eye to security if it means even nominal higher costs. Education of the risk starts the conversation.*"

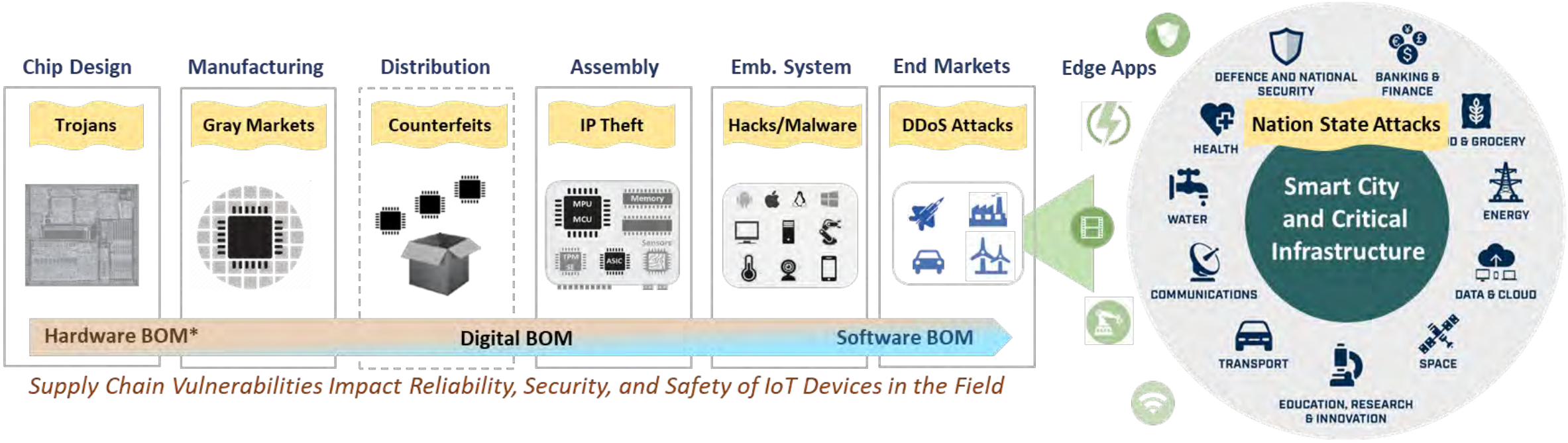
- **Perception of Investment**: Our industry prioritizes cost-efficiency views traceability as a burden
  - **Change Mindset:** Promote *Traceability for Monetization* alongside security to justify economics.

DG Connect: *"Cross-border chip supply chain traceability is very complex and needs to deal with a lot of highly sensitive data for security. Open standards can play a key role…"*

- **Complexity of Security & Data Sharing**: US and EU diversity on standards and regulations.
  - **Change Mindset:** Pursue methods enabling digital marketplaces facilitating private transactions

- **Value vs. Risk Conversation**: Frame traceability as a business opportunity that justifies ROI
  - Highlight economic benefits by focusing on business use cases with clear monetization
  - Engage executives on business models and thought leaders on strategy and roadmap.

Importance of US-EU Initiative on Traceability



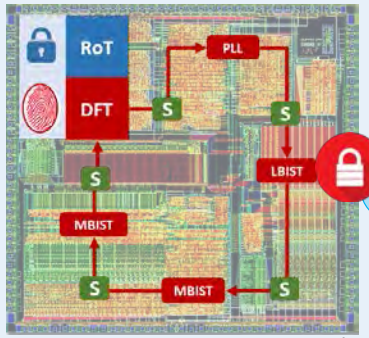
Supply Chain Vulnerabilities Impact Reliability, Security, and Safety of IoT Devices in the Field

- Safeguard allied nations' markets from being flooded by adversaries' legacy chips
- Strengthen export control and prevent western chips weaponized against our allies
- Drive resilience and new business models (analytics marketplaces, HaaS, AIoT)

*Source: NIST IoT Advisory Board Report Page 25

Business Use Case Examples

Automotive - Silicon Lifecycle Management (SLM)



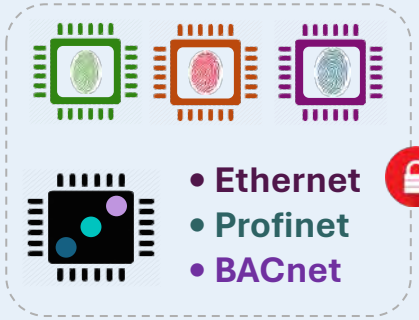
Functional Safety

Fleet Monitoring



*Source: Semiconductor Eng

Industrial - Chip Licensing & Multi Market Product



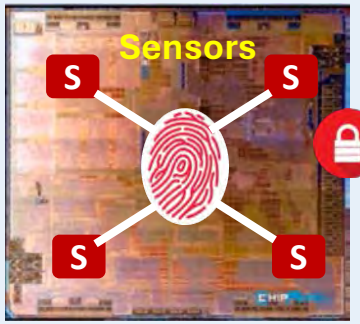
HW + SW Provisioning



*Sources: Intel - Pay-as-you-go Chip Licensing, Samsung - Memory Chip Rental Service

Global Chip ID

Aerospace & Defense - Manufacturing Integrity

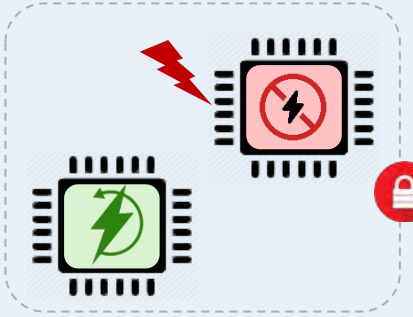


Failure Prevention



Source: ERI Summit 2020

Supply Chain - Monitoring & Regulating Field Use



Disable Adversary

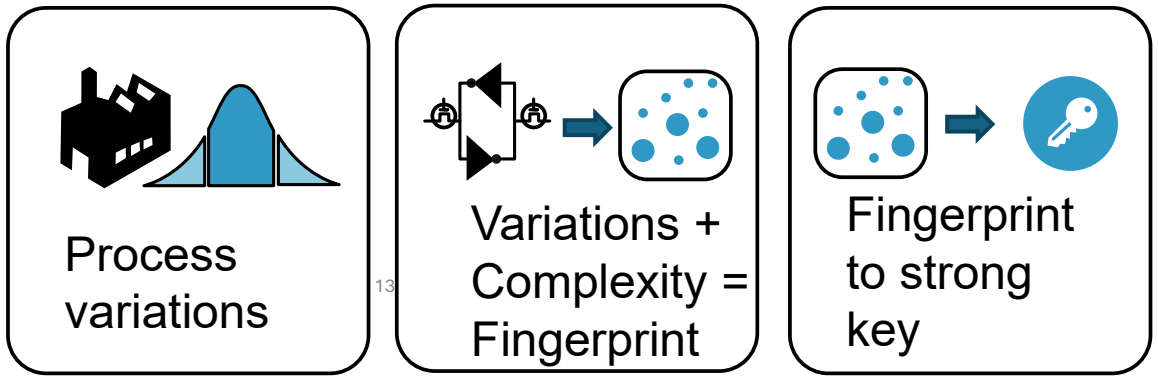


Sources: Reuters - Western chips in Russian drones, WSJ - Cheap drones in battlefields

Sources of Provenance for Assurance

- Entropy
  - Natural/physical sources for randomness
  - Foundry processes battle and carefully measure effects of entropy
  - Entropy and variation is embedded as a fingerprint in each device

- Complexity
  - Encryption
  - Obfuscation
  - Unique marking
  - Large number of states



- Multi-factor contemporaneous Data
  - Temporal - when did the occur, how does it vary, etc.
  - Spatial – where was my wafer, distribution of physical variation, etc.
  - Spectral – visible, acoustic, electrical, radiation, etc.

Examples of Design Provenance

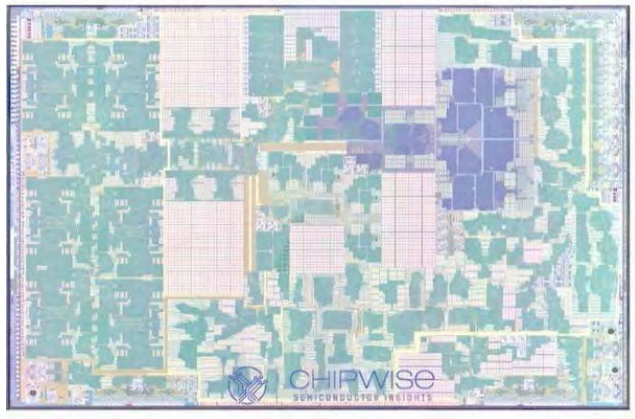
Design Provenance

- EDA and secure design environments can deliver key-stroke and executable level traceability
- Schematics and test vector can yield unique signatures



Layout Complexity

- Layout optimization and variation creates identity provenance
- Design for manufacturing IP can create test structures and built in self-test for physical provenance



IP Compliance/Assurance

- Foundries offer IP compliance services to major IP providers
- IP compliance can be extended by “deep hash” to soft IP and customers IP
- IP Assurance as a service can identify vulnerabilities before fab

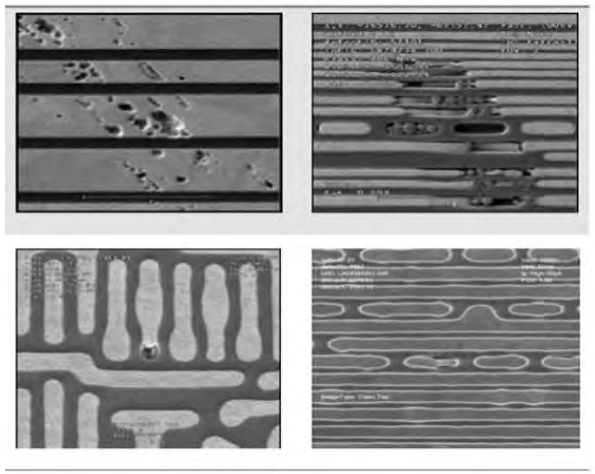


Design “digital twins” offer a rich opportunity to “deep hash” elements of design processes and output IP

Examples of Intrinsic Process Variation

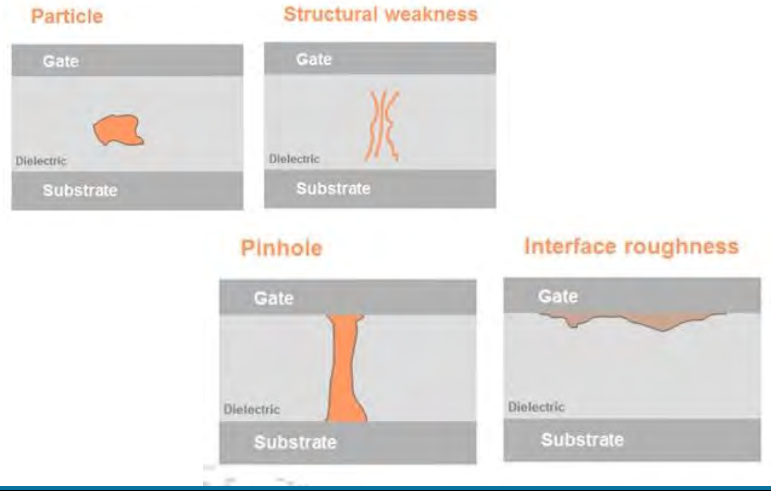
Metals

- Grain variations on small feature sizes
- Lithographic variations



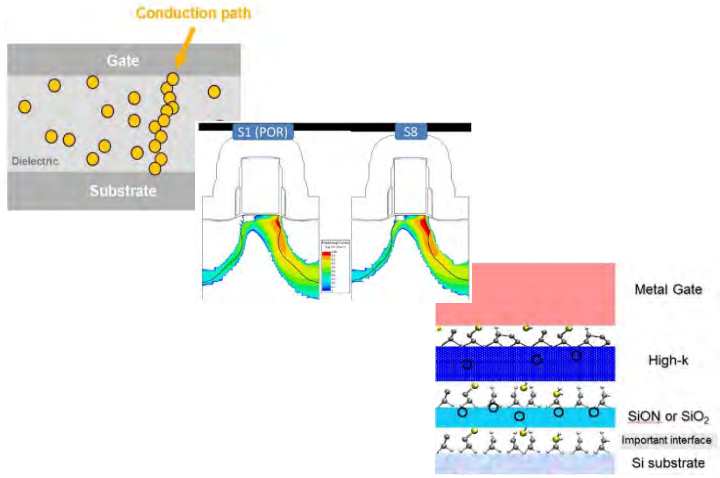
Oxides

- Oxides thickness variation
- Gate Oxide variations cause performance changes



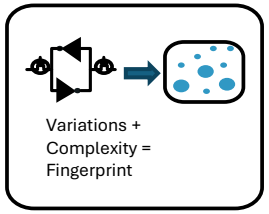
Transistors

- Time dependent breakdown
- Bias Temp instability
- Hot carrier injection



Intrinsic variation can be easily measured per die through process monitors and “canary” structures

Examples Extrinsic Variation



Die Markings

- Wafers are all marked
- Opportunity for die level marking using direct write and femto-lasers, dust, etc.
- Must be cost effective and have a high level of complexity or hash to other data

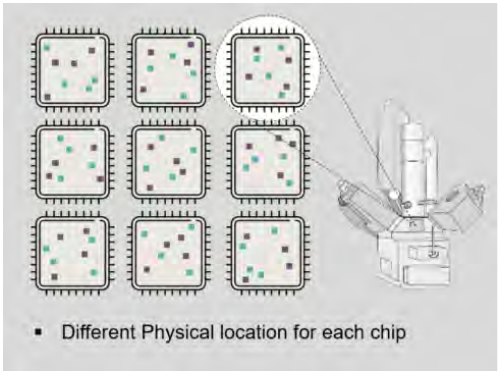
Programmable

- One-time programmable (OTP) memory allows for unique state or electrically read labels
- Embedded nonvolatile memory (eNVM) elements that are programmable and stable in state of operation can be leveraged for uniqueness

Tagging /data embedment

- Direct write of certain mask levels can create highly complex labels and embed data
- Can support electrical, optical, radiation, and other readout mechanisms
- Easy to read after packaging to tie provenance back to die



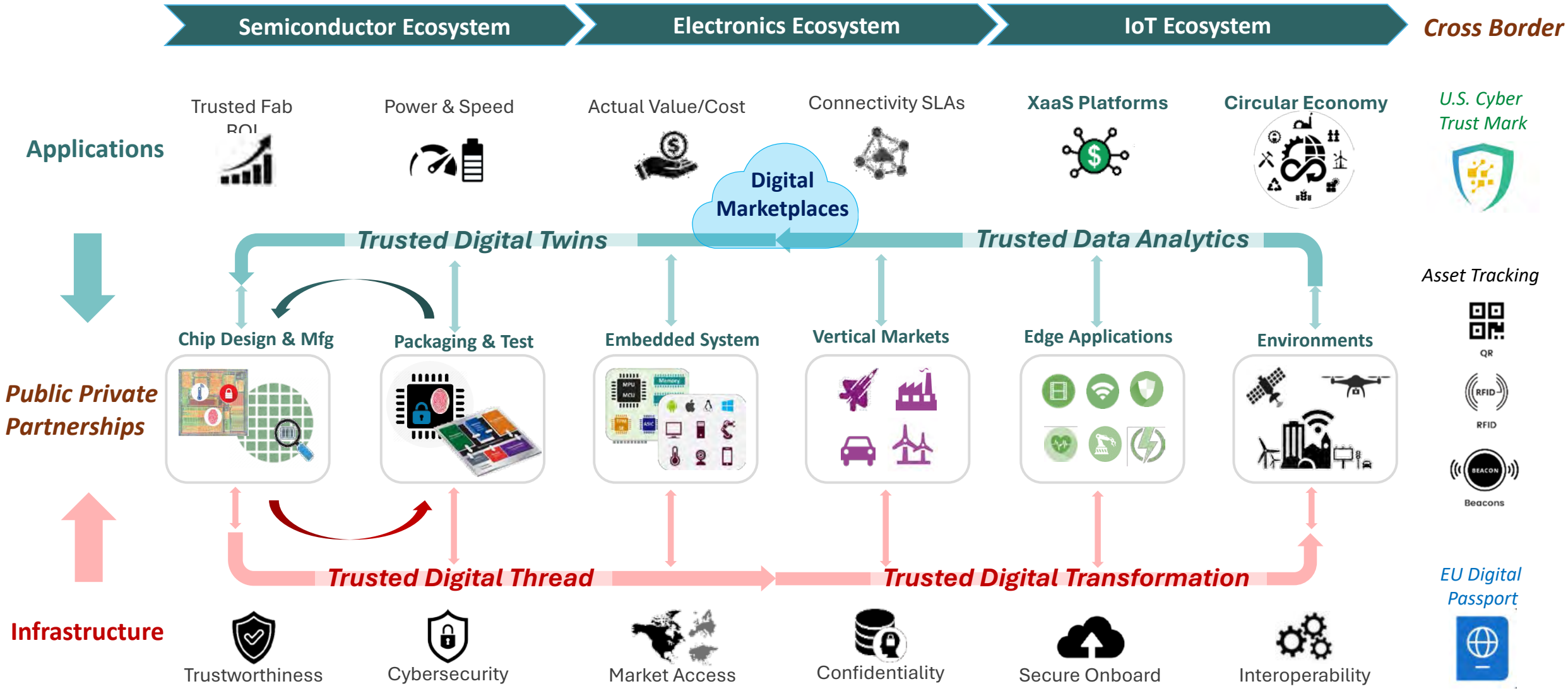




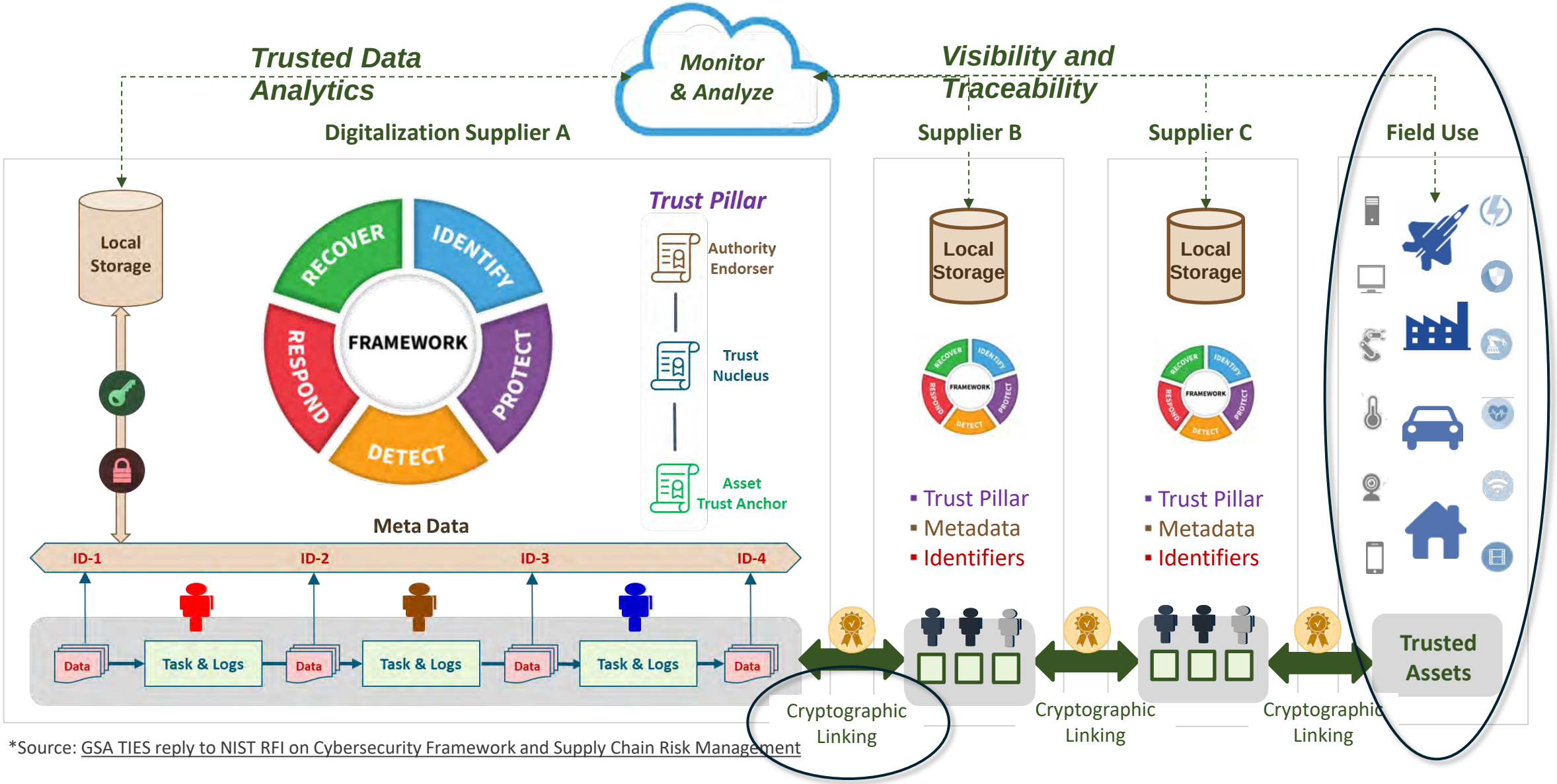
Extrinsic variation can increase ability to uniquely mark die and hash other data into the physical part

Traceability for Security and Monetization

*Included in the report of the Department of Commerce appointed IoT Advisory Board report



Digitalization of Value Chain: Data Marketplaces



*Source: GSA TIES reply to NIST RFI on Cybersecurity Framework and Supply Chain Risk Management

Needs for Adoption of Traceability



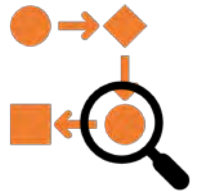
Policy and Market Behavior

- **Drive demand** tied to assurance to increase production capacity
- **Establish market incentives, policies and standards** that reduce risk of supply disruption
- **Promote the monetization of security** through traceability that can be valued by end users and consumers



Trusted Digitization Solutions

- **Illuminate supply chain** through provenance (e.g., trusted certificates, blockchain, etc.)
- **Model market risks** including non-market forces
- **Create the infrastructure** to monetize assured supply and security
- **Measure the impact of assured supply** to end-markets through market-level traceability and preference

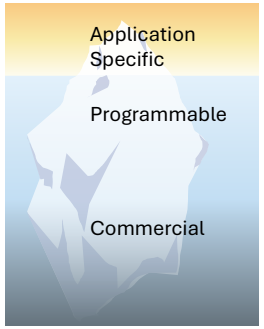


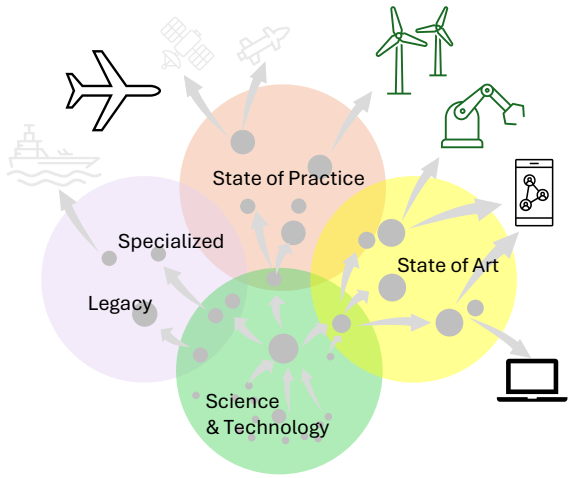
Physical Traceability & Supply Chain

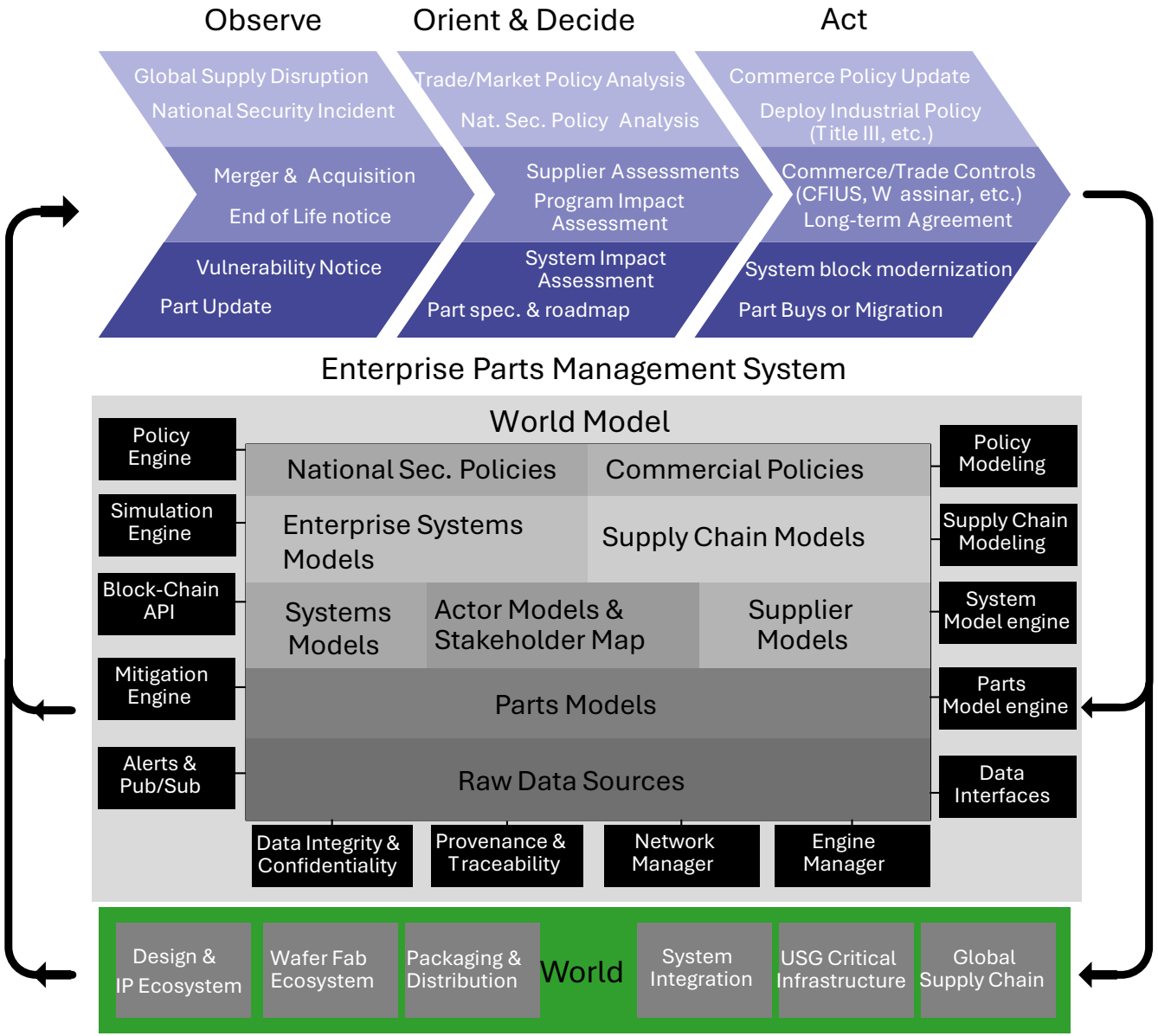
- **Implement immutable physical traceability** and validation infrastructure industry-wide
- **Standardize and validate root of trust** and hardware as a service to deliver differentiated technology through assured supply chain
- **Promote consumer level traceability tools** and marketplace

Architecture for Enterprise Management

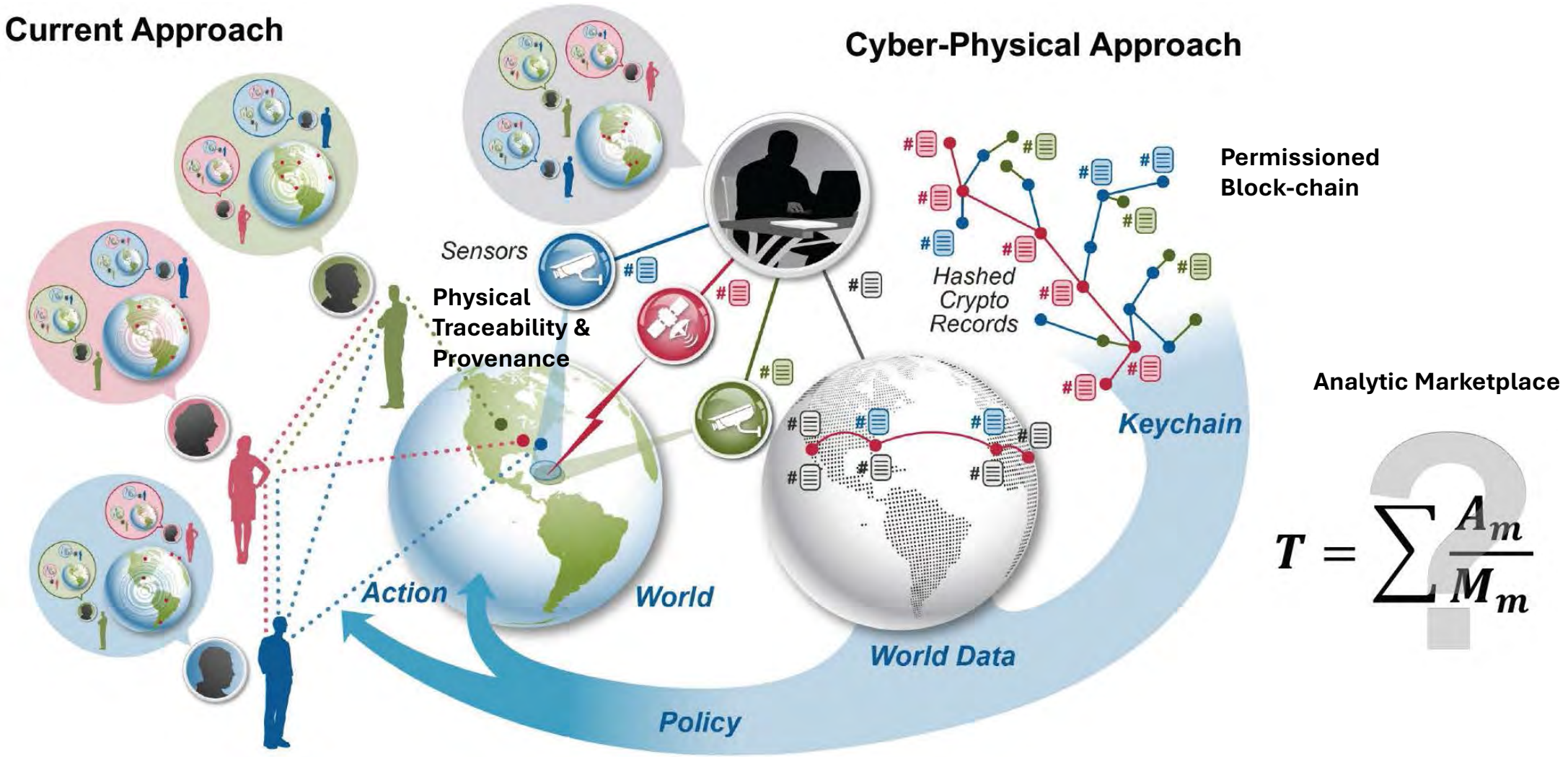
Observe, Orient, Decide, Act to Manage Parts & Supply Chains







Modern Supply Chain Assurance



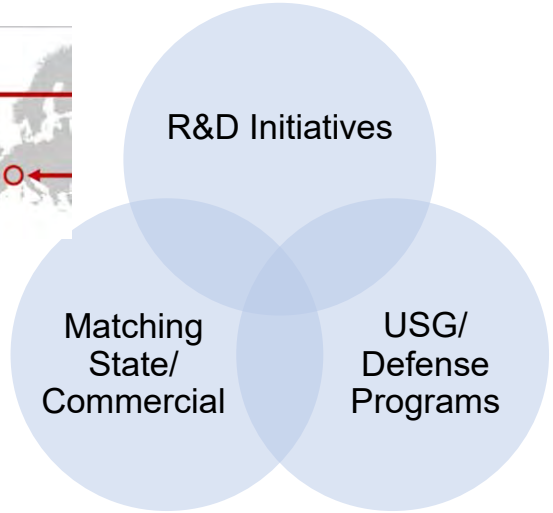
Industry and consumers adopt and USG values traceability and supply chain assurance

Assurance USG/Industry Opportunities

Dual Use Roadmap

- Senior Leader Directive & funding
- Funded dual-use roadmap (Services, DIB, ME Supply Chain, etc.) secure supply map
- Identify Assured Supply Chain mappings to Critical Infrastructure (EPMS, AMARO, MQA, DHS, etc.)

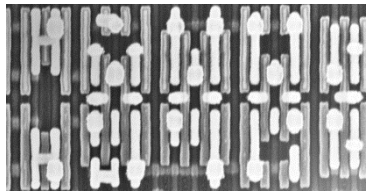




Assured Prototype Programs

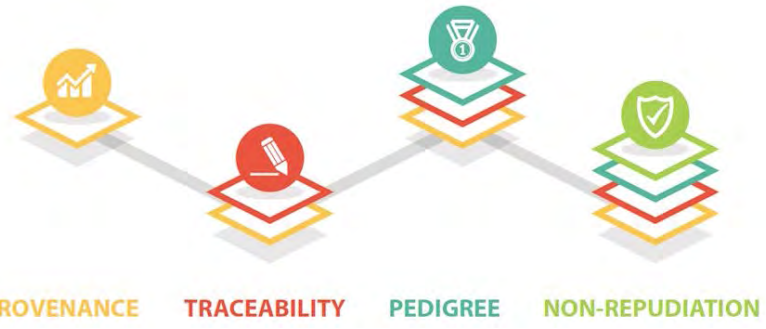
- Restock Obsolescence replacement
- Attritable Systems
- New Capability for legacy program (critical infrastructure)





Reverse Engineering

Verification & Validation



Acquisition/R&D Policy

- SWAP-C, where A = Assurance of mission, supply chain, tech overmatch, obsolescence avoidance, etc.
- 15% of Program budget for ME dedicated to demo of new ME tech every 2 years (don't have to buy it)
- Policy and Budget reform in phases to support R&D, Rapid Prototyping, Obsolescence Avoidance through assured R&D ecosystem



MICROELECTRONICS COMMONS
BRIDGING THE GAP FROM LAB TO FAB

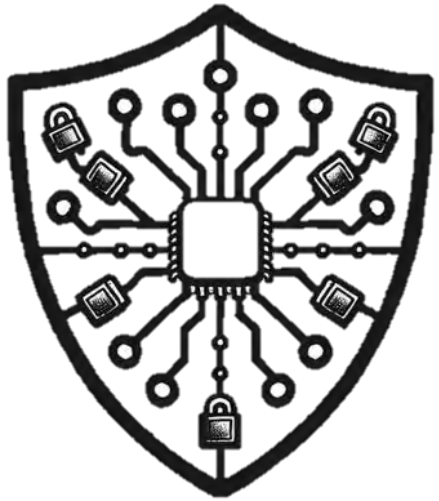
Ecosystem Participants

- **Roles and Responsibilities**:
  - **Design and Manufacture**: Ensure accurate documentation and traceability of chips from creation to production to delivery.
  - **Suppliers**: Maintain records of chip origins and ensure compliance with traceability requirements.
  - **Regulatory Bodies**: Oversee and enforce export control regulations, ensuring that all chips meet legal standards.
  - **End-Users**: Verify the traceability of chips received and ensure they are used in compliance with export control laws.
- **Focus on Defense and Dual-Use Applications**: Pay special attention to chips used in defense and dual-use technologies, ensuring strict adherence to export control regulations.



The STAMP Team Leads

- Team of Volunteers from EU and US has formed to drive the Semiconductor Traceability and Market Provenance (STAMP) initiative, promote workshops and panels, and gather support and funding for pilots
  - Team Europe
    - Eduard Hoeberichts, MA & MBA - ex Div President ASML, Founder SandGrain, CEO FabMax
    - Ir. Hans Dekker – Chief Security Architect Irdeto
    - Dr. Patrick Langlois - Former Thales, ST, and European Defense Agency
    - Prof. Dr. John Schmitz – Former Dean TU Delft and NXP VP Research and Chief IP Officer
    - Dr. Rob Hartman - Former Director of ASML Public Programs
  - Team USA
    - Tom Katsioulas – Member DoC IoT Advisory Board, Former Chair of GSA TIES
    - Dr. Jeremy Muldavin – Former MIT LL, DoD, and OSD, Distinguished Technical Staff at GF
    - Don Davidson - Executive Director, Mission Critical
    - Harvey Reed - Decentralized Capability Lead at MITRE
    - Daniel DiMase – CEO Aerocyonics, Inc.
    - Jim Gobes – Former Founder CEO Intrinsix



Progress to Date



- Meetings, letters, and engagements with EU/EC EVPs
- Meetings, support letters, commitments for engagement from EU industry leaders (several companies.)
- Meetings and indication of support from GF, Micron, Intel, and others for the general topic of traceability
- US-Korea Standards summit presentation on initiative
- Meetings with Commerce/CHIPS office leaders on with follow up meetings this week
- Meetings with EOP CyberSecurity leaders on topic with interest and support for meetings, speakers
- Meetings with OUSD(RE) senior leadership
- Meetings with Dutch senior leaders where Traceability and Market Preference are identified initiatives
- Meeting with Canadian Embassy
- Alignment and meetings with standards bodies (SEMI, SIA, etc.)
- Initial EU stakeholder and introduction meeting after SEMI Europa
- This Sandia sponsored workshop today

Upcoming Opportunities

- GOMAC Tech panel session (Jeremy Muldavin to Moderate)
- NIST NCCoE will host key US industry stakeholders meeting on April 15
- Larger international workshop in the late summer 2025



Call to Action

- **Act with Urgency:** Timing to secure our chip supply chain is now. Swift action is needed to address rising security risks and maintain global leadership.
- **Leverage Momentum:** Exploit on the massive investment in new fabs and infrastructure to drive traceability initiatives forward with industry-wide impact.
- **Start Collaborating:** Develop strong public-private partnerships. Unite industry leaders and governments to share resources and expertise
- **Accelerate Roadmap:** Start by driving awareness with workshops, launch pilot projects to validate and demonstrate the value of global Chip IDs.
- **Expand Networks:** Use trusted alliances to engage stakeholders, and drive adoption thorough business use case across the global value chains.

Closing Remarks and Next Steps

- The need for traceability and importantly market preference for trusted and assured supply is critical and momentum for action is growing
- You could be strong contributors to the initiative and could benefit from showing traceability and the value of trust beyond the defense community
- We welcome feedback and volunteers
  - Technical workshops
  - Building and Identifying funding opportunities
  - Promotion of Proof-of-concept pilots and public private partnerships

Bottom Line Up Front

Current State: Issues/Challenges/Security concerns

- Huge risk of supply disruption, dumping, attacks on critical infrastructure
- No market preference for assured supply[1]
- Insufficient funding/incentives for infrastructure, standards, and process development

[1]*Assured Supply refers to availability, confidentiality & integrity of the product*

Desired State

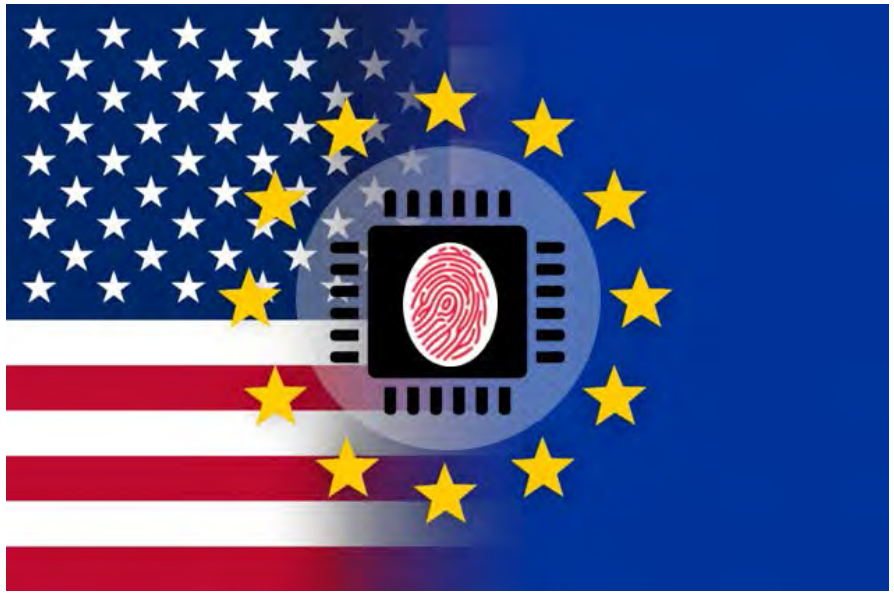
- Significant increase in allied production tied to assured supply preference for critical infrastructure
- Critical Infrastructure and consumers both value and benefit from assured efficient supply
- Public/private partnership to build traceability & provenance of assured supply market preference

What's needed:

- Market preference/policy for assured supply
- Accelerate targeted funding to build traceability and provenance for assured supply
- Fund increased government/industry participation in development of prototype infrastructure investments leveraging assured supply and traceability

Next Steps (TBD):

- Support and fund engagement in international standards and policy (workshops, high-level EU/US leadership syncs)
- Build funding program and RFS for traceability and provenance of assured ME supply in targeted pilots for critical infrastructure and national security
- Policy focused to build market preference to assured supply for critical infrastructure



Global Chip Traceability Initiative

Global Unique and Immutable Chip Identifiers

A Trans-Atlantic Initiative

Introduction – EUROPE Status

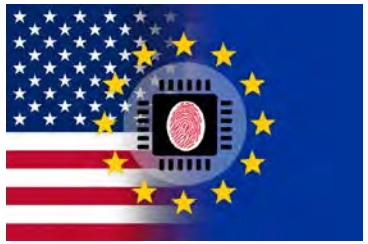
STAMP Workshop USA

Presentation



1. Team + SEMI
2. Initiative goal and vision
3. Pilot Feasibility Study 2025
4. February 2025 - Status of initiative
5. Targeted US, EU & Allied Nation Organizations
6. Traceability Adoption - implementation path
7. Global Chip ID vs other Federated Database Concepts
8. Relevance of the initiative for EU institutions
9. Discussion Traceability & Security

Members of the (Ecosystem) Expert Team



Team Europe

- Eduard Hoeberichts - former Division President ASML, Founder SandGrain, CEO FabMax
- Dr. Patrick Langlois - former Thales, ST and European Defense Agency
- Prof. Dr. John Schmitz - NXP (Fab Director, VP Research & Chief IP Officer) and Dean TU Delft
- Dr. Rob Hartman - former Director of ASML Public Programs
- Ir. Hans Dekker - CSA Irdeto Cyber Security expert

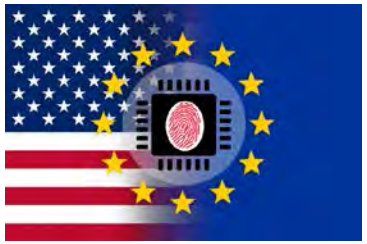
Team USA

- Tom Katsioulas – Archon-DS, ex-Member IoT Advisory Board & Chair GSA Trust IoT Ecosystem (TIES)
- Dr. Jeremy Muldavin - former MIT LL, DOD and OSD and Program Director GlobalFoundries
- Don Davidson - Executive Director, Mission Critical
- Harvey Reed - Decentralized Capability Lead at MITRE
- Daniel DiMase – Chair NDIA Electronics Trust & Assurance Committee, CEO Aerocyonics
- Jim Gobes - Vice Chair NDIA Electronics Trust & Assurance Committee, Former CEO - Intrinsix

SEMI is Uniquely Qualified to Address the Industry's Top Challenges that Require Global Collaboration

	Foundational	Expanded Programs and Scope			2025 Top Priorities
3,000+ members worldwide **Spanning the Semiconductor and Electronics Design and Manufacturing Supply Chain** **Driving Global Programs**	Thought Leadership	Worldwide Offices	Market Intelligence Reports	Tech partners: imec, Fraunhofer, CEA-Leti, IEEE, ITRI, AIST	**Supply Chain Resilience**
	Standards	2,300+ Program Hours			**Global Advocacy & SIPS Platform** **Workforce Development**
	SEMICON® Expositions/ Conferences	170+ Tech Programs	Smart Initiatives	Strategic Tech Communities: ESDA, IESA, FOA, FlexTech, MSIG, SOIIC	**Sustainability**
	EHS	20+ Tech Communities	Think Tanks		**PFAS** **Cybersecurity & AI**

Initiative goal – Global Chip Traceability



- **Traceability of chips is beneficial to all stakeholders**
  - Safeguard allied nation markets from being flooded by adversaries' legacy chips
  - Strengthen export control and prevent western chips weaponized against our allies
  - Increase supply chain resilience and trust across enterprises in chips value chains
  - Drive new business models (analytics marketplaces, HaaS, IoT and AI applications)
- **Global unique identification for tracing chips is urgent and essential**
  - Current practices are inadequate (local traceability, varied mechanisms)
- **This initiative aims to align allied nations on a "Global Chip Identifier"**
  - Identifier can link to Businesses, Assets, and related Data for chips and electronics

*From Initiation document "2024-10-02 Global Chip Traceability - Initiation V3.2 final.pdf"

Vision *



To ensure the growing success of semiconductor technology, a significant innovation is necessary to enable per chip traceability …..

A global unique identifier used throughout chip lifecycle, starting from chip design and manufacturing to end applications (and EOL) ….

….will enable governments and the industry to establish assured supply and create new opportunities for chip-based monetization and economic growth.

*From Initiation document "2024-10-02 Global Chip Traceability - Initiation V3.2 final.pdf"

Pilot Feasibility Study 2025*



- **Objective**:
  - Accelerate adoption through a trans-Atlantic public-private partnership for a pilot feasibility project demonstrating value of a Global Unique Chip ID
- **Implementation Plan**:
  - Develop a practical, comprehensive implementation plan as a starting point
- **Initial Focus**:
  - Design and test a traceability system ***for export-import control and preventing chip misuse in advanced electronics for aerospace-defense industries***
- **Comprehensive Analysis**:
  - Facilitate a thorough analysis of the Global Chip ID's role across the entire ecosystem

*From Initiation document "2024-10-02 Global Chip Traceability - Initiation V3.2 final.pdf"

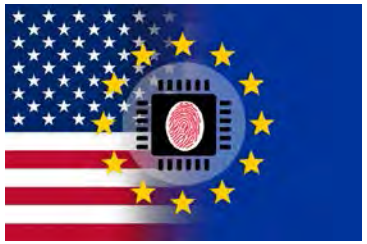
EU 1st Workshop November 19th



- **Workshop Purpose** was to kick off and assess the implementation of lifecycle traceability of individual chips, and to propose a first use case, focusing on:
- **"Export control enforcement for defense and dual use chips"**
- **Key Work Group Focus Areas**:
  - Design and governance of the Global Chip ID database
  - Analysis and testing of traceability of chip from design to front-end & back-end over the life cycle
  - Testing of the use case with relevant organizations (government and industry)

- **US Workshop March 4**
- **EU Workshop June t.b.d.**

Targeted US, EU & Allied Nation Organizations



Ongoing discussions ….evolving

In EU:

- Policy makers: European Commission (e.g.: DG CONNECT, DG HOME, DG TRADE,…)
- Standardization bodies and agencies: ENISA, EU executive agencies
- National governments: e.g. Netherlands MEA
- Industry: European leading IDM & Foundries, OSAT
- RTOs: Private & public research center
- Industry Associations (European chapter...)

Scalable to other countries like Taiwan, South-Korea, China, Japan...

In US:

- Policy makers: U.S. Department of Commerce, CHIPS International Engagement Office, US Trade Representative, and Customs and Border Protection.
- Standardization bodies: SEMI, NIST, JEDEC, IPC, SAE-32 plus more downstream
- Industry: US leading IDM & Foundries, OSAT
- Industry Associations (US chapter...)

https://engineering.purdue.edu/semiconductors/news/development-summit-2024/index_html

Traceability Adoption - implementation path



- A Global Chip ID standard that is cryptographically linked to proprietary Local Chip IDs will speed adoption of cross-border traceability and growth of new business models

- Global Chip IDs* must be unique, electronically verifiable, cryptographically secure, traceable to a root of trust, and capable of supporting varying levels of authentication

- **Provenance** starts during chip design & manufacturing

- Physical IDs can be embedded during lithography and bonded with Root of Trust Based IDs

*The DoC IoT Advisory Board report to Congress recommends a Global Digital Identifier and U.S.-EU to lead on traceability (2024)

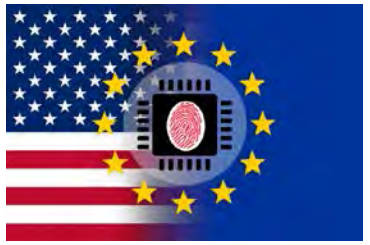
Federated Databases – other Concepts



- Data Spaces Business Alliance (ESBA – Europe)
  - **Gaia-X** is a European initiative to create a **federated** and **secure** data infrastructure that promotes data **sovereignty & interoperability**
  - **I**nternational **D**ata **S**paces **A**ssociation (IDSA): secure, sovereign data sharing
  - **Big Data Value Association**: Innovation in big data and AI supporting Europe's data economy

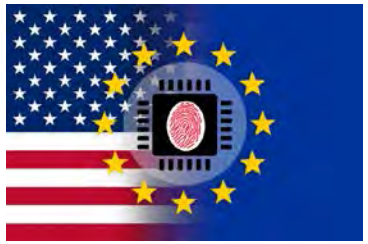
- Similar concepts in other domains and countries
  - **Catena-X** (Automotive Industry, Europe)
  - **ONC** Trusted Exchange Framework and Common Agreement (TEFCA) (Healthcare, US)
  - **Industrial Data Space (IDS)** (Global/Europe)

Relevance of the initiative for EU institutions



- **Alignment with EU Strategy (new CHIP ACT 2.0):**
  - Simplification and implementation of regulatory frameworks
  - Integration with ongoing semiconductor technology strategies
  - More robust & resilient supply chain
- **Coordination of meetings between U.S. and E.U officials**
  - Conference with policy leaders from the U.S. and EU, along with representatives from major chip makers and leading industry associations from both regions
- **Pilot Project Preparation**:
  - Provide inputs for defining objectives and implementation steps
  - Cybersecurity and database management
  - Physical implementation of the Global Unique Chip Identifier
- **Funding (TBC):**
  - Exploration of potential funding sources: **Coordination Support Action (CSA) in 2026**
  - European Work Program 2026 for the pilot project

Discussion Traceability & Security



- Open floor for questions and feedback

- Exploration of potential collaboration and support
- Questions:
  - How the traceability initiative fit with US activities on trustworthy electronics
  - How can we align / complement each other's activities / programs
  - Who would be willing to join now

- Outline of the next steps and follow-up actions

- Closing remarks and appreciation

Annexes

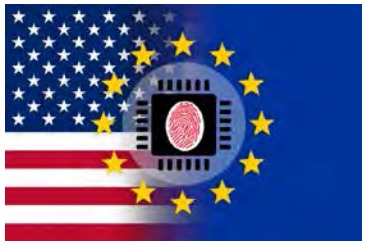
Context



- **Traceability is a global problem** that requires coordinated leadership
  - U.S.-EU collaboration with allied nations (AUKUS*, Japan, Taiwan, South Korea, etc.)
- **The U.S.-EU Trade Technology Council (TTC)** can lead global collaboration
  - Coordinate CHIPS Acts investments toward a cross-border traceability platform
- **A Trusted consortium** is needed to managing Global Chip Identifiers
  - Supranational, federated, non-profit, and driven by allied government agreements
- **Allied nation harmonization** of methods, standards and policies is required
  - Global Identifiers linked to standards and proprietary methods can facilitate adoption

https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/

Uses Cases & beneficiaries



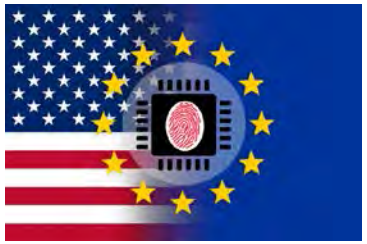
Traceability key use cases	Industry Large & SME	Governments incl. institutions	Society Societal Goals
Chip counterfeit	+++	+++	++
IP protection	+++	+	+
Misuse of electronics by foreign entities	++	+++	++
Export control enforcement	++	+++	+
Supply chain	++ (digitization)	+++ (resilience)	++
Advancing cyber security	+++	+++	++
Circularity of electronics	++	++	++
Reducing AI Energy footprint	++	++	++

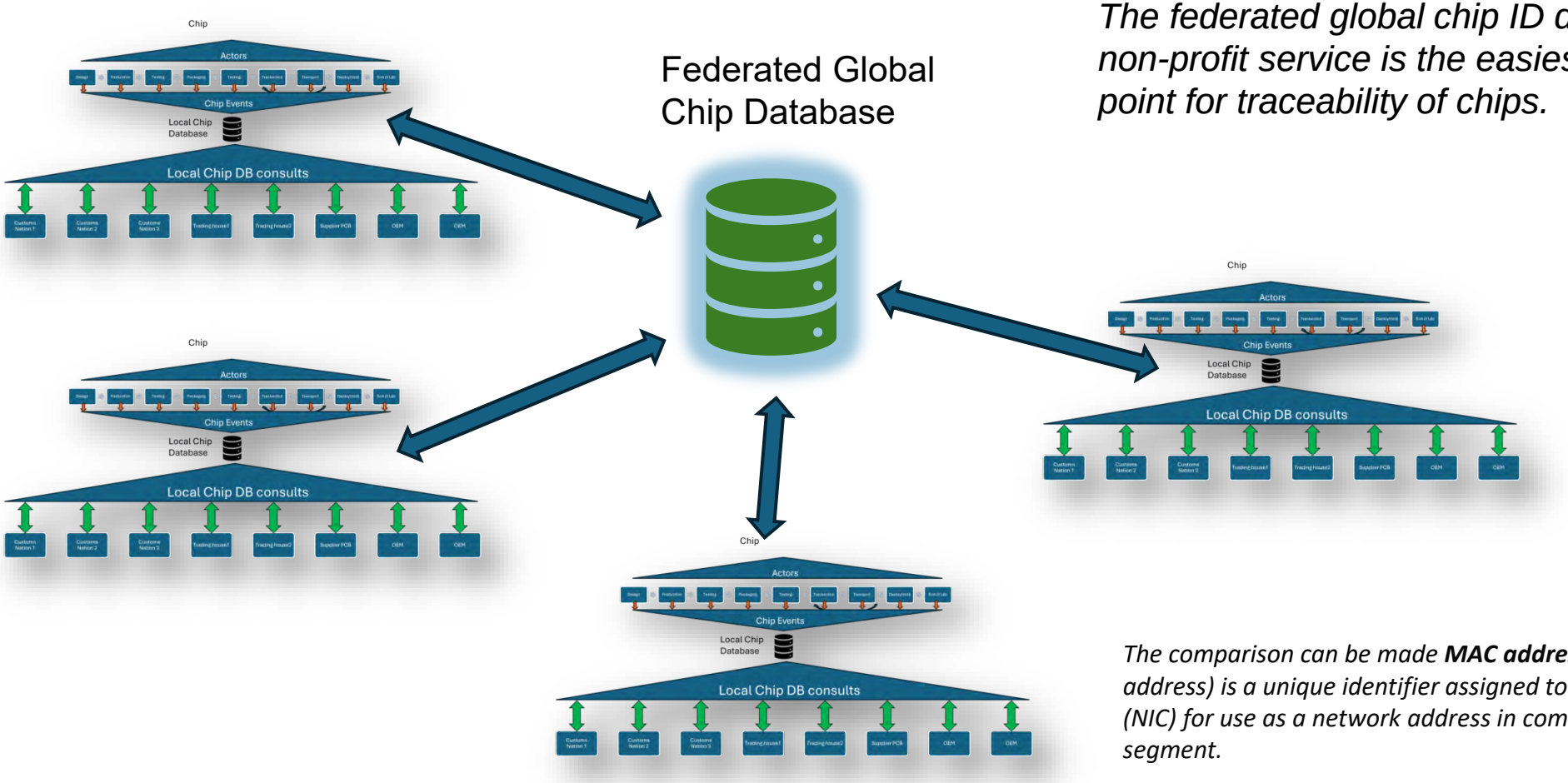
Plethora of use cases in society as the chip has become the essential element of many products and services.

Traceable chip leads to more trusted Digital Marketplaces of the future.

Federated Global Chip ID Database

...unites existing local databases





The federated global chip ID database as a public non-profit service is the easiest & fastest entry point for traceability of chips.

*The comparison can be made **MAC address** (Media Access Control address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.*

SEMI Slide for CHIPS JU Meeting

Melissa Grupen-Shemansky / CTO & VP of Technology

Communities / February 6, 2025

SMCC SEMICONDUCTOR MANUFACTURING CYBERSECURITY CONSORTIUM

semi

Governing Council — Strategic oversight and bylaws & policies

Steering Committee — Operational management, alignment

WG1,2: Factory CyS implementation and compliance	WG3: Supply Chain cybersecurity	WG4: International Regulation and Specs	WG5: Threat Sharing	WG6: Pre-Standards engineering	WG7: Programs and Events	WG8: EU Regulation and CRA
Operationalize and comply with SEMI E187 to ensure tools arriving in factories are cybersafe by default	Establish methods for ecosystem (supply chain) security implementation and management	Develop strategy for legislation & global standards such as NIST CSF 2.0, DFARS, IEC 62443	Implement methods for cyber threat intelligence sharing	Architect comprehensive strategy for new & updated SEMI standards	Execute awareness campaigns for semiconductor cybersecurity	Interpret CRA and educate the industry, develop a collective approach to implement EU CRA regulations

Semiconductor Manufacturing Cybersecurity Consortium (SMCC) – A SEMI Technology Community

Vision: **Strengthen cyber resilience and protection** of the global semiconductor supply chain against evolving threats.

Mission: Develop and promote a **standards-based, industry-wide** approach to improve cybersecurity and accelerate implementation of actionable solutions.

Optimal Member Profile

- Mix of **DMs & OEMs** representing **large and small** companies
- Active participation in **pre-competitive** environment with focus on **problem-solving**

Key focus areas

SMCC workgroups are focused on implementing Cybersecurity controls into our industry factories & supply chain

1. Develop a **robust framework** for cybersecurity that incorporates **lessons learned** from the recent transition and embraces open collaboration.
2. Create a **semiconductor industry-specific framework** to assess the strength of cybersecurity across the supply chain and **implement measures** to better protect ecosystem networks.
3. Incorporate **best practices from other industries** such as **automotive and medical** with the aim to modernize security protocols and facilitate greater collaborative information sharing through SEMI.

For more information or to join, contact cybersecurity@semi.org

SEMI Standards Related to Traceability

	Title	
T25	Blockchain for Semiconductor Supply Chain Traceability	Defines the technical information to manage the information needed to achieve supply chain traceability for semiconductor devices using blockchain.
T23	Single Device Traceability for the Supply Chain	Defines, at a high level, the minimum requirements for device ID and traceability for new design and manufacturing implementation as well as for backwards compatibility with existing methods.
T22	Traceability by Self Authentication Service Body and Authentication Service Body	Define the structure, behaviors, and services for the configuration and objects for generating the access logs in the distribution points of the semiconductors and relevant products using industry specific ASB and SASB.
T21	Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain	Specify the identification of components, container-box, and the organization.
T20	Authentication of Semiconductors and Related Products	Describe the system architecture aspect of an authentication process to establish the trusted identity of products or objects.
T18	Parts and Components Traceability	Specifies fundamental functions and messaging capabilities on equipment and its supervising systems, based on SEMI T12 with some extension.
T17	Substrate Traceability	Specifies data representation, communication, and related items to make capability for tracing substrates on the machine compliant to SEMI T13.
T13	Device Tracking: Concepts, Behavior, and Services	Specifies transfer information required for realizing tracing in such semiconductor products as dice and packaged devices.
T12	Tracing Jigs and Implements	Tracing of equipment tooling ensuring required information, communications and services are contained.
7234	Ballot: Electronic Supply Chain Traceability Using Distributed Ledger Technology	Define the immutable and secure recording and authentication of “assets” as they flow between members of an electronics manufacturing supply chain.
7301	Ballot: Traceability identification label of parts and materials	Unique identification scheme for parts/materials, identification format, and how to take measure against counterfeit label.

Velektronik

PLATFORM FOR TRUSTED ELECTRONICS AND SECURE SUPPLY CHAINS

JOHANNA BAEHR

Fraunhofer edacentrum VDE ITG Informationstechnische Gesellschaft CHIP DESIGN GERMANY

Expert Group Velektronik

- **Goals**
  - Point of contact for trusted electronics in Germany
    - Industry, academic, authorities and government
  - Networking of all stakeholders in this area
  - Exchange of research, best practices and concepts
  - Identifying new research needs
  - Monitoring the development of new legal regulations and standardizations
- **Central activity: events, information exchange and networking**
  - Day of Trustworthy Electronics, organized annually for 1-2 days
  - Networking within Germany and with the EU

© Fraunhofer AISEC

History

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- **2020: Funding call ZEUS from German Ministry of Research (BMBF)**
- **March 2021**
  - 15 Research projects started
    https://www.elektronikforschung.de/foerderung/bekanntmachungen/zeus
  - Project Velektronik additionally as umbrella project
- **Important results of Velektronik**
  - Reference paper trusted electronics:
    https://www.elektronikforschung.de/dateien/publikationen/reference_paper_trustworthy_electronics_2022.pdf
  - 3 workshops organized: “Days of Trusted Electronics”
- **2024: Foundation of VDE ITG and ChipDesign Germany working group**
  - VDE ITG MN 5.8: Vertrauenswürdige Elektronik

 © Fraunhofer AISEC

Members

Currently 40 members from the following organizations

Industry

- Arrow
- Audi
- BMW
- Components at Service
- Codasip
- Denso
- Elmos
- Infineon
- TÜV IT
- Siemens
- Swissbit
- Volkswagen
- Zollner Elektronik

Research

- Edacentrum
- Fraunhofer
  AISEC, EMFT, ENAS, IIS, IMS, IZM
- Hahn-Schickard-Gesellschaft
- HS Offenburg
- Leibnitz IHP
- Technische Universität München
- Universität zu Lübeck

Federal Offices and Funding

- BSI
- BKA
- Cyberagentur

Individual Members

 © Fraunhofer AISEC

Target Groups

- **Supply Chain (IC / PCB / Device)**
  - Design
  - Fabrication
  - Assembly
  - Distribution
  - Deployment
  - Maintenance
  - Decommissioning
- **Applications**
  - Automotive
  - Machine construction
  - Electronics
  - Medicine
  - Critical Infrastructures
- **Research**
  - Universities
  - Research Institutes
- **Federal Offices**
  - BSI
  - Funding Agencies

© Fraunhofer AISEC

Initiatives and Ecosystem

- **European Regulation**
  - EU Chips Act
  - Cyber Resilience Act
  - Network and Information Security 2 (NIS2)
- **German Initiatives**
  - BMBF
    - Forschungsfabrik Mikroelektronik Deutschland
    - DE:Sign and DE:Sign Challenge
    - ChipDesign Germany
  - Cyber Agency (BMVg / BMI)
    - ÖvIT
  - DFG
    - Nano Security Program
  - State-funded initiatives
    - Bavarian Chips Alliance
    - Trusted Electronics Bavaria
    - Bavarian Chip Design Center
    - Silicon Saxony
    - MicroTEC Südwest

© Fraunhofer AISEC

Velektronik

Properties of Trusted Electronics

1. The hardware must **meet high levels of quality and reliability.**

Reliable operation in the field should be guaranteed over its full lifetime.

2. The hardware must comply to a **known and complete specification.**

Functionality should not deviate from the specification.

3. The hardware must be sufficiently **hardened against attacks.**

Mechanisms to ensure security and avoid vulnerabilities should be in place.

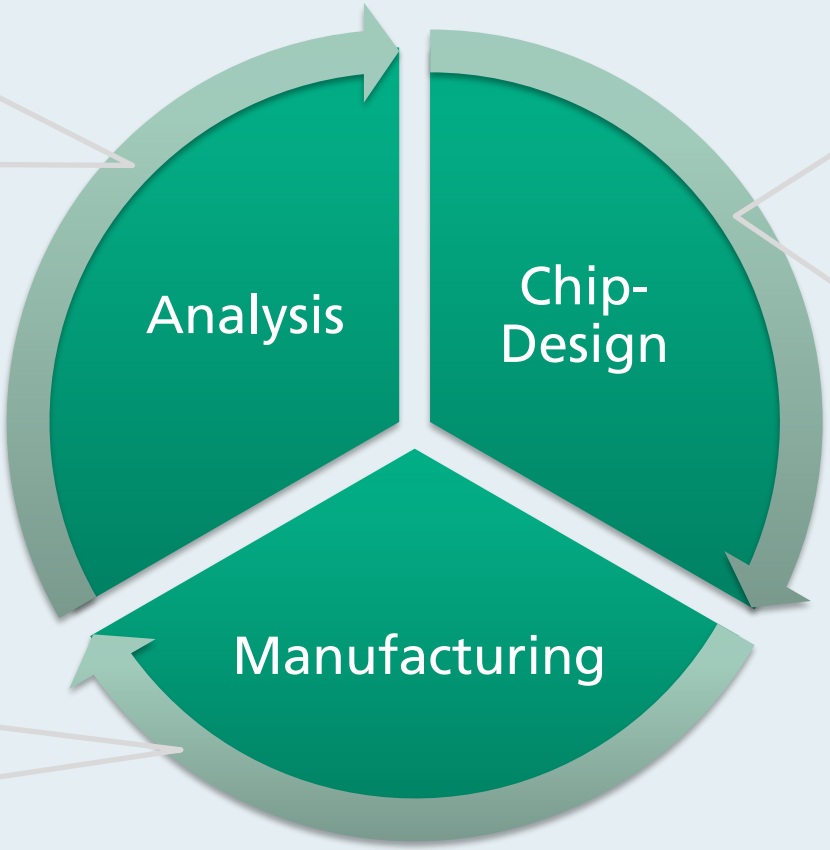
Heyzsl, Johann, et al. "Referenzpapier Vertrauenswürdige Elektronik." 2022.

© Fraunhofer AISEC

Fraunhofer edacentrum VDE ITG Informationstechnische Gesellschaft CHIP DESIGN GERMANY

Three main research areas

- Chip reverse engineering
- Fingerprinting for Identification
- Manipulation detection



Trusted Chip-Designs and IP:

- Open Source HW:
  - RISC-V CPU
  - Peripherals, e.g. PQC crypto accelerators
  - Analog designs
- PUF for identification
- Design tools

- Split Manufacturing
- Supply Chain protection
- Tamper protection

© Fraunhofer AISEC

Open Research Areas applicable to Chip Traceability

- **Authenticity Features**
  - Significant implementation costs (also to ensure quality from fabrication variations)
  - Need for standardization of back-end infrastructure
  - Importance of international harmonization for storing and comparing features
  - High costs and complexity hinder practical implementation
  - Coordination across different stakeholders and regions is essential
- **Counterfeit Detection and Mitigation**
  - Need for lightweight features and fingerprinting techniques for identification and tamper detection
- **Chain of Trust**
  - Tracking HW and SW state is essential for system security
  - Challenges in authenticating simple components without cryptography

Heyzsl, Johann, et al. "Referenzpapier Vertrauenswürdige Elektronik." 2022.
European Commission and Fraunhofer "Study on Trusted Electronics: An Overview over Requirements, Technologies and Initiatives towards More Trusted Electronics." 2024.

 © Fraunhofer AISEC

Open Research Areas applicable to Chip Traceability

- **Digital Twins**
  - Model systems at different scales (component, chip level)
  - Important for validating properties and system behavior
  - Scalability and resource effort are key challenges
- **Cross-Manufacturer Trustworthiness**
  - Challenge of ensuring trust across different manufacturers
  - Focus on technologies and processes for establishing trust

Heyzsl, Johann, et al. "Referenzpapier Vertrauenswürdige Elektronik." 2022.
European Commission and Fraunhofer "Study on Trusted Electronics: An Overview over Requirements, Technologies and Initiatives towards More Trusted Electronics." 2024.

 © Fraunhofer AISEC

CONTACT US

fg-velektronik-kontakt@fraunhofer.de

Velektronik

PLATFORM FOR TRUSTED ELECTRONICS AND SECURE SUPPLY CHAINS

 © Fraunhofer AISEC

Fraunhofer edacentrum VDE ITG Informationstechnische Gesellschaft CHIP DESIGN GERMANY

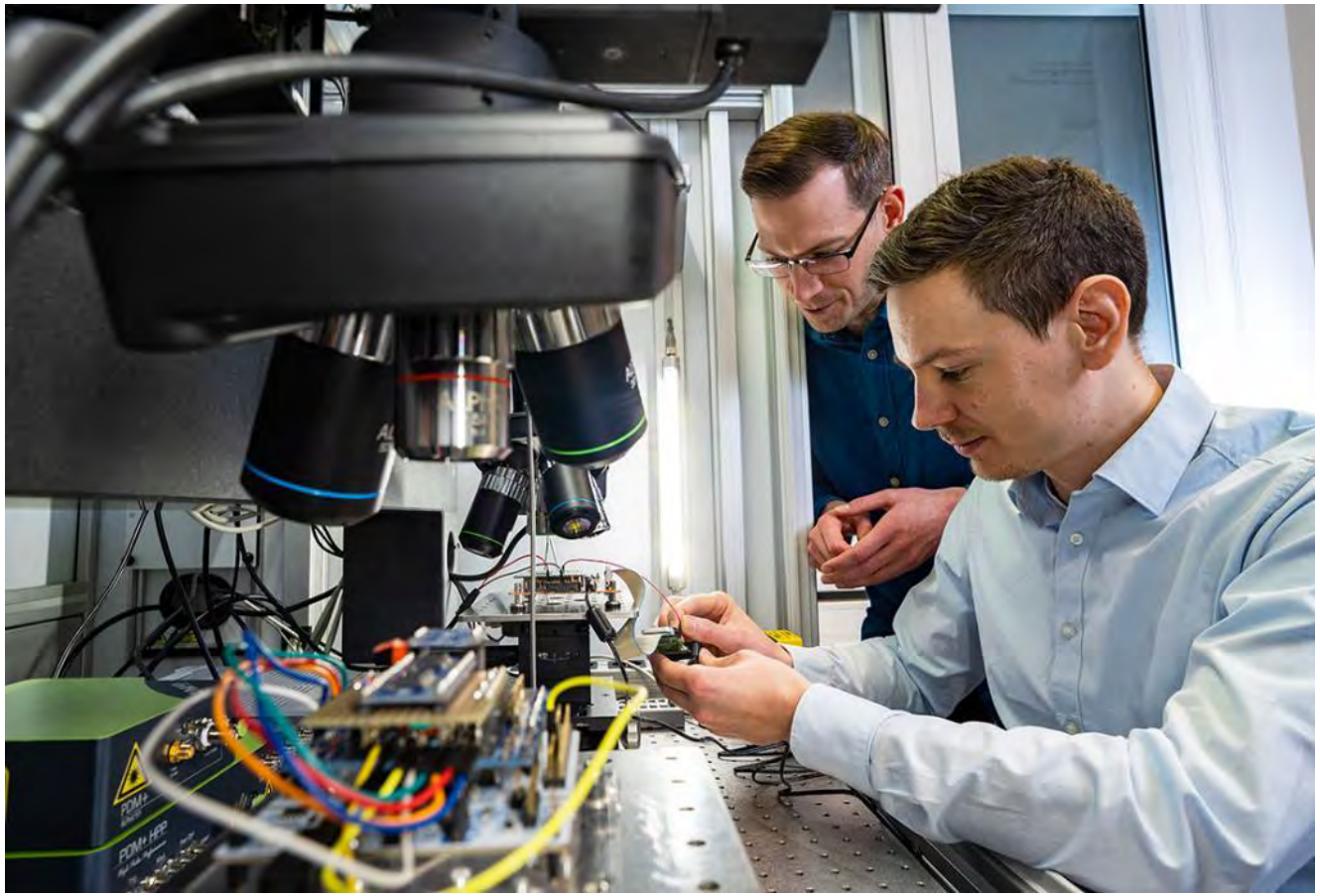
Fraunhofer AISEC

Mission

Fraunhofer AISEC translates **excellence in IT security research into application-oriented** solutions for greater

- dependability,
- **trustworthiness and**
- **tamper protection**

for IT-based **systems and products.**



© Fraunhofer AISEC

Fraunhofer AISEC

Facts & figures

- **Founded:** 2009
- **Budget (incl. investments):** 17 million (2023)
- **Employees**: approx. 250

- **Locations**: Garching near Munich (main locaton), Berlin, Weiden i.d. Oberpfalz
- **International**: Partner institute of Fraunhofer Singapore
- **Universitv connections:**

Technische Universität München — Prof. Dr. Eckert und Prof. Dr. Sigl

Freie Universität Berlin — Prof. Dr. Margraf

Ostbayerische Technische Hochschule Amberg-Weiden — Prof. Dr. Loebenberger

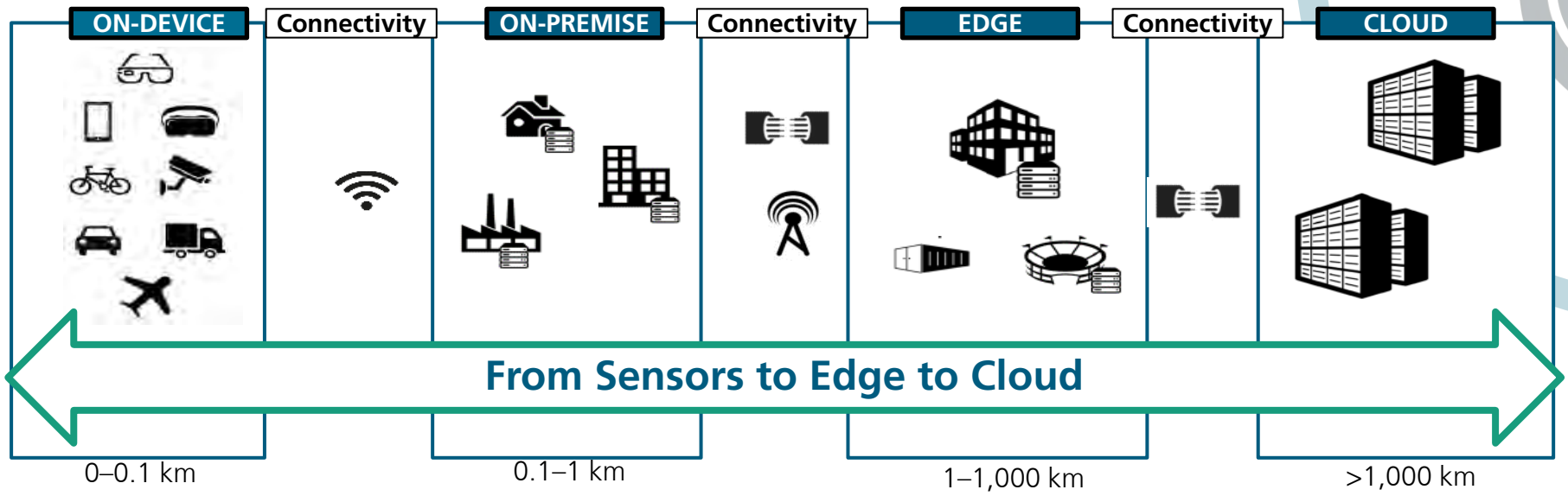


© Hans Georg Esch

Velektronik

Fraunhofer AISEC

Technologies, methods, tools and architectures



Fraunhofer AISEC

Hardware Security, Trusted Electronics	Secure OS & Embedded Security	Software, Application & Cloud Security	Secure AI & AI 4 Security	Advanced Crypto & Privacy	Secure Systems Engineering	Security & Quantum Computing

Cross-cutting topics: risk assessment, offensive IT security (testing, analysis), security concepts

Sectors: automotive, production/automation, healthcare, critical infrastructure

Fraunhofer edacentrum VDE ITG Informationstechnische Gesellschaft CHIP DESIGN GERMANY

Velektronik

Hardware Security

Assessing, designing, and safeguarding IT security

The Hardware Security area of expertise offers customers protective measures for **integrated circuits, chips** and **assemblies of multiple chips on printed circuit boards**.

Security concepts and architectures for SoCs and embedded systems (Physical Unclonable Functions, Crypto implementations)

Manuals, validation of FPGA designs, setup of laboratory environments

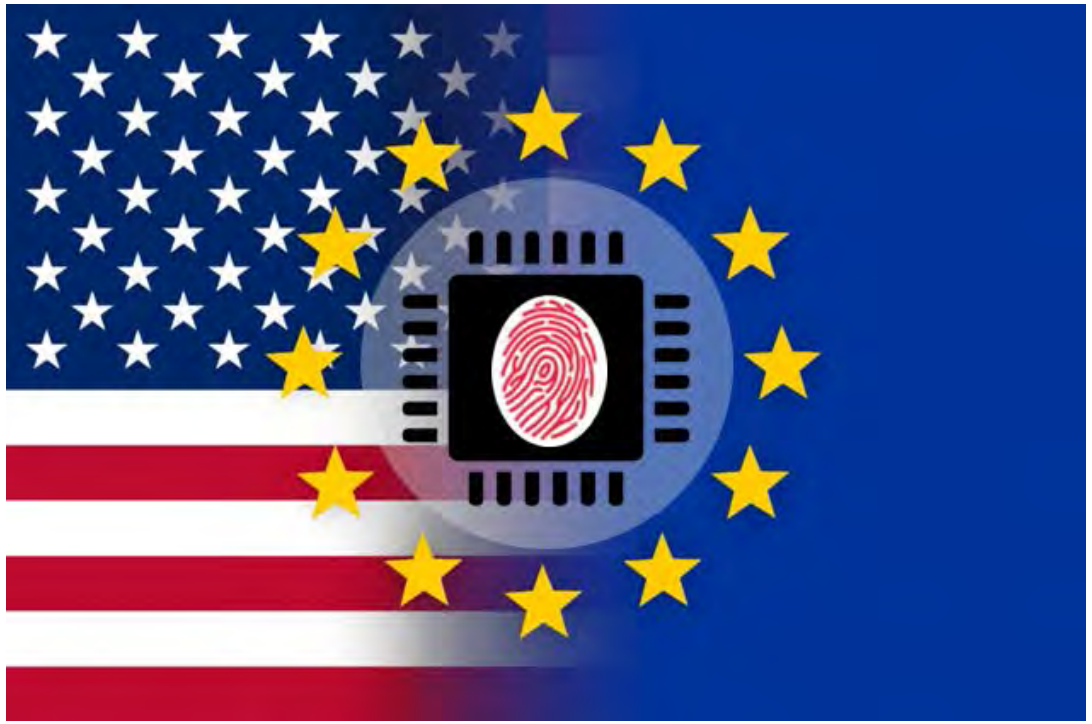
Hardware Security Lab (Side-channel attacks and fault attacks, visual analysis, e.g., photon emissions, microcontroller analysis)



© Fraunhofer AISEC

https://www.aisec.fraunhofer.de/en/fields-of-expertise/HWS.html

Fraunhofer edacentrum VDE ITG Informationstechnische Gesellschaft CHIP DESIGN GERMANY



Global Chip Traceability Initiative

A Trans-Atlantic Initiative for Cross-Border Chip Identification

Architectural Solutions Discussion and Panel:

Will Address Some Solution "Categories", Existing/Emergent Technical Solutions, and Structural Differences

- As semiconductor global supply chains face increasing security threats, robust architectural solutions are critical for ensuring provenance, authenticity, and integrity. This panel will explore three key solution categories—

  (1) Evidence Extraction,

  (2) Fingerprint Generation,

  (3) Fingerprint Enrollment,

- Panelists will present their respective approaches within these categories, discuss existing/emergent solutions, and examine architectural trade-offs in security, scalability, and interoperability. Through an interactive discussion, they will identify complementary techniques, evaluate challenges in real-world adoption, and explore potential areas for cross-disciplinary collaboration. This session will provide a structured framework for understanding the landscape of provenance attestation, offering insights into the technological, operational, and policy considerations shaping the future of secure semiconductor architectures.



Some Solution “Categories”:

- (1) **Evidence Extraction**, which utilizes physical, electrical, optical, or thermal properties to generate unique fingerprints;

- (2) **Fingerprint Generation**, which compacts and transforms extracted evidence into usable, verifiable identifiers;

- (3) **Fingerprint Enrollment**, which securely stores and manages these fingerprints for authentication and tracking; to include: Data Sharing and Privacy, which ensures secure access, controlled distribution, and compliance with regulatory requirements when sharing provenance information.



Solutions Panel

Moderator:

- **Don Davidson** is Executive Director for Strategy & Technology at Mission-Critical.org don.davidson@mission-critical.org

Panelists:

- **Jeff Shiner** is a Technical Director for Business Development at Micron jshiner@micron.com
- **Dr. Yiorgos Makris** is a Professor of Electrical and Computer Engineering at the University of Texas at Dallas and an IEEE Fellow. yiorgos.makris@utdallas.edu
- **Dr. Sumaiya Shomaji** is an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of Kansas. She is the Co-Director of ASTHA (Assurance of Security and Trust for Human and Hardware) Lab. shomaji@ku.edu
- **Manu Fontaine** is the Founder and CEO of Hushmesh Inc., a dual use, VC-backed, US-based cybersecurity Public Benefit Corporation manu@hushmesh.com



Don Davidson is Executive Director for Strategy & Technology at Mission-Critical.org

Education-

- Graduate USMA at West Point NY with BS in Engineering
- Graduate National War College at National Defense University with Masters Degree in National Security Strategy (focused in Information Systems Management)
- Graduate of OPM's Leadership for a Democratic Society Course at Federal Executive Institute (FEI)
- Defense Leadership & Management Program (DLAMP)
- LOGTECH at Kenan-Flagler Business School at UNC
- OPM's Executive Leadership 1&2 (Brookings Institute).

Experience-

- 44+ years in DoD (w/ 15 specifically in SCRM, finishing as Deputy Director for Cybersecurity SCRM)
- 4+ years in Synopsys as Director SCRM in their Chief Security Office (CSO)
- 1+ years as Executive Director for Strategy & Technology at MISSION-CRITICAL.org



https://mission-critical.org/

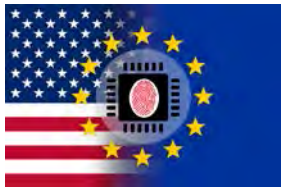
Collaborative Critical Infrastructure Cybersecurity Research



Don Davidson is an Executive Director at https://mission-critical.org/

Mission Critical exists to:

- Improve the security and resilience of the 16 US critical infrastructure sectors;
- Facilitate collaboration between thought leaders, policymakers, and pivotal stakeholders;
- Elevate the national dialogue around critical infrastructure information security topics.
- Mission Critical achieves its objectives by developing publicly-available research and meeting the needs of trusted partners, sector communities, and the US public.

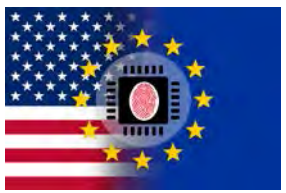


Providing- Expert Focus, Collaborative Methodology, Objective Research, Non-Partisan Commitment and Non-Technical Communications on Technical Topics.

About

- Jeff Shiner, a cyber-security expert in the semiconductor industry, is currently a Technical Director, Business Development Sales at Micron Technologies. At Micron, Jeff spent eight years driving a new disruptive silicon-to-cloud technology initiative and the ecosystem of software and cloud service partners to support this platform called Authenta™. Prior to Micron, he has led sales and marketing efforts for additional disruptive technologies at AMD, Spansion and Cypress.
- While driving the Authenta™ initiative, his focus was to establish partnerships and a new type of certificate authority based on silicon born trust anchors to help shift left a new type of trust and extend this to supply chain needs as well as evolving field services. Additionally, this platform approach was to provide a framework that enabled OEM's and cloud service partners incentive to collaborate on full firmware and software solution stacks from silicon-to-cloud.
- He has served in various industry consortiums supporting cybersecurity frameworks and supply chain traceability initiatives including GSA TIES and the Industry Internet Consortium developing the Industrial Internet Security Framework (IISF).





About

- Dr. Yiorgos Makris is a Professor of Electrical and Computer Engineering at the University of Texas at Dallas and an IEEE Fellow. He has spent over two decades developing and demonstrating solutions for ensuring quality, reliability, security and trustworthiness of integrated circuits and systems and he is broadly recognized for pioneering the use of machine learning in semiconductor manufacturing and testing. He is the director of the **T**rusted and **REL**iable **A**rchitectures (TRELA) Lab, the leader of the Safety, Security and Healthcare thrust of the **T**e**x**as **A**nalog **C**enter of **E**xcellence (TxACE), and a co-founder of the NSF Industry/University Cooperative Research **C**enter on **H**ardware and **E**mbedded-System **S**ecurity and **T**rust (NSF CHEST I/UCRC).



About

- Dr. Sumaiya Shomaji is an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of Kansas. She is the Co-Director of ASTHA (**A**ssurance of **S**ecurity and **T**rust for **H**uman and H**a**rdware) Lab. By leveraging her expertise in the interdisciplinary field of machine learning, computer vision, and data structures, she aims to solve the emerging problems in various domains of IoT, especially human authentication, hardware security, and healthcare.



About

- **Manu Fontaine** is the Founder and CEO of Hushmesh Inc., a dual use, VC-backed, US-based cybersecurity Public Benefit Corporation.
- Hushmesh is developing and operating ”the Mesh”, a global decentralized information infrastructure that automates cryptographic provenance, integrity, authenticity, traceability, confidentiality, and privacy at internet scale.
- The Mesh solves cryptographic identification and traceability for everyone and everything, while preserving confidentiality and privacy for all stakeholders.
- The Mesh leverages the latest in chip-level cryptographic security (Confidential Computing) to secure critical supply chains. Only *secure chips* can secure *secure chips*!



Connect on LinkedIn

Manu Fontaine
manu@hushmesh.com

Some Solution “Categories”:

- (1) **Evidence Extraction**, which utilizes physical, electrical, optical, or thermal properties to generate unique fingerprints;

- (2) **Fingerprint Generation**, which compacts and transforms extracted evidence into usable, verifiable identifiers;

- (3) **Fingerprint Enrollment**, which securely stores and manages these fingerprints for authentication and tracking; to include: Data Sharing and Privacy, which ensures secure access, controlled distribution, and compliance with regulatory requirements when sharing provenance information.



Solutions Panel

Moderator:

- **Don Davidson** is Executive Director for Strategy & Technology at Mission-Critical.org don.davidson@mission-critical.org

Panelists:

- **Jeff Shiner** is a Technical Director for Business Development at Micron jshiner@micron.com
- **Dr. Yiorgos Makris** is a Professor of Electrical and Computer Engineering at the University of Texas at Dallas and an IEEE Fellow. yiorgos.makris@utdallas.edu
- **Dr. Sumaiya Shomaji** is an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of Kansas. She is the Co-Director of ASTHA (Assurance of Security and Trust for Human and Hardware) Lab. shomaji@ku.edu
- **Manu Fontaine** is the Founder and CEO of Hushmesh Inc., a dual use, VC-backed, US-based cybersecurity Public Benefit Corporation manu@hushmesh.com



Architectural Solutions for Provenance Attestation: Evidence Extraction*

Yiorgos Makris
(yiorgos.makris@utdallas.edu)

Trusted & **REL**iable **A**rchitectures Laboratory



*Partially supported by:

- AFRL/Northrop Grumman, “Provenance Attestation Methods for Integrated Circuits,” 2020-2023
- NSF CHEST I/UCRC, “Wafer-Level Provenance Attestation: Machine Learning to the Rescue,” 2023-2025

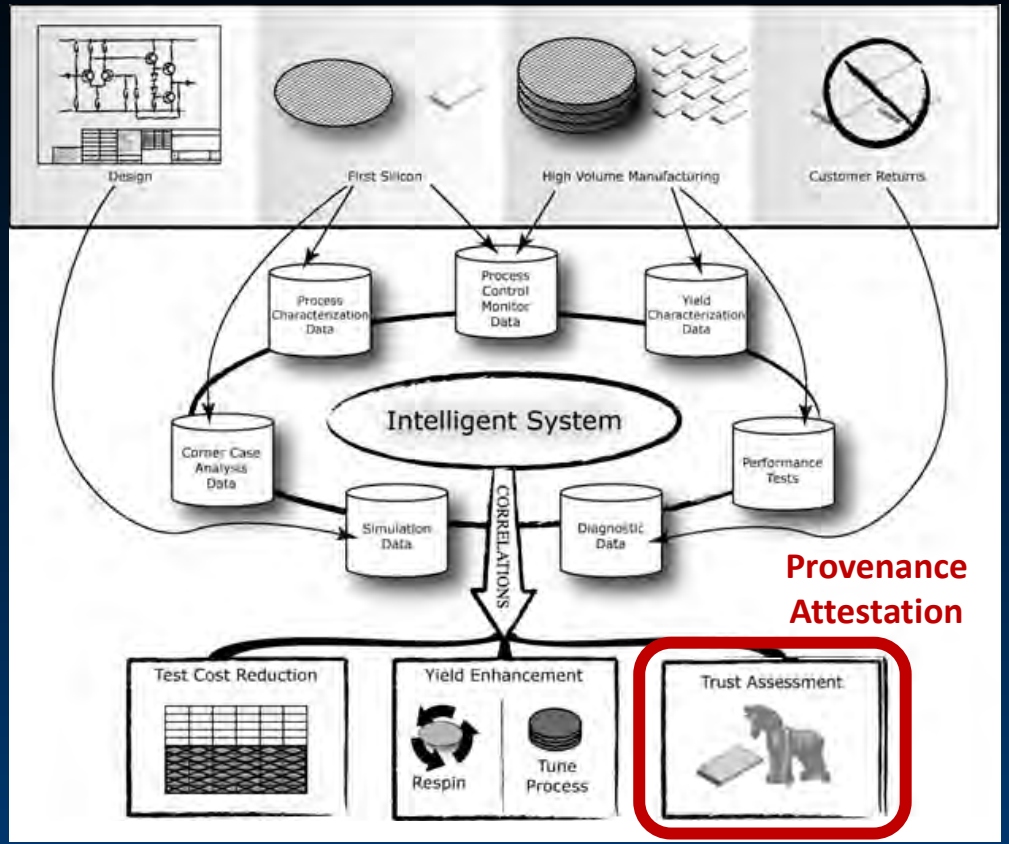
TRELA Lab Vision (circa 2005)

Biography Snapshot:

- Ph.D., UCSD, 2001
- Faculty of EE & CS, (Yale, 2001-2011)
- Faculty of ECE, (UT Dallas 2011-now)

Research Interests:

- Develop, demonstrate and evaluate end-to-end solutions for ensuring quality, reliability, security and trustworthiness of integrated circuits



What is Provenance Attestation?

prov·e·nance

/ˈprävən(ə)ns/

noun

noun: **provenance**

the place of origin or earliest known history of something.

at·tes·ta·tion

/ˌaˌteˈstāSH(ə)n, ˌadəˈstāSH(ə)n/

noun

noun: **attestation**; plural noun: **attestations**

evidence or proof of something.

Source: Oxford Dictionary

"Certify where an artifact of interest originated from"

Options:

- Paper-trail & policy





- Added watermark



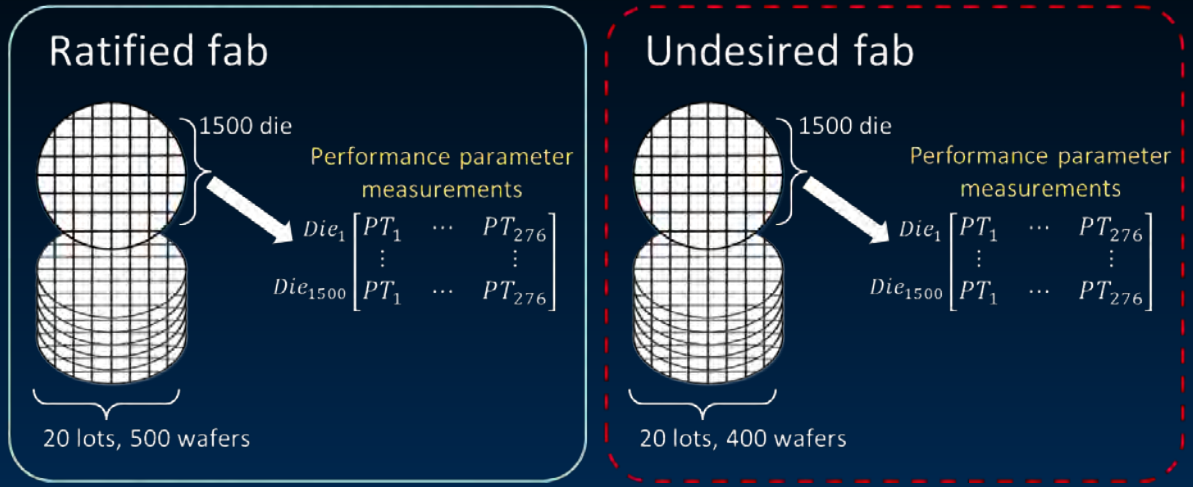
- Innate process



- Note: Provenance attestation certifies source authenticity but does not verify functionality

Fab-of Origin Attestation using Probe Tests*

Data from 65nm TI RF transceiver fabricated in two fabs (Dallas/Aizu)



Confusion matrix		Actual	
		P	N
Attested	P	TPR = 85.5%	FPR = 14.5%
	N	FNR = 15.5%	TNR = 84.5%

Single chip attestation results

Confusion matrix		Actual	
		P	N
Attested	P	TPR = 96.7%	FPR = 3.3%
	N	FNR = 4.2%	TNR = 95.8%

Lot attestation results

Where Did My Chips Come From?





*A. Ahmadi, M. Bidmeshki, A. Nahar, B. Orr, M. Pas, **Y. Makris**, "A Machine Learning Approach to Fab-of-Origin Attestation," *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 92-97, 2016

Mask-Set Attestation using Metrology/WAT*

GF 12LP FinFET Process:

- Data from 8181 wafers
- Duplicate for 4 of 26 layers
- Wafers made with all 16 mask-set combinations
- Only mask-shop variation

Original Mask-Set (All 26 Front-End Layers)



4 Duplicate Mask Layers (Identical)



Diff. Count	Set ID	M3	M2	M1	M0	# of Wafers
0	0	0	0	0	0	236
1	1	0	0	0	1	851
	2	0	0	1	0	178
	4	0	1	0	0	511
	8	1	0	0	0	501
2	3	0	0	1	1	541
	5	0	1	0	1	550
	6	0	1	1	0	191
	9	1	0	0	1	1021
	10	1	0	1	0	168
	12	1	1	0	0	599
3	7	0	1	1	1	493
	11	1	0	1	1	960
	13	1	1	0	1	466
	14	1	1	1	0	321
4	15	1	1	1	1	594

Available Data:

Type of Data	Count
# of Wafers	8181
Metrology Data	252 measurements/wafer
WAT Sites	13 sites/wafer
WAT Data	5,109 measurements (393/site)

Data-Split:

Data Source	Experimental Setup
Training Set (Mask-Set 0)	177 (9 lots)
Test Set (Mask-Set 0)	59 (4 lots)
Test Set (Mask-Set 1-15)	7945 (332 lots)

*S. Tellakula, C.-Y. Chiang, C. Vasileiou, M. Nigh, Y. Makris, "Mask-Set Attestation Using Metrology and Wafer Acceptance Tests," *Manuscript in Review*, 2025

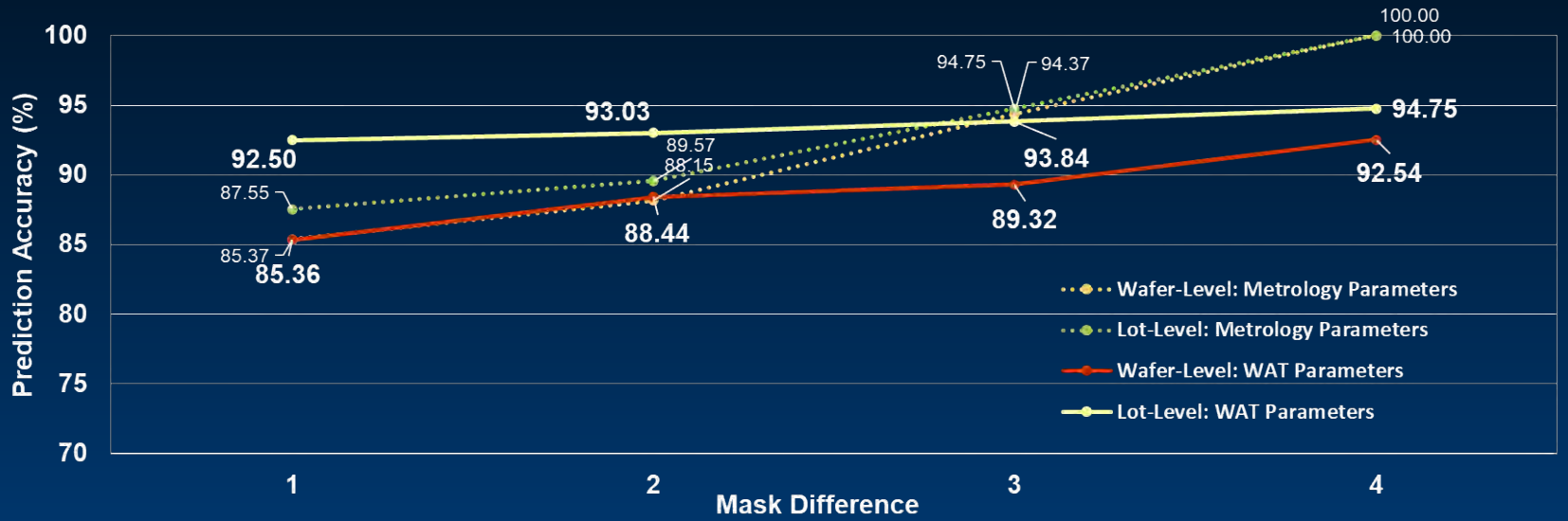
Mask-Set Attestation using Metrology/WAT*

Attestation with In-Line Tests:

Dataset	Accuracy (Wafer-Level)	Accuracy (Lot-Level)
Training (Wafers from Mask-Set 0)	88.64%	92.09%
Testing (Wafers from Mask-Set 0)	84.91%	90.33%
Testing (Wafers from Mask-Sets 1-15)	90.04%	91.18%

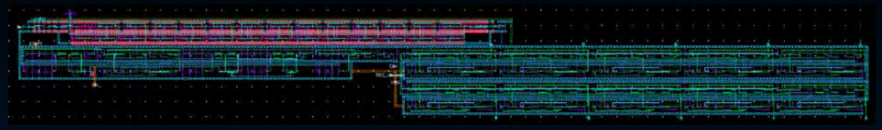
Attestation with E-Tests:

Dataset	Accuracy (Wafer-Level)	Accuracy (Lot-Level)
Training (Wafers from Mask-Set 0)	86.61%	91.87%
Testing (Wafers from Mask-Set 0)	80.81%	86.47%
Testing (Wafers from Mask-Sets 1-15)	88.56%	94.01%

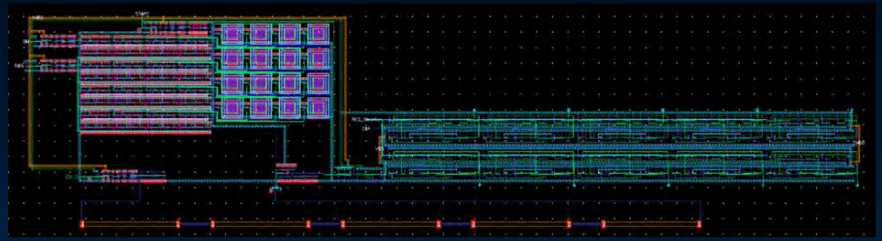


*S. Tellakula, C.-Y. Chiang, C. Vasileiou, M. Nigh, Y. Makris, "Mask-Set Attestation Using Metrology and Wafer Acceptance Tests," *Manuscript in Review, 2025*

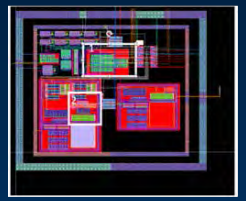
On-Die Sensors for Provenance Attestation



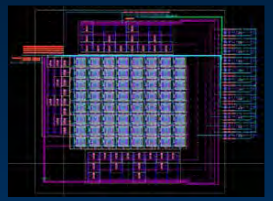
11-Stage Ring Oscillator (RO)



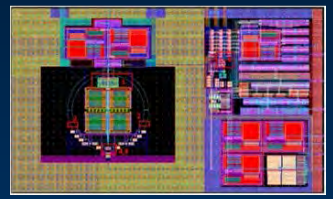
Open Circuit Voltage Decay (OCVD) Sensor



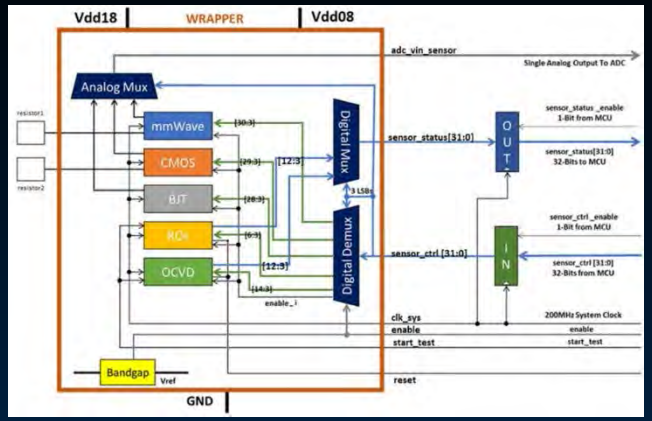
CMOS Array

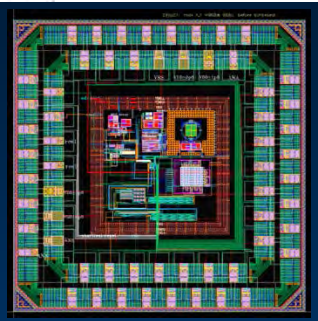


BJT Array



mmWave LC-VCO





- Takeaway Point: Systematic variation introduced by fab/mask-set/equipment-line can be harnessed for die-level or wafer-level provenance attestation in integrated circuits

Panel: Architectural Solution

EVIDENCE GENERATION

YIORKIS

University of Texas at Dallas

RAW IDs for CHIPs

FINGERPRINT GENERATION and MANAGEMENT

SUMAIYA*

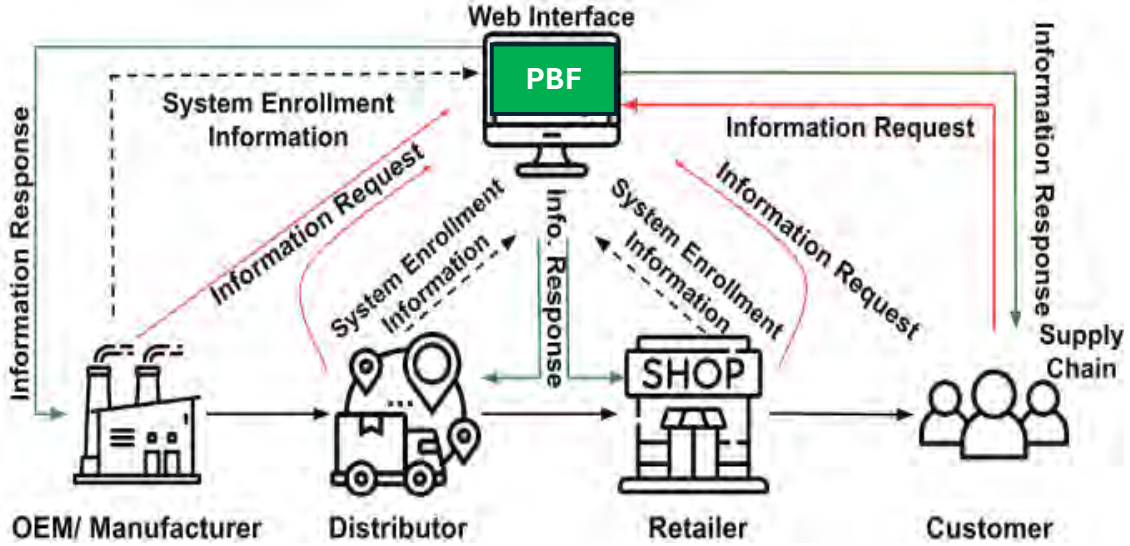
University of Kansas

OFFCHAIN DB for CHIPS

SECURE PROVENANCE

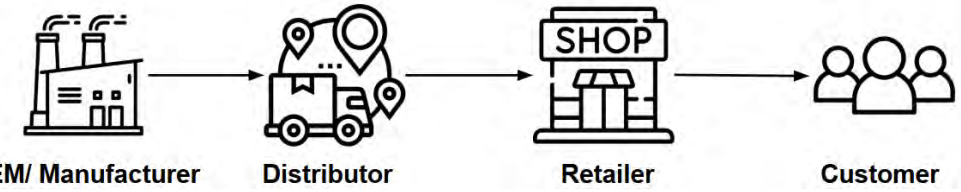
MANU

Hushmesh Inc.



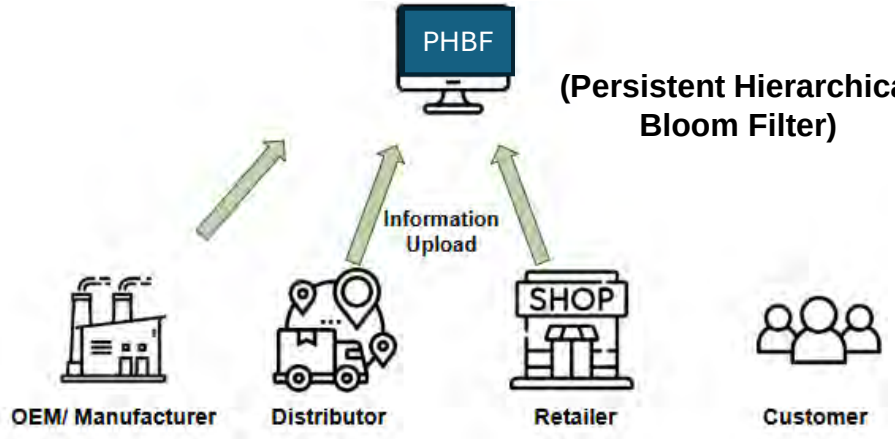
Fingerprint/ID Generation and Management

Challenges:



- No. of Entities
- No. of Location
- No. of Days

Project Goal/ Target:



(Persistent Hierarchical Bloom Filter)

5 Desired key properties for CHIP IDs:

- High Accuracy in Authentic vs. Counterfeit IC Detection
- Compact Representation of IDs
- Enable Fast Query Processing
- Effective Noise Handling
- Security to the Templates

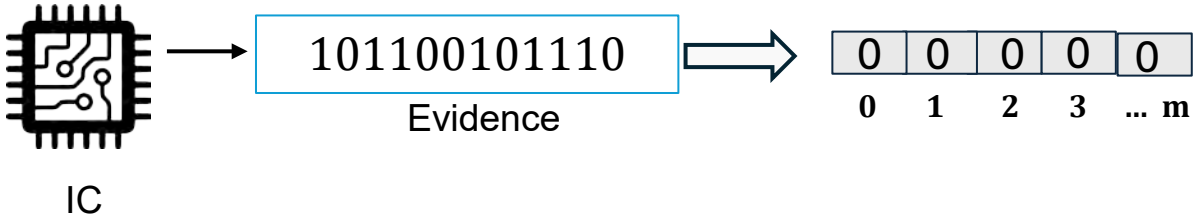
Existing Studies:

Methods	Low Storage	Fast Query	Noise Handling	Security	High Performance
Neural Networks	✗	✗	✓	✗	✓
Nearest Neighbor	✗	✓	✓	✗	✗
Cryptographic Hashing	✗	✗	✗	✓	✗
Probabilistic Structure (BF)	✓	✓	✗	✓	✓
Proposed PHBF	✓	✓	✓	✓	✓

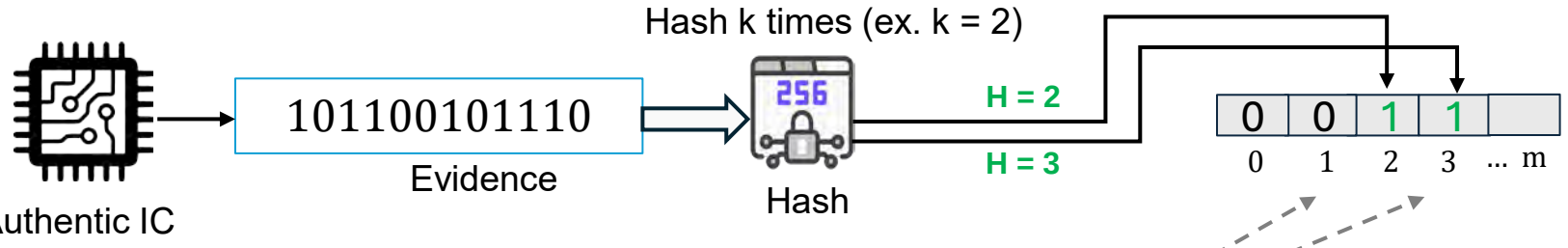
PHBF For Fingerprint Generation & Management

Bloom Filter (BF)-based ID Generation:

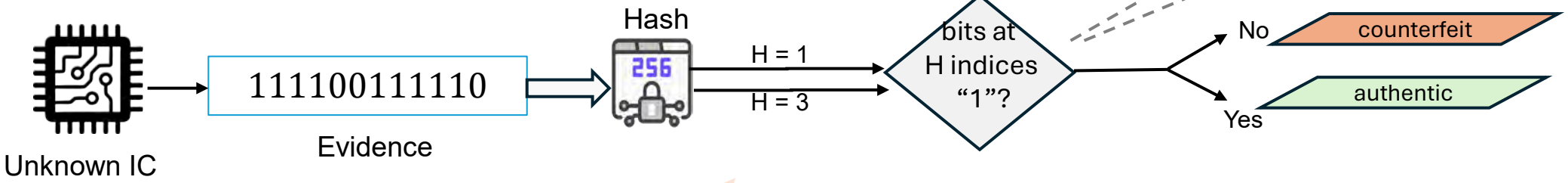
- Probabilistic data structure
- Compresses data
- Enrolls in a vector → tests membership



ID Generation and Enrollment:



Query Processing:

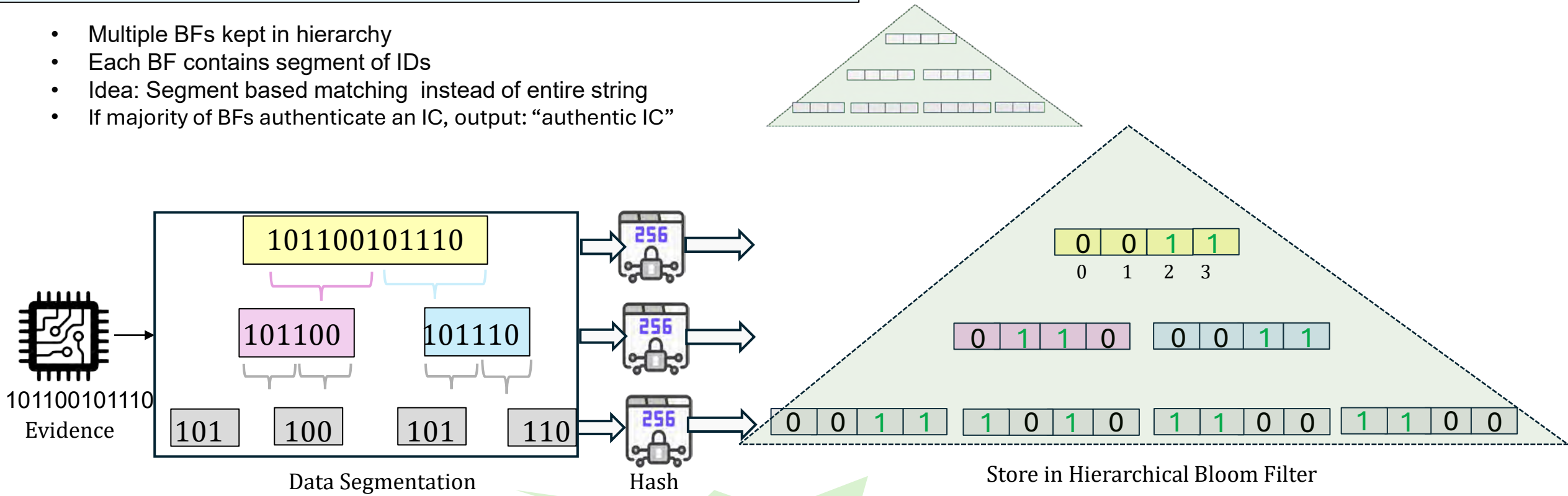


Limitation: can't handle noise, but evidences are noisy, even if IC is genuine!

PHBF For Fingerprint Generation & Management

Hierarchical Bloom Filter (HBF)-based ID Generation [1,2]:

- Multiple BFs kept in hierarchy
- Each BF contains segment of IDs
- Idea: Segment based matching instead of entire string
- If majority of BFs authenticate an IC, output: “authentic IC”



Solves noise handling problem!

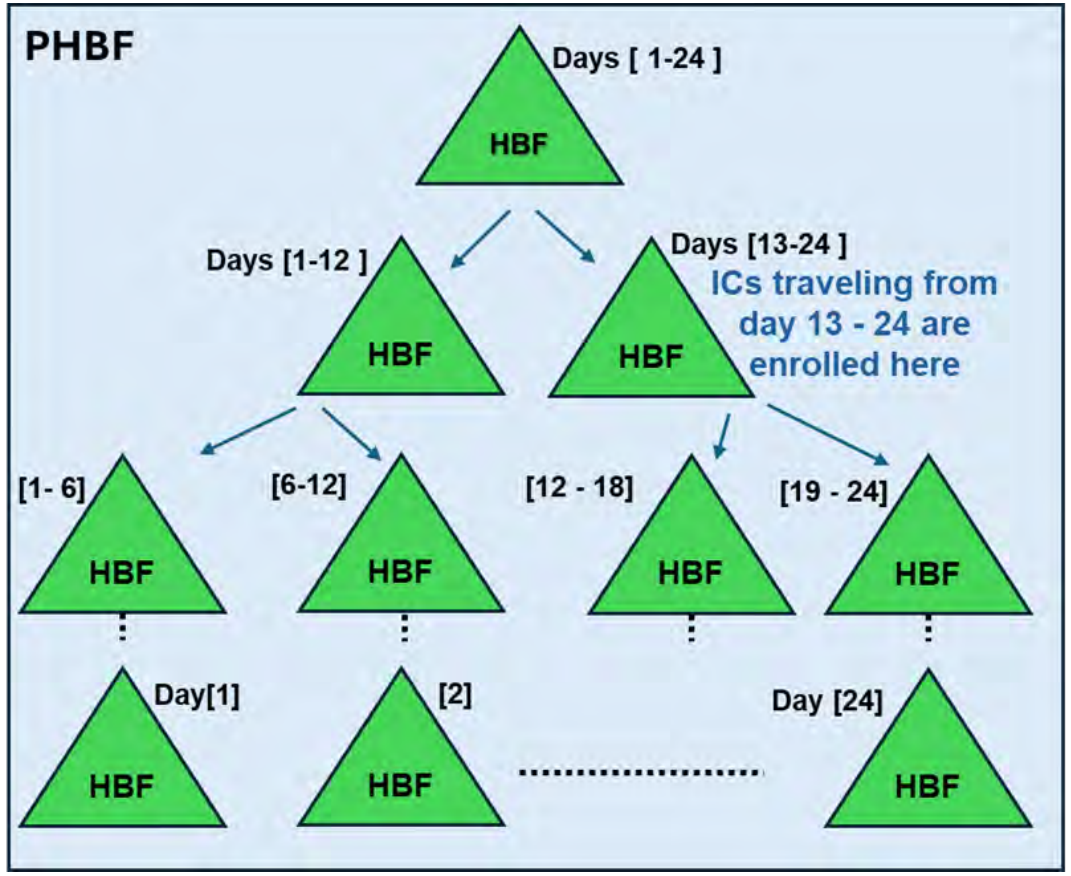
Ref: **1. S. Shomaji**, P. Ghosh, F. Ganji, D. Woodard, and D. Forte, “An Analysis of Enrollment and Query Attacks on Hierarchical Bloom Filter-based Biometric Systems”, *in IEEE Transactions on Information Forensics and Security (TIFS)*, 2021.

2. S. Shomaji, F. Ganji, D. Woodard, and D. Forte, "Hierarchical Bloom Filter Framework for Security, Space-efficiency, and Rapid Query Handling in Biometric Systems", in IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1-8), 2019.

PHBF For Fingerprint Generation & Management

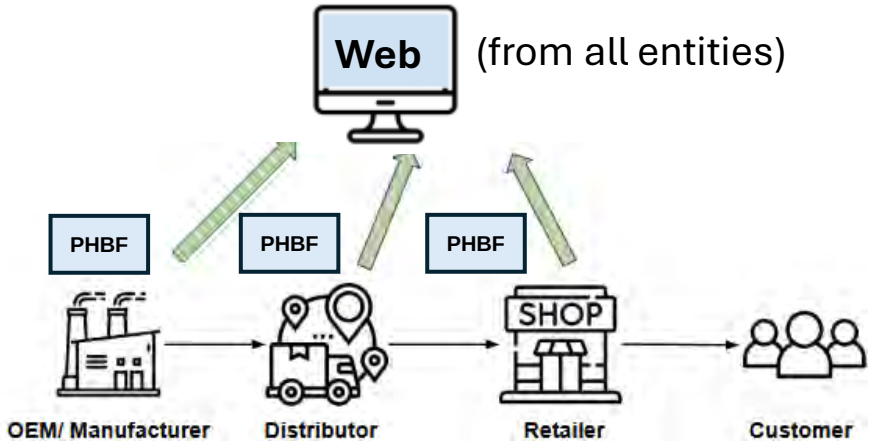
Proposed PHBF-based ID Generation [3]:

- PHBF = Persistent Hierarchical Bloom Filter
- Multiple HBFs kept in hierarchy → to support time-based query
- Each HBF contains ICs for a specific time range (ex. day 13- 24)
- Useful for time range-based query (ex. *was IC 'x' Present in time-range 13-24?*)



Assume, total travel days = 24

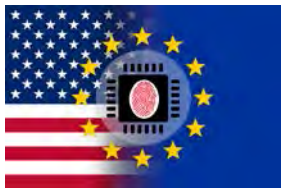
Re-modeling Supply Chain with Proposed PHBF:



Conclusion:

Key Concepts in PHBF	5 Desired Attributes
Data Segmentation	Noise Handling
SHA256 + FNV Hash	Security
Probabilistic Distribution	Compact Storage
Index-based Lookup	Faster Query Processing
User Defined False Positive Rate	High Authentication Accuracy

Ref: 3. M. M. Rizvee*, T. Hossain, T. Hoque, D. Forte and **S. Shomaji**, "A Hierarchical Bloom Filter-based Framework for Authentication and Tracking of ICs," in *3rd International Workshop on Silicon Lifecycle management (SLM Workshop)*, October 2023.



hushmesh

Hushmesh Inc. is a DC-based, dual-use, cybersecurity

Public Benefit Corporation

and

NATO DIANA startup

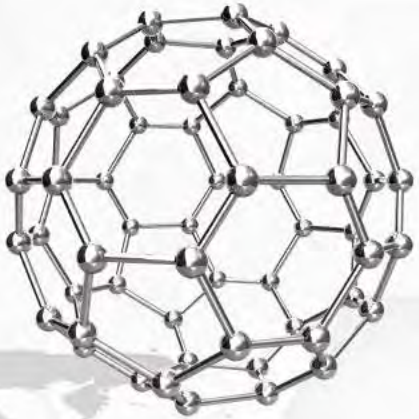


Semiconductor Traceability And Market Provenance (STAMP) Initiative

NATO OTAN

Defence Innovation Accelerator for the North Atlantic (DIANA)

hushmesh



The Mesh

is a global, decentralized

information infrastructure

Like the Web

But with built-in, universal

cryptographic provenance, integrity, traceability, confidentiality, and privacy



Semiconductor Traceability And Market Provenance (STAMP) Initiative

hushmesh

Automated cryptographic security for

all types of global entities

People, organizations,

physical things, and **digital things**

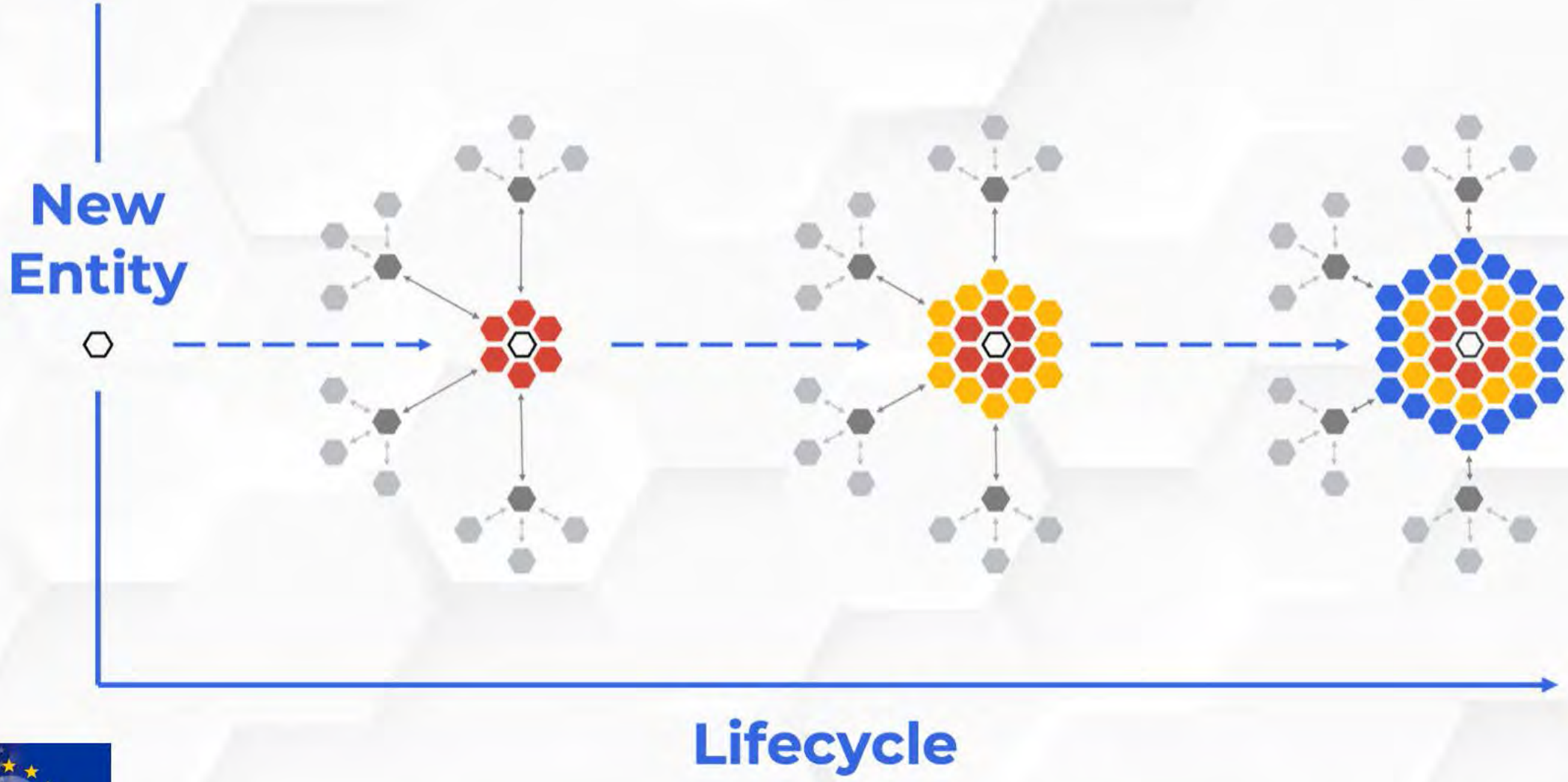
Each with its own independent

lifecycle, history, policies, and **relationships**



Semiconductor Traceability And Market Provenance (STAMP) Initiative

hushmesh



Semiconductor Traceability And Market Provenance (STAMP) Initiative

hushmesh

Universal Name System (UNS)

A global, decentralized, automated, cryptographic name system
unified across all types of entities: people, organizations, physical things, and digital things

Universal Certificate Authority (UCA)

A global, decentralized, automated, cryptographic key infrastructure
to solve provenance, integrity, authenticity, reputation, confidentiality, and privacy

Universal Private Ledgers (UPL)

Each entity has its own cryptographically isolated
information space, keychain, wallet, and private ledger

Universal Private Computing (UPC)

Any organization can automate the deployment of confidentiality and privacy-preserving,
cryptographically attested and verified code



Semiconductor Traceability And Market Provenance (STAMP) Initiative

Made possible by Confidential Computing

Semiconductor innovation!

Only *secure chips* can secure *secure chips*!



Confidential Computing Consortium

confidentialcomputing.io

Semiconductor Traceability And Market Provenance (STAMP) Initiative

hushmesh

The optimal cybersecurity blueprint

Smallest global attack surface mathematically possible

Orders of magnitude smaller than all other approaches

Least-trust blueprint technically possible

Cross-domain zero trust at internet scale

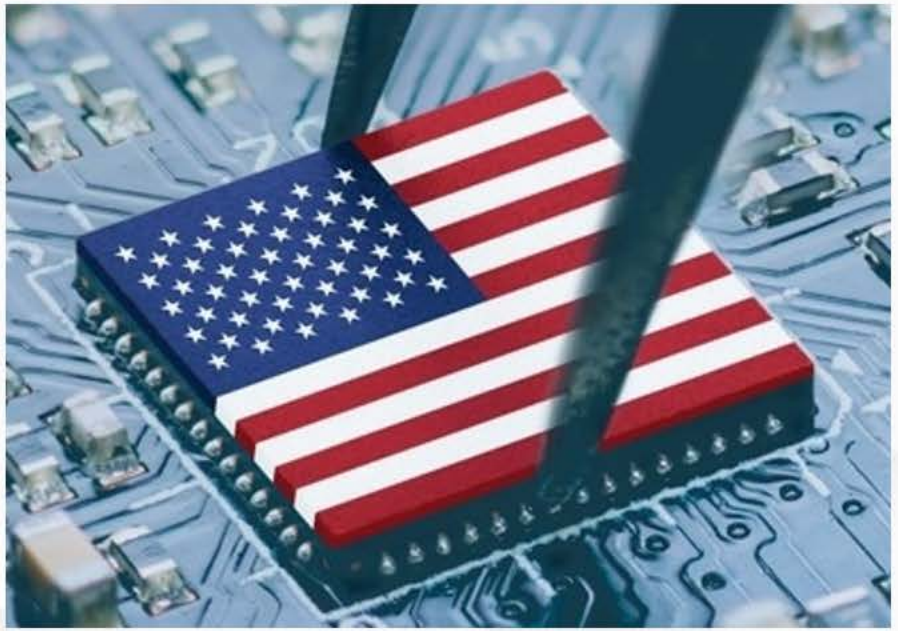
Entity-centric security

Software-defined cryptography



Semiconductor Traceability And Market Provenance (STAMP) Initiative

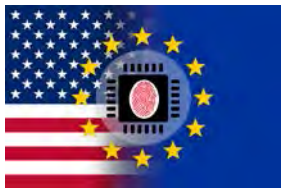
Fixing cybersecurity is the trillion-dollar business case





Semiconductors and Cybersecurity strategies

MUST be addressed jointly



Who burdens the cost of Multilateral trust

Customers

Expect security, but don’t like paying more for it

System OEMs

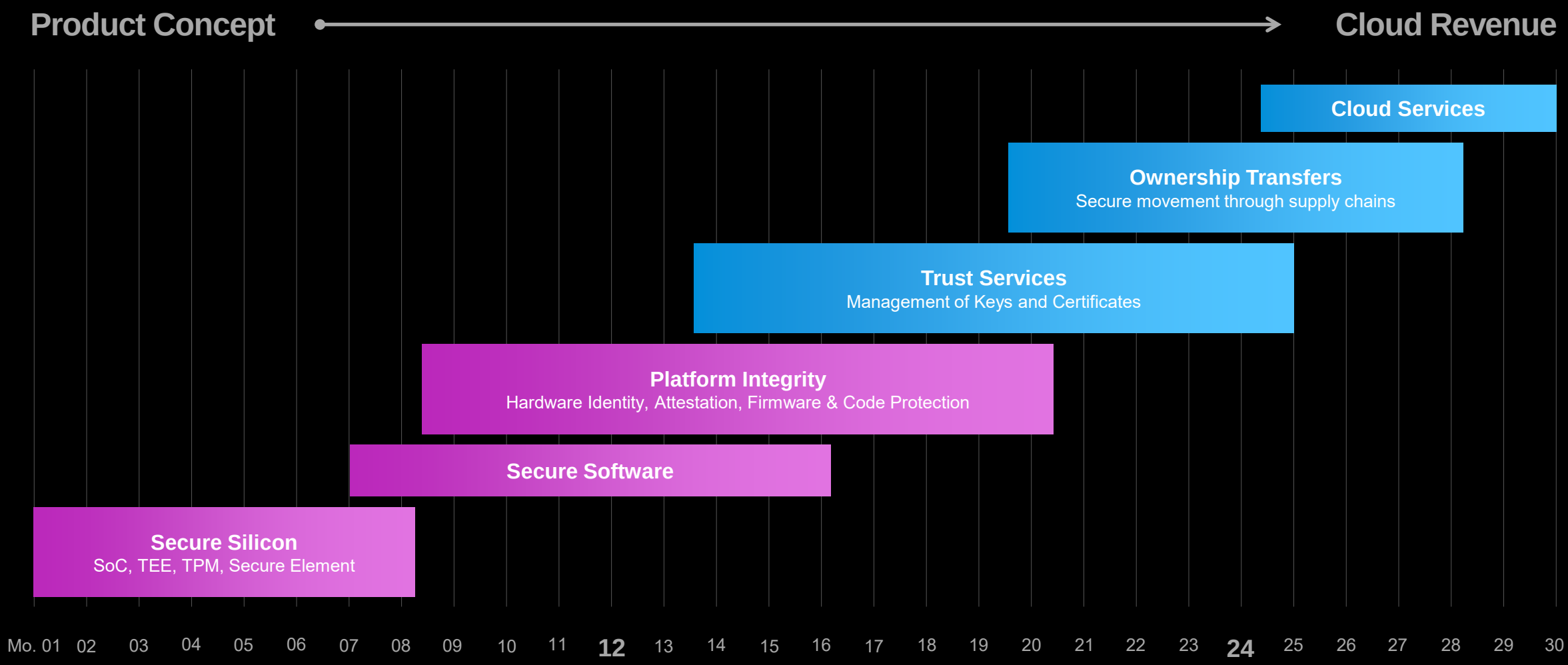
Need lower cost, easier to use, silicon to cloud security

Cloud Providers

Can’t deliver services if they don’t trust the connected products



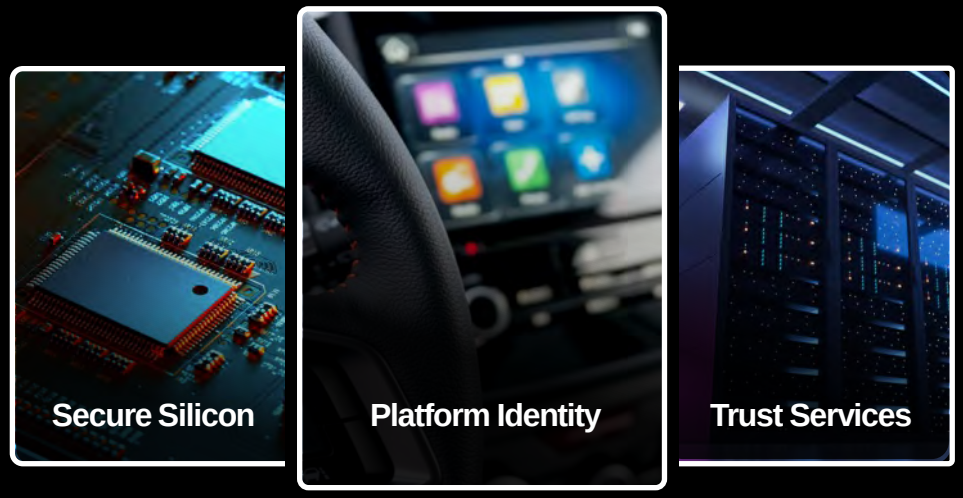
Integration time; the hidden cost



A Global Cloud Platform Approach

One platform. Simplified security. Unlimited potential.

Connected Products



Cloud Services

Bringing the next generation of connected products and services to life faster, more easily and more securely than ever before.

hushmesh

Hushmesh Inc. is a DC-based, dual-use, cybersecurity

Public Benefit Corporation

and

NATO DIANA startup

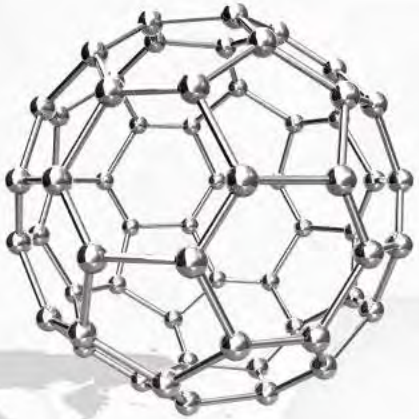


Semiconductor Traceability And Market Provenance (STAMP) Initiative

NATO OTAN

Defence Innovation Accelerator for the North Atlantic (DIANA)

hushmesh



The Mesh

is a global, decentralized

information infrastructure

Like the Web

But with built-in, universal

cryptographic provenance, integrity, traceability, confidentiality, and privacy



Semiconductor Traceability And Market Provenance (STAMP) Initiative

hushmesh

Automated cryptographic security for

all types of global entities

People, organizations,

physical things, and **digital things**

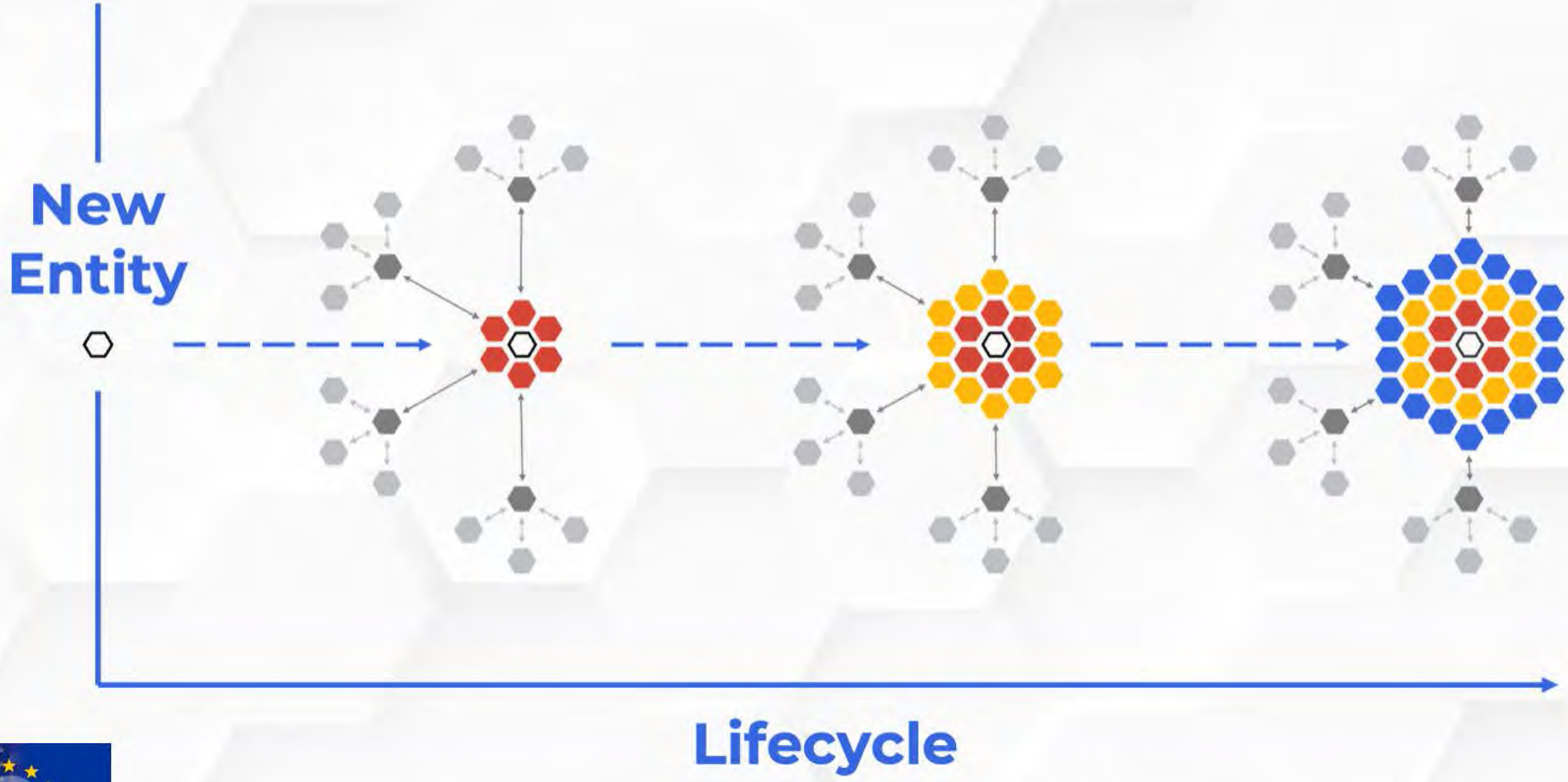
Each with its own independent

lifecycle, history, policies, and **relationships**



Semiconductor Traceability And Market Provenance (STAMP) Initiative

hushmesh



Semiconductor Traceability And Market Provenance (STAMP) Initiative

hushmesh

Universal Name System (UNS)

A global, decentralized, automated, cryptographic name system
unified across all types of entities: people, organizations, physical things, and digital things

Universal Certificate Authority (UCA)

A global, decentralized, automated, cryptographic key infrastructure
to solve provenance, integrity, authenticity, reputation, confidentiality, and privacy

Universal Private Ledgers (UPL)

Each entity has its own cryptographically isolated
information space, keychain, wallet, and private ledger

Universal Private Computing (UPC)

Any organization can automate the deployment of confidentiality and privacy-preserving,
cryptographically attested and verified code



Semiconductor Traceability And Market Provenance (STAMP) Initiative

Made possible by Confidential Computing

Semiconductor innovation!

Only *secure chips* can secure *secure chips*!



Confidential Computing Consortium

confidentialcomputing.io

Semiconductor Traceability And Market Provenance (STAMP) Initiative

hushmesh

The optimal cybersecurity blueprint

Smallest global attack surface mathematically possible

Orders of magnitude smaller than all other approaches

Least-trust blueprint technically possible

Cross-domain zero trust at internet scale

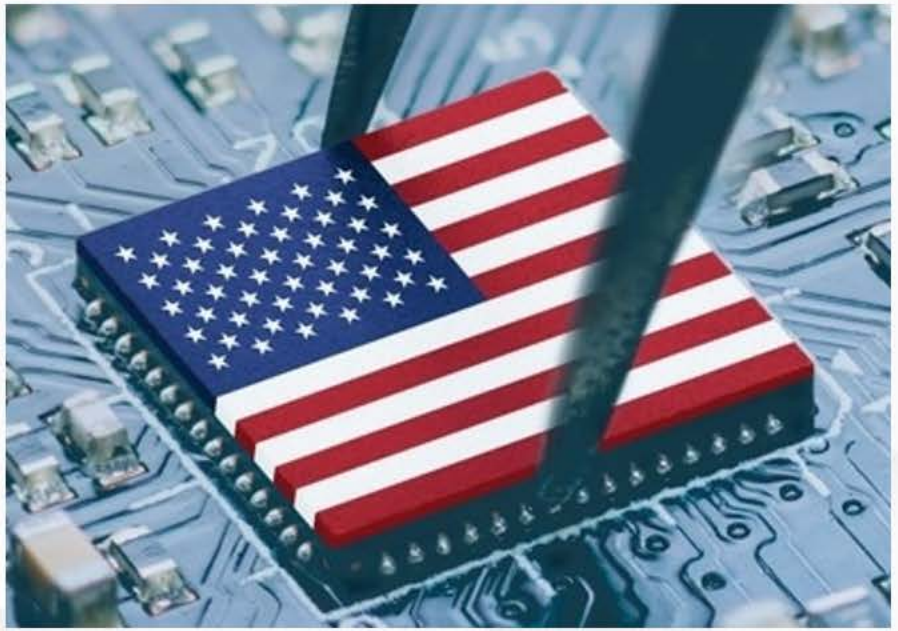
Entity-centric security

Software-defined cryptography



Semiconductor Traceability And Market Provenance (STAMP) Initiative

Fixing cybersecurity is the trillion-dollar business case





Semiconductors and Cybersecurity strategies

MUST be addressed jointly

Standards Panel Abstract



- **Global microelectronics traceability relies on strong, interoperable standards –** Key Areas of Focus:
  - **Blockchain frameworks** for secure transactions.
  - **Single-device traceability** to track individual components.
  - **Digital certificate issuance** for authentication.
  - **Cybersecurity and assurance protocols** to prevent threats.
  - **Data privacy and encryption methodologies** for secure communication.

- **Policies are needed to guide implementation for a seamless global system –** Panel Discussion Covers:
  - Prioritization of standard development.
  - Harmonization strategies across different regions.
  - Balancing technical and policy-driven approaches.

- **Goal:** Foster collaboration to build secure, traceable semiconductor standards



Digital Marketplaces

Trusted Digital Twins

Trusted Data Analytics

SEMI 6504 - Specification for Electronic Supply Chain Traceability Using Distributed Ledger Technology

Chip Design & Mfg

Packaging & Test

Embedded System

Vertical Markets

Edge Applications

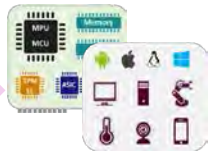
Environments



JA6801 HwA



JA6801 HwA



JA6801 HwA



JA6801 HwA



JA6801 HwA



NIST Cybersecurity Framework (CSF)

JA7496 - Cyber-Physical Systems Security Engineering Plan

NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

SAE J3327 EV Battery Traceability

SEMI T22 Specification for Traceability by Self and Authentication Service Bodies

IPC-1783 - International Standard for Component-Level Authentication

SEMI T23 Specification for Single Device Traceability for the Supply Chain

NIST IR 8536 Supply Chain Traceability: Manufacturing Meta-Framework

SEMI T25 Specification for Blockchain for Semiconductor Supply Chain Traceability

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

SEMI T225 Specification for Blockchain for Semiconductor Supply Chain Traceability

Trusted Digital Thread

Trusted Digital Transformation

Our Panelists



Moderator: Daniel DiMase – Aerocyonics, Inc.

- **SEMI – Paul Trio**: Director, Standards
- **SAE – Rich King**: Director Government & Industry Affairs
- **IPC/USPAE – James Will**: Executive Director
- **NIST – Sanjay Rekhi**: Group Leader of the Security Components and Mechanisms Group within the Computer Security Division
- **Ford Motor Co - Gloria D'Anna**: – SAE G-32 Co-Chair

Standards Opening Questions



1. **Current Landscape:**
    - "What are the most significant gaps in the current standards landscape for microelectronics traceability?"
    - "How are your organizations addressing the increasing demand for end-to-end traceability in the semiconductor supply chain?"
2. **Role of Standards:**
    - "How do standards help prevent counterfeit components and secure the integrity of critical systems?"
    - "What lessons from other industries can we apply to semiconductor traceability?"

SEMI Standards Overview

STAMP Initiative Workshop 2025

March 4, 2025

SEMI is Uniquely Qualified to Address the Industry's Top Challenges that Require Global Collaboration

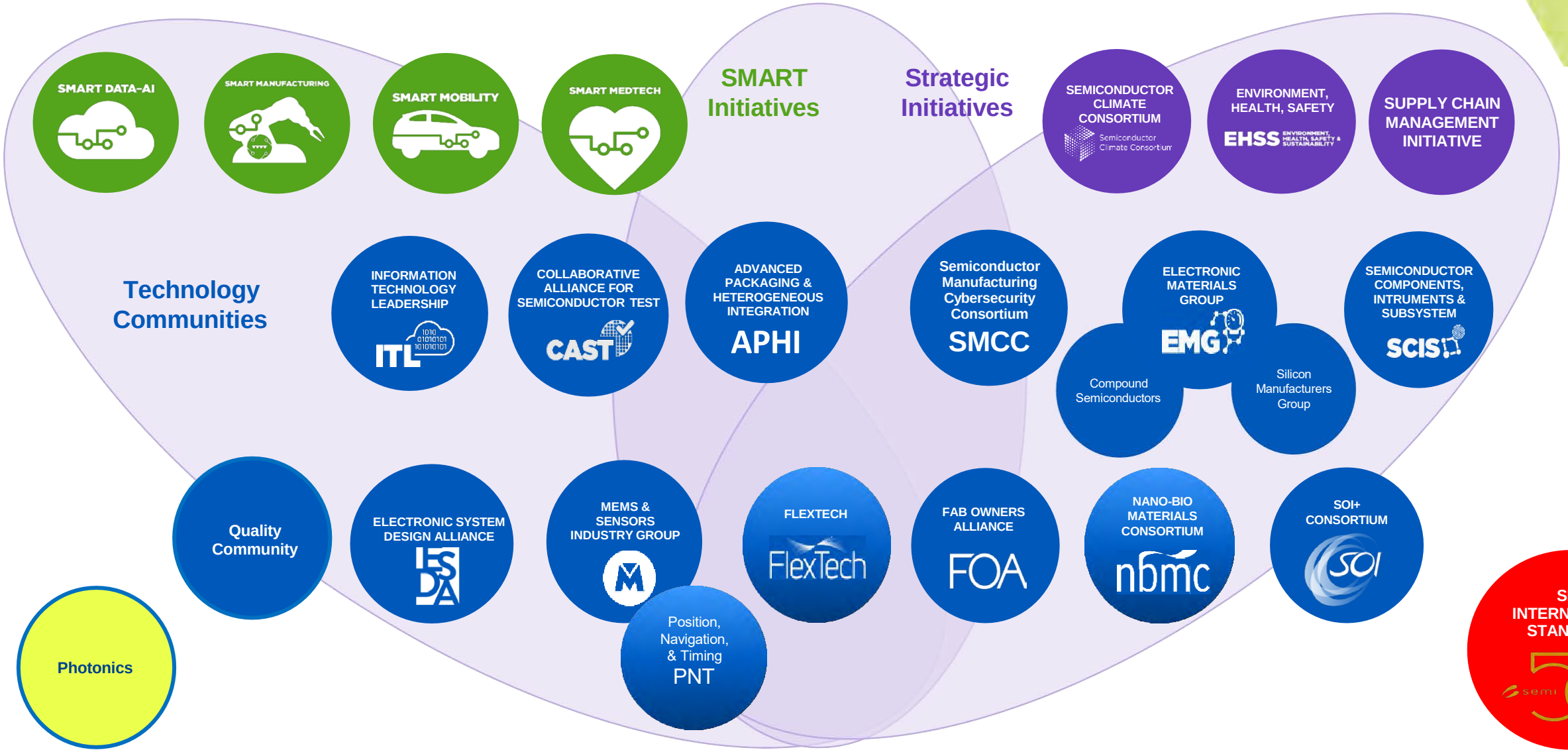
SEMI	Foundational		Expanded Programs and Scope			2025 Top Priorities
3,000+ members worldwide **Spanning the Semiconductor and Electronics Design and Manufacturing Supply Chain** **Driving Global Programs**	Thought Leadership	Worldwide Offices	Market Intelligence Reports	Tech partners: imec, Fraunhofer, CEA-Leti, IEEE, ITRI, AIST	**Supply Chain Resilience**	**Global Advocacy & SIPS Platform**
	Standards	2,300+ Program Hours				**Workforce Development**
	SEMICON® Expositions/ Conferences	170+ Tech Programs	Smart Initiatives	Strategic Tech Communities: ESDA, IESA, FOA, FlexTech, MSIG, SOIIC		**Sustainability**
	EHS	20+ Tech Communities	Think Tanks			**PFAS**
						Cybersecurity & AI

CONNECT - **COLLABORATE** - INNOVATE

SEMI Technology Communities

PROVIDING TECHNOLOGY STEWARDSHIP & COLLABORATION ACROSS THE ECOSYSTEM

PARTICIPATE | CONNECT | CONTRIBUTE | LEARN | LEAD | ENGAGE | COLLABORATE | TEACH | NETWORK | DISCUSS | CHALLENGE



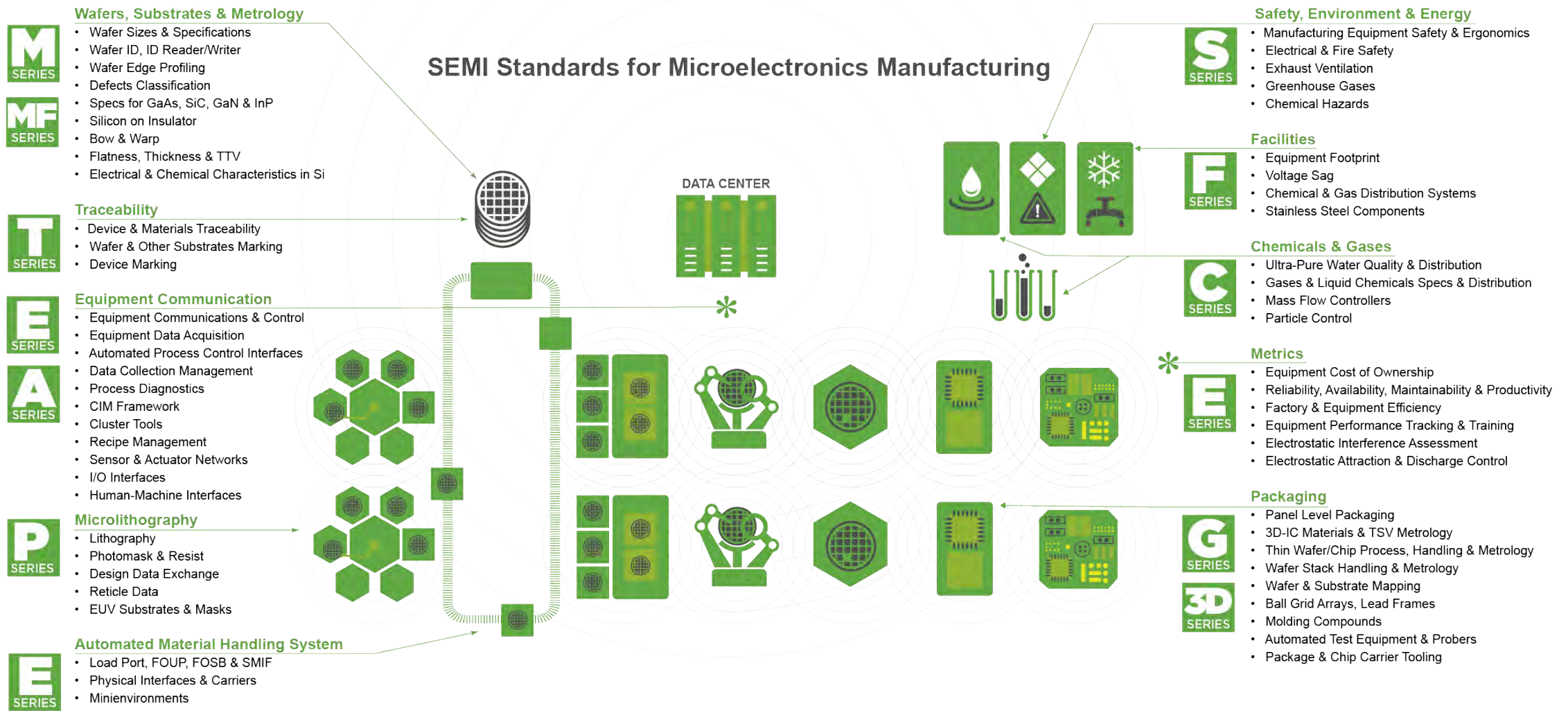
SEMI International Standards Overview



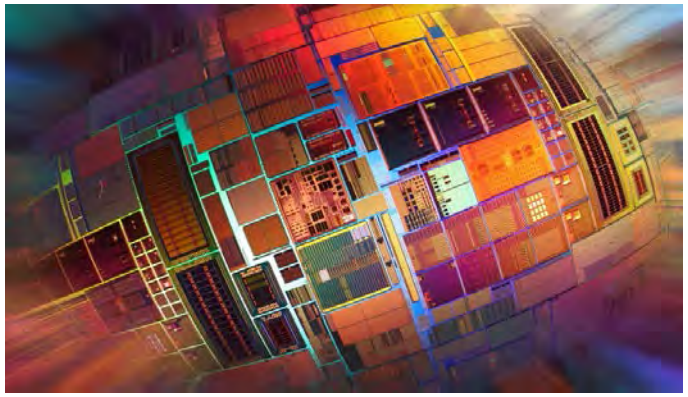
- **Established in 1973**
- **1,075+** published SEMI Standards & Safety Guidelines
- **5,000+** volunteer experts
  - 21 global Technical Committees
  - 200+ global Task Forces
- **2,000+** participating companies
- **Experts from semiconductor, PV, LED, MEMS & Display industries**
- **International presence**

Exchange ideas and develop globally-accepted technical standards

SEMI Standards: Oxygen for the industry



Staff Contact



Paul Trio
SEMI
Director, Standards
ptrio@semi.org



STAMP Standards Panel

STAMP Initiative Workshop, March 4th, 2025

Rich King, Director, Government & Industry Affairs – Aerospace email:Richard.king@sae.org

STAMP: Associated SAE Standards

1. **G-19: AS 6496A/AS9970/AS5553E;AS6301/AS6081A/AS6462/AS5553C;**
2. **G-19A: AS6171/10**
3. **G-21B: 7492**
4. **G-32: JA7496-202206**
5. **Please go to SAE Standards Works or Mobilus for more details.**

Copyright © SAE International.
Further use or distribution is not permitted without permission from SAE

STAMP Questions:

1. **Most significant gaps in the current standards landscape for microelectronics traceability?**

a. *Critical gaps still exist in traceability standards; still need a clear definition of the element to be traced;*

b. *Many existing standards lack clear, quantifiable metrics for assessing traceability performance or the risk of counterfeit parts;*

2. **Preventing counterfeit components and securing integrity of critical systems?**

a. *When unique requirements are used, the supply chain may be forced to develop a unique solution for each customer's requirement, which increases the risk of escapes;*

b. *Robust Traceability Protocols; Integration with Cyber-Physical Systems; Adoption and Interoperability are required;*

Copyright © SAE International.
Further use or distribution is not permitted without permission from SAE

STAMP Questions: Contd:

3. **How best to apply, get best value, and better monitor the implementation of assurance practices outlined in standards?**

a. Embed assurance practices directly into production, developing measurable KPIs to capture their value, and leverage advanced technologies like blockchain, to monitor compliance;

Copyright © SAE International.
Further use or distribution is not permitted without permission from SAE

STAMP: Associated SAE Standards

1. **G-19: AS 6496A/AS9970/AS5553E;AS6301/AS6081A/AS6462/AS5553C;**
2. **G-19A: AS6171/10**
3. **G-21B: 7492**
4. **G-32: JA7496-202206**
5. **Please go to SAE Standards Works or Mobilus for more details.**

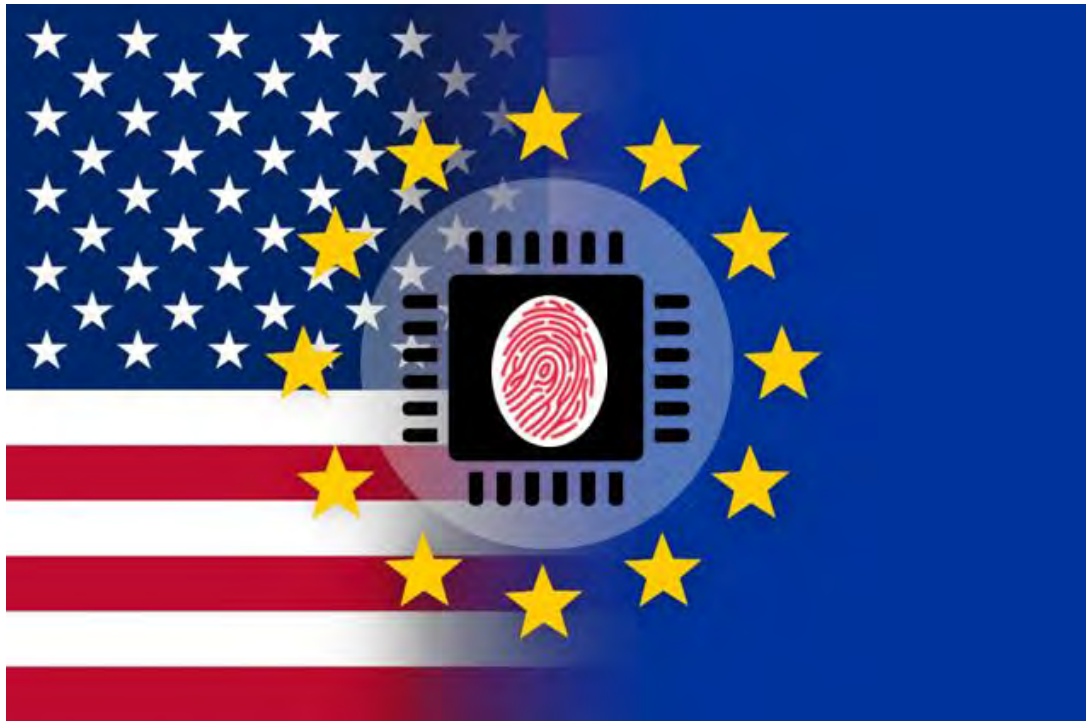
Copyright © SAE International.
Further use or distribution is not permitted without permission from SAE



STAMP Standards Panel

STAMP Initiative Workshop, March 4th, 2025

Rich King, Director, Government & Industry Affairs – Aerospace: email Richard.king@sae.org



Global Chip Traceability Initiative

A Trans-Atlantic Initiative for Cross-Border Chip Identification

USPAE

U.S. Partnership for Assured Electronics

STAMP Workshop Brief

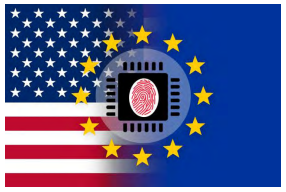
March, 4th 2025

www.uspae.org

Semiconductor Traceability And Market Provenance (STAMP) Initiative

About USPAE

- Mission is to ensure the USG has access to trusted, assured and resilient electronics supply chains.
- Facilitate interactions between USG and industry as a trusted and neutral 3rd party, including alliance partners, which range from traditional large defense prime contractors to small start-ups, non-traditional and academia, covering nearly all aspects of the electronics ecosystem.
- Identify major gaps in national electronics capabilities and capacity, raising awareness of these issues and developing solutions to address them.
- IPC subsidiary



www.uspae.org

About IPC

IPC is the global association that helps OEMs, EMS, PCB manufacturers, cable and wiring harness manufacturers and electronics industry suppliers build electronics better. IPC members strengthen their bottom line and build more reliable, high-quality products through proven standards, certification, education and training, thought leadership, advocacy, innovative solutions and industry intelligence.

IPC MEMBERS REPRESENT THE ENTIRE ELECTRONICS INDUSTRY SUPPLY CHAIN

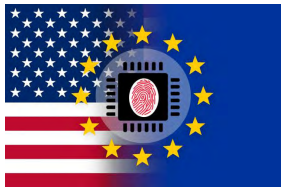


Assurance Standards

- Drive demand to Assured Sources
  - *Start with current standards, certifications, and industry best practice*
  - *Tiered assurance standards*
  - *Standards ineffective if not aligned with Policy and Acquisition requirements*

- DoC and EU CHIPS, DPA Title III, and other Allied + Industry investments are infrastructure focused
  - *Business fails without demand and pipeline, loss of industry and taxpayer investment*
  - *Adversary wins NON-TENABLE*

- Geopolitical and economic forces at play
  - *Assurance standards moot if adversary controls the market*
  - *Need to think strategically*



G-32 Overview

Gloria D’Anna – Co-Chair

March 3, 2025

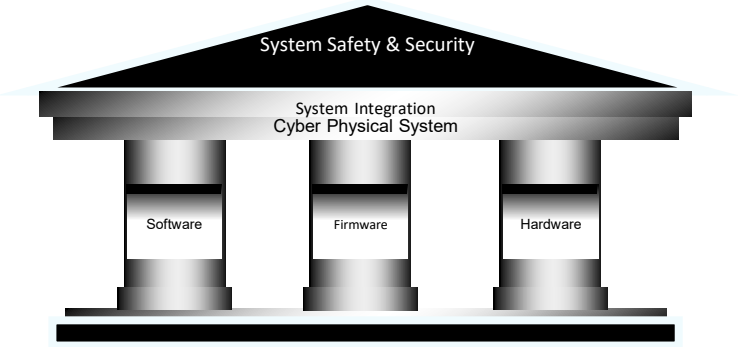
SAE G-32 Cyber Physical Systems Security Committee

G-32 Mission

❖Develop standards by characterizing and addressing the risks to Cyber Physical Systems Security (CPSS), assessing weaknesses and vulnerabilities, and recommending System Engineering focused mitigation actions defined by the operational, functional, and architectural systems engineering elements.

❖Share and establish standard methods for identifying weaknesses and vulnerabilities in cyber physical systems introduced at any point in the CPSS life cycle and mitigating impacts.

❖Develop validation and verification methods to ensure security requirements are addressed.



Gloria D'Anna Ford Co-Chair, USA	Bill Scofield Boeing Co-Chair, USA	Joel Heebink Aerocyonics Secretary, USA

Global Contributors

Aircraft/Engine Manufacturers, Automotive, Commercial Vehicles, Tier 1 and 2 Suppliers, Operators, Regulators, MRO Service providers, IT Product & Service Providers, Consulting Firms and Standards Organizations.

If you would like to Contribute to the work of SAE G-32, please visit:
https://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG32.

Standards in Progress for the Commercial Aviation, Defense and other high reliability and/or critical systems in aerospace, transportation, medical, etc.

JA7496	Cyber Physical Systems Security Engineering Plan (CPSSEP) **(Published June 2022)**
JA6678	Cyber Physical Systems Security Software Assurance (Est. Publication**: 2025**)
JA6801	Cyber Physical Systems Security Hardware Assurance (Est. Publication: **2025**)
JA7151	Netlist Analysis Techniques for Assurance (Est. Publication**: 2025**)

Contact: Dorothy Lloyd, Dlloyd@sae.org for more information or to participate on G-32 Committee.

Video 0

CPSSEP

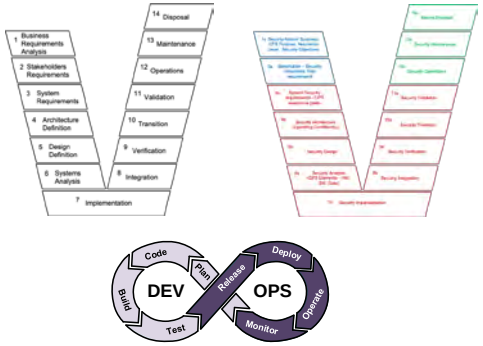
TECHNICAL PROCESSES

SECURITY ELEMENTS

INTEGRATED RISK MANAGEMENT

CPS ASSURANCE CASE

CPS SEP GOAL/ CLAIM

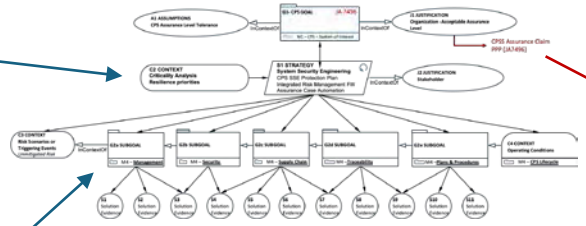


Video 1

Video 2



OUTPUT



STANDARDS (pan-industry)

Video 3

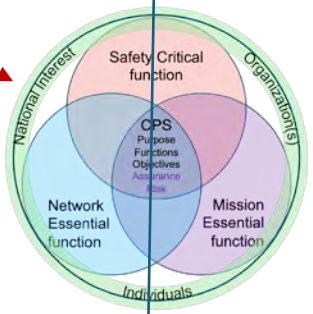


DOMAINS OF CONSIDERATION

FILTER
To focus solutions

Video 4

including (SwA, HwA)



CYBERSAFE
CYBERSECURE
CYBERRESILIENT
NETSECURE

The Role of Standards

- **How do standards help prevent counterfeit components and secure the integrity of critical systems?**

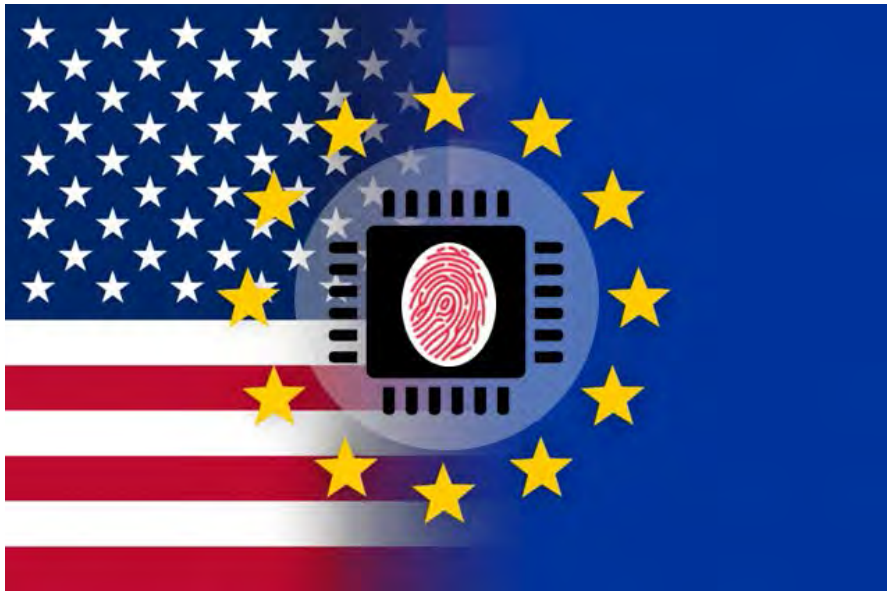
- By integrating a systems engineering approach to traceable security artifacts into technical processes, risk management, assurance case and electronic system bill of materials

The Role of Standards

- **What lessons from other industries can we apply to semiconductor traceability?**

- By implementing an explicit and unambiguous/ standardized taxonomy to bridge and consider pan-industry standards.
- By providing unambiguous and measurement standards to guide risk management and assurance activities throughout the product lifecycle.
- By acknowledging the limitations of traditional ordinal scale risk measurements, and unintentional bias when using different ordinal based risk measurement scales across different industry standards.

Global Chip Traceability Initiative



Panel – *Traceability Economics and Business Models*

Traceability Economics and Business Models

- **Supply chain traceability emerging markets and end to end solutions and services**
  - **Consumer Markets -** ID + Blockchain Based Services (Luxury Goods, Pharma, F&B, Textiles)
  - **Electronics Markets:** ID + RoT + Security Solutions (e-Fuse/Crypto, TPM, SE, DRM, PKI, CA…)

- **Lack of chip traceability due wafer singulation and fragmented supply chain gaps**
  - Lack of asset/data provenance (Forward/Backward) for failure analysis, tracing, prediction
  - Multiple countries of origin (design, manufacturing, assembly) and layers of distribution

- **End market driven partnerships for traceability across supply chains are necessary**
  - Opportunity for digital twins, solutions, and services based on **ID + Security + Certificates**
  - Requires partnerships starting from provenance (Foundry, EDA/IP, OSAT and Fabless IC)



Our Panelists

Moderator: Tom Katsioulas, Archon Design Solutions, Inc.

End Market

- **Lockheed Martin** - Brian Gabriel, Critical Materials Senior Manager
- **Airbus** - Andreas Schweiger, System Architect, Defense & Space

Design Foundry OSAT

- **Infineon -** Theodore Varelas: Director Strategic Initiatives, Digital Security & Identity
- **GlobalFoundries** - Ezra Hall: Worldwide Aerospace-Defense Business leader
- **Integra Tech** - Sultan Lilani, Technical Business Development
- **PDF Solutions** - Christophe Begue: VP of Corporate Strategic Marketing

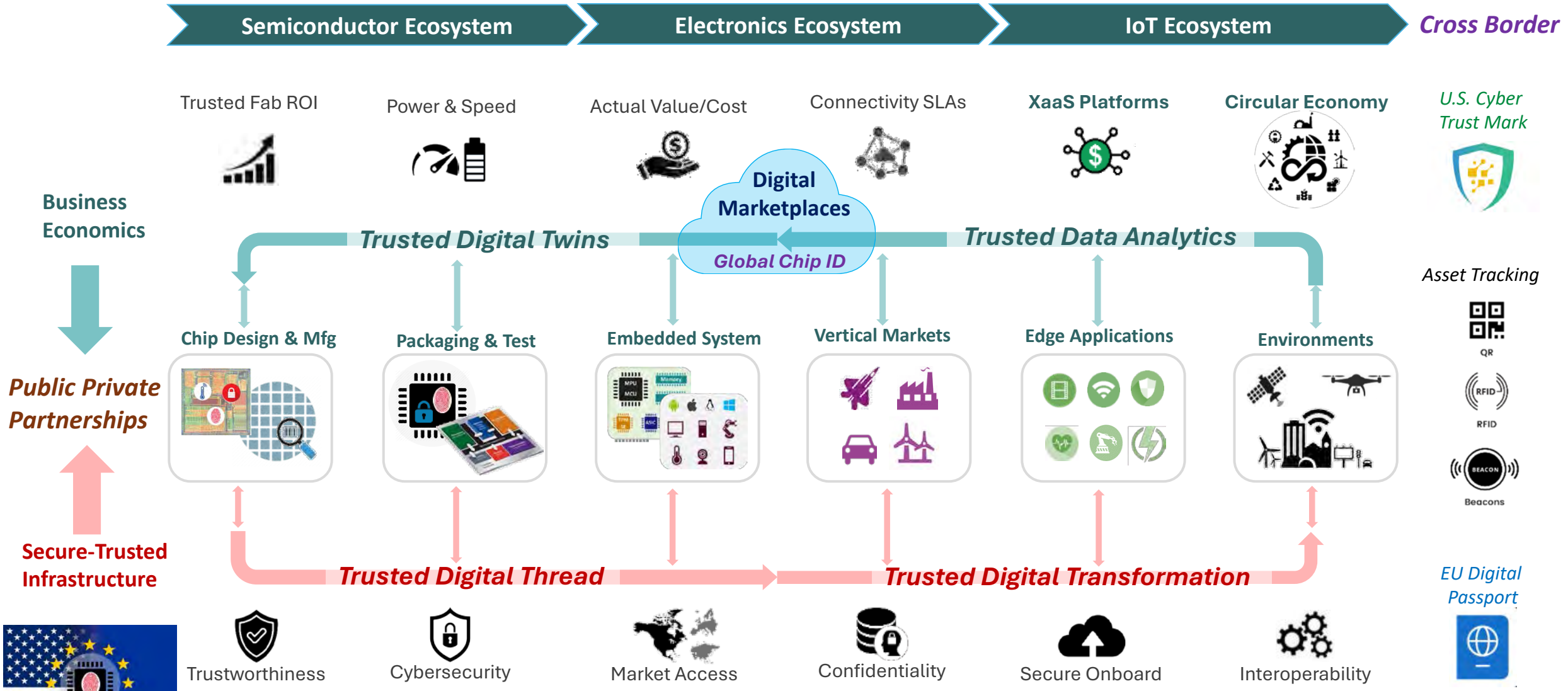
IP and EDA

- **Tartan Silicon** - Alan Aronoff: Founder and CEO
- **Synopsys** - Reed Hinkel, Director, Strategic Programs
- **Cadence -** Steve Carlson, Technology and Market Strategist



End to End Traceability Vision*

*Source: IoT Advisory Board Report



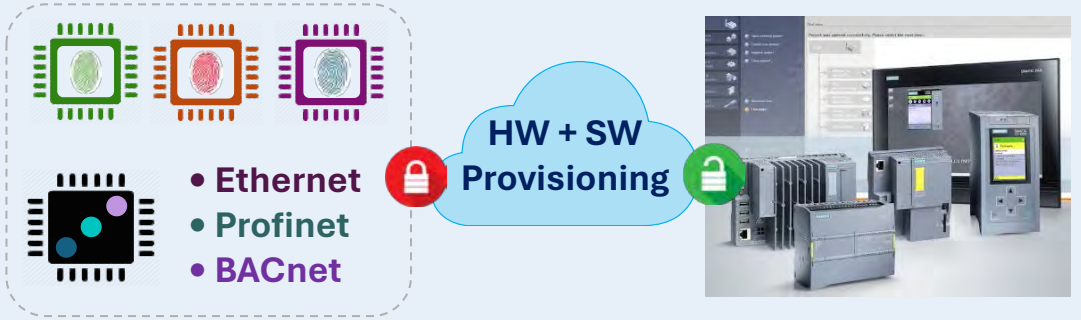
End-Market Driven Business Use Cases

Aerospace & Defense - Manufacturing Integrity (SLM)



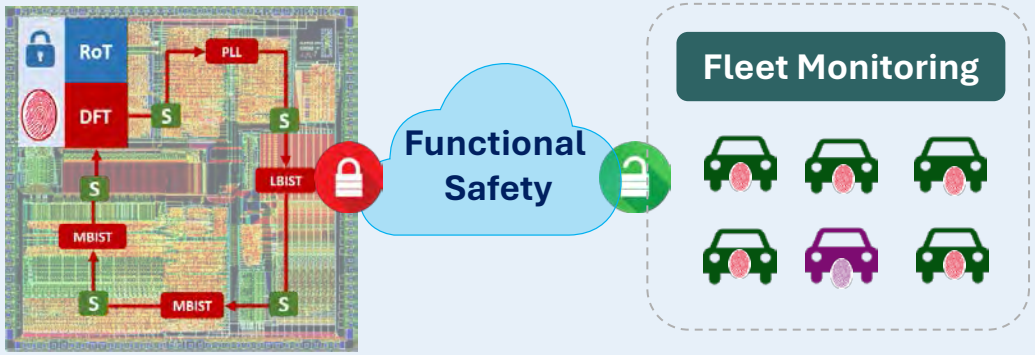
Source: ERI Summit 2020

Industrial – Critical Infrastructure Multi Market XaaS



*Sources: Intel - Pay-as-you-go Chip Licensing, Samsung - Memory Chip Rental Service

Automotive - Silicon Lifecycle Management (SLM)



*Source: Semiconductor Eng

Supply Chain - Monitoring and Regulating Field Use



Sources: Reuters - chips in Russian drones, WSJ - Cheap drones in battlefields



Panel Discussion

Traceability Enhanced Business Use Case Topics

End Market Problem → **Partner Solution** → **Stakeholder Benefits** → **Economic Value**

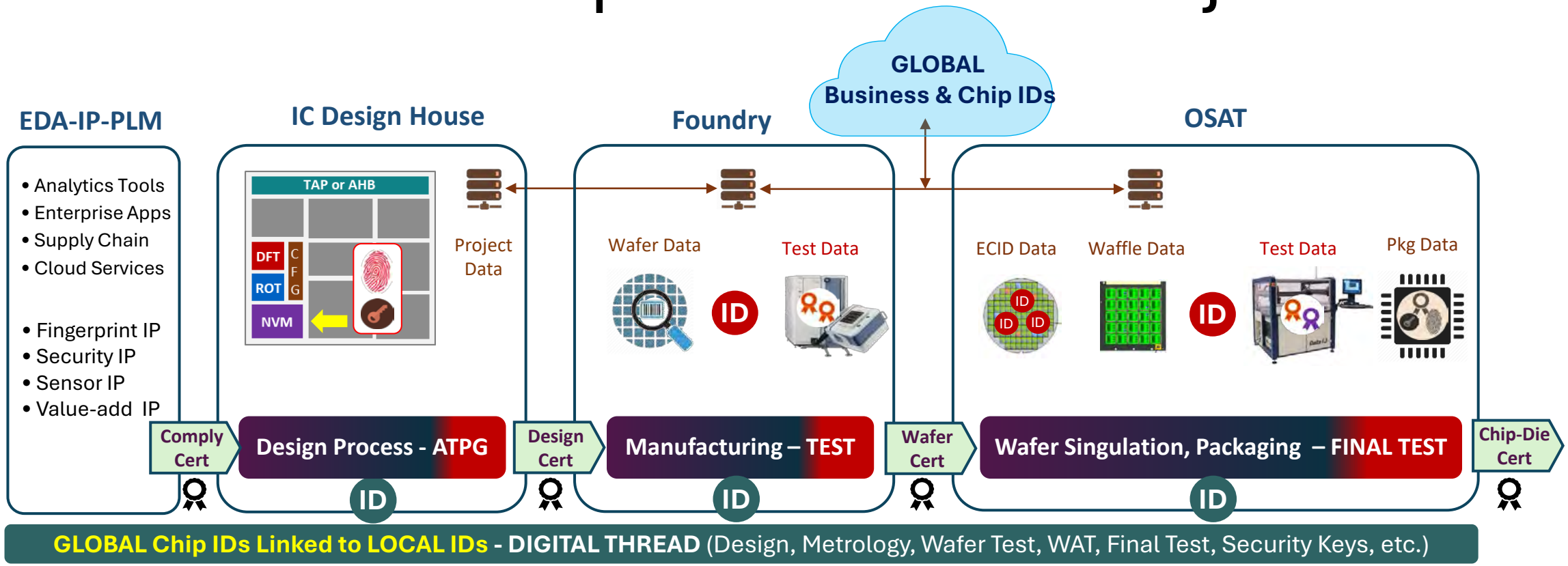
1. Regulatory Compliance and Supply Chain Security & Trust
2. Characterization Data and Digital Twins for Troubleshooting
3. End-to-end solutions for SLM, FuSa*, Root Cause Analysis
4. Authentication, Tamper Detection, and Field Attestation

Stakeholders discuss solution from based on how their companies contribute to it



*Silicon Lifecycle Management, Functional Safety

Solution Partnerships Toward Pilot Projects



1. EDA, IP, ATE:
2. Fabless IC:
3. Foundry:
4. OSAT:

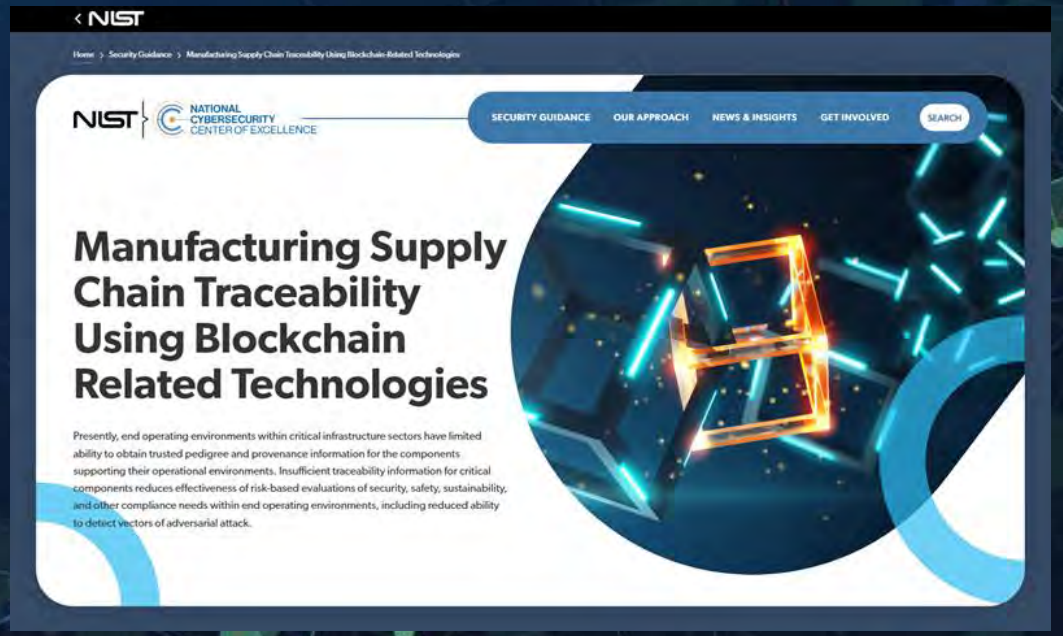
- EMS, OEM
- End Application
- Economic Value



Manufacturing Supply Chain Traceability Research and Reference Implementation

Manufacturing Meta-Framework

National Cybersecurity Center of Excellence



2025 March

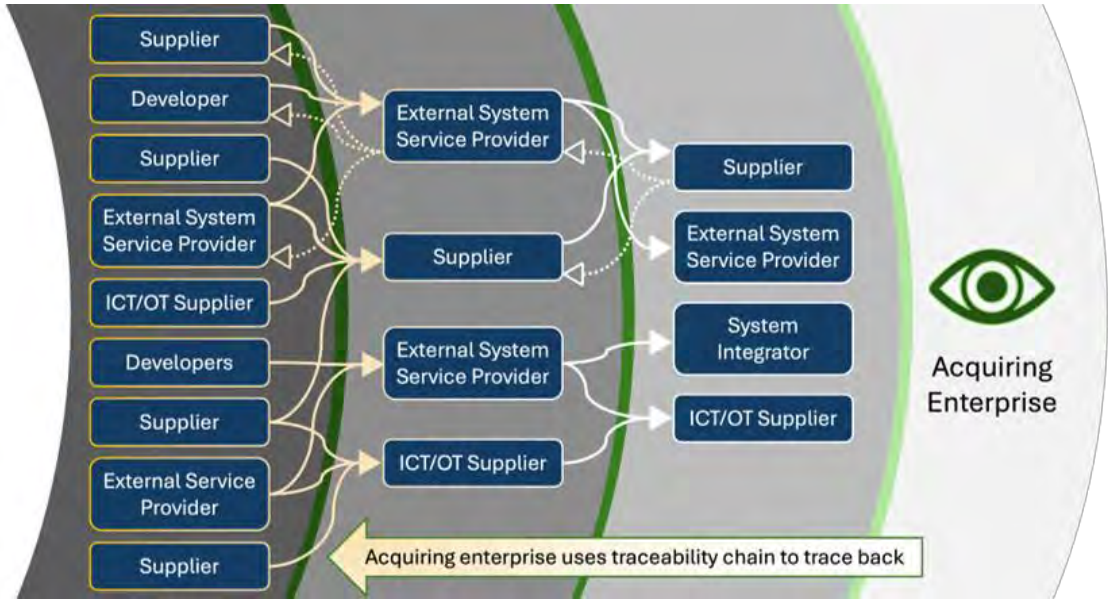
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMERS

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

WHAT IS SUPPLY CHAIN TRACEABILITY?

- **Recognizing Different Perspectives**
  - ***Internal (Digital Threads)*:** Tracking materials, designs, processes, and product data within and between organizations. Example: PLM, MES, ERP systems capturing “as-designed,” “as-built,” and “as-maintained.”
  - ***External (Industry, Regulatory, & Consumer Requirements)*:** Sharing data with partners, acquirers (e.g., customers), or regulators to prove origin, compliance, provenance, pedigree, etc.
- **Common Goal**:
  - Ensure **who**, **what**, **when**, and **where** data is verifiable and easily accessible—improving **visibility**, **risk management**, and **compliance** across the entire supply chain.
- **Why It Matters**:
  - **Traceability:** Industry needs a way to consistently link pedigree and provenance information for products, including semiconductors.
  - **Counterfeit Prevention**: Validate authenticity.



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Modified from NIST SP 800-161r1

THE NCCOE META-FRAMEWORK

Bridging Internal & External Views:

- Organizations have **internal** information systems (e.g., digital threads, traceability systems).
- The Meta-Framework allows organizations to leverage existing systems and **selectively** provide **externally** required traceability data (e.g., compliance or customer-facing info).

Interoperability & Flexibility:

- Designed as a **vendor-agnostic "blueprint"** that can unify diverse technologies (traditional databases, blockchain, IoT platforms, etc.).
- Encourages **standard data models** so stakeholders can share or request the data and have that data being readable and interpretable to support multiple end user use cases.

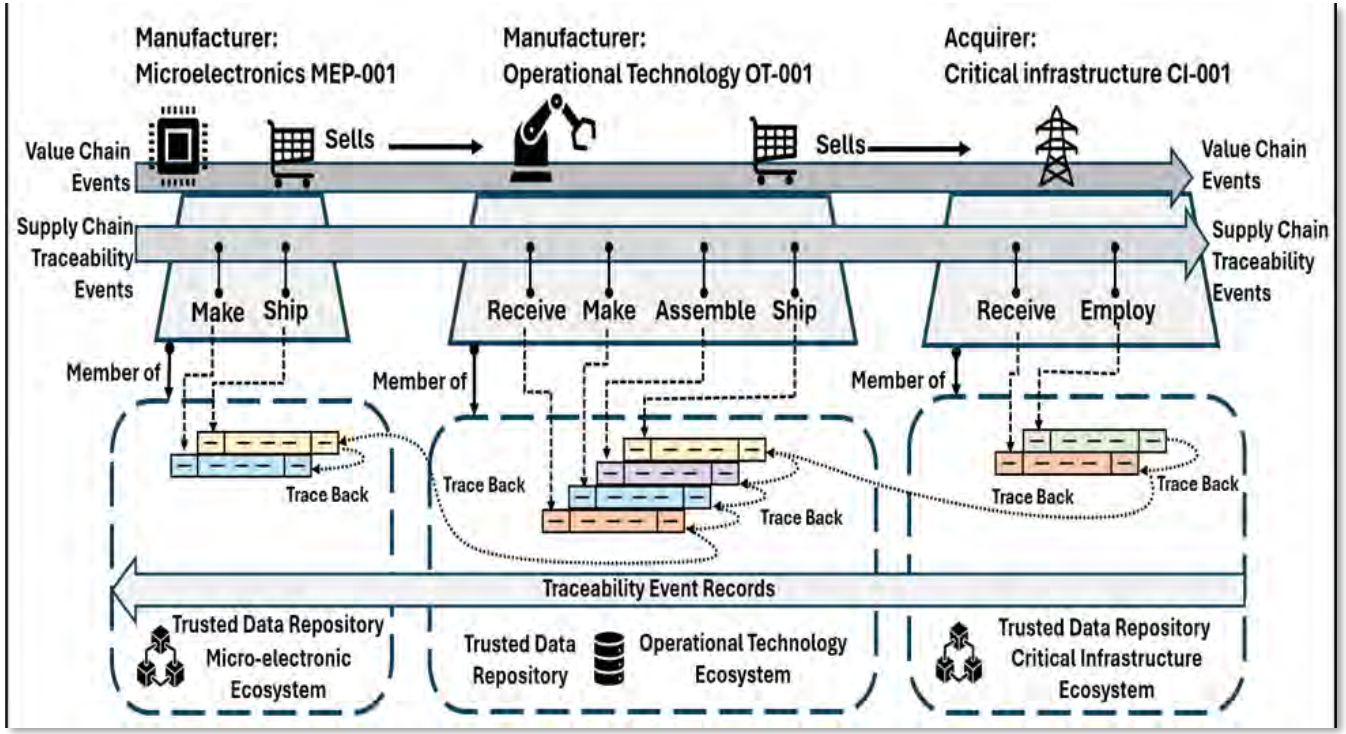
Selective & Secure Data Sharing:

- Allows publishing of **only** essential info (like batch IDs, certificates, and other regulatory data) while keeping **proprietary data private**.
- Allows including **supplemental reference** links to more detailed data that might be tokenized or protected behind appropriate access controls.

Benefits for Organizations:

- **Lower Integration Costs**: A reference model and ecosystems save time vs. building a unique solution from scratch.
- **Simplified Compliance**: Aligns with regulations by providing a standard method to share verifiable information.

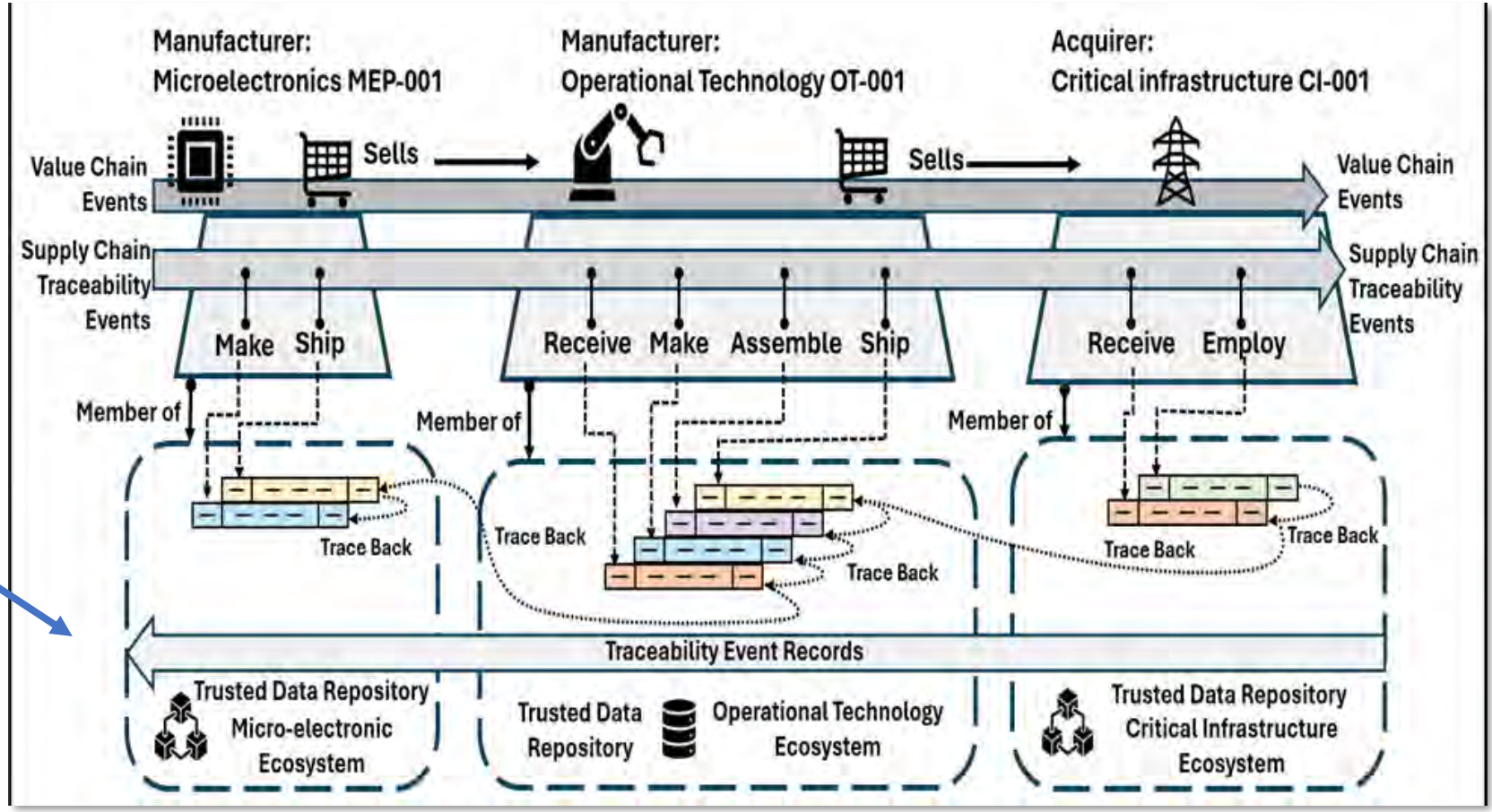
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



NIST IR 8536 IPD Figure 4 - Value and Supply Chain Traceability Events Across Ecosystems

PRINCIPAL TRACEABILITY WORKFLOW

- **Workflow 1**
  - Manufacturers write traceability records, incrementally creating a traceability chain
- **Workflow 2**
  - End customer reads the traceability chain to inform their risk analysis



NIST IR 8536 IPD Figure 4 - Value and Supply Chain Traceability Events Across Ecosystems

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

KEY TAKEAWAYS & NEXT STEPS

Why It Matters: Traceability is central to compliance, risk management, and consumer trust.

Meta-Framework's Role: Facilitates interoperability, secure data references, and modular adoption.

Next Steps:

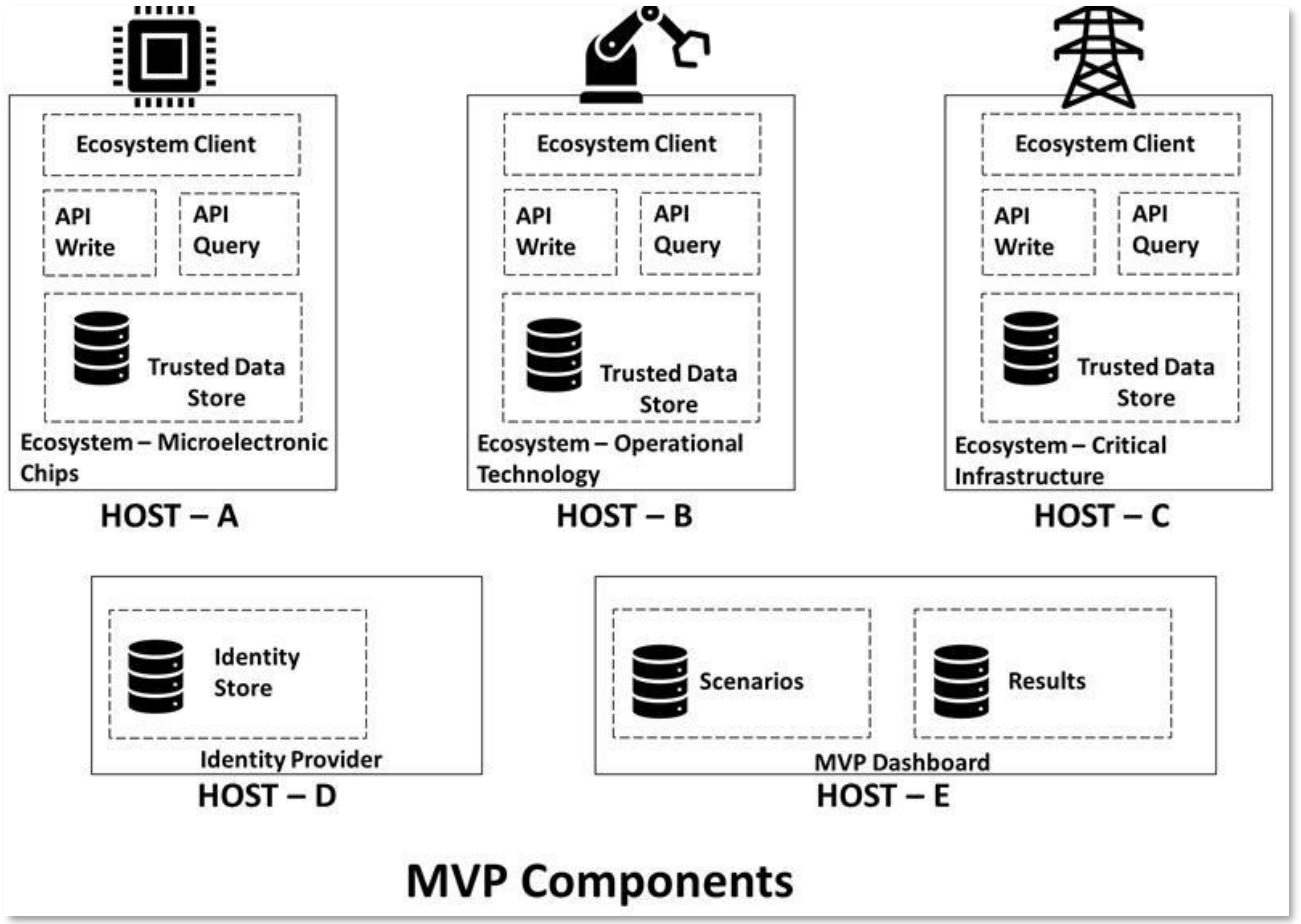
- The Initial Public Draft is being revised based on the comments received, and we expect to complete the update within the next couple of weeks.
- A second Public Review is being considered toward the end of March or we will submit the updated paper for final publication.
- Development of a Reference Implementation for lab experimentation and research has begun with a target release of the end of September.

RI/MVP HIGH-LEVEL ARCHITECTURE

Goal: ***create a functional implementation that allows stakeholders to observe and test supply chain risk management practices in a controlled lab environment***.

Approach:

- **Establishing a module platform** for deploying one or more ecosystems that can support or implement different Identity Providers, APIs, and data repositories including Blockchains/Distributed Ledger Technologies, NoSQL, traditional SQL, or other data storage technologies.
- **Provide a Dashboard / Administrative Interface** to monitor/manage the ecosystems and collect KPI data.

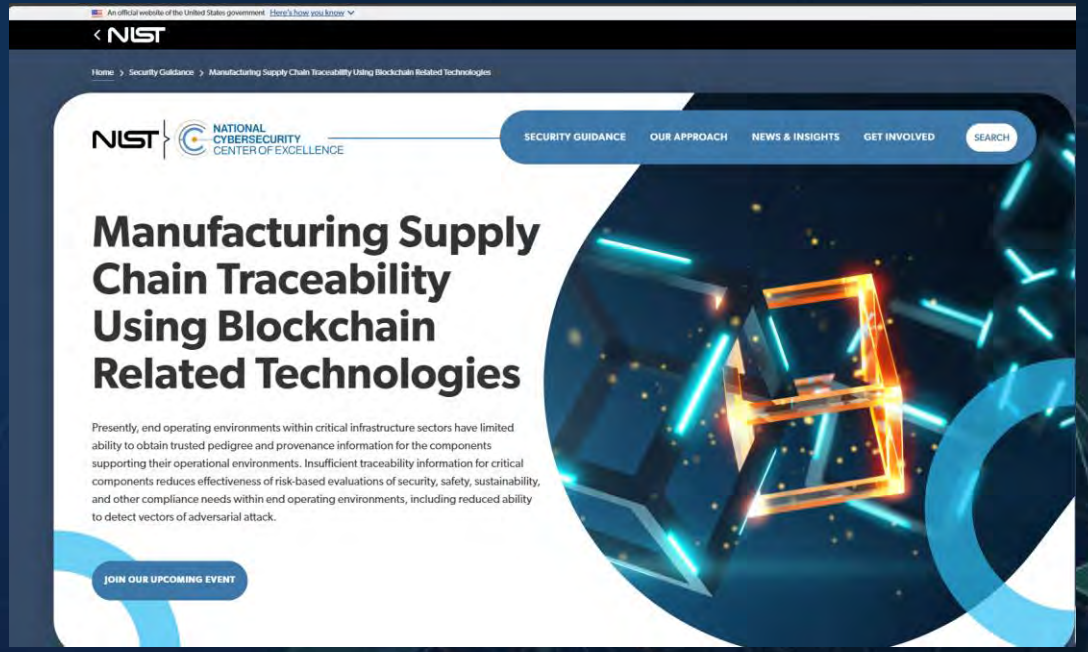


NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE "Manufacturing Supply Chain Traceability Using Blockchain Related Technologies"

https://nccoe.nist.gov/projects/manufacturing-supply-chain-traceability-using-blockchain-related-technologies

blockchain_nccoe@nist.gov



nccoe.nist.gov

@NISTcyber

EXAMPLE

Scenario Context:

WidgetCo needs to meet domestic sourcing rules (e.g., Berry Amendment, Buy American Act) for a Government contract requiring specialty steel from U.S. suppliers.

Key Challenges

- Verifying **domestic content** across multiple supply tiers.
- Providing **credible documentation** without exposing proprietary design details.
- Ensuring data is **tamper-proof** for audits and investigations.

Using the Meta-Framework

- **Event Logging**: Each steel shipment is recorded internally, and relevant data (lot numbers, certificates) is published in a standardized Meta-Framework "make, ship, and receive events."
- **Selective Sharing**: Pedigree and provenance information in the traceability record can contain only regulatory-required information such as test certificates or origin documents, hashed for integrity checks.
- **Secure & Auditable**: Contractors can verify the provenance and confirm certifications have not been altered without accessing internal/proprietary systems or details.

Outcome

- Easier compliance audits, less risk of non-compliance, faster verification for contract award, and for supporting Government acceptance testing.

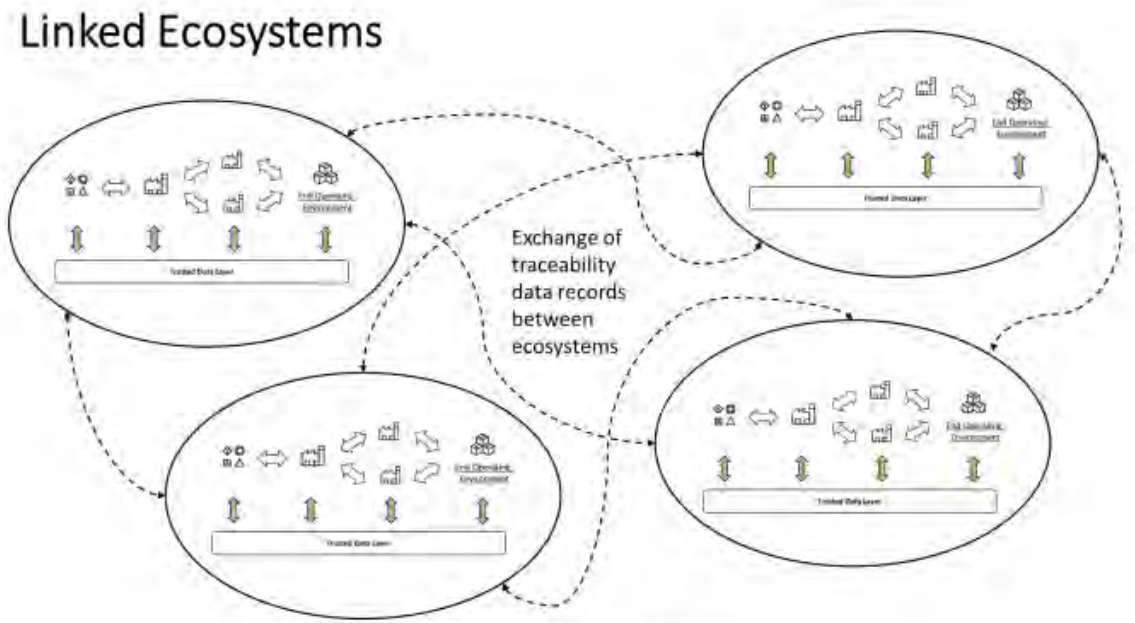


Figure 10 - Network of traceability ecosystems

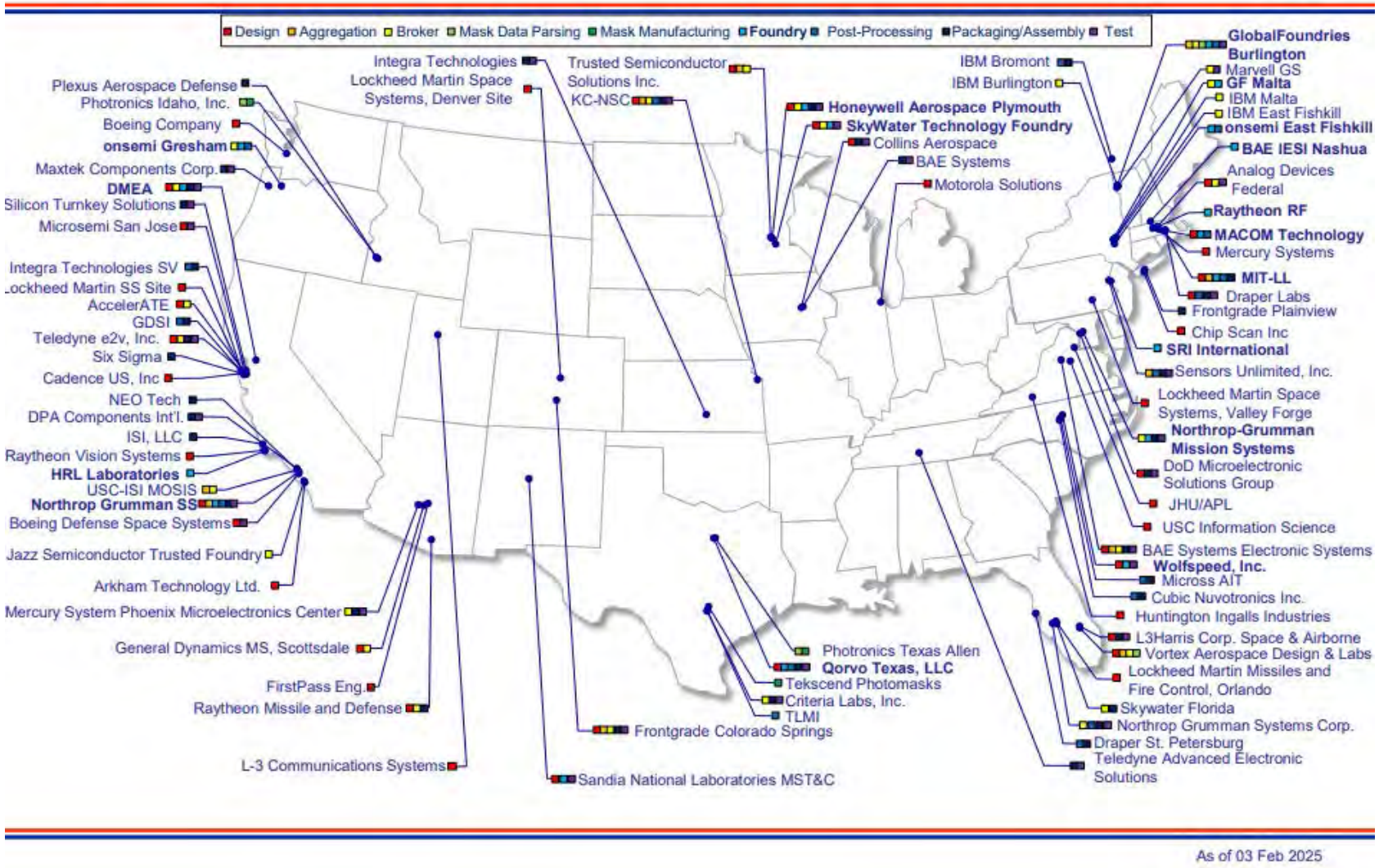
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DMEA/TAPO - Trusted Supplier Program

- DMEA is the program manager for the DoD Trusted Supplier program. The program provides a cost-effective means to assure the integrity and confidentiality of integrated circuits during design and manufacturing while providing the US Government with access to advanced microelectronics technologies for both Trusted and non-sensitive applications.

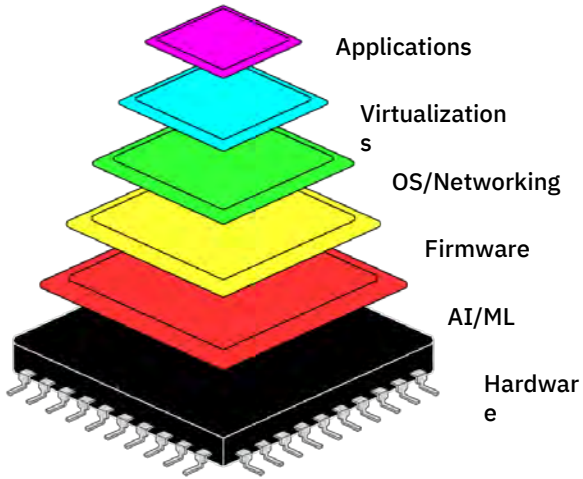
- The DMEA Trusted Supply program represents a balanced approach:
  - It leverages the innovation and agility of the private sector.
  - It provides strategic direction and support from the government.

82 Trusted Suppliers



Chip Scan

Chip Scan is a secure supply chain specialist in the area of military and intelligence microelectronics. We were founded over a decade ago to address this threat before the threat was widely known.



Supply Chain Layer Coverage

- Pioneer in chip supply chain analysis tools
- Innovator in use of beacons for post fabrication integrity validation
- Automated Chip Reverse Engineering
- DMEA Category 1a Trusted Supplier
- ATEA Anti-Tamper ID/IQ Program
- Secure Processor Innovations

Proprietary. Copyright © Chip Scan. All Rights Reserved

Calvin Chu



Calvin Chu, COO

Calvin Chu is the Chief Operating Officer and President of Chip Scan, spearheading the mission to protect microelectronics and their supply chains from cyber threats. With a strong background in hardware startups and security, Calvin's previous ventures have included innovations in aviation situational displays, consumer and military GNSS systems, firmware cybersecurity, AI, medical hardware, and imaging. His extensive expertise in developing advanced hardware solutions and understanding supply chain complexities is bringing Chip Scan to the forefront on hardware assurance.

STAMP Initiative: *Next Steps & Path Forward*



- Workshop Summary & Discussion | March 4, 2025

Open Discussion & Closing Remarks



- Final input from attendees:
  - Key takeaways?
  - Next steps for collaboration?

Thank you for your Contribution!

Questions for Attendees



- Why should this be done?
- How should this be done?
- When should this be done (short-term <1 year, long-term >1 year)?
- What mechanisms/consortiums can we leverage?

Key Discussion Points



- **Why should this be done?**
  - Address critical supply chain risks, security gaps, and provenance challenges
  - Align with global semiconductor trust and traceability efforts (CHIPS Acts, industry standards)
  - Enable new business models through trusted microelectronics and digital marketplaces
- **How should this be done?**
  - Define short-term and long-term goals for implementing semiconductor traceability
  - Develop actionable steps for cross-industry adoption and policy alignment
  - Identify priority areas in sourcing, manufacturing, distribution, 3rd party IP, and compliance

When Should This Be Done?

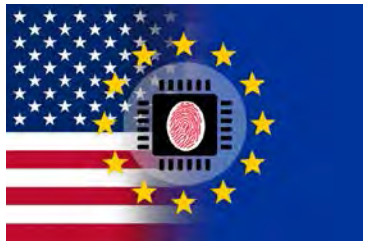


- **Short-term (0-12 months):**
  - Document industry priorities & challenges
  - Engage with key stakeholders, policy groups, and standards bodies
  - Launch pilot initiatives (e.g., chip ID proof-of-concept)
- **Long-term (1+ years):**
  - Scale implementation across the global supply chain
  - Align with government policies & regulatory frameworks
  - Develop an industry-backed roadmap for full traceability adoption

What Mechanisms/Consortiums Can We Leverage?



- Industry Bodies & Standards: SEMI, NIST, SAE, JEDEC, IPC, ISO
- Government & Policy Groups: U.S. DoC, EU CHIPS Office, NIST NCCoE
- Existing Initiatives: Global Chip Traceability, U.S.-EU TTC, Cyber Trust Mark
- Public-Private Partnerships: Aerospace & Defense, Automotive, IoT sectors



BACKUP

Actionable Next Steps



✓ Establish a Core Working Group to refine key takeaways and a strategic roadmap

✓ Plan participation in upcoming industry events (e.g., GOMAC Panel, NIST Workshop – April 15, 2025)

✓ Define and document an initial implementation roadmap

✓ Identify funding and support mechanisms for pilot projects

✓ Prepare a post-workshop report summarizing key findings and next actions

💡 Discussion: What additional steps should be prioritized?