Global Chip Traceability: Securing the Semiconductor Supply Chain for a Resilient Future

Jeremy Muldavin (Moderator)

Cadence Design Systems, Inc.

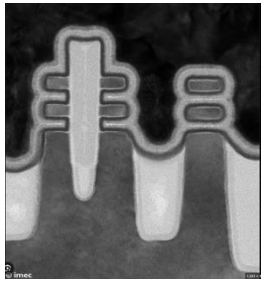
Contact Information

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

Our Cyber-Physical Infrastructure

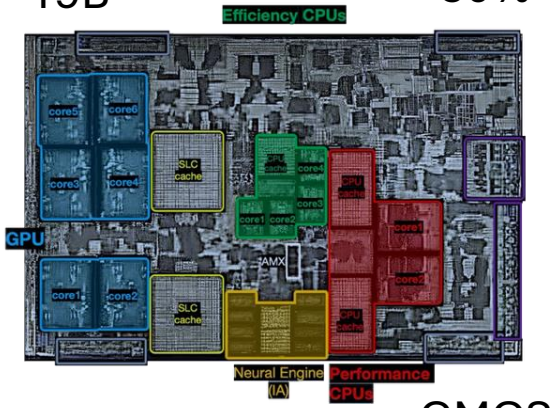
Connected

Complex



"3nm"
19B

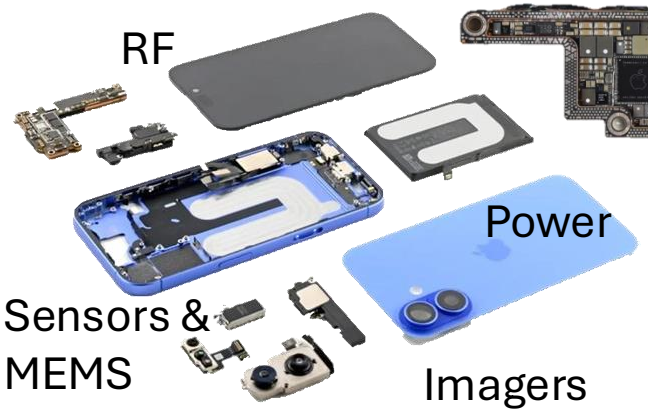
50%



CPU
GPU
NPU

CMOS

RF



RF-SOI

Power

GaN

SiC

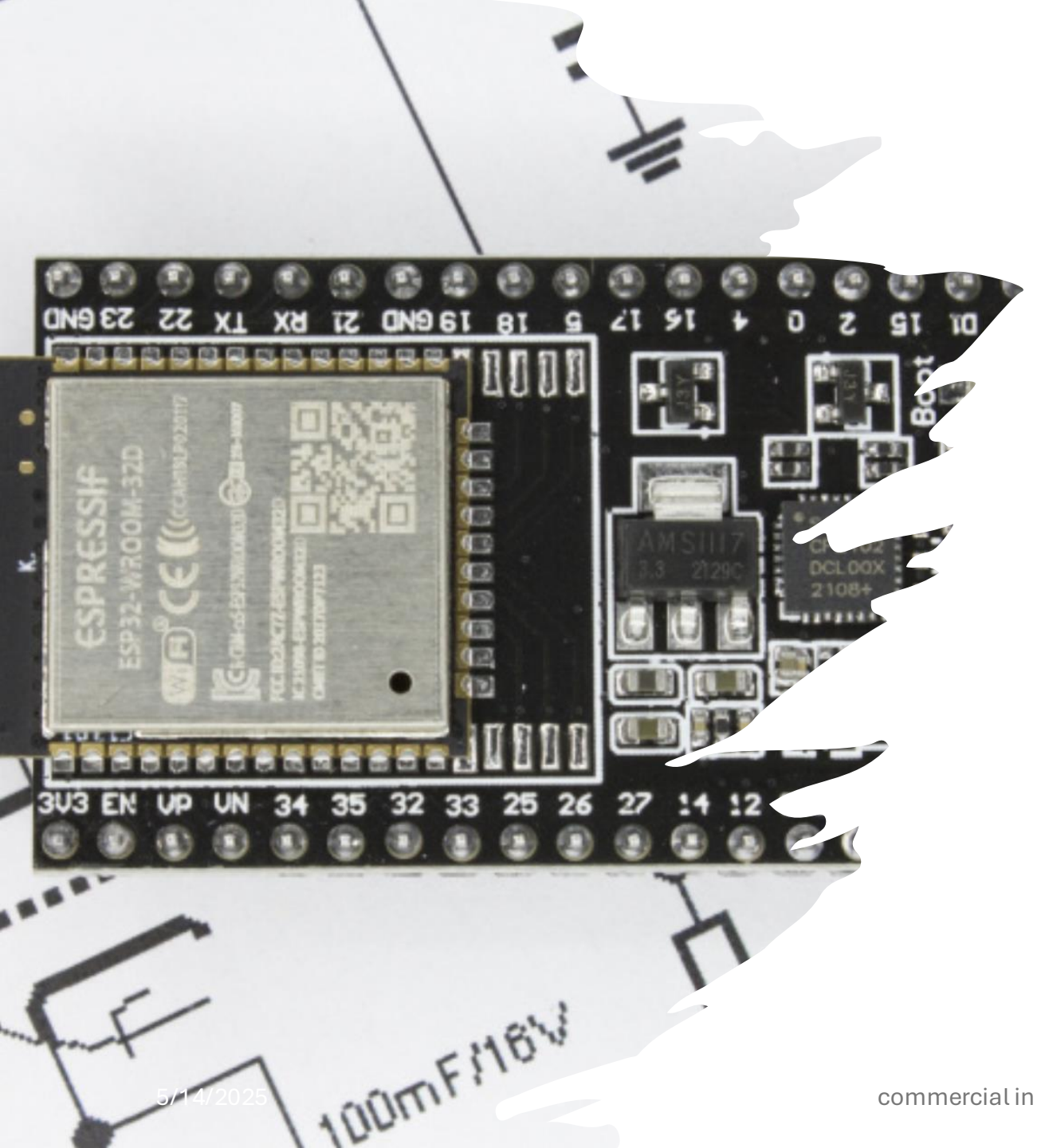
Sensors &
MEMS

Imagers

Distributed

Semiconductor Supply Stages

Apple Suppliers 2024



Risks

Hidden Backdoor in IoT Chip (ESP32, 2025)

- Tarlogic researchers revealed an undocumented feature in the popular ESP32 Wi-Fi/Bluetooth microcontroller that acts as a potential backdoor.
- This low-cost chip (over 1 billion units sold) was found to have hidden commands allowing arbitrary memory writes and device impersonation.
- An attacker exploiting these commands could inject malicious code and permanently infect millions of IoT devices, bypassing normal code audits.
- Such a vulnerability could facilitate large-scale supply chain attacks or covertly insert backdoors into countless gadgets, posing a widespread security risk.

Risks

Counterfeit Cisco Hardware in Critical Systems (2024)

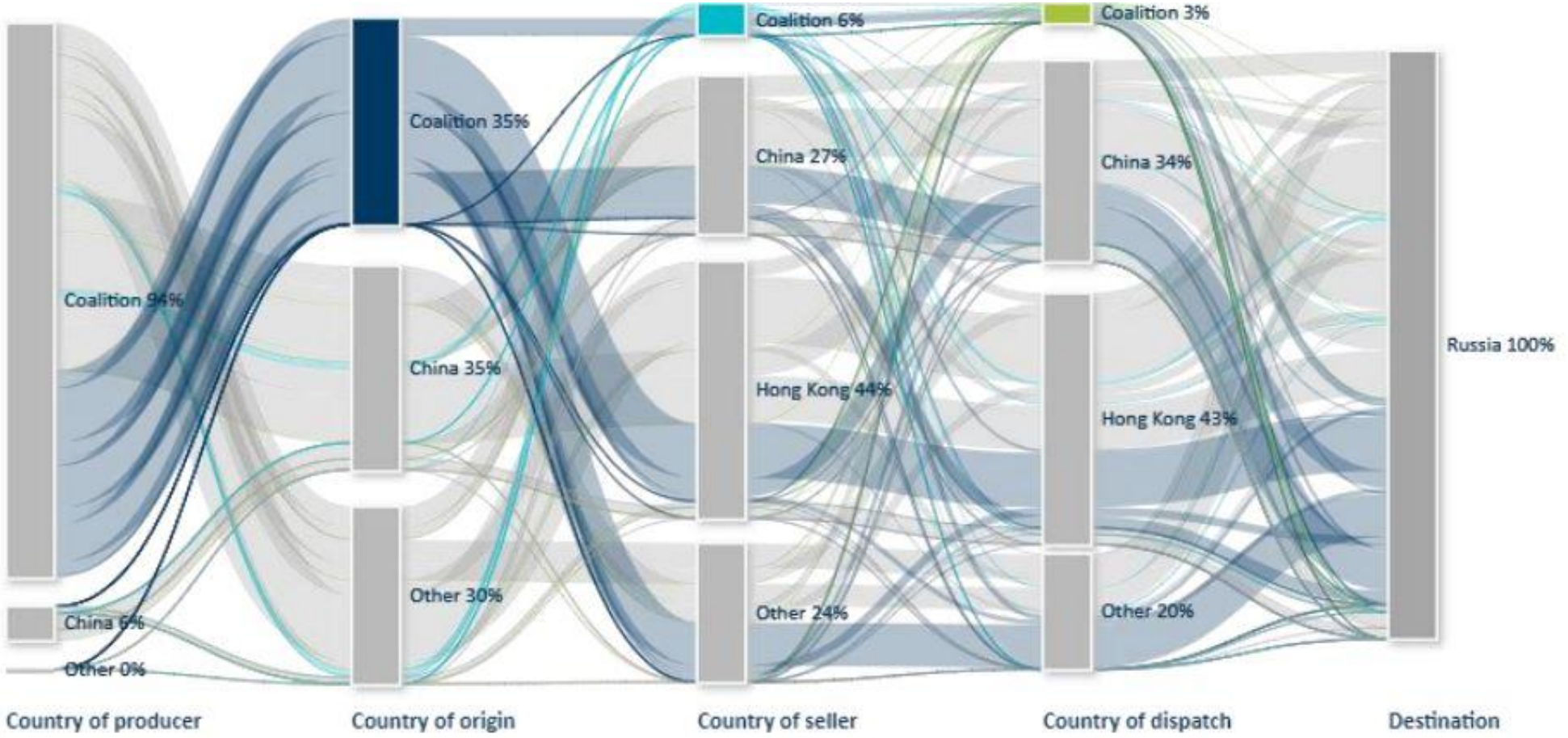
- A massive scheme was uncovered in which tens of thousands of fake Cisco networking devices from China were sold into the U.S. supply chain.
- These counterfeit routers and switches ended up in hospitals, schools, and even military networks – including systems supporting U.S. fighter jets and other defense platforms.
- The substandard gear often failed or had hidden flaws, compromising national security and safety.
- This case (one of the largest ever prosecuted) underscores how lacking traceability enables adversaries to flood supply lines with illegitimate hardware, a threat that rigorous provenance checks could have mitigated.

Risks

Chinese “Spy Chip” in Weather Station (2023)

- South Korea’s intelligence agency discovered malicious microchips embedded in Chinese-made weather monitoring instruments used by a government agency.
- Dubbed a “spy chip,” the hardware backdoor was found hidden in the devices’ circuitry – marking the first such case in Korean equipment.
- The chip’s malicious code could enable remote espionage (stealing technical data or eavesdropping on communications), all under the guise of a normal sensor.
- The discovery prompted an audit of over 10,000 Chinese-supplied devices in government use, illustrating how adversarial implants in the microelectronics supply chain can directly threaten geopolitical and security interests.

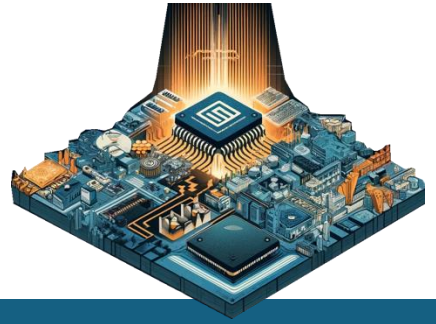
Serious Traceability Challenges Today



Source:
KSE Institute

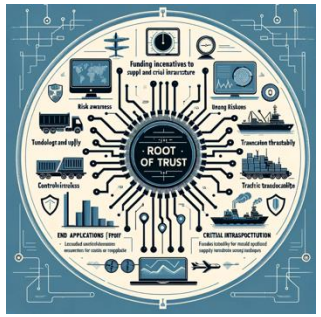
[US Senator urges chipmakers to help keep their chips out of Russian weapons]

Problems Must be Addressed



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....

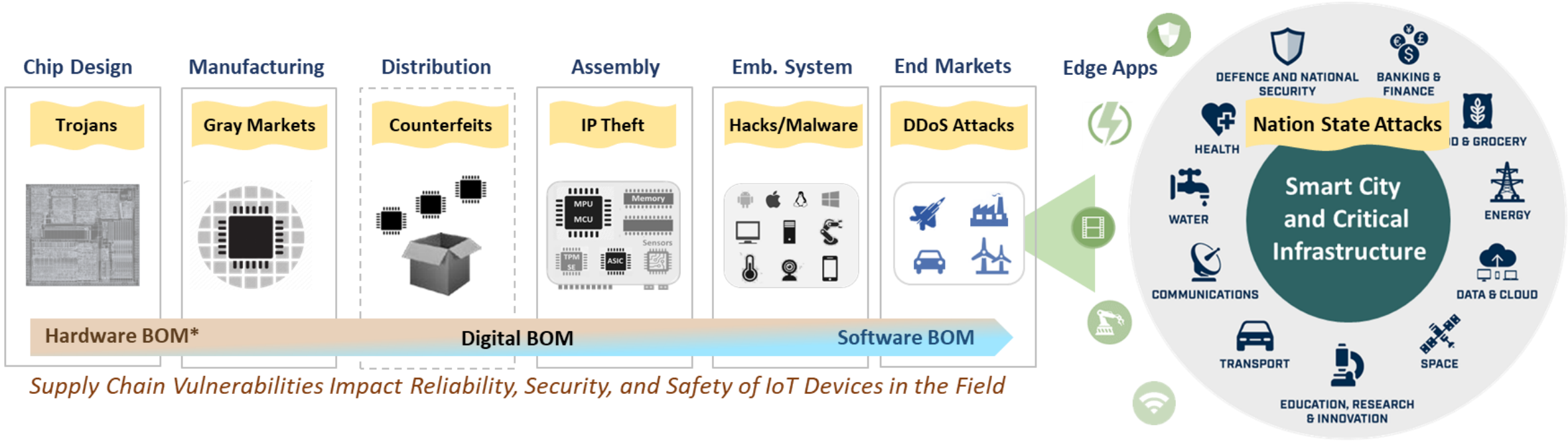
Secure Supply Chain Attributes

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

Importance of US-EU Initiative on Traceability

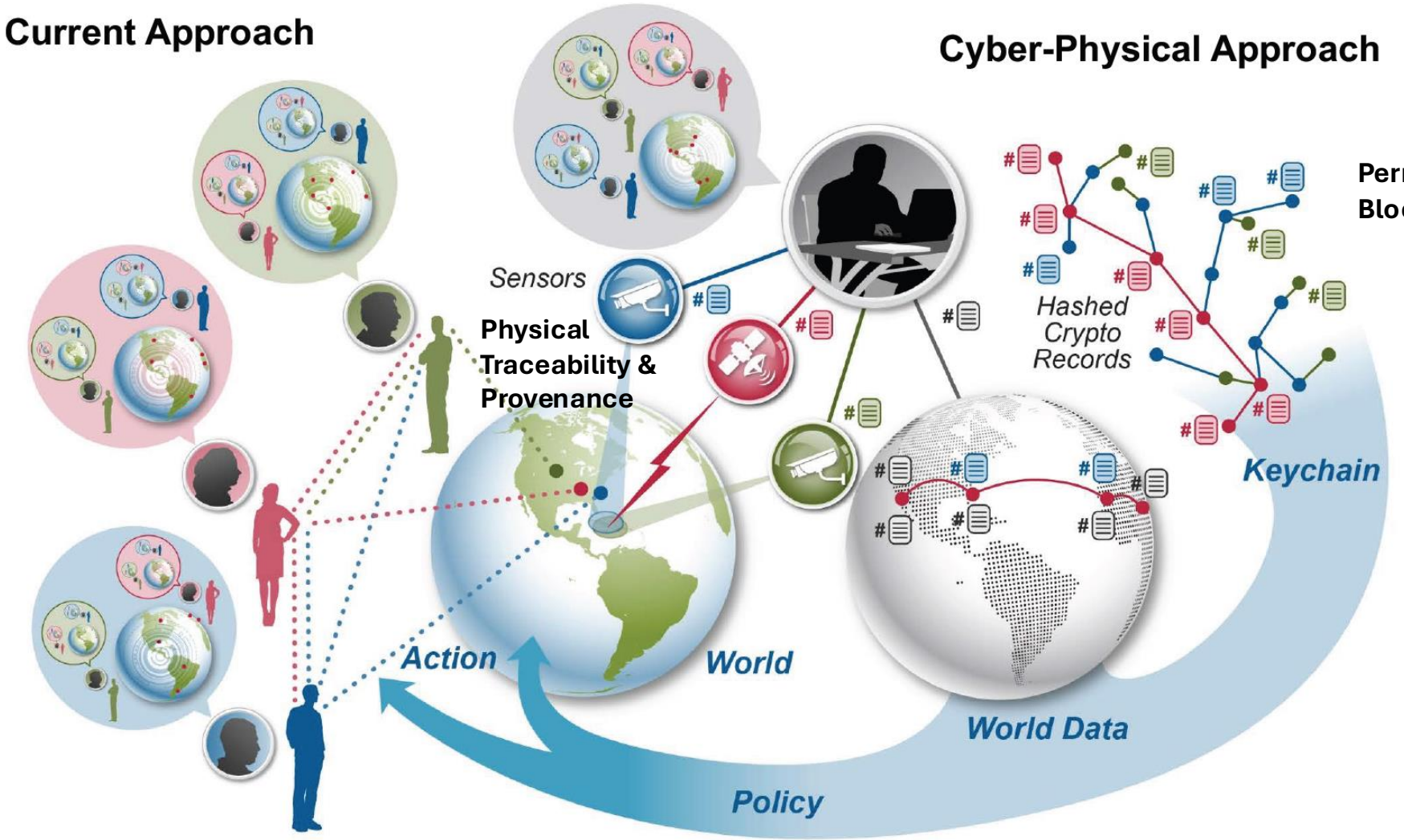


Supply Chain Vulnerabilities Impact Reliability, Security, and Safety of IoT Devices in the Field

- 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

Modern Supply Chain Assurance

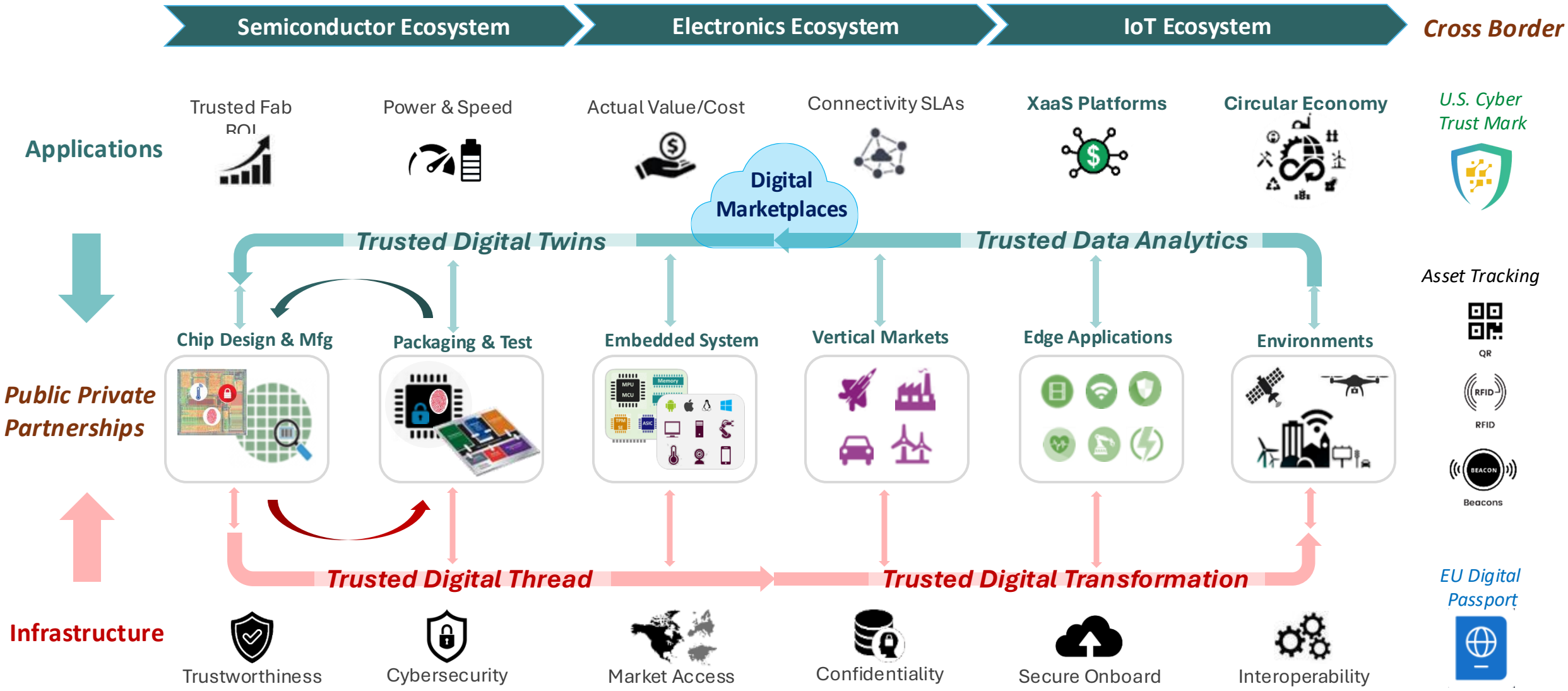


$$T = \sum \frac{A_m}{M_m}$$

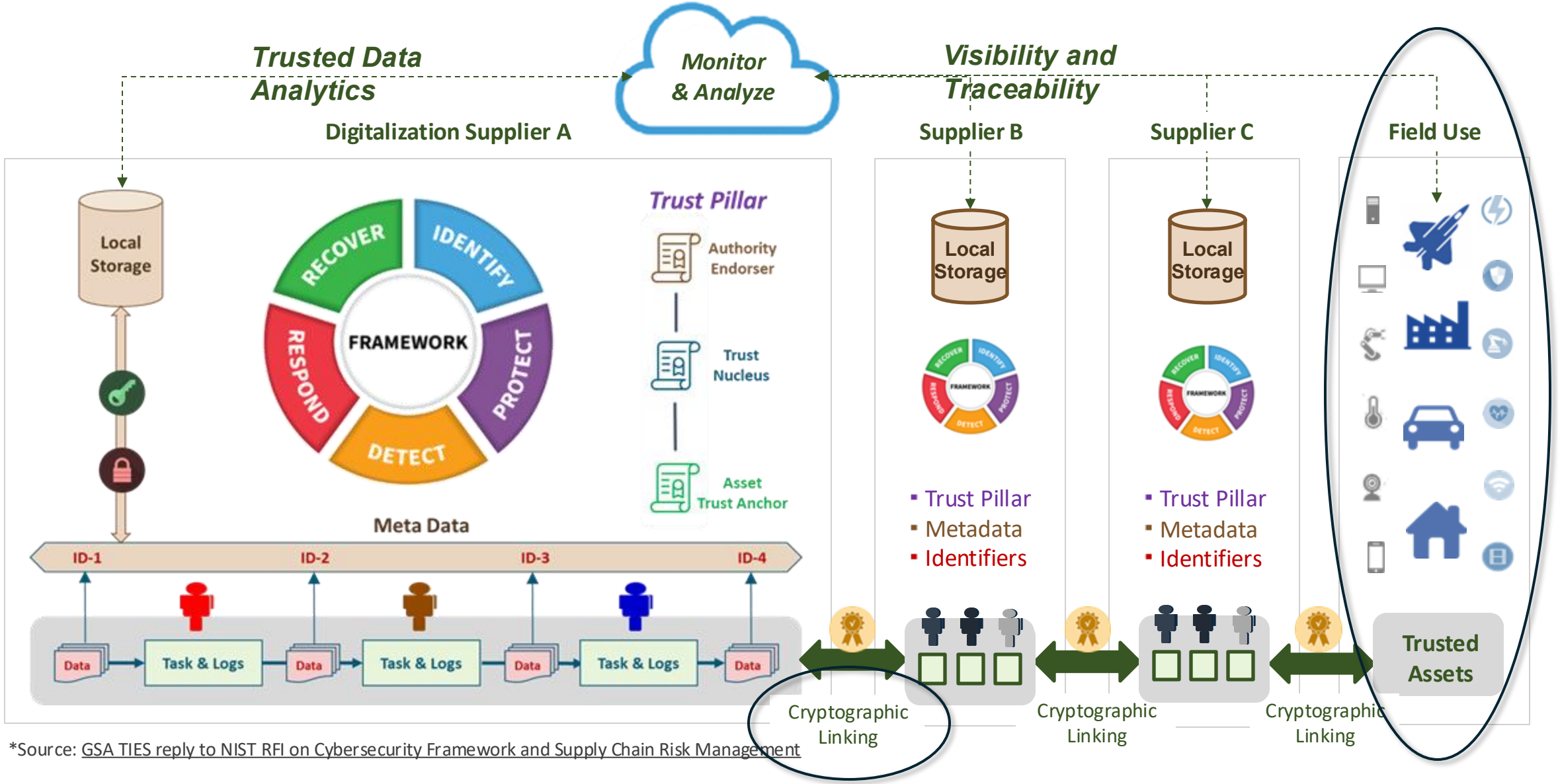
Industry and consumers adopt and USG values traceability and supply chain assurance

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

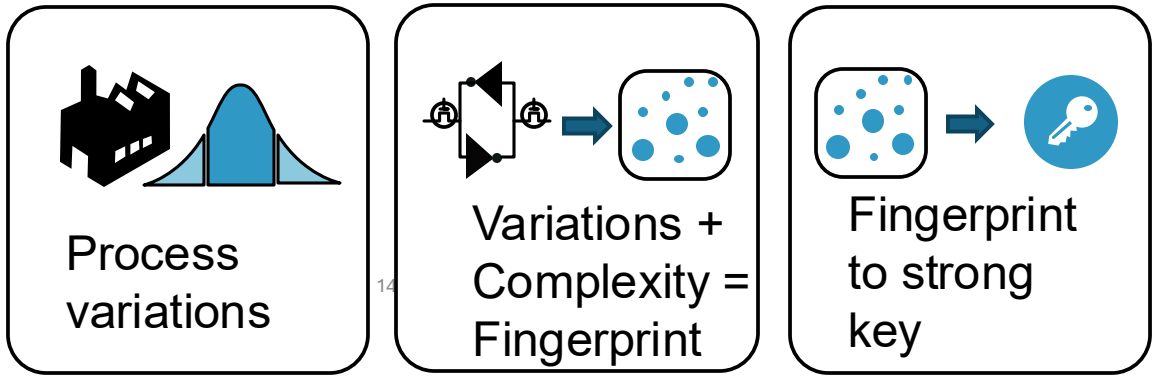
Physical Traceability & Supply Chain

- **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

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

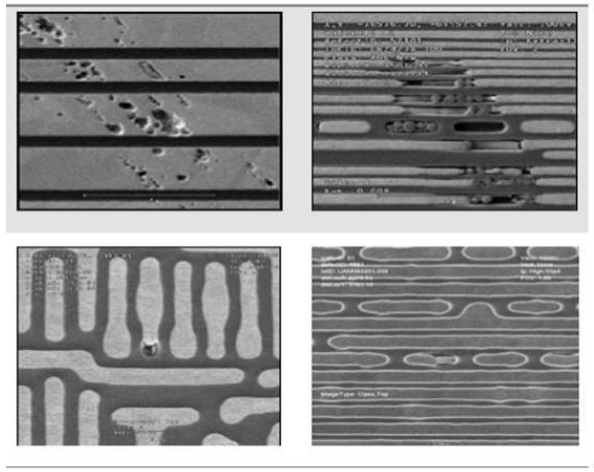
- Foundries offer IP compliance services to major IP providers
- IP compliance can be extended by “deep hash” to soft IP and customers IP
- IP Assurance as a service can identify vulnerabilities before fab

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

Examples of Intrinsic Process Variation

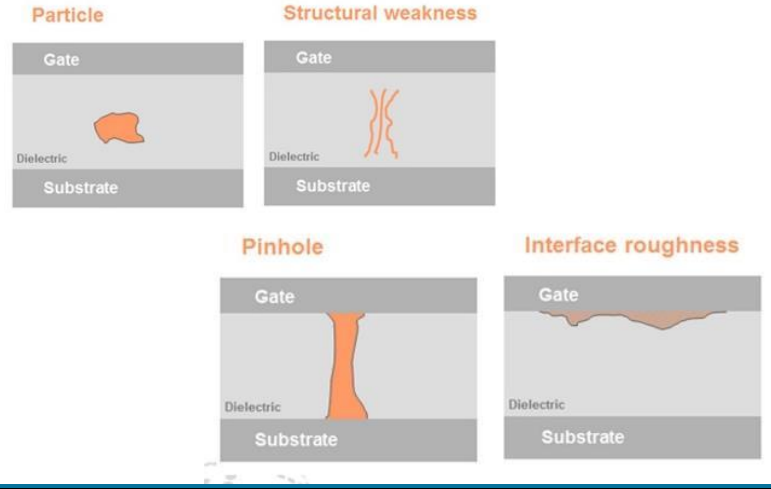
Metals

- Grain variations on small feature sizes
- Lithographic variations



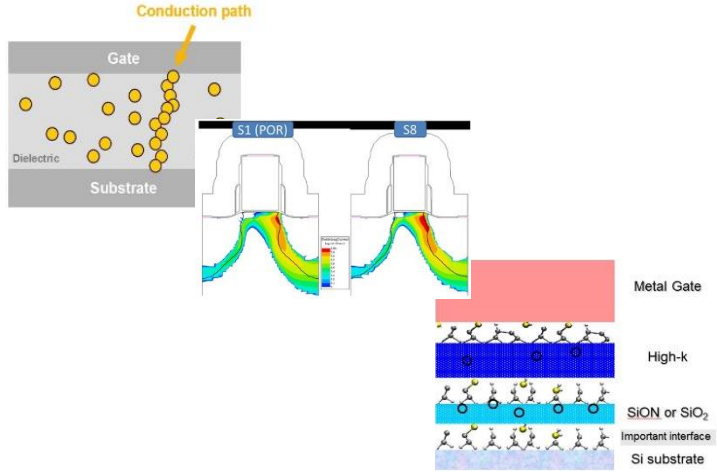
Oxides

- Oxides thickness variation
- Gate Oxide variations cause performance changes



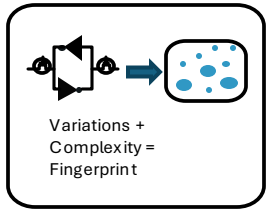
Transistors

- 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

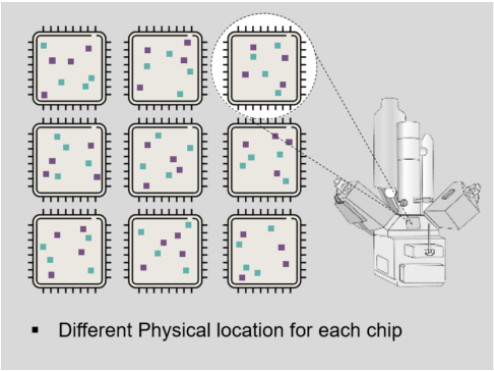
Programmable

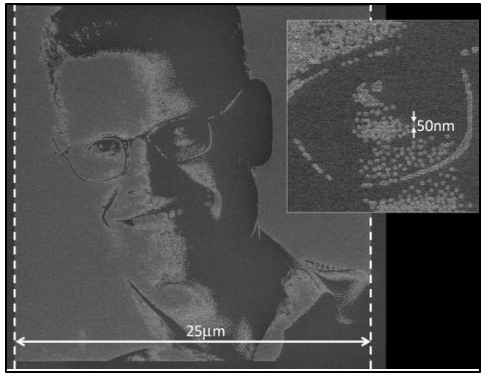
- One-time programmable (OTP) memory allows for unique state or electrically read labels
- Embedded nonvolatile memory (eNVM) elements that are programmable and stable in state of operation can be leveraged for uniqueness

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

Optical image of the fs-laser micro-marking





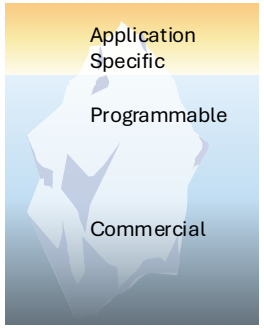
Extrinsic variation can increase ability to uniquely mark die and hash other data into the physical part

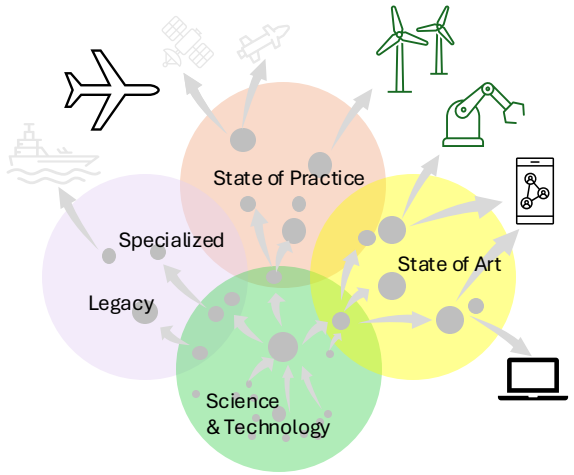
IP Compliance Example

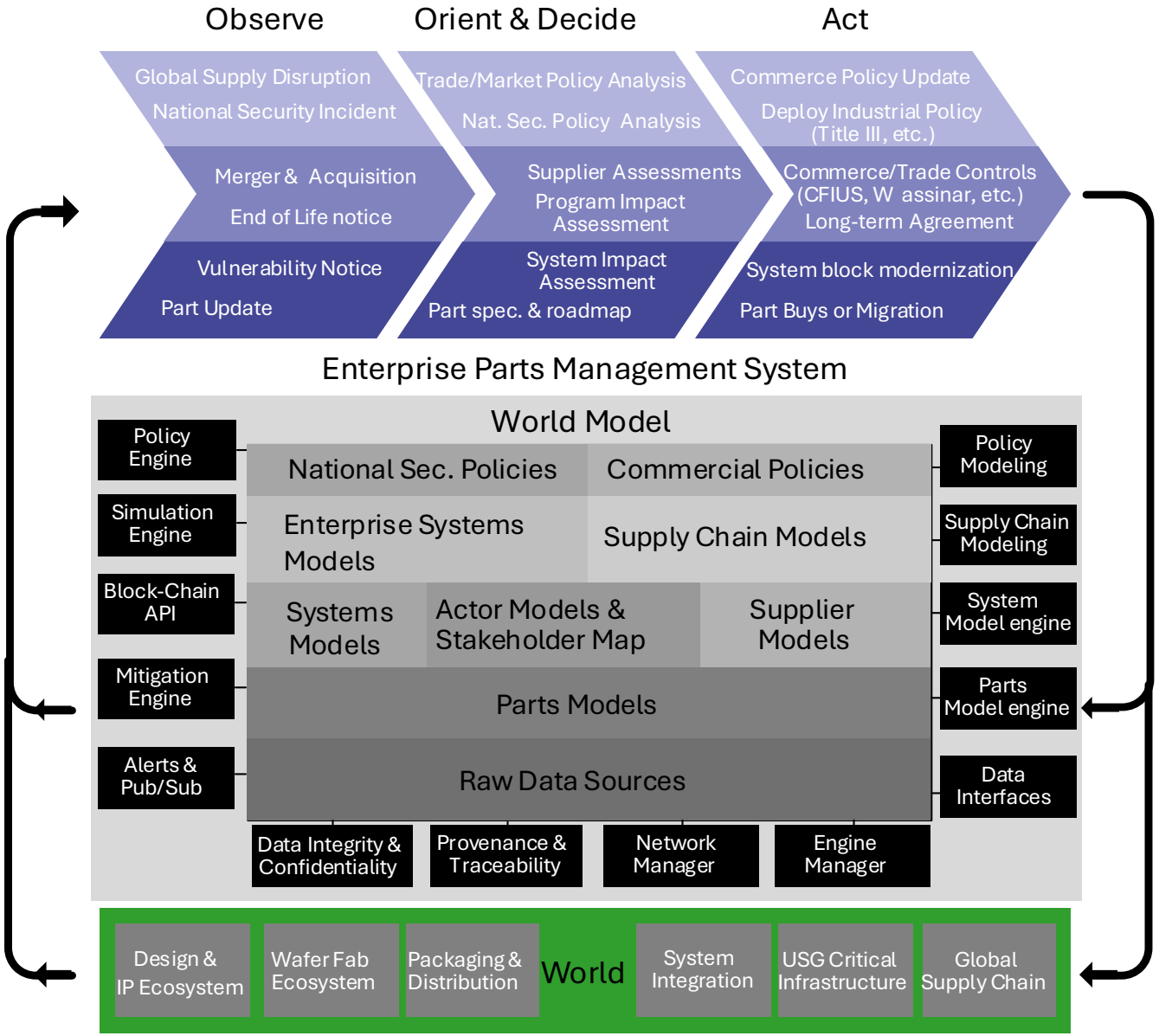
- Start with 5 at-scale Foundries (must give them GDS to get chips)
  - Offer IP compliance as a service
    - Black Box IP (already scanned and replaced by foundry)
    - 3rd Party Soft IP – perform “deep hash” of various forms (DGS, schematic, etc.) and compare to reference and deliver a certificate
    - Customer IP – perform deep has and allow customer to obtain IP compliance certificate if IP shows up again (show you didn’t steal it)
  - Assurance as a service – identify common IP blocks to facilitate a BOM and offer mitigation services for known vulnerabilities before committing to high volume production
  - Certificate and Identity injection into the chip
    - Include IP compliance provenance and identity into certificate embedded into RoT & database
    - Include select foundry provenance
    - Physical injection of identity and hash of certificate for chips that cannot support full RoT
- Expand backward to the design environment and forward to packaging, board
  - Opportunity to include rich design information, test and verification, non-repudiation, etc.
  - Leverage a cryptographic link to board level and sub-system level ID and roots of trust

Architecture for Enterprise Management

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





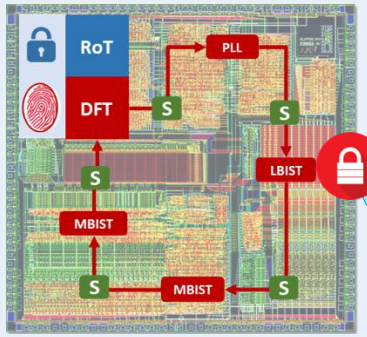


Ecosystem Participants

- **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 market preferences and standards, ensuring that all chips meet assurance standards.
  - **End-Users**: Verify the traceability of chips received and ensure they are used in compliance with assured systems.
- **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.

Business Use Case Examples

Automotive - Silicon Lifecycle Management (SLM)

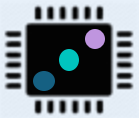


Functional Safety

Fleet Monitoring

*Source: Semiconductor Eng

Industrial - Chip Licensing & Multi Market Product



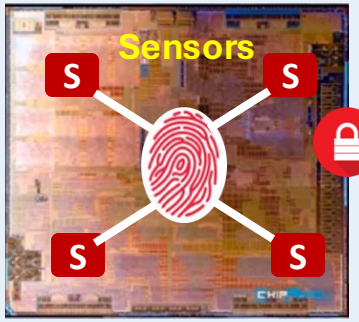
- Ethernet
- Profinet
- BACnet

HW + SW Provisioning

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

Global Chip ID

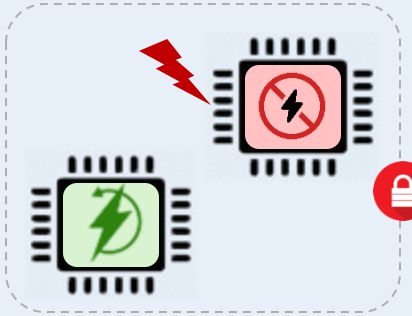
Aerospace & Defense - Manufacturing Integrity



Failure Prevention

Source: ERI Summit 2020

Supply Chain - Monitoring & Regulating Field Use



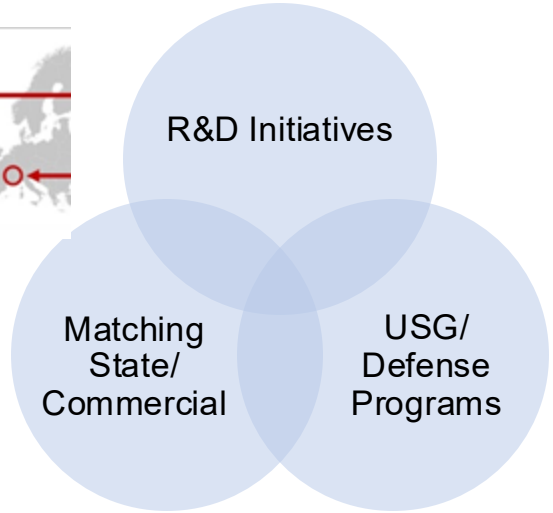
Disable Adversary

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

Assurance USG/Industry Opportunities

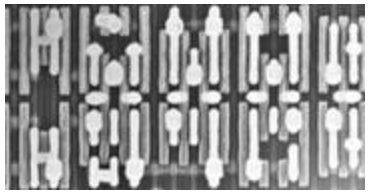
Dual Use Roadmap

- 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

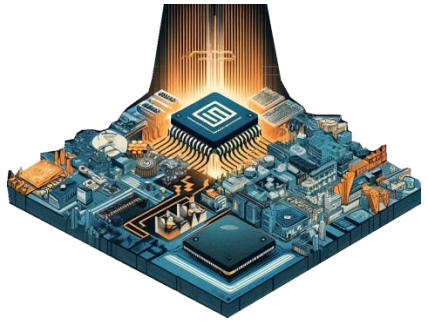
Acquisition/R&D Policy

- 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

COMMONS
MICROELECTRONICS COMMONS
BRIDGING THE GAP FROM LAB TO FAB

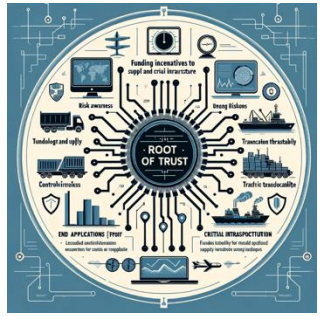
Global Traceability Initiative

- **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.



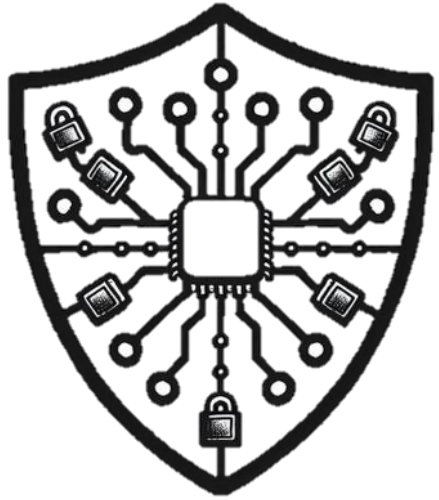
- **Strategic Alignment:** Closely aligned with the U.S. CHIPS Act, EU CHIPS Act, and U.S.-EU Trade and Technology Council. The initiative enhances economic resilience, prevents adversarial threats, and secures global infrastructure.

- **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.



The STAMP Team Leads

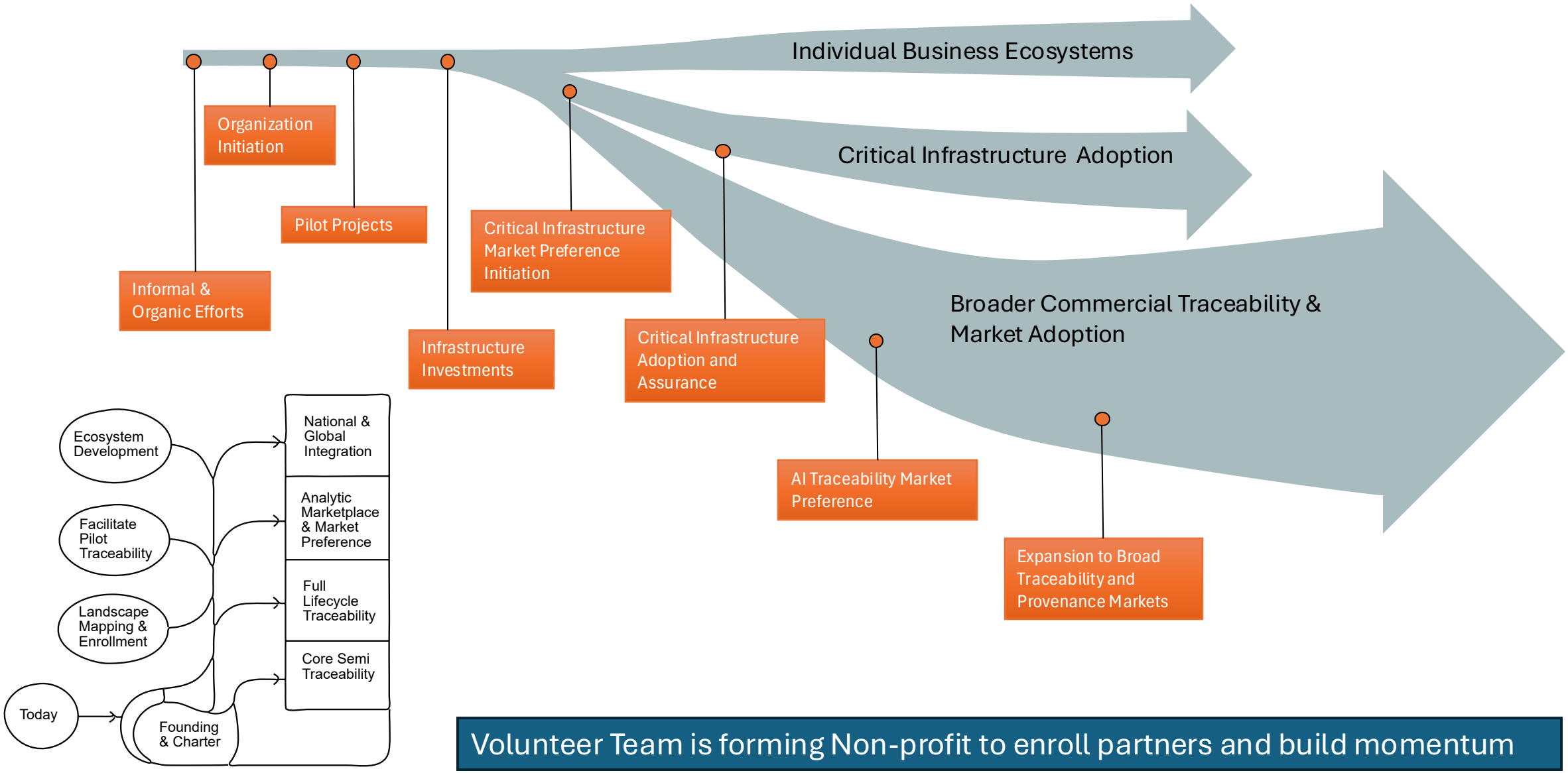
- Team of Volunteers from EU and US has formed to drive the Semiconductor Traceability and Market Provenance (STAMP) initiative, promote workshops and panels, and gather support and funding for pilots
  - Team Europe
    - Eduard Hoeberichts, MA & MBA - ex Div President ASML, Founder SandGrain, CEO FabMax
    - 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
- 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, NIST workshop in April

STAMP Future Timeline & Milestones



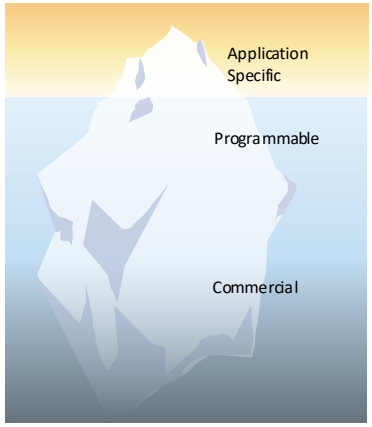
Volunteer Team is forming Non-profit to enroll partners and build momentum

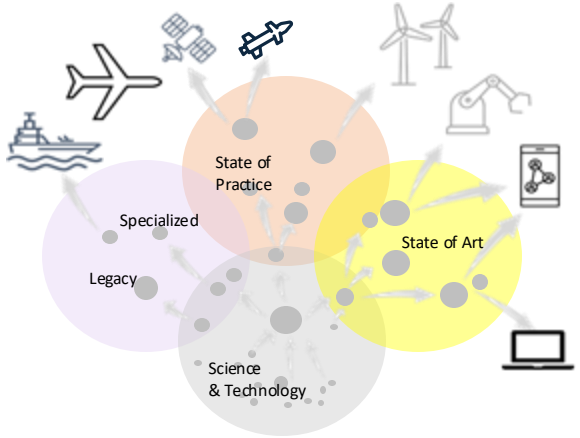
Upcoming Opportunities

- NIST NCCoE will host key US industry stakeholders (hyper-scalers & end users) for a workshop in the late summer 2025

Backup

Microelectronic Supply Chain 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

Traceability and market preferences can fortify ME Demand for Supply Chain Security