

Status of Standards for Microelectronics Assurance & Traceability

February 2024



Bottom Line Up Front

Current State:

Issues/Challenges/Security concerns

- Huge risk of supply disruption
- No market preference for assured supply¹
- Insufficient funding for infrastructure, standards, and process development

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

Desired State

- Significant increase in 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 and provenance of assured supply

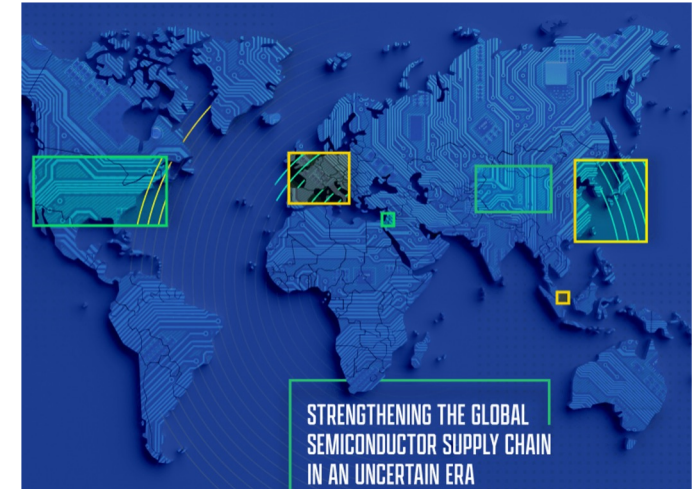
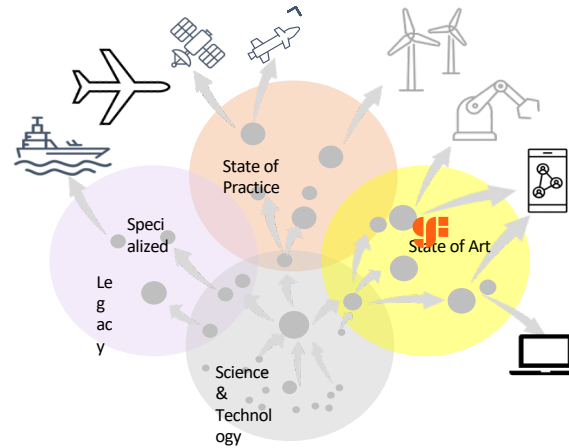
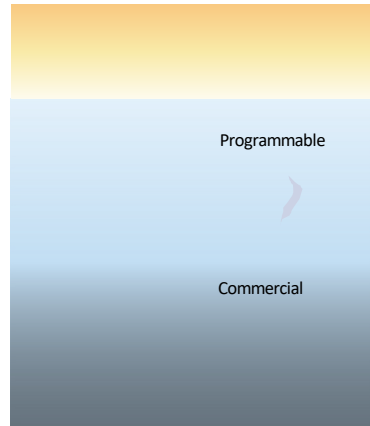
What's needed:

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

Next Steps (TBD):

- Support and fund engagement in standards activity
- Build funding program and RFS for traceability and provenance of assured ME supply in targeted pilots
- Policy focused to build market preference to assured supply for critical infrastructure

Our View of Microelectronic Needs



Commercial Foundation

- **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 foundries**
- 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

Elements Needed for Market Adoption



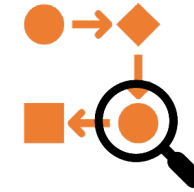
Policy and Market Behavior

- **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

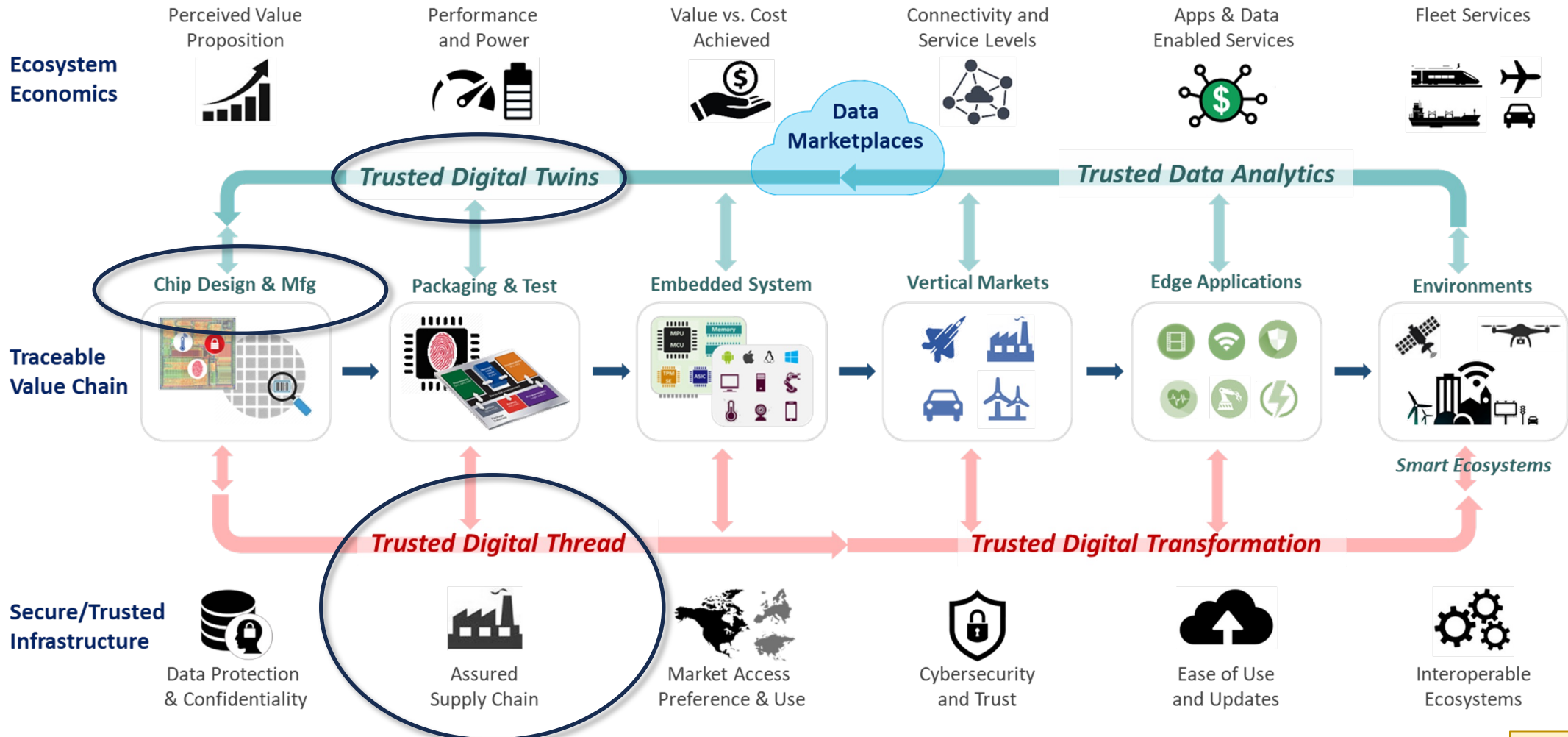


Physical Traceability & Supply Chain

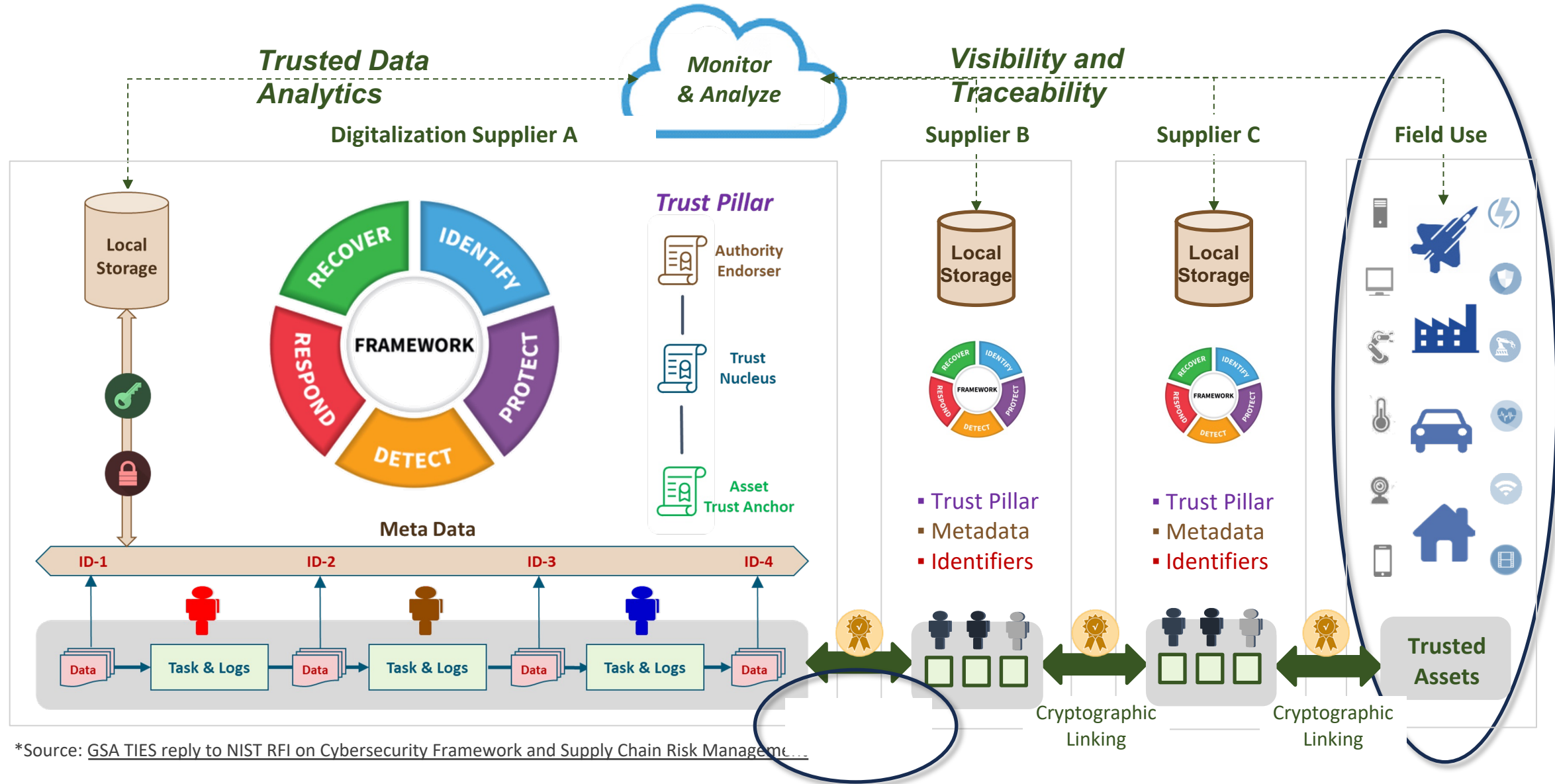
- **Implement immutable physical traceability** and validation infrastructure industry-wide
- **Standardize and validate root of trust** and hardware as a service to deliver differentiated technology through assured supply chain
- **Promote consumer level traceability tools** and marketplace

Assurance & Preferred Supply through Provenance & Traceability

Semiconductor Ecosystem - US + EU CHIPS Acts Electronics Ecosystem - Cybersecurity Labeling IoT Edge Ecosystem - DIGIT Act for IoT



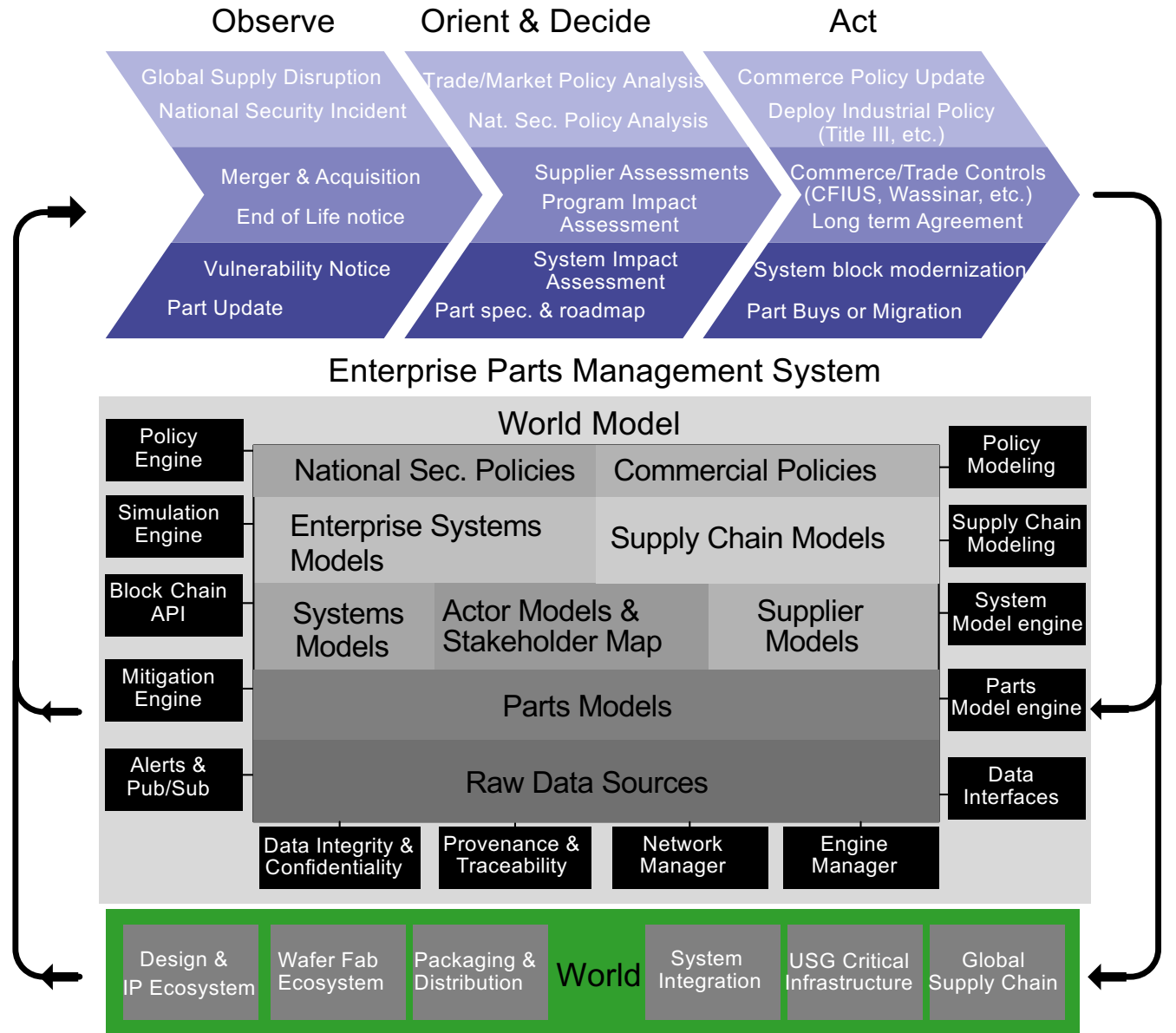
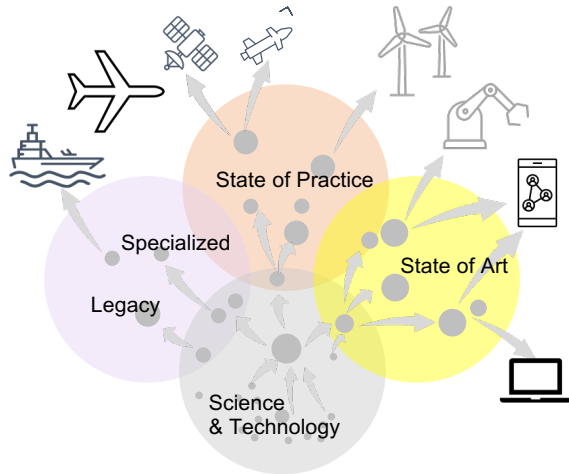
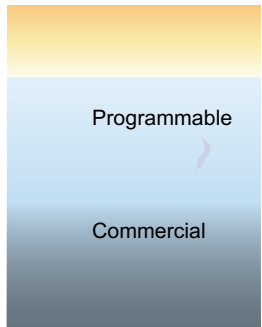
Digitalization of Value Chain Enables Data Marketplaces



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

Architecture Overview for EEPMS

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



Status of Standards Activity

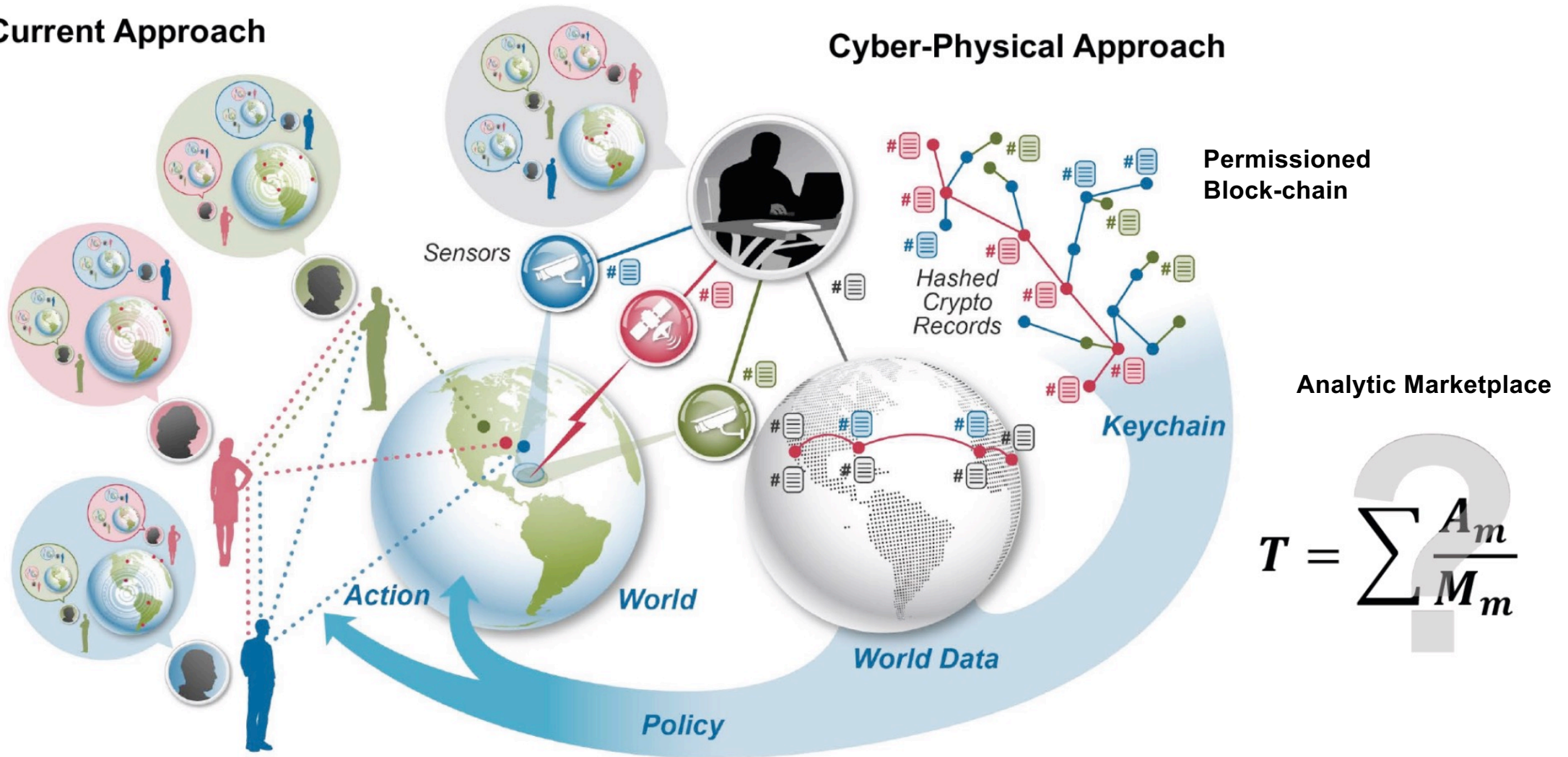
	PPP/CPI	Design	Verify	Mask	Fabrication	Packaging & Test	V&V	Config & SW	Distribution	Integrate & Test	Operations & Maintenance	
Cyber Physical Systems Security	JA7496 - Cyber-Physical Systems Security Engineering Plan ¹											Published
	Note - Rev. A in progress											
	¹ References 100's of cross-sector standards not uniformly adopted and used											
	JA7496 Compliance Standard or Guide (includes Audit Checklist)											
SwA	JA6678 - Cyber Physical Systems Security Software Assurance											In Development
	JA6678 Compliance Standard or Guide (includes Audit Checklist)											
									JA6678/1 Config & SW/Integration SwA Standard			
HwA	JA6678/1 Compliance Standard or Guide (includes Audit Checklist)											Gap (Proposed)
	JA6801 - Cyber Physical Systems Security Hardware Assurance											
											IPC-1791 Trusted Electronic Designer, Fabricator, and Assembler Requirements	
Traceability	IPC-1791 Certification Scheme offered by IPC											Published
	Design & Verify Standard for Traceability								IPC-1782 - Standard for Manufacturing / Supply Chain Traceability of Electronic Products			
	Note - Supply chain elements in revision (currently in ballot)											
	IPC-1782 Compliance Standard or Guide (includes Audit Checklist)											
	SEMI E142 Specificatin for Substrate Mapping											
						SEMI 6504 - Specification for External Device Traceability						
SEMI 6504 Compliance Standard or Guide (includes Audit Checklist)												
Counterfeit Avoidance & Detection	IPC-1783 - International Standard for Component-Level Authentication											Published
	IPC-1783 Compliance Standard or Guide (includes Audit Checklist)											
	Anti-Counterfeit (premetive controls) for Design & Verify			JESD243 - COUNTERFEIT ELECTRONIC PARTS: NON-PROLIFERATION FOR MANUFACTURERS			Anti-Counterfeit Mechanisms for Packaging		AS6171 - Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts and specific test method slash sheets		AS6496 Fraudulent/Counterfeit Electronic Parts... Authorized/Franchised Distribution	
AS6174 - Counterfeit											Published	
Distributors												

Significant Gaps in Early Design and Manufacturing of ME Hardware and Supply Chain

Modern Supply Chain Security

Current Approach

Cyber-Physical Approach



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

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

Next Steps/Recommendations

- **Promote standards** - Accelerate and support standards for Microelectronics Assurance, Provenance, and Traceability
- **Inclusion of funding for standards participation and development** - Support development of technology to deliver Assurance, Provenance, and Traceability along with requirements and funding for standards participation of the stakeholders
- **Robust funding for pilot** - Encourage industry and government to robustly implement and require market preference for Assurance, Provenance, and Traceability