



KGx – Known Good x

September 7, 2022

Today's Presenters



Tom Katsioulas
GSA Global



Marc Hutner
ProteanTecs



Jay Rathert
KLA

Technical Program Committee (TPC)



Abram Detofsky
Intel



Neal Edwards
AMD



Zoe Conroy
Cisco



Dave Armstrong
Advantest



Ira Feldman
Feldman Engineering

Support MEPTEC

Membership and sponsorship enable MEPTEC to produce events and publications with the highest quality technical content relevant to the packaging, test, and design communities.

Membership

- Registration discounts
- MEPTEC Report subscription

Join/renew at www.meptec.org

Sponsorship

Multiple levels of corporate sponsorships are available for virtual and upcoming in-person events.

Questions about joining or sponsoring?

Please contact Bette Cooper bcooper@meptec.org

Trusted IoT Ecosystem Security (TIES)

*Component-based supply chain provenance,
traceability and digital thread of test data*

Tom Katsioulas

Board Chair, GSA TIES

Email: tomkat@gsaglobal.org



September 2022



GSA TIES Motivation

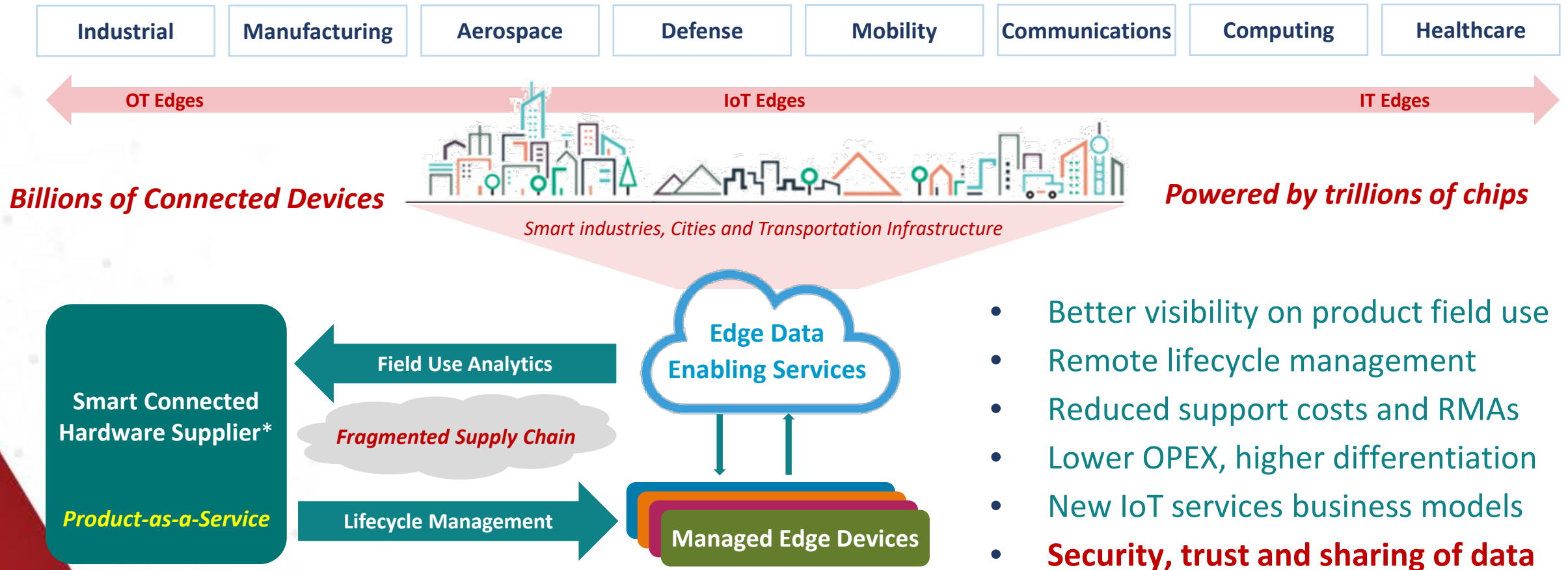
- **IoT, 5G, Cloud Computing, and AI will create \$20 trillion* for the global economy**
 - Attacker sophistication outpacing defender capabilities can cost over \$3 trillion
 - Geopolitical and supply chain issues require a holistic view to security & trust
- **Lack of visibility of electronics parts in the supply chain creates major risks**
 - Disaggregation of the value chain, unregulated distribution channels, organization silos
 - Supply chain traceability of ICs and test data is key for the quality, reliability and security
- **GSA TIES focuses on an ecosystem strategy to incentivize supply chain traceability**
 - 300+ GSA members in semiconductors, devices, systems, software and applications
 - Leverage ecosystem IQ to drive a digital thread for trusted electronics and digital twins

Enable value-creating interactions with a platform-based business ecosystem

Mission, Goals and Objectives

- **Mission** - Develop collaborative ecosystem for end-to-end solutions for the IoT value chain
 - Consists of EDA, IP, IC, Foundry, OSAT, OEM, EMS, CSPs, PLM, and Software vendors
 - Focus on promoting use cases and **end-to-end solutions** that reduce risk and maximize value
- **Goal** - Drive a shared success model toward secure & trusted Digitalization* solutions
 - Accelerate adoption, growth and use of **connected chips, devices, systems and edge apps**
 - Enable new services revenue streams and scalable business models for the IoT value chain
- **Objective** - Grow a business ecosystem where stakeholders add value in a standardized way
 - Establish governance to leverage the collective **Ecosystem IQ** and maximize network effects
 - Promote a **“shift left”** from the end application to chips to accelerate monetizable solutions
- **Value** - Accelerate transformation of the value chain with secure & trusted IoT suppliers
 - Network to pursue shared interests, harmonize silos and achieve economies of scale for IoT
 - **Partner outside of GSA** to pursue joint solutions & services and accelerate IoT adoption

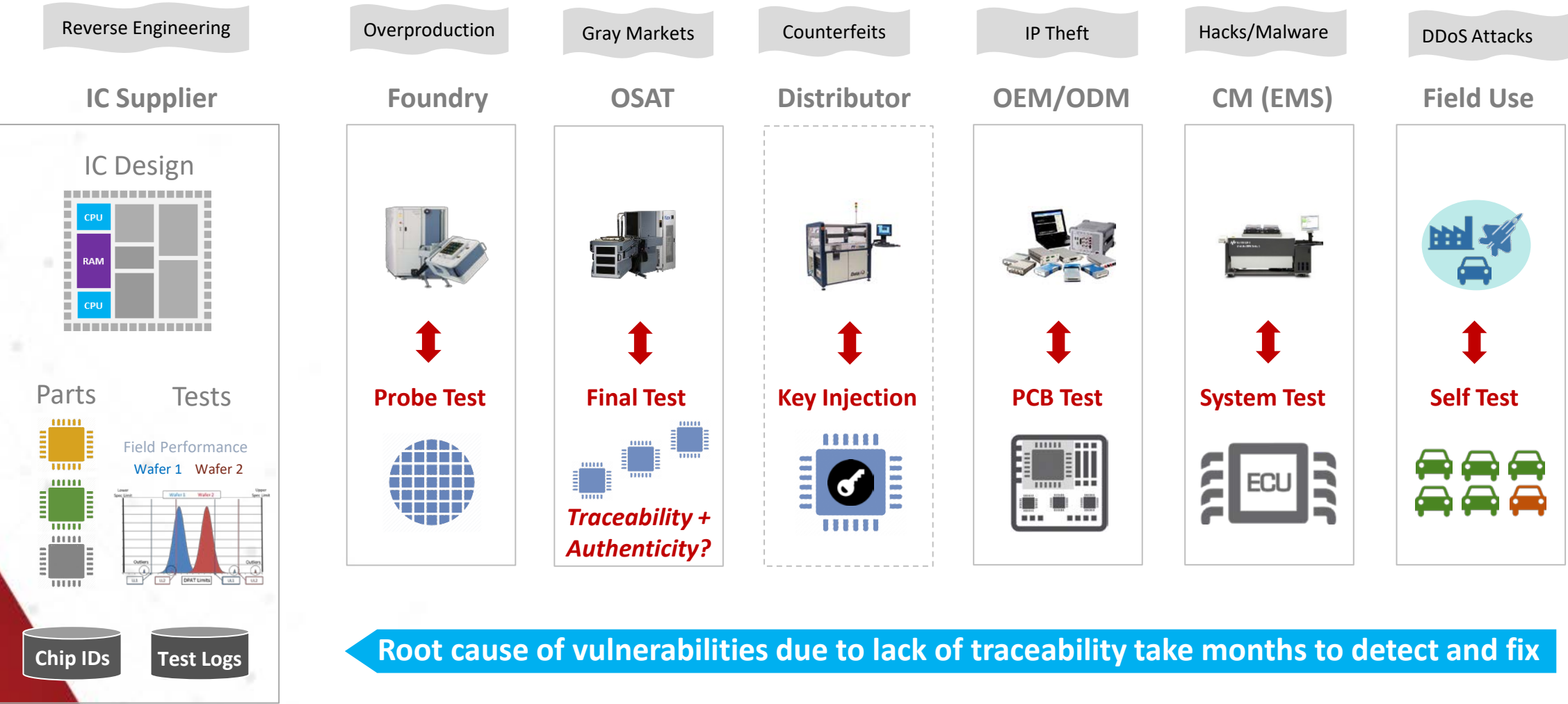
Secure-Connected Product Supplier Economics



*Sources: HBR, HPE

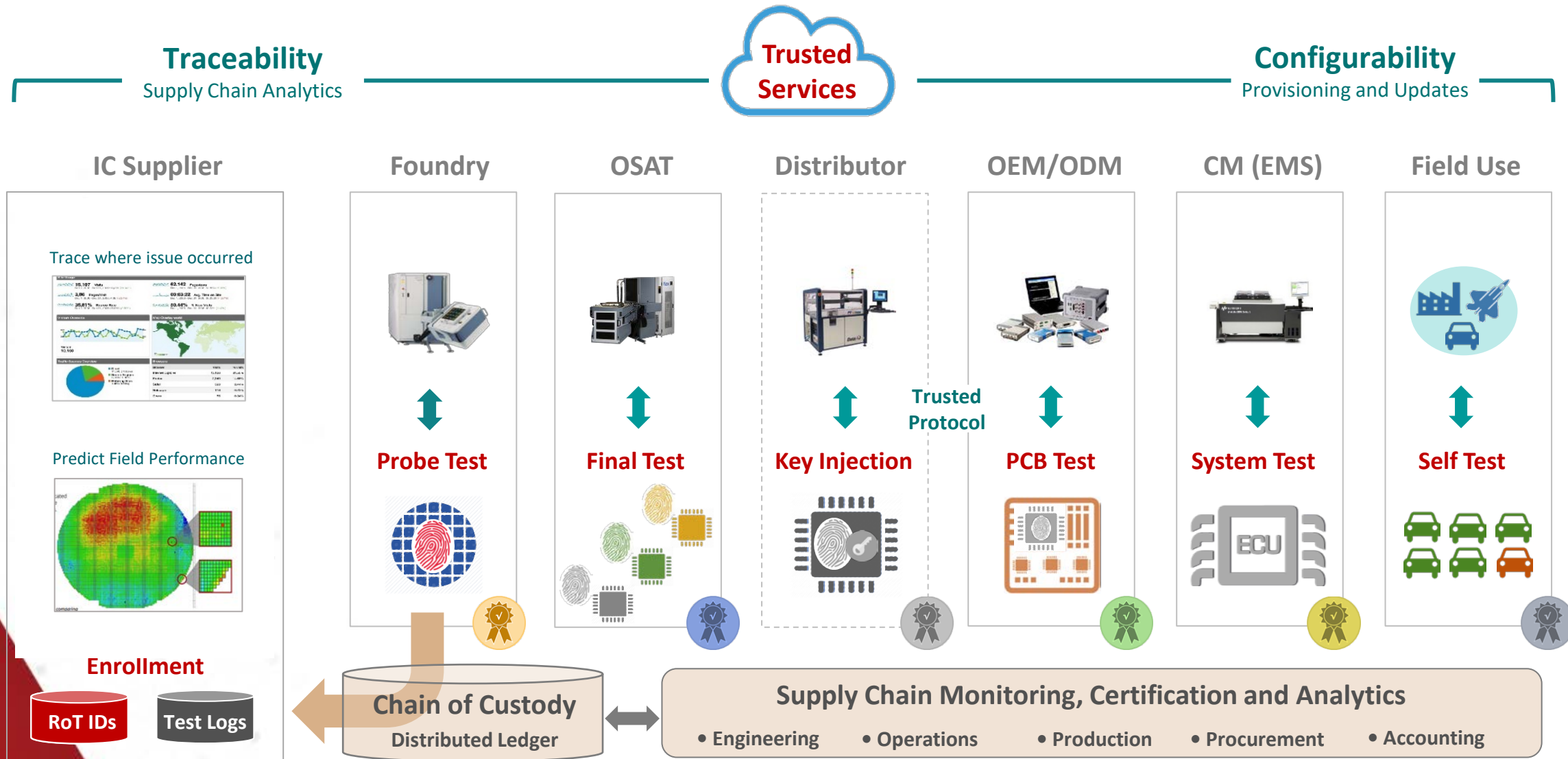
How to evolve trusted traceability solutions with data to enable economic value?

Use Case - Supply Chain Quality, Security and Trust Issues



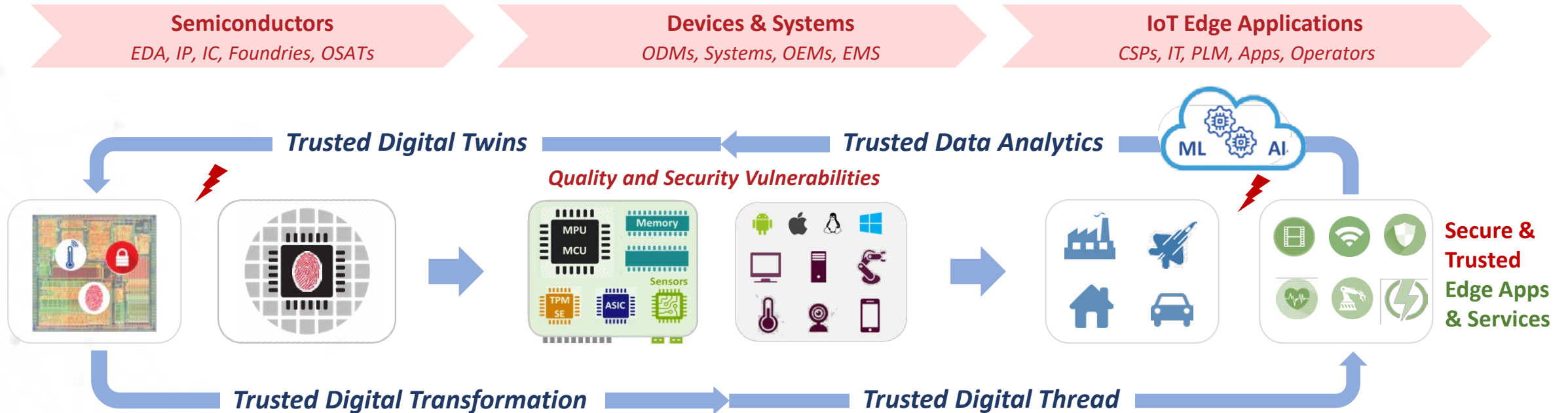
Root cause of vulnerabilities due to lack of traceability take months to detect and fix

End-to-End Vision - Trusted Supply Chain Traceability



TIES - Platform Based Business Ecosystem

*Source: <https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/>



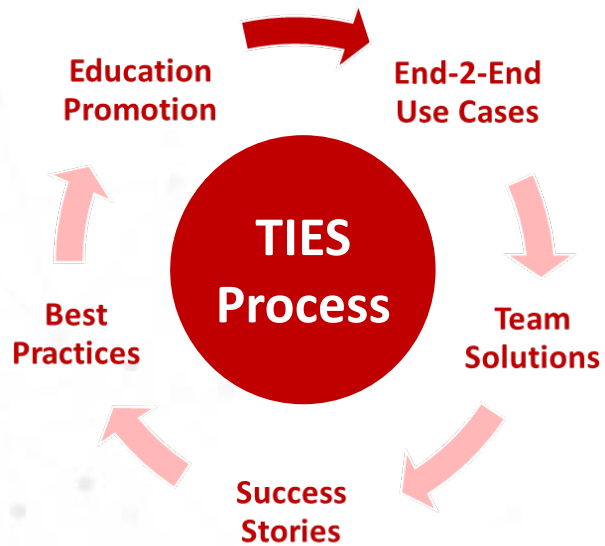
GSA Collaborative Platform

- Global Brand with [300+ Members](#)
- Industry Leading [Board of Directors](#)
- Over 75% of \$550 Billion Industry

TIES Connected Value Creation*

- **Architecture** - Open and Participatory
- **Governance** - Rules for Shared Success
- **Interactions** - Network Effects Broaden IQ

Use Case Driven Operating Model



Content Categories
Hardware Design Security
Trusted Supply Chain
Vulnerability & Trust Metrics
Embedded System Security
Security Infrastructure
Edge, ML, AIoT Applications
Trusted Digital Twins
New XaaS Business Models

Content Type
White Papers*
Presentations
Webinars
PoC Demonstrators
Security News Letters
Standards Taxonomies
Best Practices Guides
Liaison ORG Synergies

*Basis to start networking & collaborate

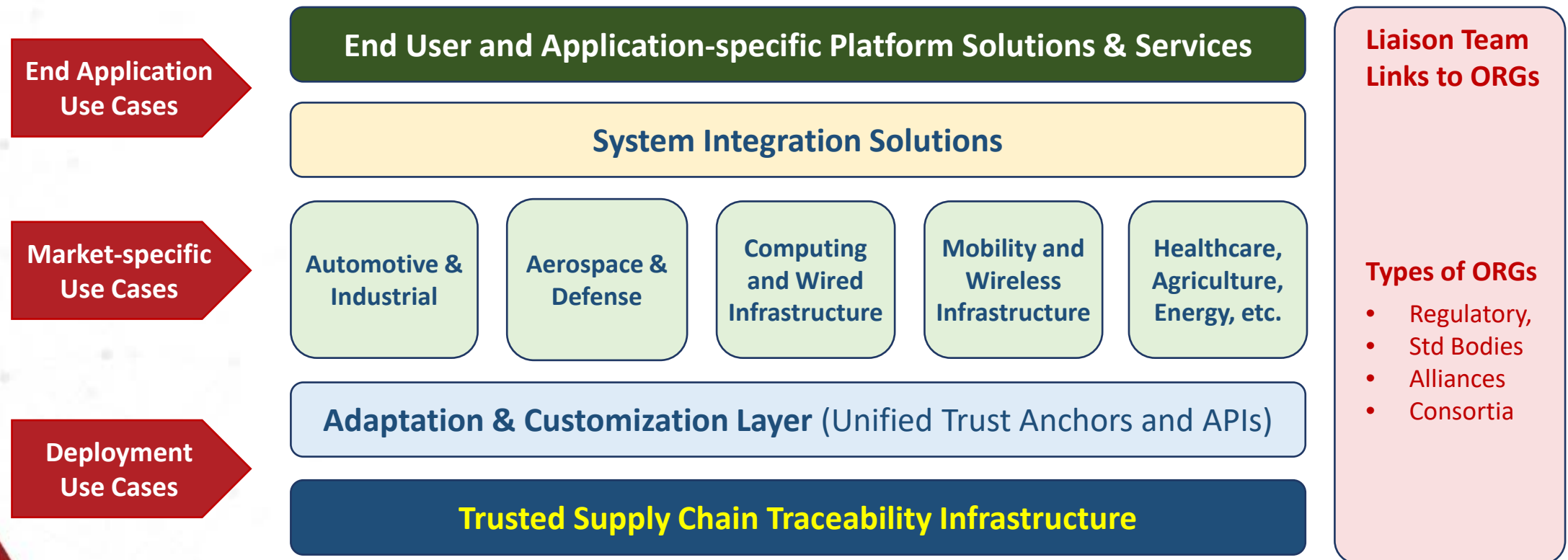
Elevator Briefs*
Executive Summary
Industry Problem
Use Case Examples
Proposed Solution
Beneficiaries
Value Proposition
Industry Guidelines
SWG Team Formation

*Example of content delivery template

- **Use Cases:** Identify challenges in the IoT value chain by vertical market or application
- **Solutions:** Describe end-to-end solutions carried out by collaborating stakeholders
- **Value-add:** Steer groups to articulate clear benefits and business value proposition
 - *Accelerate adoption, reduce OPEX/Cost/Risk, increase product value, enable new revenue streams, etc.*

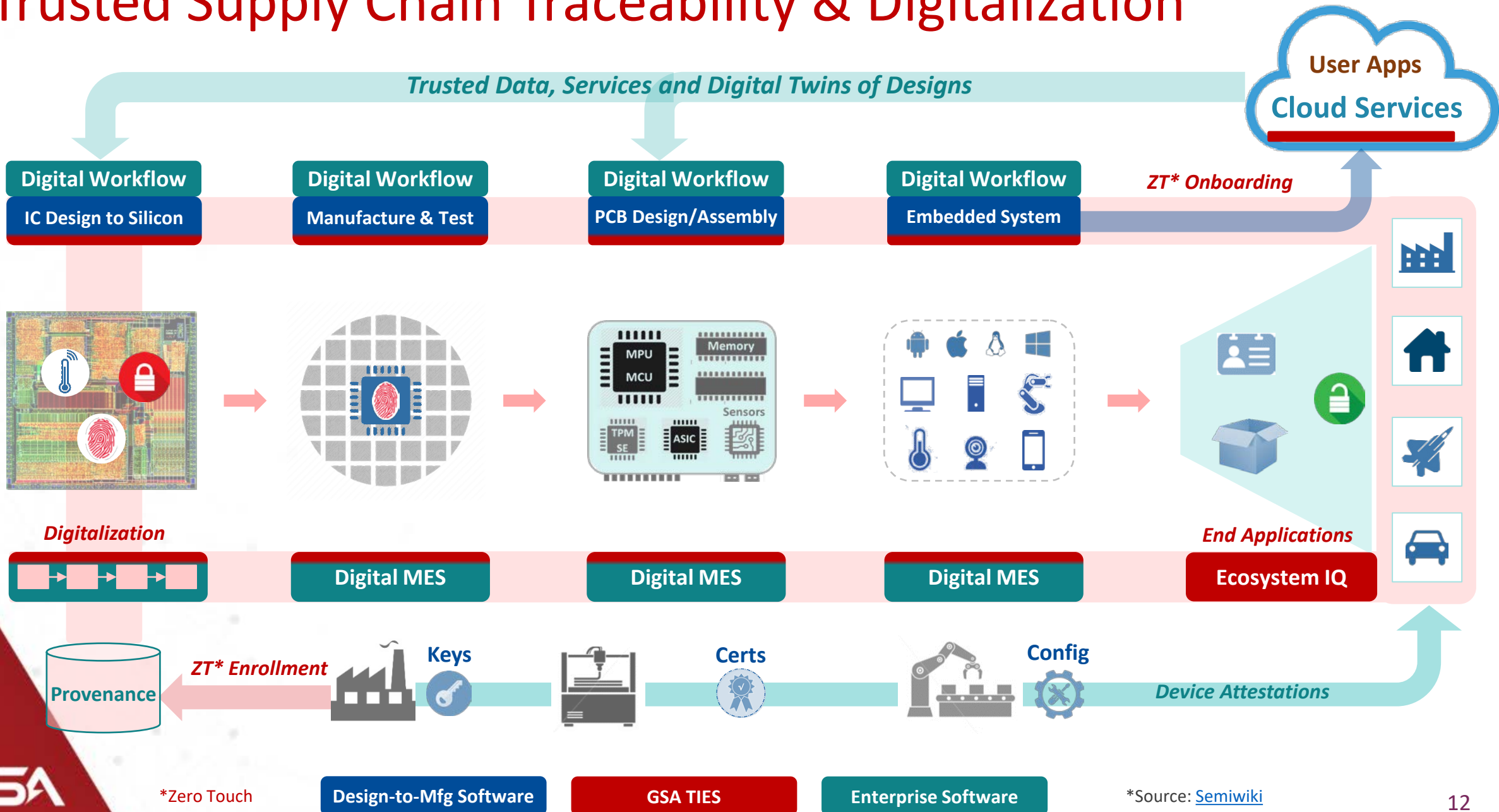
Taxonomy and Types of Use Cases*

Use Case: A description of a problem, steps and actions as experienced in a market or application by end users which can be addressed with end-to-end solution among collaborating stakeholders to create business value.

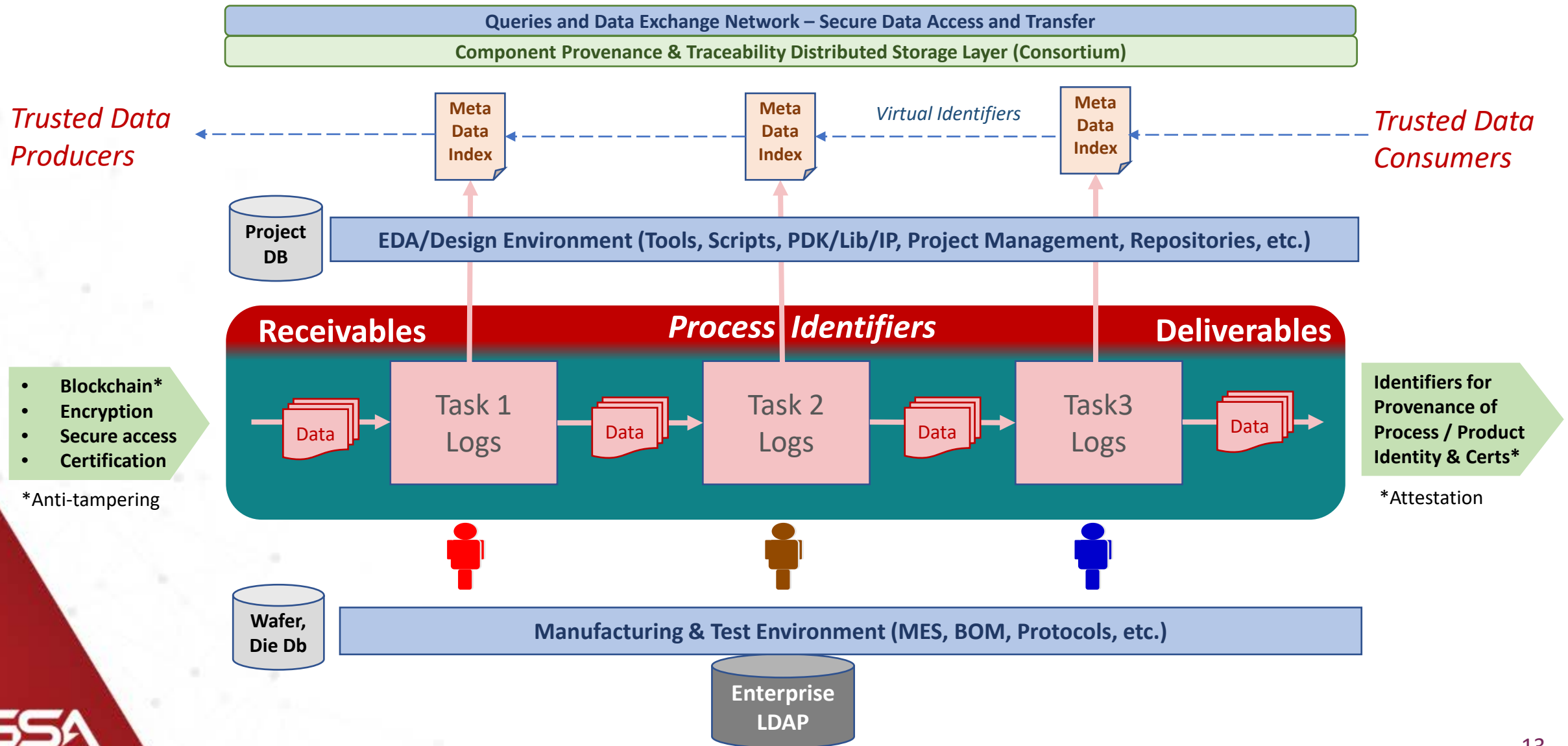


*Use cases driven by subject matter experts on different industries and markets

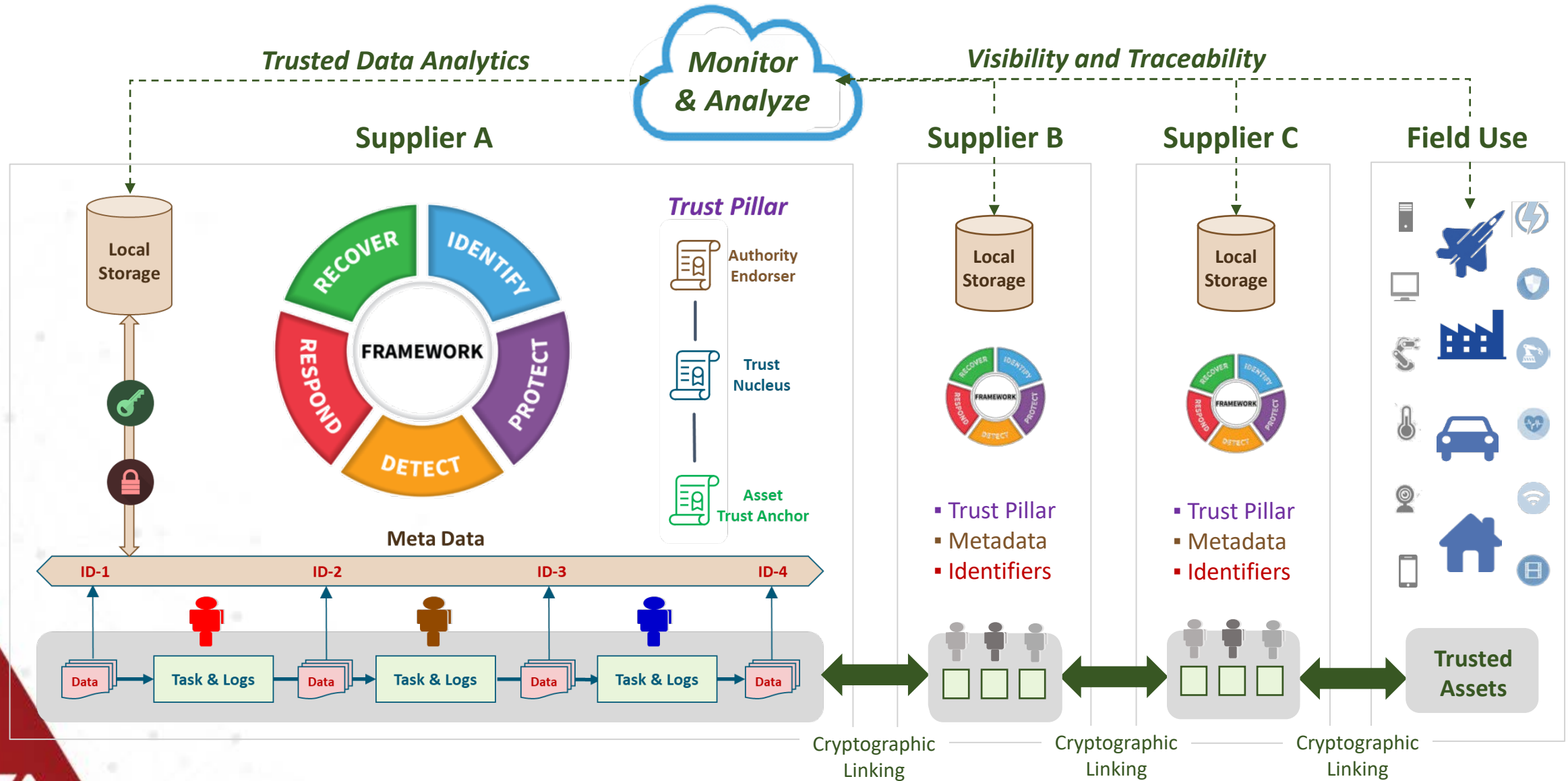
Trusted Supply Chain Traceability & Digitalization



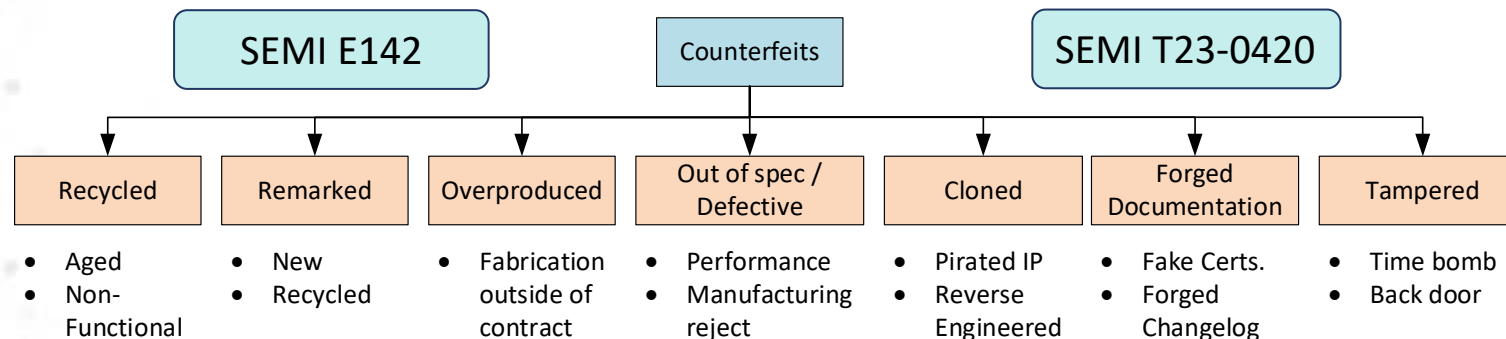
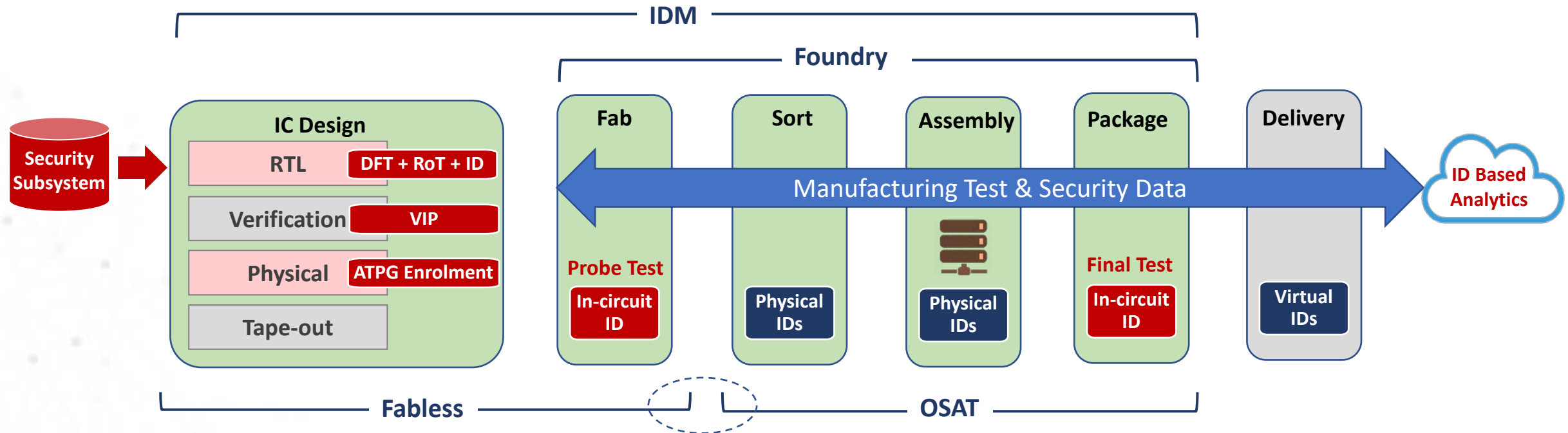
Generic Digitalization Model for Any Process



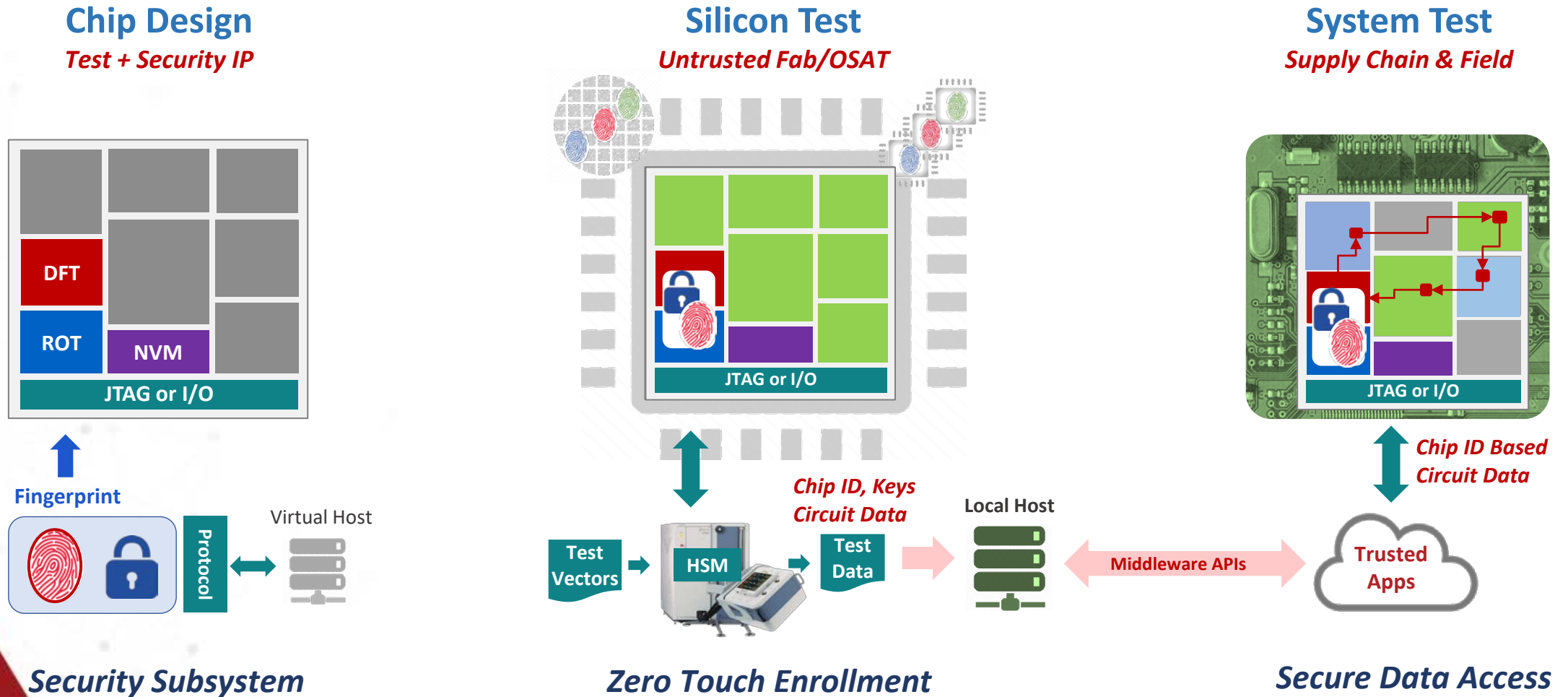
Scaling Visibility & Traceability Across the Supply Chain



Traceability Starts at IC Design & Manufacturing

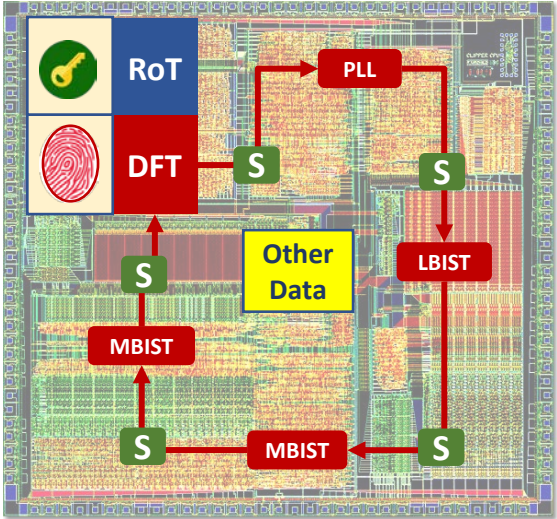
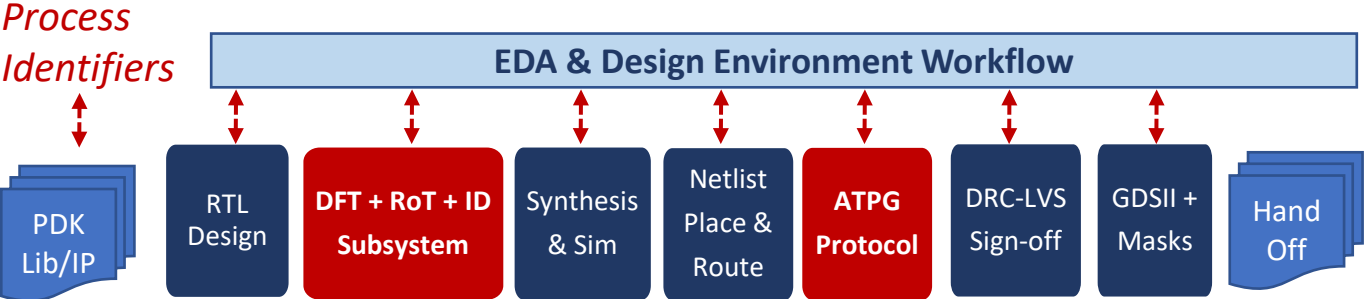


Foundation for Trusted Supply Chain Traceability

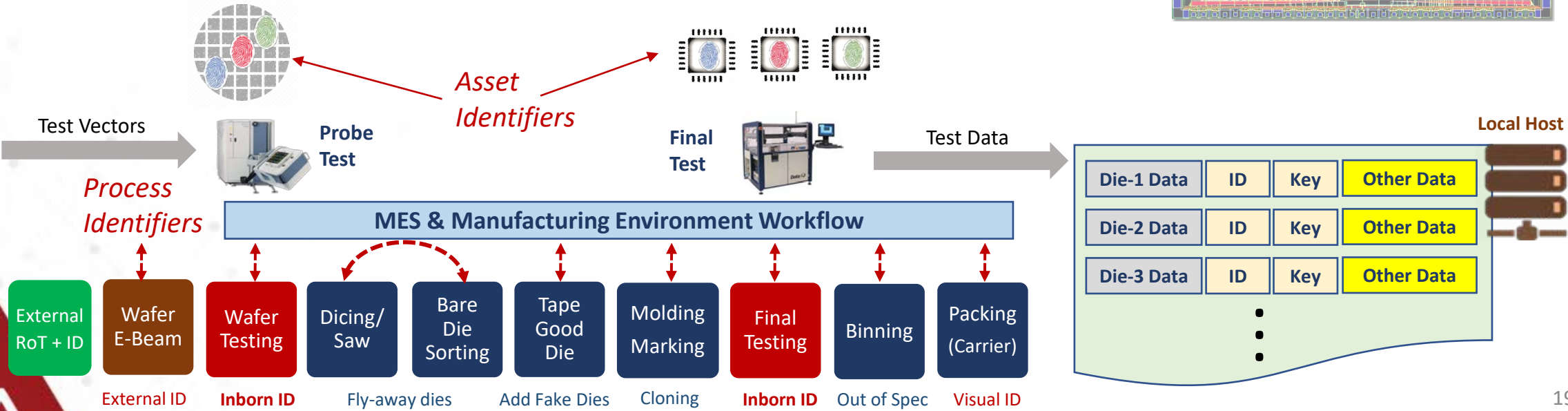


Provenance Starts in IC Design & Manufacturing

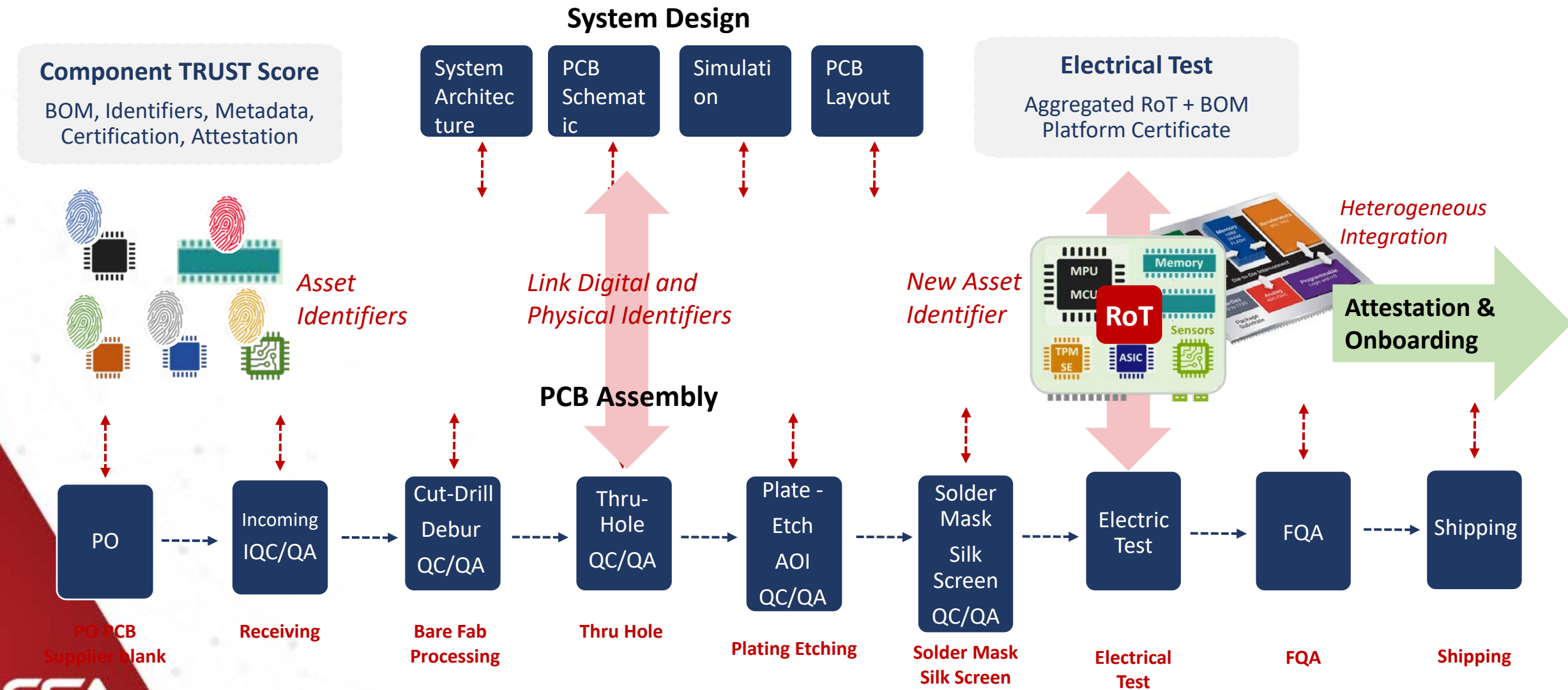
Design



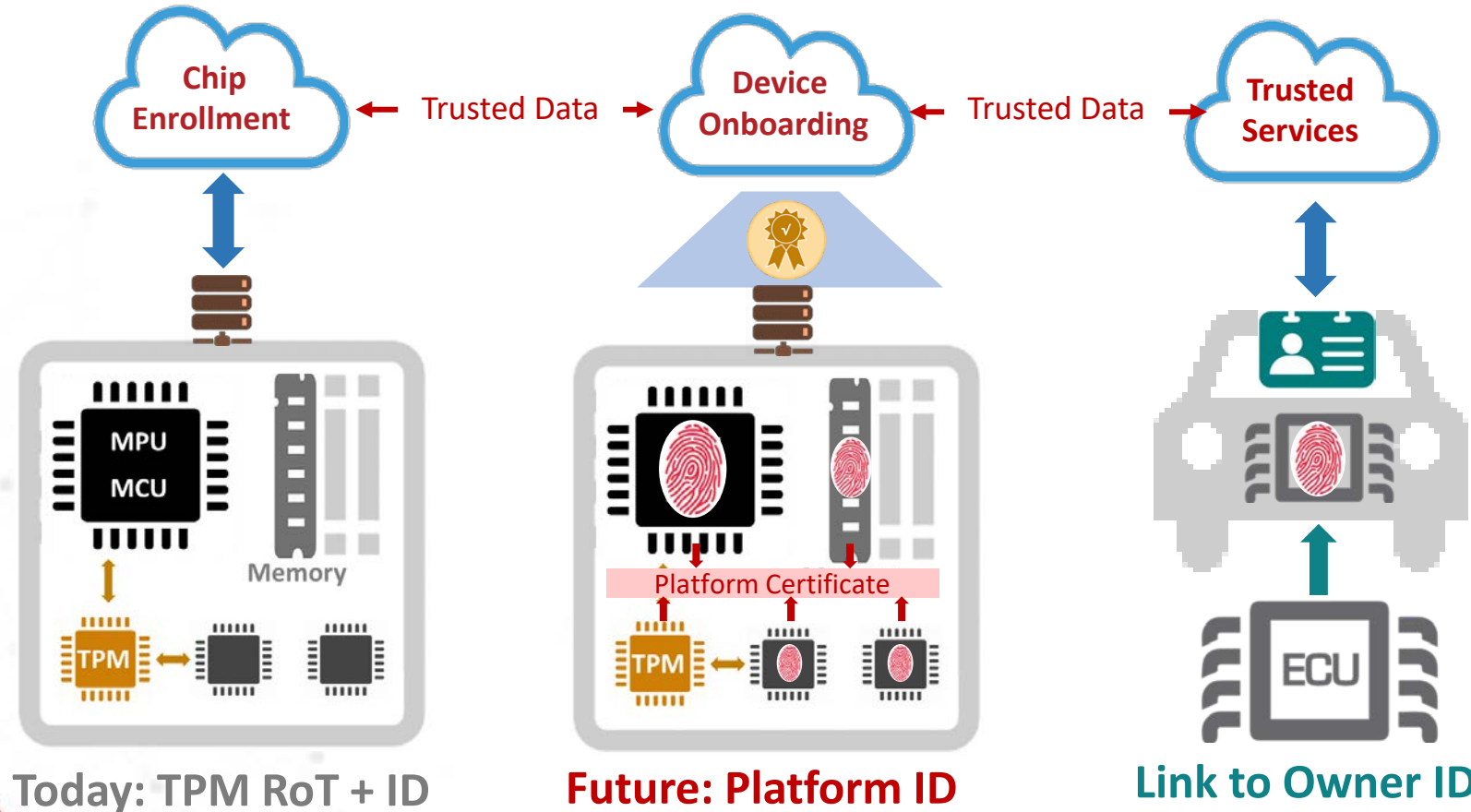
Manufacturing



System Design and System Assembly



Secure Connected Device Enabled Services



Traceability Services

- Monitor Shipments
- Origin & Provenance
- Chain of Custody
- Field Use Analytics

Enablement Services

- Owner Registration
- Device Onboarding
- Device Provisioning
- OTA Management

Which services are valuable and can we trust devices and data to deliver value?

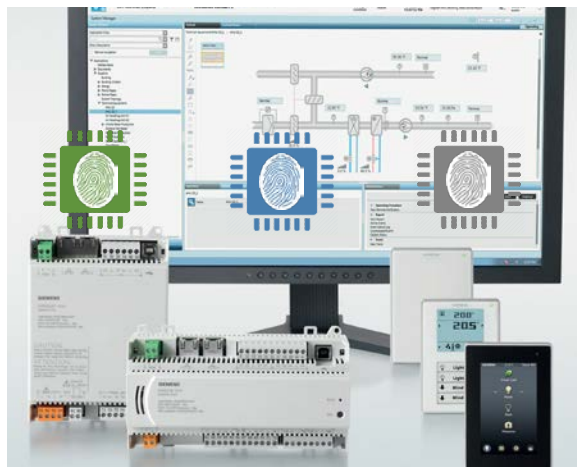
Chip Enabled Security Use Cases and Benefits

Electric Bike Options



Offer differing charging speeds, distance and tracking service

Multi Market Product



One SKU supporting many protocol standards provisioned upon delivery

Late Binding of Features

Bios/Images, Firmware, Security Credentials



Shipping generic products and securely configuring features and analytics OTA

- Battery life can be extended (ala Tesla)
- Product performance can be increased
- RMAs can be diagnosed even inside chip
- Compromised systems can be disabled

OTA Applications

Smart Connected
Device Supplier*

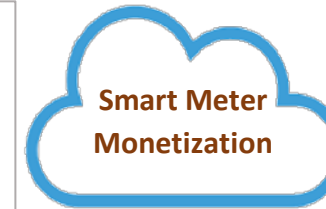
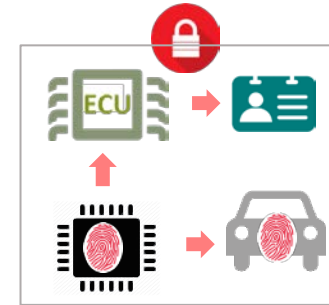
*Source HBR

- Ease adoption of new products/services
- Reduce recalls with in-field diagnostics
- Enable Hardware-as-a-Service business
- Deactivate stolen/unauthorized products

Chip & Device Enabled Secure IoT Services

- **Smart Infrastructure: Identity Based Metering**

- Goal: Simplify and automate parking experience
- Problem: Auto-charge & analytics on queues & traffic
- Solution: Identity-based ECU and PLC connectivity



- **Aerospace & Defense: Manufacturing Integrity**

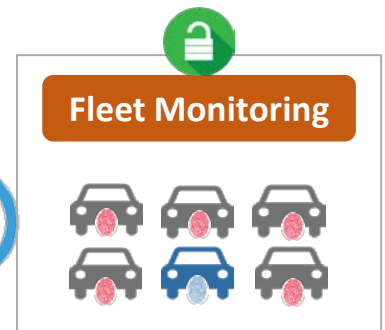
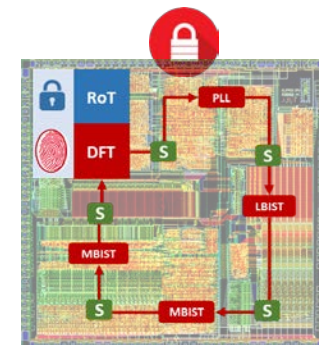
- Goal: Assess real time microelectronics reliability
- Problem: Tools, models and tester exist only in the fab
- Solution: Identity based chip data analytics to cloud



*Source: DARPA CRI

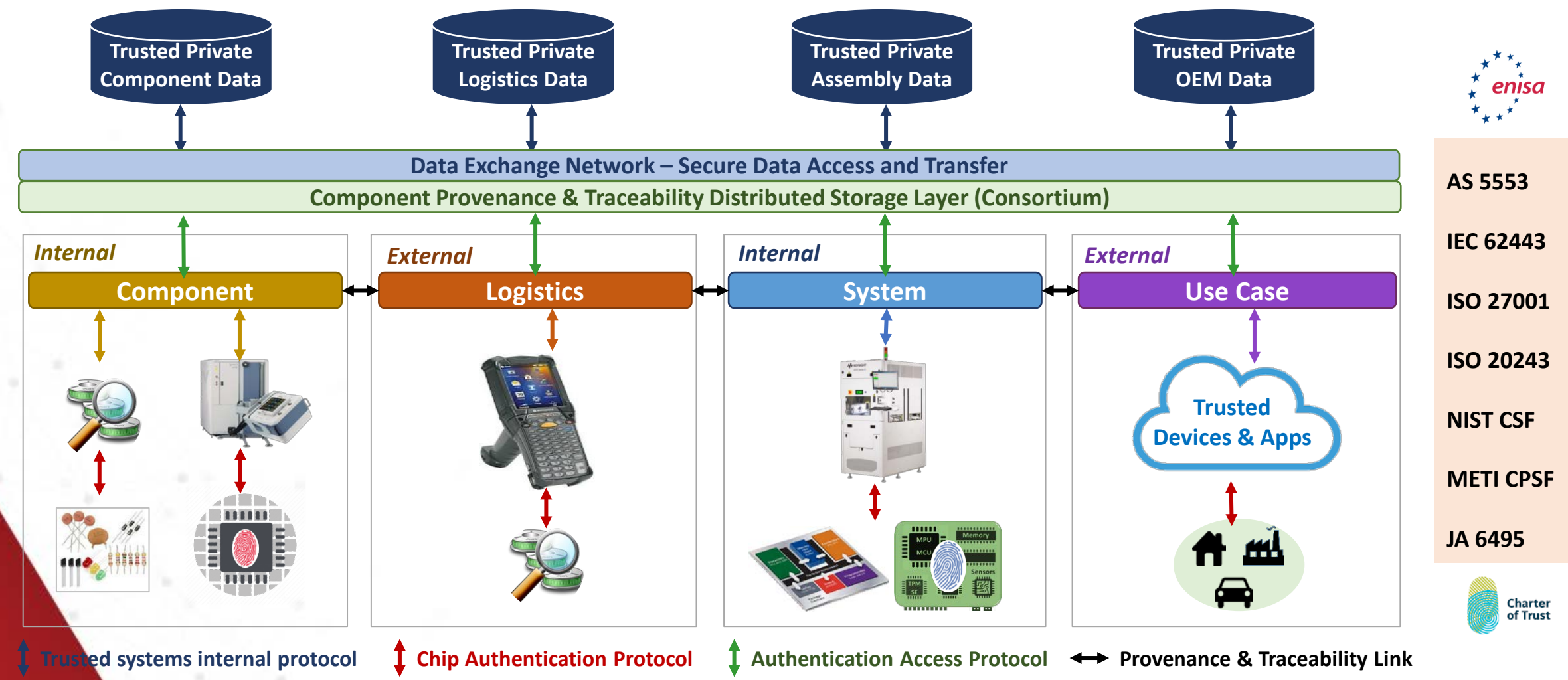
- **Autonomous Vehicles: Silicon Lifecycle Management**

- Goal: Analyze chip performance across fleets of cars
- Problem: When is right place/time to diagnose and fix
- Solution: Identity based OTA self-test and analytics

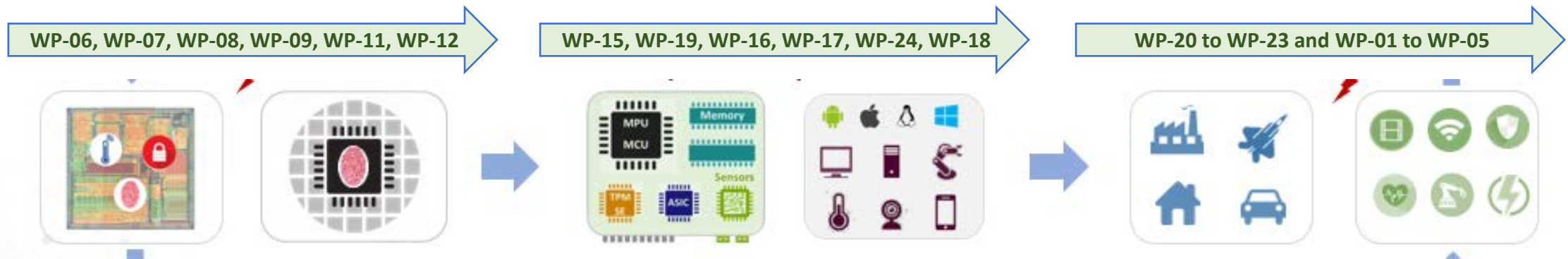


*Source: Semiconductor Eng

TIES Traceability Domains and Liaison to Standards ORGs



End-to-end Solutions Topics in Supply Chain Continuum



- WP-06 to WP-08 IC design and manufacturing test
- WP-09 to WP-12 IC manufacturing (incl. mask prep)
- WP-12 to WP-14 IC packaging, procurement and delivery
- WP-15 in-field IC provisioning (distributor or assembly)
- WP-19 links between IC delivery and PCB consumption
- WP-16 to WP-17 PCB assembly and system integration
- WP-24 adding certificate to systems & software on delivery
- WP-18 is secure device onboarding (for services enablement)
- WP-20 to WP-23 enablement and services for end applications
- WP-01 to WP-05 automotive use cases (post device onboarding)

What we need from MEPTEC

Enrich ecosystem IQ with packaging, assembly, test experts

Contributors get visibility and ability to partner on solutions

Summary

- **GSA TIES** - Platform-based business ecosystem for Secure & Trusted IoT value chain
 - EDA, IP, IC, Foundry, OSAT, ODM, OEM, EMS, CSPs, PLM, Services vendors, etc.
 - Ecosystem principles: **Open Architecture, Governance Rules, Network Effects**
- **Collaboration** - Contributing stakeholders share the benefits of end-to-end solutions
 - Leverage ecosystem IQ to minimize silos and accelerate adoption of IoT services
 - Collaborate on **use cases** that provide value and enable partnerships outside of GSA
- **Acceleration** - Facilitate digital transformation and adoption of secure IoT services
 - Shared success model to advance infrastructure and protecting the new gold - **Data**
 - Ecosystem re-aggregation of the value chain and analytics for ML and Digital Twins

Trusted IoT Ecosystem Security (TIES)

COPYRIGHT NOTICE

This presentation in this publication was presented at the **Known Good X (KGx) Workshop** (September 7, 2022). The content reflects the opinion of the author(s) and their respective companies. The inclusion of presentations in this publication does not constitute an endorsement by MEPTEC or the sponsors.

There is no copyright protection claimed by this publication. However, each presentation is the work of the authors and their respective companies and may contain copyrighted material. As such, it is strongly encouraged that any use reflect proper acknowledgement to the appropriate source. Any questions regarding the use of any materials presented should be directed to the author(s) or their companies.

www.meptec.org