



**Supply Chain Security Assurance
through an
Authentication Data Network**

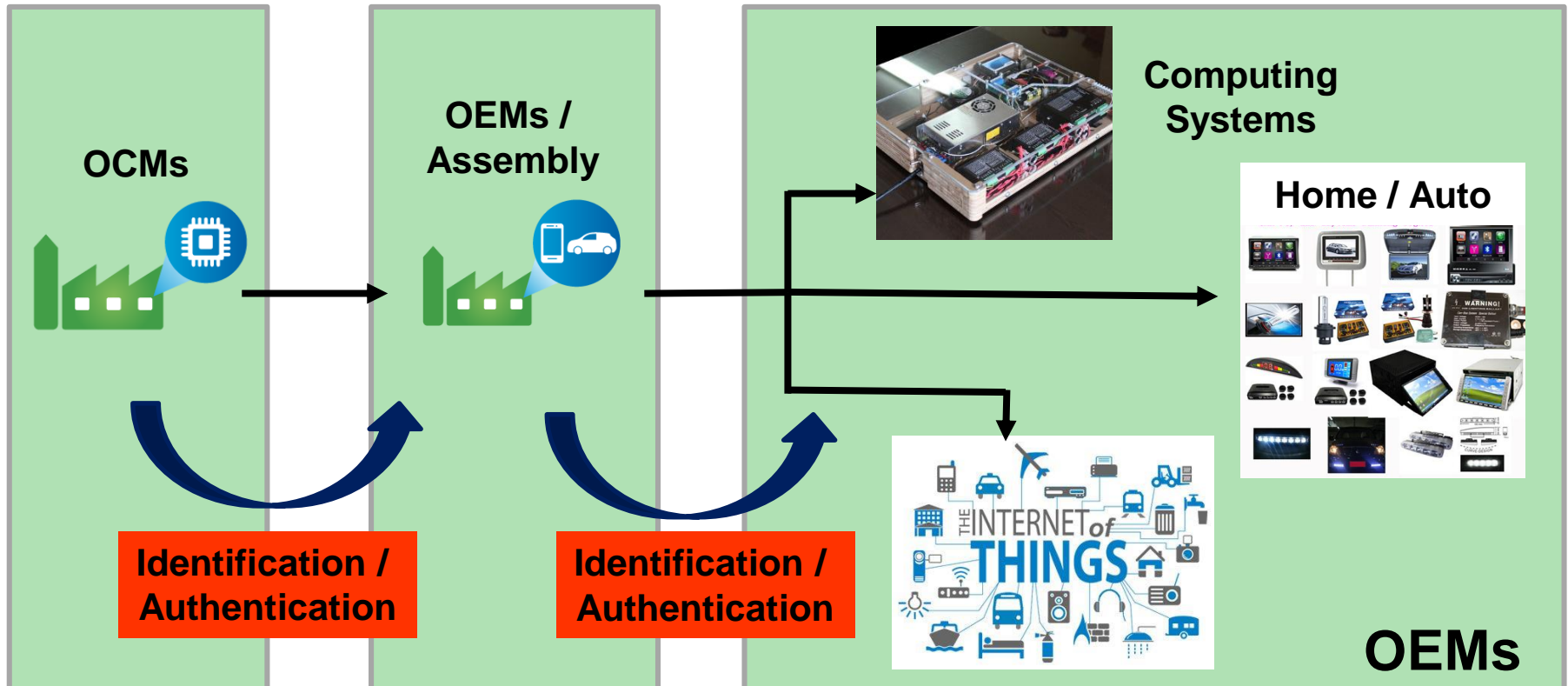
Michael Schuldenfrei, CTO



OPTIMAL 
Manufacturing Intelligence

Necessity for Device Authentication

- ❖ **Modern supply chain is very complex**
 - Devices move around the globe before being used in system
- ❖ **Devices and systems are subject to attacks**
 - Systems fail in use; loss of business, reputation and trust
- ❖ **> 50 billions IoTs in the supply chain by 2020**
 - Each IoT device must be authenticated; Secure upgrade needs authentication



Problems Addressed by IC Authentication

❖ Recycled or Refurbished ICs/PCBs/Sys

- Previously used parts reclaimed from scrapped assemblies
- Devices which have been refurbished, but represented as new product.

❖ Remarked

- ICs marked with falsely elevated performance or reliability
- Changed the brand name of the IC supplier

❖ Defective

- ICs failed or rejected on marginal test results, but returned as “good” to the supply chain

❖ Cloned

- Create copies of pirated or reverse-engineered design

❖ Over-Orders

- CM orders more parts than necessary for OEM “A” and sell the excess to OEM “B” for higher price

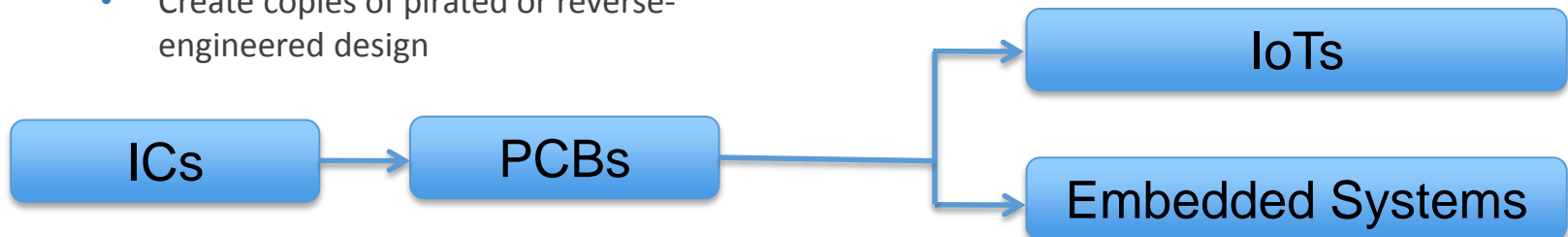
❖ Overproduced

- Foundry can produce more parts, fabricate the yield data and sell the extra chips to the market.
- Can produce extra chips without sending the information to the design house

❖ Excess Inventory/Unconsumed parts

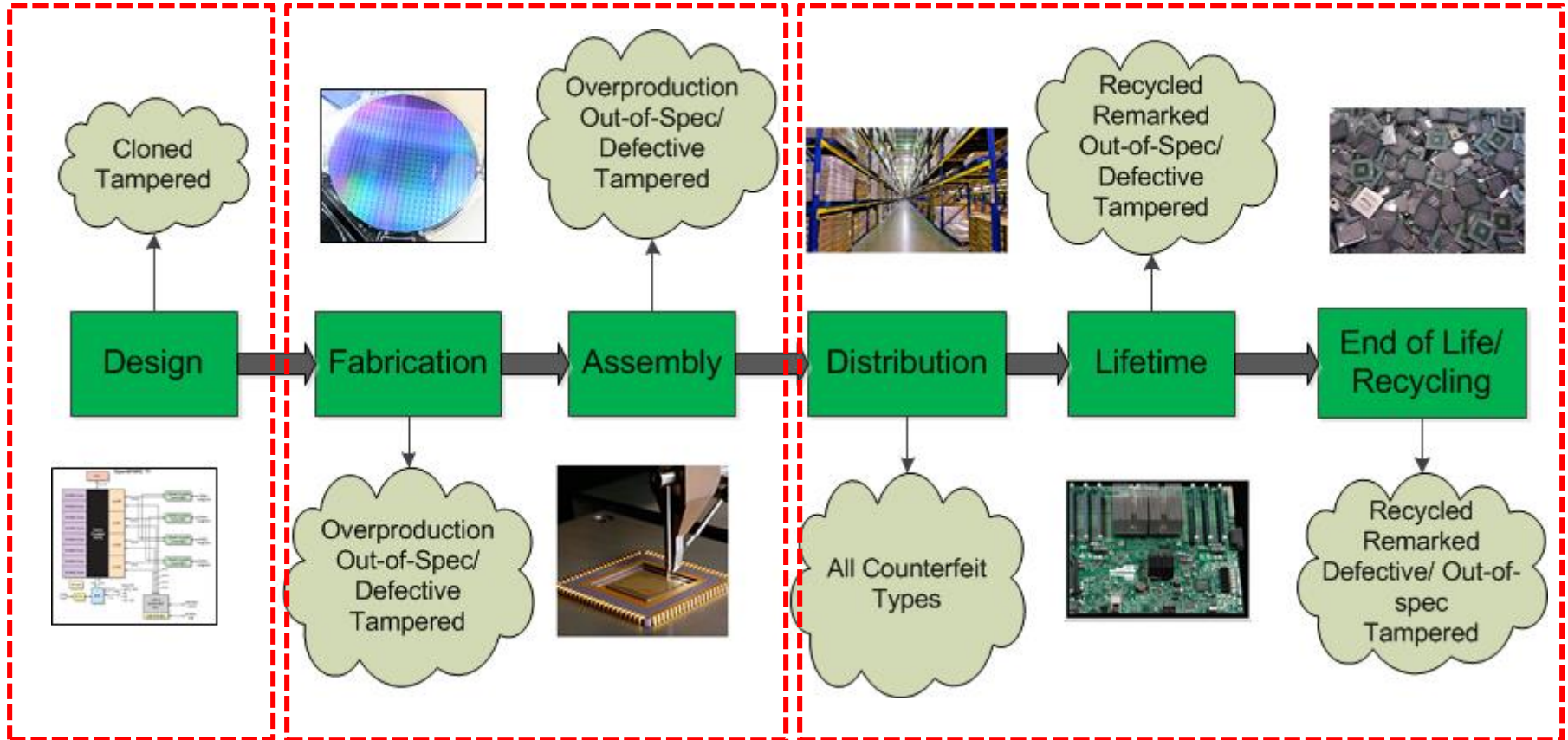
- CM or OEM sells unreported inventories of parts back to the distribution channel

❖ Theft



Entire Supply Chain is Vulnerable

Supply chain assurance begins with “authentication”



Optimal+ Comprehensive Authentication Solutions

Senate Armed Services Committee Report

ABOUT

HEARINGS

NOMINATIONS



LEGISLATION

PRESS

LIBRARY



UNITED STATES SENATE COMMITTEE ON **ARMED SERVICES**

[Home](#) / [Press](#) / [Press Release](#)

Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts

Monday, May 21, 2012

WASHINGTON -- A Senate Armed Services Committee investigation discovered counterfeit electronic parts from China in the Air Force's largest cargo plane, in assemblies intended for Special Operations helicopters, and in a Navy surveillance plane among 1,800 cases of bogus parts, [a committee report released today](#) [PDF 1.44 MB] shows.

Related Files

[Senate Armed Services Committee
Releases Report On Counterfeit
Electronic Parts](#)

Cisco's Call to Action



Edna Conway, CSO, global supply chain, Cisco Systems

June 01, 2015

CSO'S DESK

<http://www.scmagazine.com/detecting-and-reducing-counterfeit-chips/article/414290/>



Detecting and reducing counterfeit chips

In a world where the risks of counterfeit or tainted information and communication technology (ICT) are ever-present,

I propose a call to action:

ICT original equipment manufacturers (OEMs) and our brethren in the semiconductor industry should embark on a coordinated effort to share chip identification information.

How might this work? Let's walk through a simple model.

1. A semiconductor manufacturer programs the unique identity into a register on the device and **creates a repository of those unique identities.**
2. That repository is made accessible on a controlled, limited access basis to those OEMs and their manufacturers who are using the chips.
3. A simple pre-assembly validation step could then be implemented as a first phase of electronic circuit counterfeit detection and mitigation. The OEM would compare the unique identity from the semiconductor manufacturer's controlled register to the list that has been provided by the supplier of the chip.
4. If the unique identity from the component supplier is on the list from the semiconductor manufacturer, the assembly process can move forward. Next, the OEM would log that specific identity into a list of all those identities acknowledged as genuine but already assembled onto a printed circuit board.
5. **An OEM could thereby detect a potential counterfeit chip** by the fact that the identity was duplicated and therefore already used on a board.
6. The OEM would also be able to associate each chip and its unique identity to a specific printed circuit board-level serial number.

Challenges and Solutions

Challenges:

- ❖ Billions of devices connected to network, many can be fake or counterfeit
- ❖ Existing authentication **solutions are incomplete and expensive!**
 - Authentication solutions are often done on a **small sample of chips**
 - Ineffective for mass production environments – **cost, speed and design** implications
 - **Semi OCMs and Electronics OEMs are silos** so traceability is not possible

Solutions:

- ❖ **Only Optimal+** has the missing ingredients to solve the problem
 - Information highway infrastructure to connect OCMs to OEMs
 - Already collecting and storing chip ID and “fingerprint” data of billions of chips
 - Well-established and trusted partner, managing sensitive semiconductor data
 - Authentication and identification solutions for integrity check at all levels can easily be built on our existing infrastructure

Who is Optimal+

Optimal+ Manufacturing Intelligence™

- ❖ **Big data analytics company** founded in 2005
- ❖ **Transforms** fragmented data across the semiconductor global supply chain into intelligence for actionable business decisions
- ❖ **Transforms** disjointed Big Data into a unified Big Picture
- ❖ **Enables** unprecedented visibility into manufacturing operations and the global supply chain
- ❖ **Measurably improves yields, quality, reliability, throughput, and test efficiency**

Strong Market Presence Worldwide

35B+
Chips

Processed each year using Optimal+

Over 90%
Foundry and OSAT coverage

Networking fragmented Big Data and converting into a unified Big Picture

~7000
testers

With O+ software in IDMs, foundries and subcons worldwide

Up to 2%
gain

In product yield recovery based solely on test

Up to 20%
increase

In operational efficiency & productivity improvements

Up to 50%
reduction

In test escapes, improving quality and reducing RMAs

Our Customers – 100% Coverage



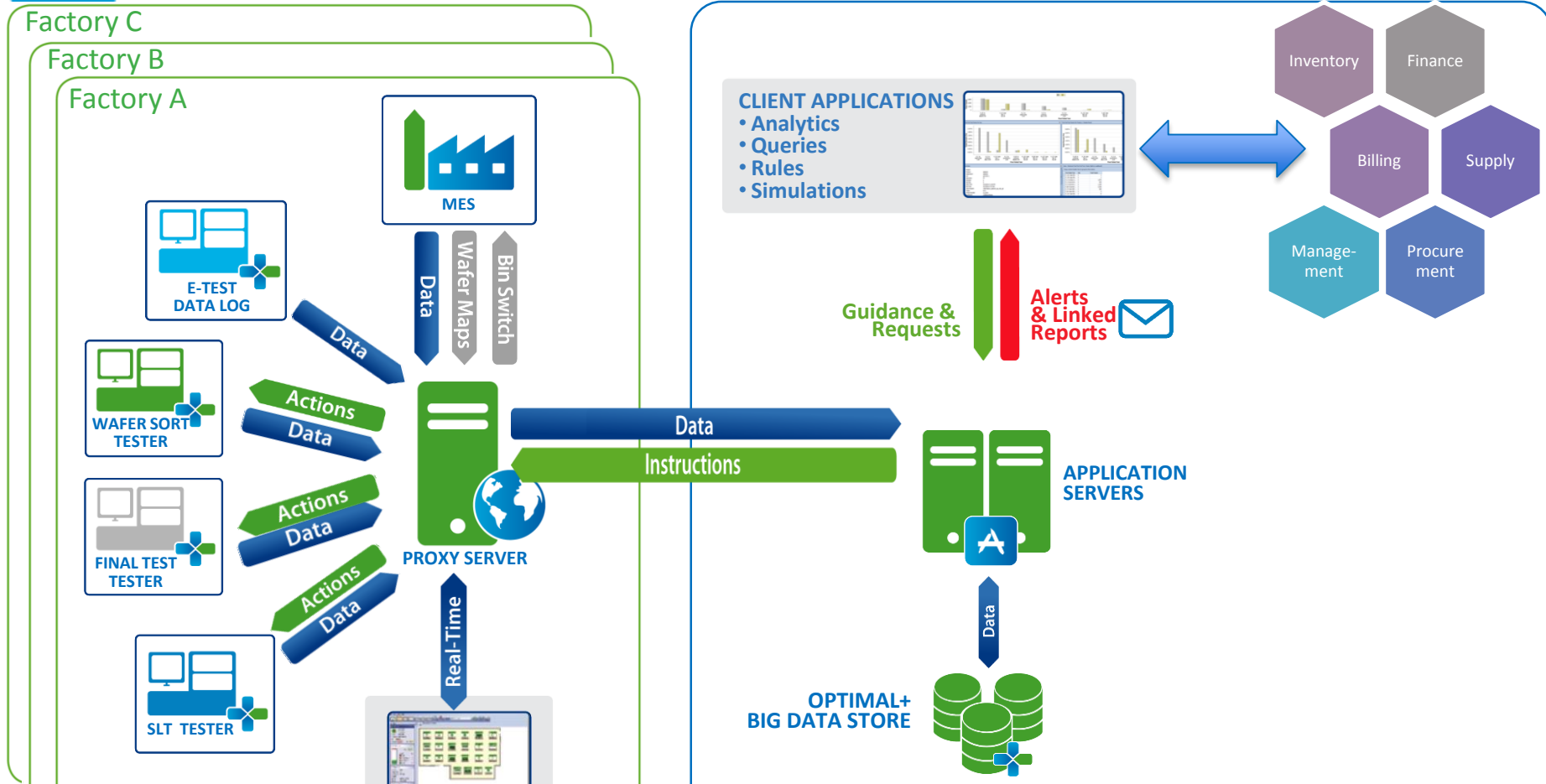
Deployed– 90% WW Supply Chain



Optimal+ Architecture in Semiconductor

Test Floors

Fabless / IDM Headquarters



The Result

An existing Big Data Store with all of the test data, ECIDs and UIDs needed for chip authentication

Expanding from Semi into Electronics

Available Now
(Market Leaders)

2016

2017

2019

IC & Multi Chip

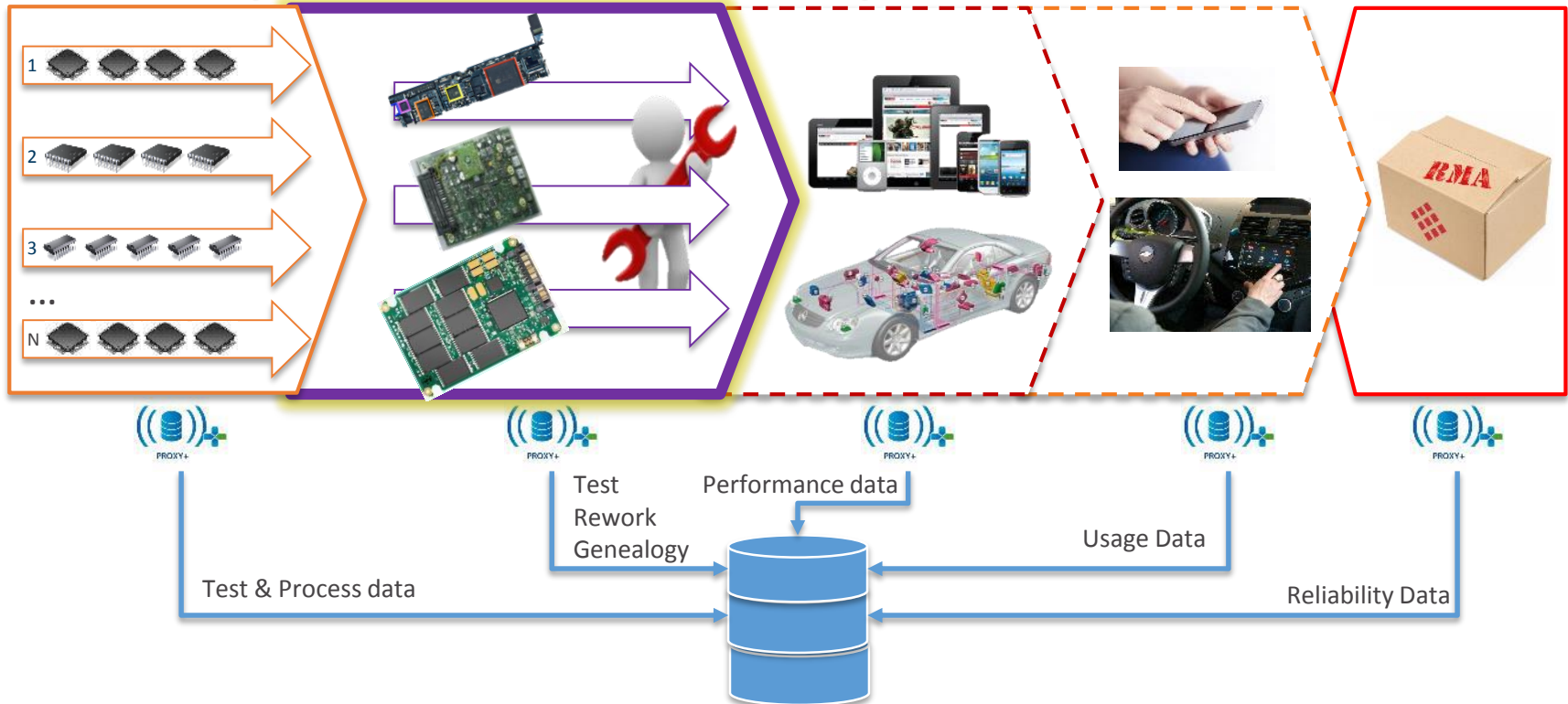
Boards

Rework

Systems

In-Use

Returns



First cross-industry platform connecting electronics to the semiconductor supply chain.

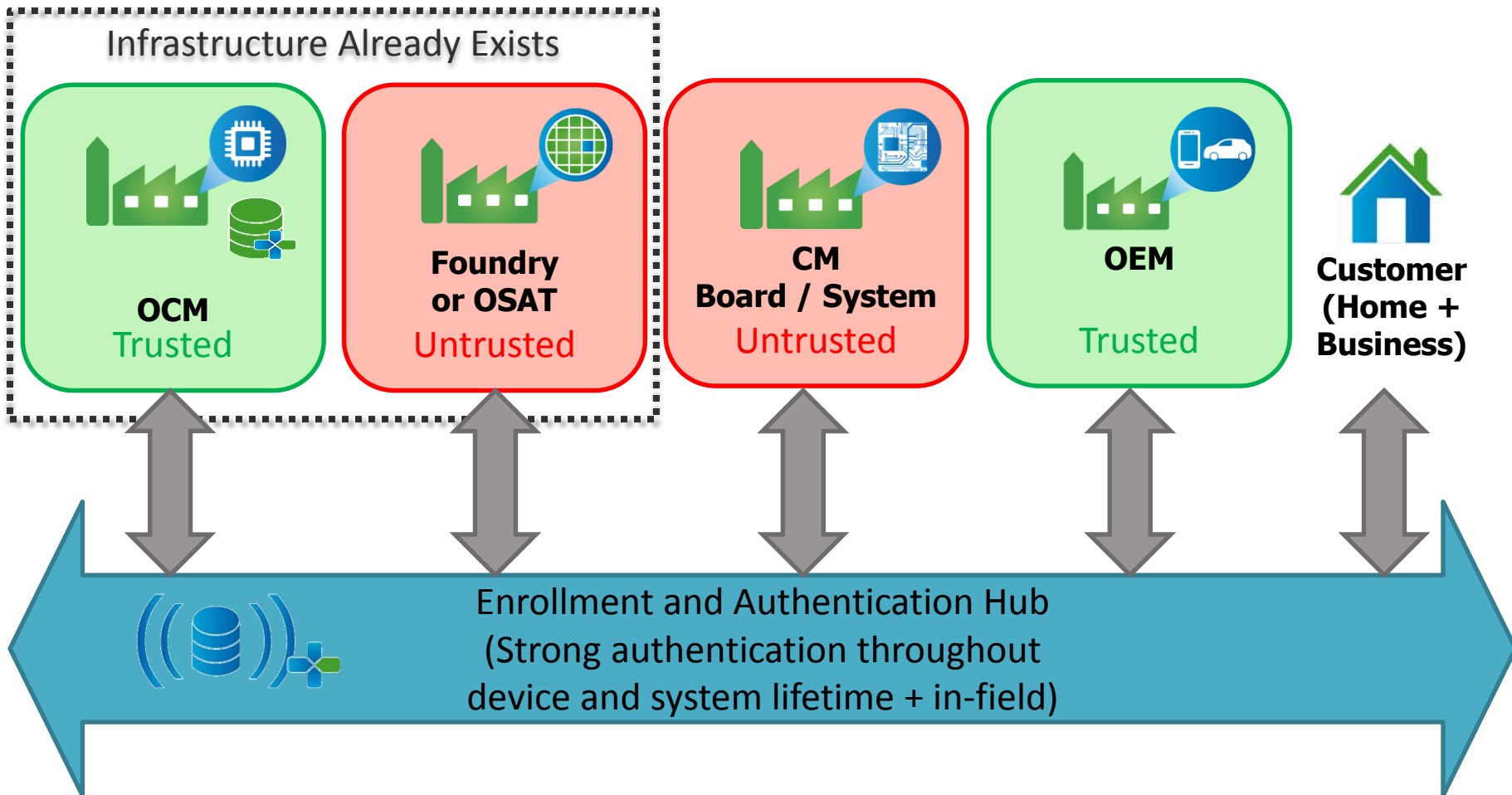


The Ingredients for End-to-End Authentication

- ✓ Comprehensive chip test database (chip DNA)
 - ✓ ECIDs, UIDs, Binning, Measurements, Performance, etc.
- ✓ Data accumulated as part of normal chip operations (no overhead)
- ✓ Data highway connecting OCMs to their suppliers
- ✓ Trusted third-party to support and manage the reliable and secure transfer of information
- ✓ Data highway connecting OEMs to their suppliers (coming soon)

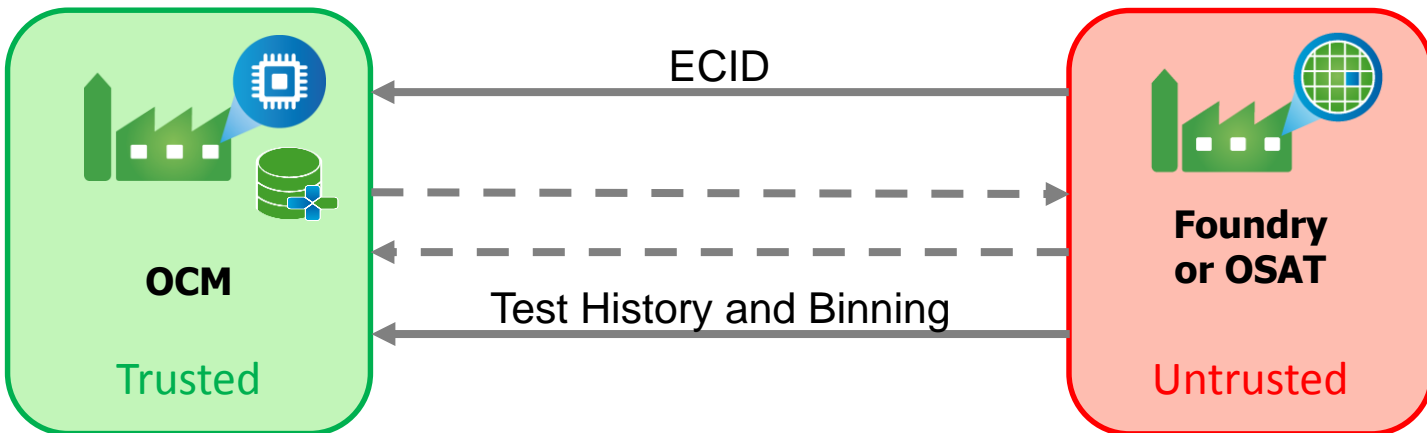
Optimal+ has the missing ingredients to solve the problem!

Enrollment & Authentication Flow



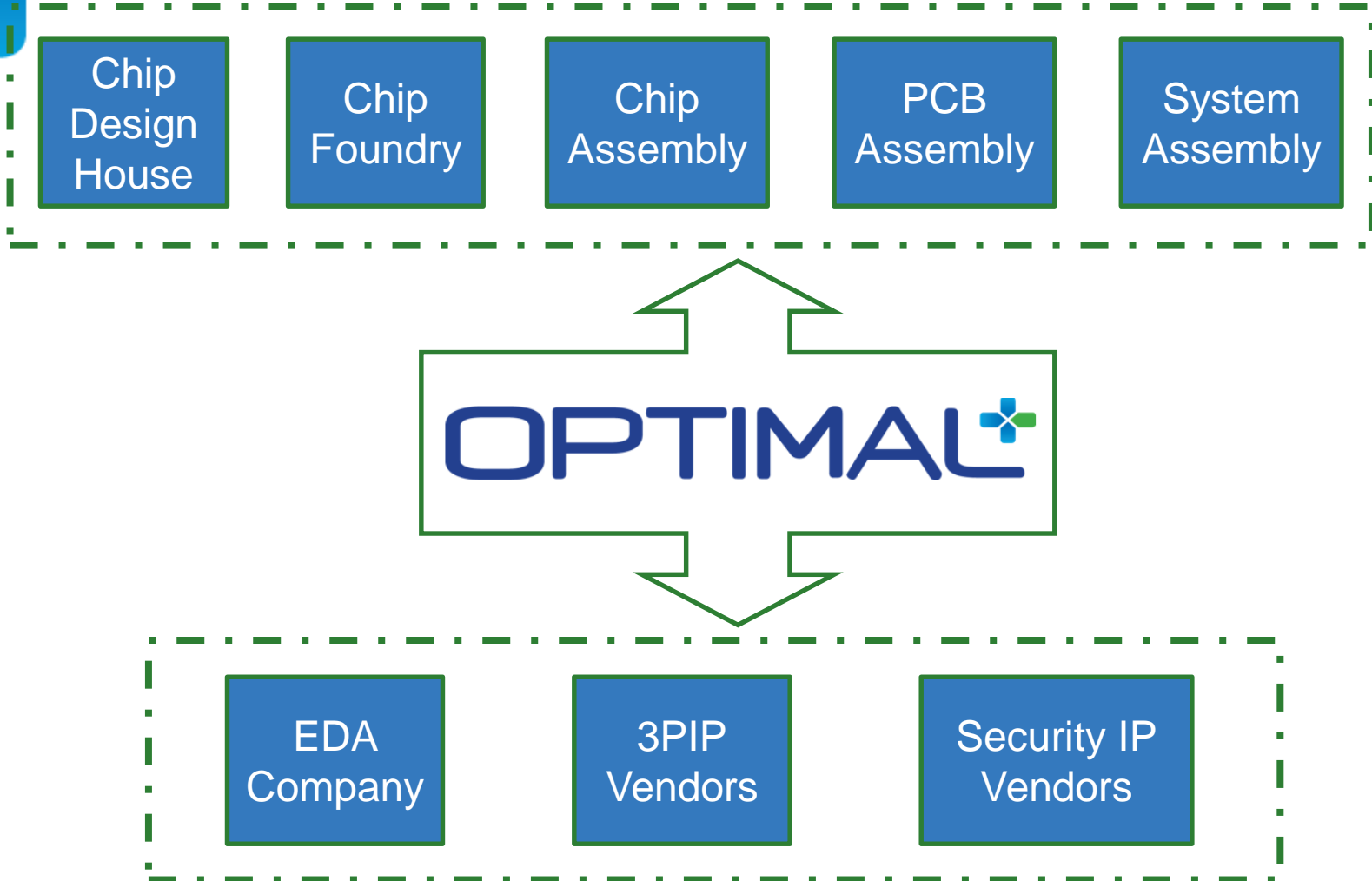
Infrastructure Already Exists!

- ❖ Chip fabricated by foundry is enrolled in DB at the OCM
 - Electronic Chip IDs (ECIDs)
 - Unclonable IDs (UIDs)
 - Strong challenge-response communication
 - All test and binning data
- ❖ Collected by Optimal+ Proxy software on the tester



More detailed information will be shared with design partners

Within the Ecosystem



Call to Action – Join the Authentication Network

- ✦ What are we looking for?
 - We are already working with multiple OEMs and OCMs to support hub-based data exchange for quality purposes
 - We are looking to add more design partners (at least one OEM and one of its OCM suppliers) to leverage the same infrastructure to address supply chain integrity threats
- ✦ What is required from the design partners?
 - Provide use-case and data
 - Participate in a production pilot
 - Provide feedback on the solution and be a part of its evolution
- ✦ What do the design partners get?
 - Influence the direction of the O+ solution
 - First access to the solution



Thank You!

OPTIMAL 
Manufacturing Intelligence