SIEMENS

SIEMENS DIGITAL INDUSTRIES SOFTWARE

Secure end-to-end traceability and digitalization

Ensuring security with a semiconductor specific data model from silicon to system

Semiconductor Lifecycle Management

End-to-end traceability for Semiconductor security

Our connected world runs on semiconductors, operating everything from F-35 fighter planes to cell phones, medical devices, and smart buildings. Being able to trust the data and the devices that protect our privacy and our security really matters.

In the past, customers could take a manufacturer's word for the authenticity of each semiconductor device, and the integrity of the data, but that is no longer the case.

Counterfeiting, malicious code, backdoors, susceptibility to cyberattacks and critical chip shortages have all made us question the supply chain to the point where every device must be verified.

In the case of medical, aerospace, defense and automotive applications, product non-performance can result in devastating consequences. For governments, supply chains are critical to national security, so verifying them is now a top priority.

As a result, we now live in a new era of zero trust. Everything must be verified. That is where secure end-to-end traceability and digitalization makes the difference.

Securing our future

In our interconnected world, having a "secure" chip supply means much more than just ensuring access to them when needed. It also means ensuring that chips are safe, secure, and reliable.

Siemens experts estimate that 10 percent of components that reach an electronics manufacturing service line are compromised, whether they be counterfeit, refurbished, or damaged. This is not surprising when you consider today's global supply chain, where components for a single chip can travel 25,000 miles (about 40233.6 km) to numerous specialized contractors before they are ready for installation, according to research from the Global Semiconductor Alliance and Accenture.

As a safeguard, every device and every device modification must be traceable.

The objective of secure end-to-end traceability is to consider a few key factors and provide the essential answers:

- Determine if the device is genuine, or is it a counterfeit
- Verify if it is built as designed
- Ensure the designs are intact and have not been tampered with
- Decide where it came from and where it was going to end up

Five fundamental assumptions of zero trust*

1. The network is always assumed to be hostile.
2. External and internal threats exist on the network at all times.
3. Network locality is not sufficient for deciding trust in a network.
4. Every device, user and network flow is authenticated and authorized.
5. Policies must be dynamic and calculated from as many sources of data as possible.

How does secure end-to-end traceability and digitalization work?

Provenance is a priority

Secure end-to-end traceability and digitalization can provide an audit trail or genealogy of a device.

It can be provided by secure software systems that can verify the authenticity of devices and data over the course of a product's life.

Secure end-to-end traceability requires that the entire genealogy of the component, the intellectual property (IP) and the chip is completely traceable to verify that as–designed specifications match as–built realities. Since a typical semiconductor company may have more than 16,000 global suppliers, achieving secure end-to-end traceability without secure software systems and sufficient capacity can be difficult. It is made more difficult by the vast amount of data generated by a semiconductor and its ecosystem over its lifecycle.

Traceability begins with connectivity

Too many systems in the semiconductor industry today are still fragmented legacy systems, most of which are unconnected, lack a common data platform or common language across systems, limit secure collaboration, and offer only limited traceability. Key design, engineering, and manufacturing functions often exist in silos where sharing information is difficult. The different tools and processes within design and manufacturing are standalone systems, which makes system-driven traceability difficult.

Secure end-to-end traceability and digitalization bridges the gap with genealogy and data for the semiconductor lifecycle

From conception to obsolescence, the lifecycle of a semiconductor product is complex. Its life gets exponentially more complex as it becomes part of a system of systems, traversing a global supply chain.

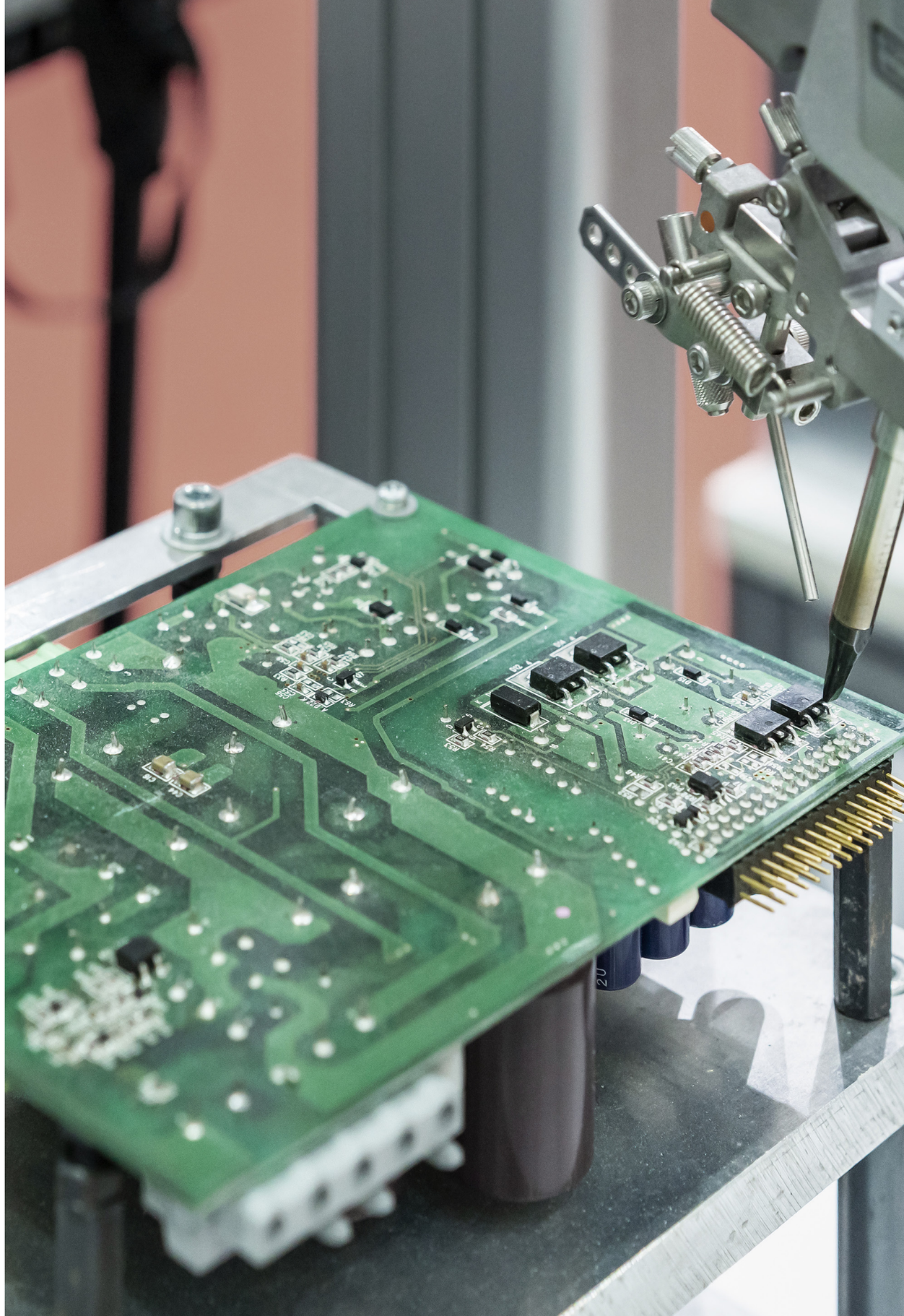
That is why secure end-to-end traceability and digitalization must be able to do what humans cannot do at scale: supervise every transaction between every data generator and report back anomalies for investigation, while providing end-to-end traceability and provenance for chip-to-system design, development, and manufacturing.

Secure end-to-end traceability and digitalization collects, links and stores product data from any system across the value chain:

- Protects the confidentiality of the design and operational information throughout the lifecycle
- Provides provenance and traceability of the product, intellectual property (IP) and all associated data
- Provides end customers with assurance that all relevant data is visible to them

> We haven’t had the ability to design an architecture until now to analyze terabytes of data in real-time. Now we do.” **

John Allgair, Program Manager, Advanced Systems Integration, BRIDG



Secure end-to-end traceability equips companies to execute one of today's most critical business imperatives: semiconductor security

Our solution ensures secure end-to-end traceability and digitalization of every product lifecycle stage needed to provide your customers with the highest level of security via fast, comprehensive verification of semiconductor devices and data. All semiconductor companies can use our solution to provide end-to-end traceability at the product – process – revision level using a unified data and process model spanning from semiconductor design to manufacturing. Secure end-to-end traceability lets you know when a decision was made and why, throughout the semiconductor lifecycle.

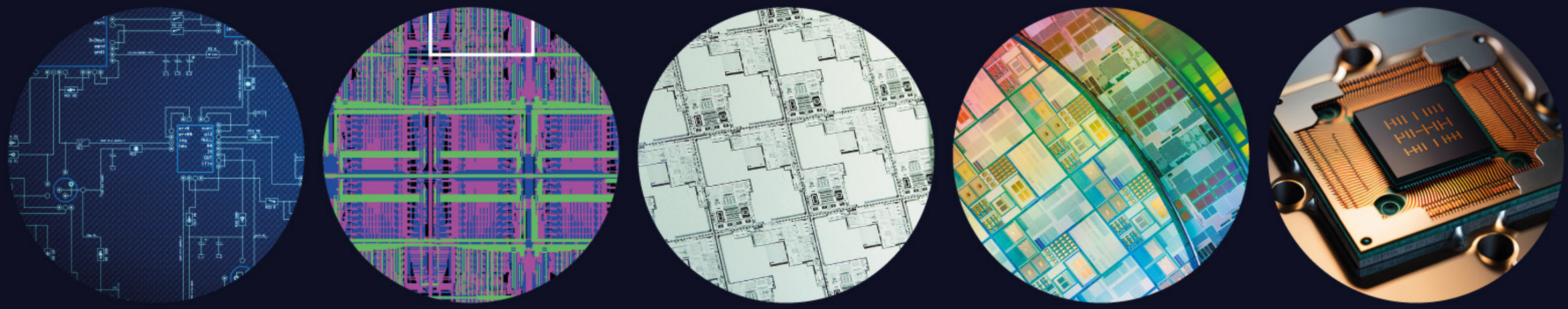
Direct benefits of secure end-to-end traceability and digitalization across semiconductor lifecycle management:

- Provides information-rich traceability across all objects in semiconductor design and manufacturing
- Enables companies to prove quantitative assurance and data provenance for ICs & IP
- Documents the genealogy of products to bring transparency into your value and supply chains
- Promotes rapid acceptance and delivery of semiconductor products, and faster time to market
- Enhances quality management in tracing down quality issues
- Equips companies to fight counterfeiting, achieve compliance and fulfill legal requirements
- Verifies information across the entire value and supply chain, from product design, raw material purchases, production tool usage, to logistics and beyond

Connected to our integrated lifecycle management for semiconductors (LMS) system, our end-to-end traceability solution lets companies manage the lifecycle from design to manufacturing in one common data and process model. It shows the connection of all digital and physical assets, die design and bill of process (BOP) items.

As the only LMS offering information-rich traceability throughout, you can run "what if" scenarios to ensure product cost-effectiveness and success, while optimizing product design resources, parts costs and manufacturing routing.

Global value chains are long and complex and often lack transparency. Gaining transparency along the value and supply chain is one of the top business priorities today, and secure end-to-end traceability provides the missing transparency along your value chain by documenting your complete product genealogy.



The role of single-device tracking in secure end-to-end traceability and digitalization

If you're making complex multi-chip devices, that's where single-device tracking (SDT) offers a real advantage. SDT is the most efficient way to deliver accurate data about every device and its processing history.

Elevating MES to a whole new performance level

Most of the popular manufacturing execution systems (MES) available today are not equipped to scale up to process the volume of traceability data required. They typically slow complex operations to a crawl. It would take seconds, not the required milliseconds, for a typical MES to process data from each transaction for every device in a lot, which will not satisfy automated high-volume production.

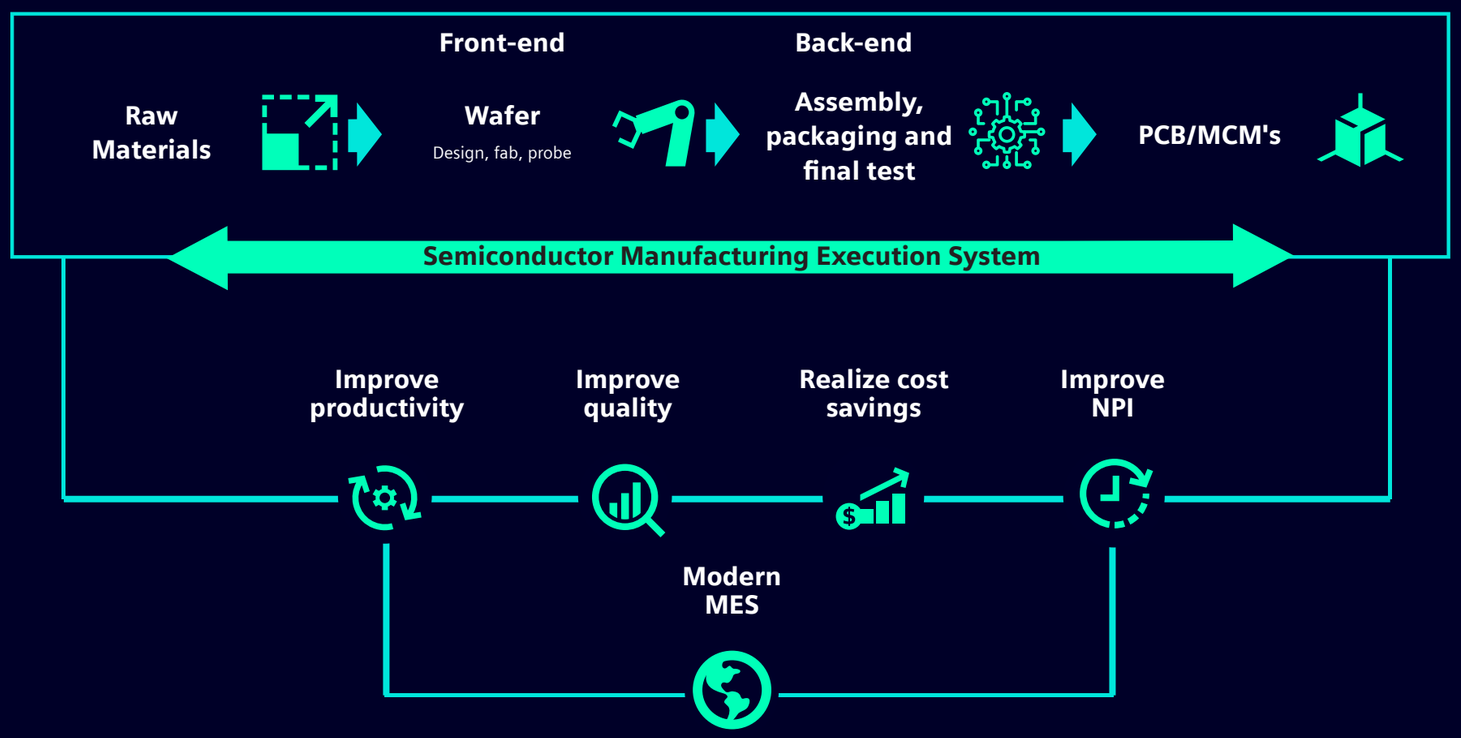
Fortunately, newer high-performance solutions are now available that integrate high-performance capabilities into MES, so it can achieve transaction speeds not previously attainable to provide high-speed single-device tracking and tracing at the pace needed by automated high-volume transactions.

Once the MES is capable of performing high-volume single-device tracking, the semiconductor manufacturer has more agility to control how each device proceeds through each process. This high-performance approach is the key to unleashing the many benefits of single-device tracking. Single-device tracking also allows you to include the metadata with single items. Even after a device is separated from the wafer, processed through splits and merges, binned and graded separately, it retains its history and can continue the process.

A high-performance approach to rapid digital transformation

Anytime a parent IoT needs to be broken down into 50 or more child transactions, the high-performance approach excels, because it uses bulk, not sequential, data writing. This digital advantage enables thousands of transactions to be written to the database using stored procedures. Using a flexible approach, it can write database actions, parameters, statements, or values with extreme efficiency.

With these high-performance capabilities integrated into a modern MES, it is easy to see how semiconductor companies can accelerate performance to provide secure end-to-end traceability and digitalization to meet the reporting needs of customers and government agencies, comply with SEMI standards, and increase throughput to today’s higher levels of performance.



Secure end-to-end traceability and digitalization makes the difference

With our end-to-end digital solution for semiconductor lifecycle management, you gain the secure end-to-end traceability and digitalization, the real-time visibility of business processes, and the secure collaboration needed across the ecosystem today.

How can semiconductor companies begin the digital transformation to secure end-to-end traceability?

Introducing secure end-to-end traceability in your environment usually begins in three phases:

- First, a Consulting Service Scoping workshop analyzes your process and data flows with the help of a questionnaire which is adapted to your specific needs. Identification of your concrete use case helps to understand how you can make the most of secure traceability in your individual situation. The outcome will be a value stream analysis and a management report comprising the workshop results.

- Next, a Digital Twin Service Creation of a plant simulation model follows with focus on traceability based on the workshop outcomes. After engineering the Digital Twin, the flow of material and information gets visualized. The secure Digital Twin, which is part of the Siemens Xcelerator business platform, is an essential element for understanding whether IC designs have been altered.

- Finally, an Evaluation system helps to connect your Digital Twin to our evaluation system and to show how secure end-to-end traceability is being applied to your specific use cases.

No other company offers a secure end-to-end traceability and digitalization solution for semiconductor lifecycle management.

When you're ready for more information, we're ready to respond.

Watch for our next eBook on Secure Collaboration at siemens.com/l-m-semi

References:

* O'Reilly Media, Inc., Evan Gilman and Doug Barth, "Zero trust networks," July 2017

**Siemens Whitepaper: "Security throughout the semiconductor lifecycle"

About Siemens Digital Industries Software

Siemens Digital Industries Software helps organizations of all sizes digitally transform using software, hardware, and services from the Siemens Xcelerator business platform. Siemens' software and the comprehensive digital twin enable companies to optimize their design, engineering, and manufacturing processes to turn today's ideas into the sustainable products of the future. From chips to entire systems, from product to process, across all industries, Siemens Digital Industries Software is where today meets tomorrow.

For more information on Siemens Digital Industries Software, visit siemens.com or follow us on LinkedIn and Twitter.

Americas: +1 800 498 5351

EMEA: 00 800 70002222

Asia-Pacific: 001 800 03061910