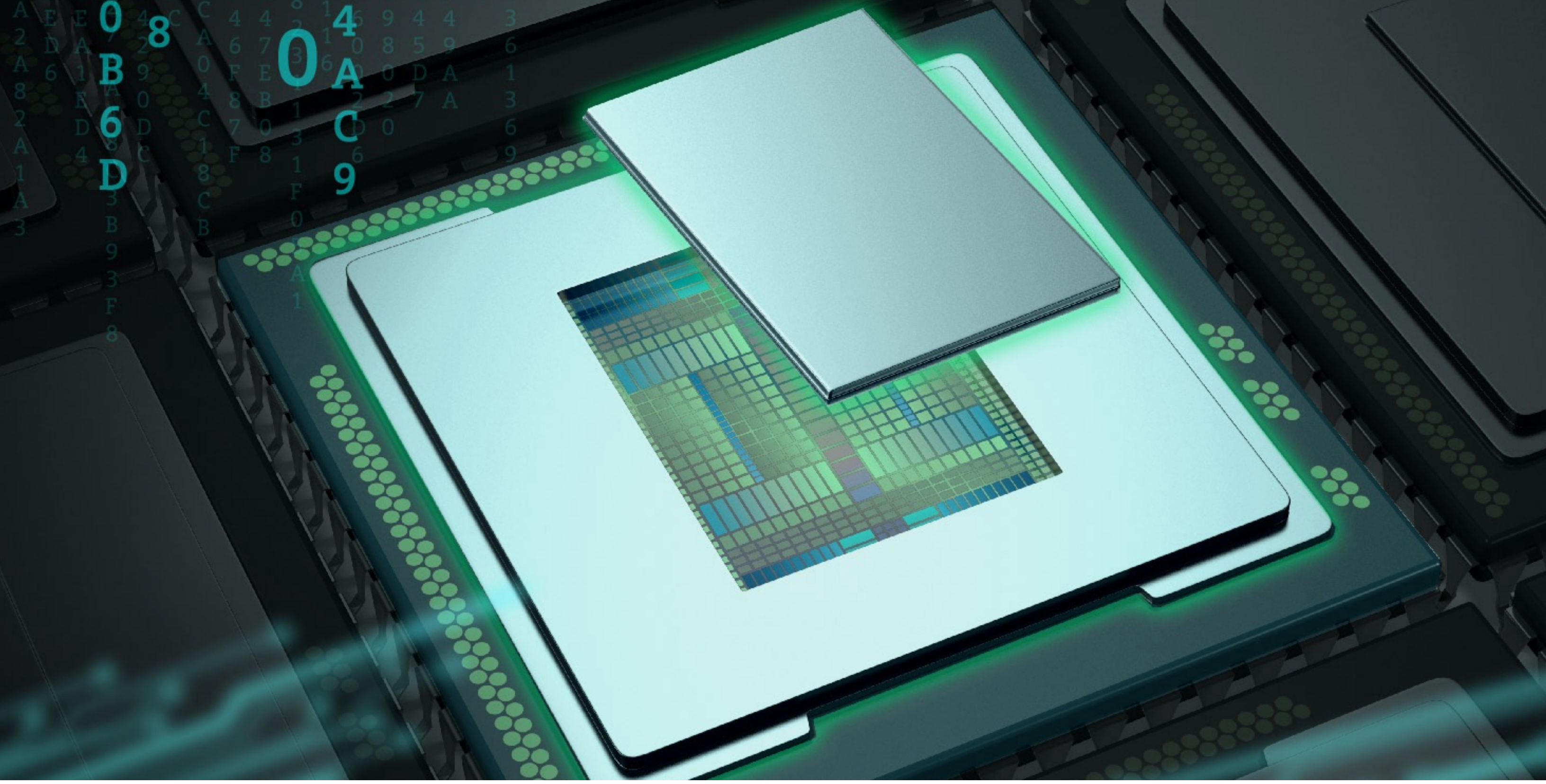


DIGITAL INDUSTRIES SOFTWARE

Security throughout the semiconductor lifecycle

Developing greater supply chain confidence in semiconductors with blockchain

Executive summary

Today's world relies heavily on electronics – so ensuring each chip's authenticity and genealogy is crucial. Siemens' Trusted Traceability initiative brings measurability to all data generated to verify the entire genealogy of a semiconductor is authentic. It is critical to establish trust between all data generators to ensure the as-made product matches the as-designed product. It is also essential to have zero-trust policies enforced by secure solutions that verify the product and terabytes of data generated throughout a semiconductor's lifecycle are authentic. The safest approach is to design in security upfront directly into the semiconductor. Now a confluence of technologies such as high-performance cloud services, internet of things (IoT) devices, smart machines and mobile devices has resulted in the emergence of trusted traceability software solutions.

siemens.com/software

SIEMENS

Introduction

Traceability is not new – genealogy has always been a critical factor for semiconductors, but more counterfeiting, backdoors, malicious code, side channels and cyberattacks have eroded trust. Traceability means following a path backward from the device's current point to where it began. An example of this would include someone who supplied a device to an original equipment manufacturer (OEM). Another example is where a particular die came from on the wafer – so this starts with the fab, using maps.

The objective of traceability is to consider a few key factors:

- Determine if the device is genuine
- Determine if it is built as designed
- Ensure the designs are intact and haven't been tampered with
- Decide where it came from and where it was going to end up

Particularly as more products become smart or autonomous, the consequences of a device failure can be life-threatening. Critical applications in defense, aircraft, vehicles, medical devices, industrial equipment and IoT feed all activities. Even smartphone chip failures can be fatal because they are used for new purposes such as health monitoring. This white paper discusses how the Siemens Digital Industries Software's secure digital twin can be used to create a Trusted Traceability solution that was not previously possible.

The trust imperative

The secure digital twin, which is part of the Siemens Xcelerator digital business platform, is an essential element for understanding whether designs have been altered. Trusted traceability can be used if the traceable items in question are ideas, raw material lots, designs, a box of intermediate materials, validated bill-of-materials (BOMs) or packaged products.

Trusted traceability for the entire semiconductor lifecycle

Trusted traceability collects links, stores and protects data about a product from any system along the value chain.

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

Defense demands

All members of the supply chain are data generators that contribute to traceability. Trusted traceability must be used to access and verify all transactions, for all data generators throughout all tiers of the supply chain. A tier-one integrator, often a product OEM, has the responsibility to determine if a device is genuine, built as designed and the integrity of designs are intact to accept it.

The U.S. Department of Defense (DoD) is a significant customer driving the need to improve traceability across the semiconductor industry. The DoD National Defense Authorization Act (NDAA)[1] Section 224 is a standard that requires defense microelectronics products to meet trusted supply chain and operational security standards by January 1, 2023. It defines:

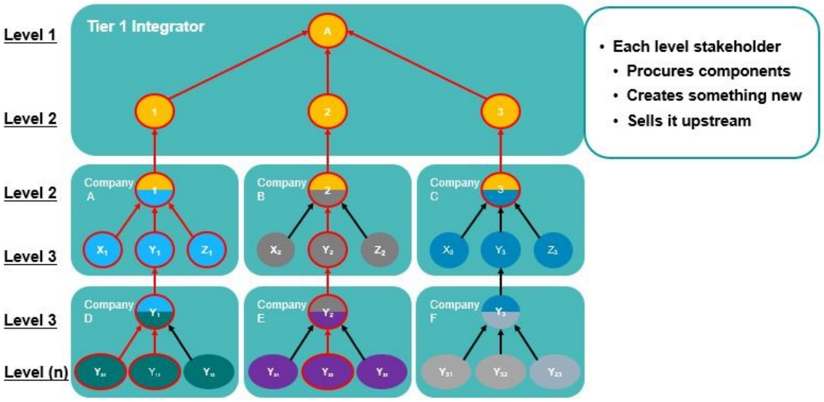
- Manufacturing location
- Company ownership details
- Workforce composition
- Access during manufacturing, suppliers design, sourcing, manufacturing, packaging and distribution processes (audit)
- Reliability of the supply chain
- Other matters pertinent to supply chain and operational security

To enable trusted traceability, gathering and analyzing data is imperative. DoD NDAA title 49 stipulates,[2] “Measurably secure semiconductors.” The word measurably is vital. To measure something requires gathering and comparing data to a governance standard such as a performance specification, stage-gate milestone criteria or behavioral characteristics such as thermal and radio emissions.

Commercial customer needs

Such defense industry requirements often stimulate commercial companies to change their supplier expectations as well. Once OEMs in other segments recognize their semiconductor suppliers have implemented such traceability measures for their defense customers, they will also expect them.

This spread is virtually inevitable. Approximately 85 percent of the DoD product content relies on outside commercial suppliers/subcontractors,[2] many of them small or medium businesses (SMBs). The DoD now requires its suppliers to achieve the Cybersecurity Maturity Model Certification (CMMC) for information systems. Semiconductor companies must get serious about attaining measurable traceability.



- Each level stakeholder
  - Procures components
  - Creates something new
  - Sells it upstream

Figure 1. Trusted traceability brings measurability to all tiers of the supply chain.

Commercial risk example

Amazon’s due diligence of a potential acquisition target,[3] Elemental Technologies, found a tiny microchip, not much bigger than a grain of rice, that wasn’t part of the video compression board’s original design. They used the radio-enhanced chip to infiltrate top U.S. companies and military networks. Until that discovery, Elemental Technologies looked utterly trustworthy. They had national security clearances and high-profile applications in streaming the Olympic Games, communicating with the International Space Station (ISS) and providing the Central Intelligence Agency (CIA) with drone footage.

Increased industry risk

A semiconductor company may have more than 16,000 suppliers worldwide, making traceability difficult. If all aspects of the semiconductor product life cycle are virtual, it makes product design information even more vulnerable to a cyber-attack. Sophisticated hackers are individuals that can potentially inspire organizations with specialized functions and teams. It poses a significant risk to design integrity, leading to counterfeit chips entering the semiconductor supply chain and potentially seeding doubt in the semiconductor industry overall.

> "There are things you can do to improve trusted traceability if you insert blockchain at the outset of design."
>
> John Allgair
> Program Manager, Advanced Systems Integration
> BRIDG

The tenet that "trust starts in silicon" underscores hardware[5] as the root of security upon which software protections are implemented.

Fake chips can range from sophisticated copies of devices to old parts refurbished to look new. In many cases, the devices are unreliable, leaving the OEM in worse shape than if they didn't have an adequate supply of genuine verified chips.

In the distributed and interdependent semiconductor ecosystem, IP owners, original design manufacturers (ODMs), foundries, joint ventures (JVs) and even research labs, each semiconductor device may change hands as many as 15 times, according to an IDC Manufacturing Insights report.[4]

New products, methods and applications are the lifeblood of industry growth. At the same time, they introduce unknown risks and opportunities for both bad actors and inadvertent errors. Similarly, globalization has drastically reduced industry costs and opened many windows of opportunity for attackers to maliciously modify hardware, firmware, or software without the knowledge of ODMs or their customers.

Design and IP

The complex ecosystem supporting semiconductor development allows best-in-class niche companies and individual subject matter experts (SMEs) to collaborate on designs in ways that was not possible until recently. This also presents opportunities for the design network to be penetrated by outsiders.

Semiconductor designs and corporate IP may be corrupted in various ways, at multiple stages and by different rogue actors throughout the lifecycle journey. Typical semiconductor lifecycle stages and examples of associated risks within each step are:

- Concept: Insider threat
- Formal design: Insider threat, design tools, third-party plugins, network hack
- Integration: Insider threat, malicious hardware/ firmware, design alteration

- Fabrication: Insider threat, trojan circuitry/components, design alteration
- Testing: Insider threat, alteration of test results, component replacement
- Provisioning/configuring: Insider threat, insecure values, improper settings
- Deployment: Insider threat, alteration in transit, alteration of firmware

As you can see from this list, insider threats are a common and recurring risk throughout the lifecycle, indicating unauthorized employee tampering poses the most common risk. Individual spies within a design team, independent partner companies, or sourced third-party software plugins may conduct industrial espionage. Attacks may also come from within the network due to security breaches that allow malicious yet initially dormant, intelligent software to reside within a design.

Procurement and production

The unexpected surge in consumer demand in all product categories has led to chronic shortages throughout the supply chain. Some OEMs are faced with booming demand for their products but hampered by inadequate supply. They are seeking elemental semiconductors (new and refurbished) from unverified suppliers.

"What's worse than a chip shortage? Buying fake ones."

"It is a very difficult thing to totally remove the risk of counterfeit parts in an efficient and cheap way," says Ian Walker, operations director, Princeps Electronics Ltd, U.K.[6]

Semiconductor manufacturers switch fabs to optimize capacity and throughput. Each fab may use different names and stock-keeping units (SKUs) for the identical component. Consequently, final product manufacturers must rely on specifications rather than SKUs or names to verify design integrity. The opportunity for counterfeit components that meet the spec to enter the supply chain is a serious issue. Older fabs, with more mature robust security systems, are less vulnerable. However, the chips they make (20nm-30nm) are not adequate to run specific electronic subsystems found in many of today's DoD and commercial products.

Maintenance and repair

Products with long lifecycles such as aircrafts, automobiles, process plant, industrial machinery, industrial air conditioning/cleanroom systems, and semiconductor fab equipment) have regular scheduled and unscheduled maintenance. This makes them vulnerable to counterfeit components entering the product through maintenance service providers.

In contrast, products with short lifecycles such as personal computers, smartphones and webcams are commonly repaired rather than maintained. Repairs make these products vulnerable to counterfeit components. The sourcing department might use a verified supplier who innocently sourced their inventory from the open market, believing it genuine. An independent repair service center also presents a risk.

Irrespective of whether the products have long or short lifecycles are maintained or repaired, there is the risk of unverified components entering. In-use repairs are another opportunity for components that weren't part of the original design to come into use.

> "Every step of fabrication, assembly and test that is not fully automated poses a significant risk. "Dicing and assembly have lots of risks – especially with humans in the loop."

John Allgair
Program Manager, Advanced Systems Integration
BRIDG

Zero trust relationships

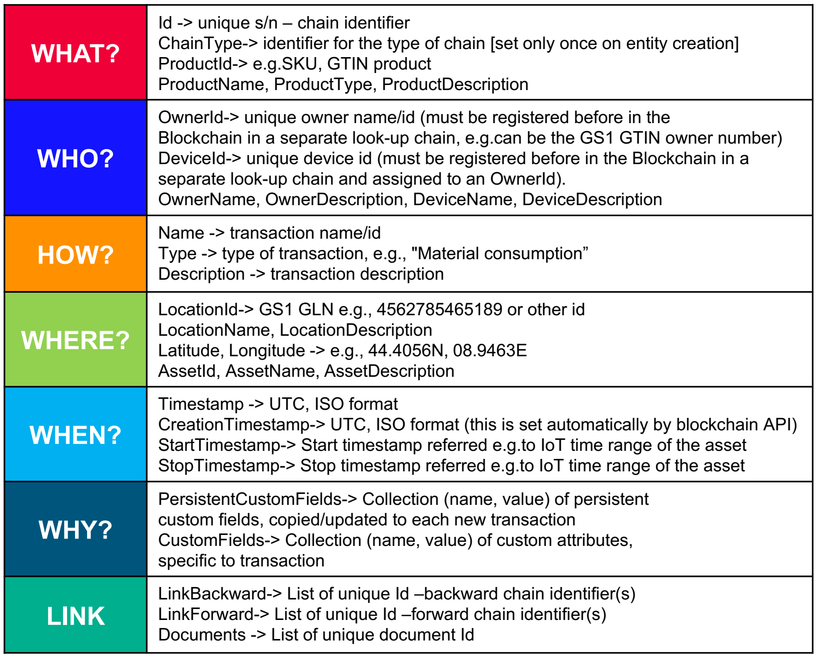
Always verify is the foundation of zero-trust. For example, to participate in a blockchain or distributed ledger such as an online payment system, you need to provide your banking information and get a wallet. In the semiconductor industry, the verification happens with every transaction.

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.[7]

There are three critical components[7] in a zero-trust network: user/application authentication, device authentication and trust. The first component has some duality in it because users do not take all actions.

Blockchain transaction interface



WHAT?	Id -> unique s/n – chain identifier ChainType-> identifier for the type of chain [set only once on entity creation] ProductId-> e.g.SKU, GTIN product ProductName, ProductType, ProductDescription
WHO?	OwnerId-> unique owner name/id (must be registered before in the Blockchain in a separate look-up chain, e.g.can be the GS1 GTIN owner number) DeviceId-> unique device id (must be registered before in the Blockchain in a separate look-up chain and assigned to an OwnerId). OwnerName, OwnerDescription, DeviceName, DeviceDescription
HOW?	Name -> transaction name/id Type -> type of transaction, e.g., "Material consumption" Description -> transaction description
WHERE?	LocationId-> GS1 GLN e.g., 4562785465189 or other id LocationName, LocationDescription Latitude, Longitude -> e.g., 44.4056N, 08.9463E AssetId, AssetName, AssetDescription
WHEN?	Timestamp -> UTC, ISO format CreationTimestamp-> UTC, ISO format (this is set automatically by blockchain API) StartTimestamp-> Start timestamp referred e.g.to IoT time range of the asset StopTimestamp-> Stop timestamp referred e.g.to IoT time range of the asset
WHY?	PersistentCustomFields-> Collection (name, value) of persistent custom fields, copied/updated to each new transaction CustomFields-> Collection (name, value) of custom attributes, specific to transaction
LINK	LinkBackward-> List of unique Id –backward chain identifier(s) LinkForward-> List of unique Id –forward chain identifier(s) Documents -> List of unique document Id

Figure 2. Knowing what, who, how, where, when and why across the supply chain and lifecycle brings provenance.

The user/application component duality means we must look at the qualities of the application in the same way that we would typically look at the qualities of a user.

Using a trust score, the application,[7] device and score are bonded to form an agent. Then, the system applies a policy against the agent to authorize the request. If the request is approved, the control plane signals the data plane to accept the incoming request.

Additionally, assuming systems and traffic within a data center can be trusted is flawed and outdated. Modern networks and usage patterns[7] no longer indicate those where perimeter defense makes sense. As a result, moving freely within a secure infrastructure is frequently trivial once a single host or link there has been compromised.

Managing large zero-trust networks of data generators creates enormous volumes of data distributed throughout data pools or silos. This environment is ideal for blockchain or distributed ledger technology.

The rise of distributed ledger

The need for trusted traceability in finance and supply chain drove the development of distributed ledger technology. Blockchain is a common and well-developed organizational system that is most valuable as a distributed ledger.

Essential operational security for a distributed ledger such as blockchain must verify every transaction from all data generators throughout the network. The distributed ledger should address:

- Unique product ID such as SKU or part number
- Unique owner name
- Unique device ID
- Transaction type and name
- Location name, description
- Target machine ID
- Quantity
- Timestamp
- Start/stop

Trusted traceability in other industries

The semiconductor industry is one of many industries requiring secure traceability. Here are some other common examples.

As automated point-of-sale and internet sale transactions continue to grow, secure payment methods have evolved to address double-entry accounting[8] and centralized processing weaknesses. Cryptocurrencies like Bitcoin or Ethereum, and the blockchain technology that powers them, make it possible to transfer value (currency) online without the need for a middleman like a bank or credit card company.

Coffee, a drink enjoyed around the world, has been found to contain contaminants[9] like ochratoxin A, acrylamide, hydrocarbons, yeast, pesticides and mold. It is often grown in developing countries like Colombia, Brazil, Vietnam and Ethiopia, which may not conform to the destination market's regulations. Additionally, the long transportation and storage journey from plantation to consumer market is often unregulated.

Many parents feed their precious child baby food purchased from a local grocery store. A recent study[10] of 168 baby foods commissioned by Healthy Babies Bright Futures (HBBF) found toxic heavy metals in 95 percent of containers tested. One in four baby foods were contaminated with all four metals assessed by a testing lab: arsenic, lead, cadmium and mercury.

Semiconductor industry blockchain needs

For semiconductors, IP traceability is as crucial as traceability of the physical product. That's because the physical device is the outcome of a long, complex system of digital processes and transactions. The design tools that complete the design and manufacturing processes are all digital and contain substantial

Trusted supply chain data layer

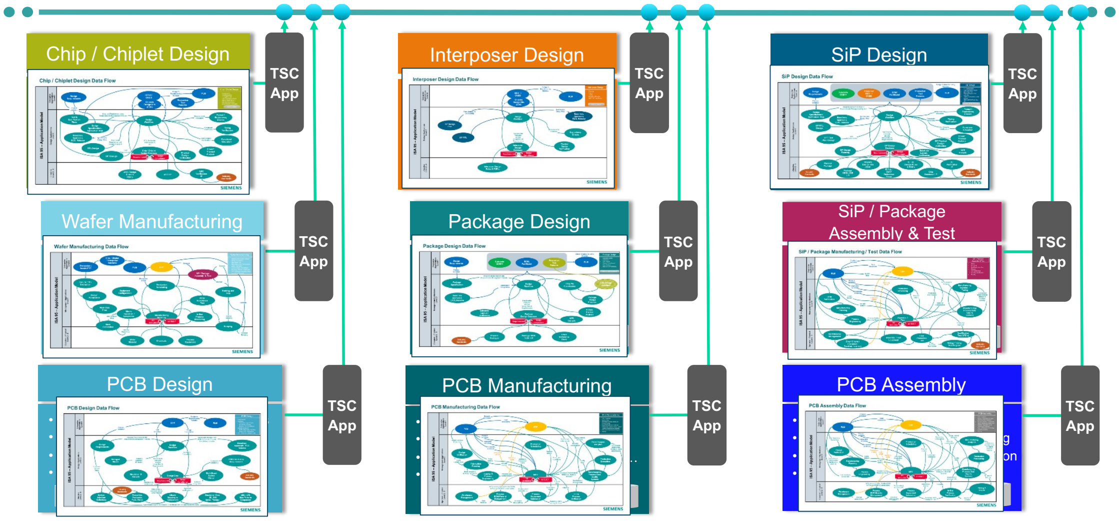


Figure 3. Lifecycle concept for a trusted supply chain solution.

amounts of corporate IP. Blockchain can protect corporate IP contained in large volumes of digital transactions that describe the semiconductor.

However, not all semiconductor data should be contained in the blockchain. Data generated throughout the vast semiconductor ecosystem, where numerous specialized actions generate data, make it impractical to capture every event. Typically, companies will only select critical elements from stage gates or when there isn't a system of record to store in the blockchain. For the remaining data, they will store only links or pointers to indicate the source data location.

Why the semiconductor industry must act now

Today's connected world relies on semiconductor traceability for its smart devices to perform as designed reliably for our convenience, efficiency and safety.

Although most counterfeit components have a negligible effect, one in five either reduces performance or appears as a random or evident failure. The five percent that is evident or random account for over 30 percent of product recalls.

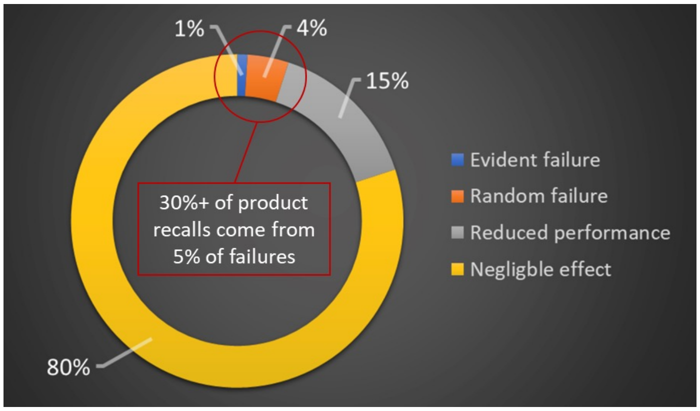


Figure 4. A few counterfeit components can become a large number of final OEM product recalls.

Examples of avoidable problems such as counterfeiting, malicious activity or inadvertent miscommunication involve comparing the as-designed to the as-built, to ensure you are preserving the design intent. Design rule checking (DRC) ensures the designs function correctly, reliably and ensures they are produced with an acceptable yield. It involves checking geometric constraints (design rules) such as physical dimensions, to ensure that you don't violate the rules based on the capability of manufacturing. Layout versus schematic (LVS) is a verification process to determine whether a particular integrated circuit layout corresponds to the original schematic or circuit diagram of the design.

Since the problems and corresponding solutions are vast, companies may feel paralyzed. Given the pressure for authentic chips, is doing nothing an option?

Verifying what, who, how, where, when and why is imperative to achieve verifiable, measurable trusted traceability across the supply chain and lifecycle. Trusted traceability means verifying all transactions between all involved data generators. That enormous scope is a daunting prospect. However, investing more in blockchain-enabled security systems rather than in redundant audits saves time and reduces risk.

Despite the scale of the challenge, it is possible to take an incremental approach. By focusing on critical aspects through lifecycle management working through challenges in phases based on business priorities, all parties gain confidence while addressing zero-trust policies. Key lifecycle stages of implementing trusted traceability are concept, formal design, integration, fabrication, testing, provisioning/configuring and deployment. Start by simulating the parts of your environment with the highest risk while still recognizing that the most common chances are insider threats.

> “Authority is the issue. Governments and commercial OEMs do not have the authority to control every transaction throughout the entire supply chain. The safest long-term approach is to design in security upfront, directly into the semiconductor.”

John Allgair
Program Manager, Advanced Systems Integration
BRIDG

Starting a project to achieve trusted traceability can help to move the entire industry forward. How? By helping set requirements for the one element currently missing: a standard for interoperability across the entire federated supply chain. The standard will focus on data in context and ability to create checksums to validate across multiple companies' blockchains and the pointers to their data in them. Companies using blockchain internally will be the first movers with experience to help shape this cross-industry move to blockchain interoperability standards.

There is an emerging solution set that will provide deeper assurances on device genealogy. This solution also enables companies to work with U.S. DoD and commercial suppliers requiring trusted traceability. A blockchain-based trusted traceability solution provides visibility into the end-to-end semiconductor lifecycle, revealing its complete genealogy by constantly gathering data and measuring all data generators.

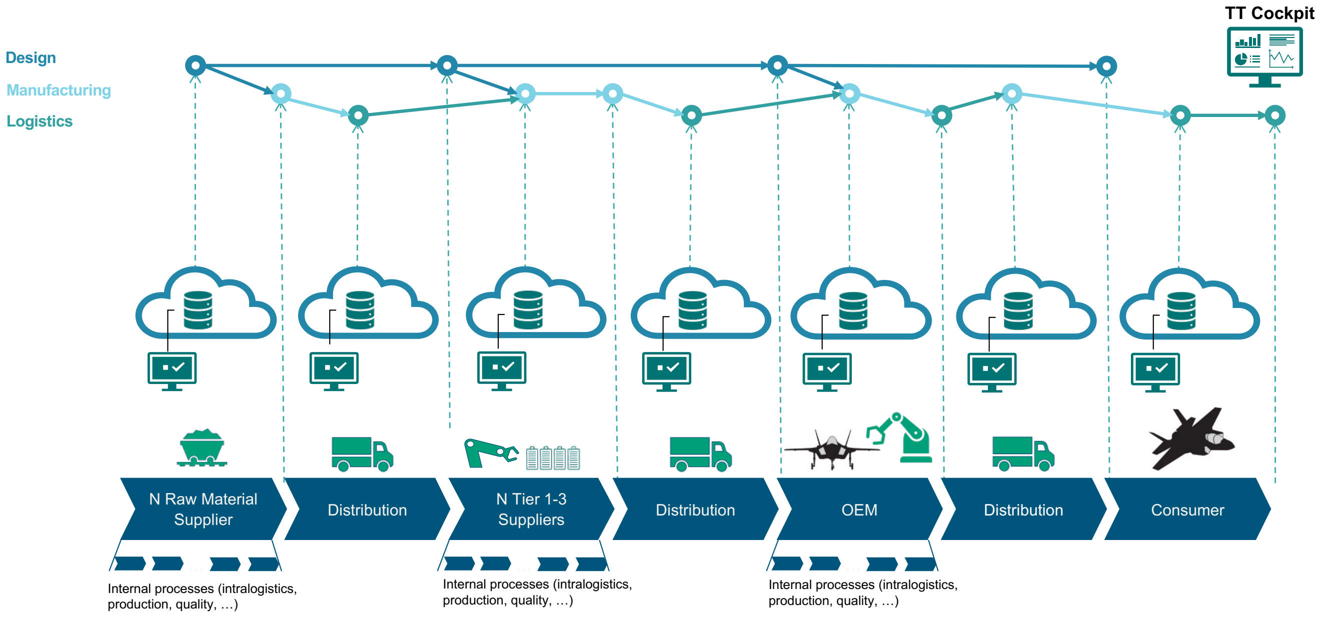

TT Cockpit
Design
Manufacturing
Logistics
N Raw Material Supplier
Distribution
N Tier 1-3 Suppliers
Distribution
OEM
Distribution
Consumer
Internal processes (intralogistics, production, quality, …)
Internal processes (intralogistics, production, quality, …)
Internal processes (intralogistics, production, quality, …)

Figure 5. Architecture concept for a trusted supply chain solution.

Conclusion

Trusted traceability software apps monitor transactions of all data generators throughout the supply chain. Siemens' Trusted Traceability solution shows analyzed information through a single supervisory dashboard to ensure as-designed matches as-built.

This Trusted Traceability for a supply chain assurance system does what humans can't do at scale: supervise every transaction between every data generator and report back anomalies for investigation immediately.

Why hasn't this been done before? Because we couldn't. "We haven't had the ability to design an architecture until now to analyze terabytes of data in real-time. Now we do." says Allgair.

References

1. Reed Smith LLP, Liza V. Craig William T. Kirkwood, "2020 NDAA section 224 effort to mitigate supply chain risks," February 5, 2020.
2. The U.S. Department of Defense, "National Defense Authorization Act 'Title 49'"
3. Bloomberg LP, Jordan Robertson and Michael Riley, "The big hack: how China used a tiny chip to infiltrate U.S. companies," October 4, 2018.
4. IDC Manufacturing Insights Report
5. Edlyn V. Levine, The Die is Cast" Communications of the ACM Vol. 64 No. 1, Pages 56-60, January 2021.
6. The Wall Street Journal, "What's worse than a chip shortage? Buying fake ones," July 15, 2021.
7. O'Reilly Media, Inc., Evan Gilman and Doug Barth, "Zero trust networks," July 2017.
8. Wikipedia, "Double-entry bookkeeping," December 2013
9. Healthline Media, a red Ventures Company, Kris Gunnars, "Mycotoxins myth: The truth about mold in coffee," January 28, 2019.
10. Healthy Babies Bright Futures (HBBF), Jane Houlihan and Charlotte Brody, "What's in my baby's food?," October 2019

Siemens Digital Industries Software

Americas: 1 800 498 5351

EMEA: 00 800 70002222

Asia-Pacific: 001 800 03061910

For additional numbers, click here.

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 – Accelerating transformation.

siemens.com/software