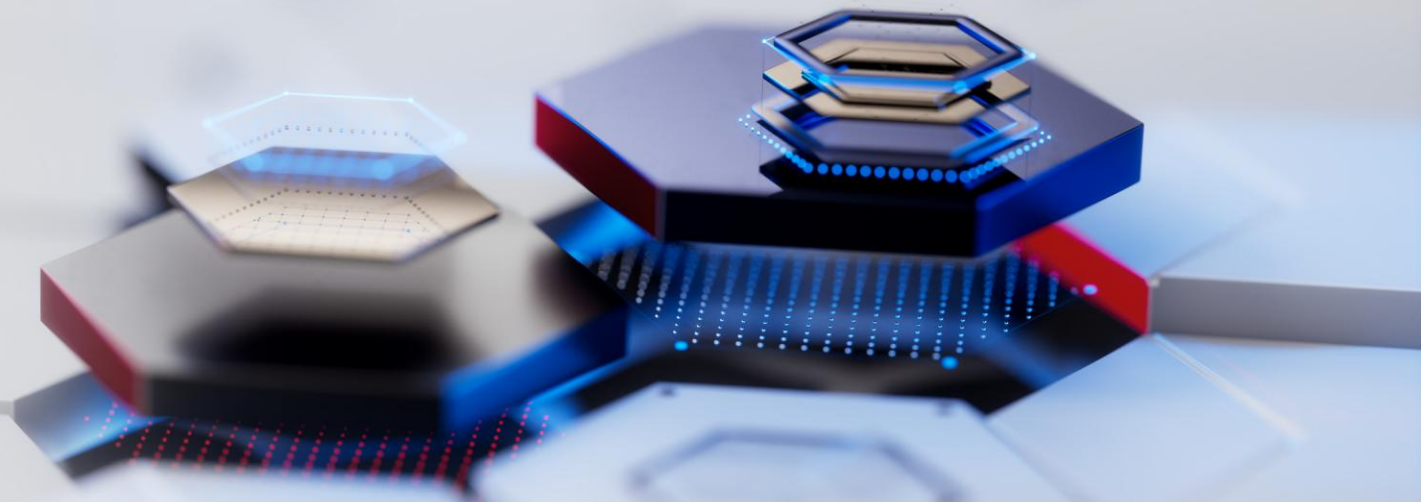
cadence®

SECURE-IC
THE SECURITY SCIENCE COMPANY

Securing Chiplet-Based AI Designs: Enabling End-to-End Protection in Modular Architectures



BRICE GAIGNOUX, FIELD APPLICATION ENGINEER

Agenda

01 Introduction - Secure-IC
The embedded security one-stop-shop

02 Understanding chiplet momentum
Market needs and design journeys

03 Accelerating SoC design in physical AI

04 Secure-IC SiP protection and secure boot

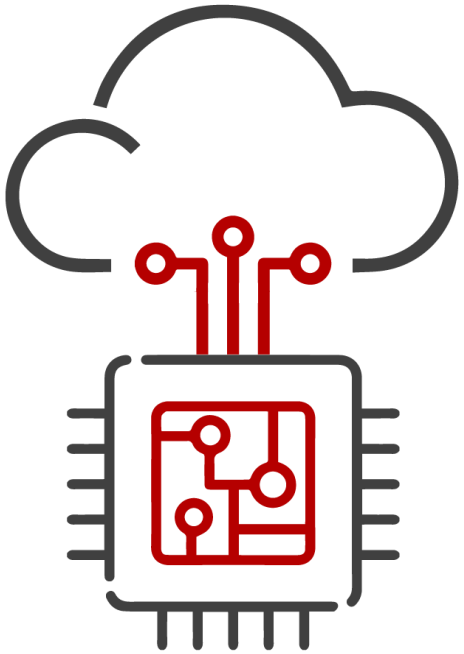
A GLOBAL LEADER IN EMBEDDED SECURITY

IoT devices being interconnected, **each and every object could be a threat for the whole network.**

Therefore, the **security of the objects or the devices with their lifecycle management is key**, and so is their data. To ensure the integrity of this data, the whole system must be secured and managed. **Trusted devices enable trusted data**.

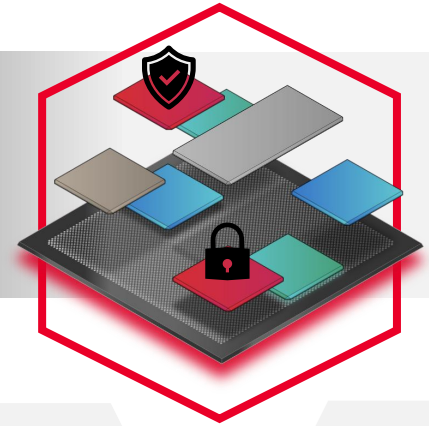
Secure-IC partners with its clients to provide them with the best end-to-end cybersecurity solutions for embedded systems and connected objects, **from Chip to Cloud**

ONE DAY, SECURITY WILL BE WORTH MORE THAN THE DEVICES



END-TO-END EMBEDDED CYBERSECURITY SOLUTIONS

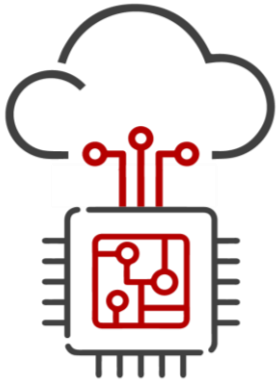
cadence® & SECURE-IC



CADENCE ANNOUNCED THE ACQUISITION OF SECURE-IC

A Leader in Embedded Security IP

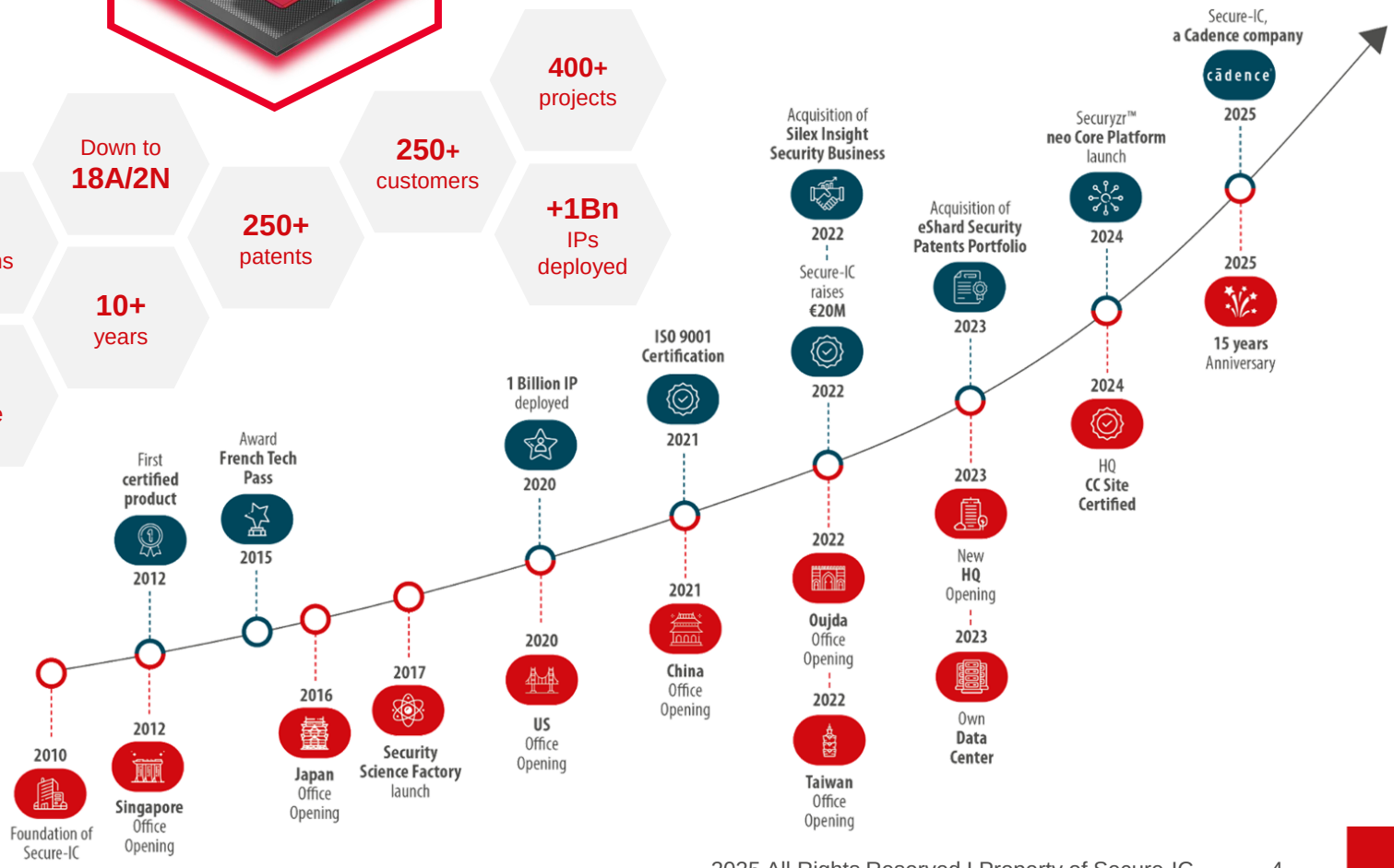
ONE DAY, SECURITY WILL BE WORTH MORE THAN THE DEVICES



PQC Post-Quantum Cryptography READY

THE ONE-STOP-SHOP FOR ALL YOUR EMBEDDED SECURITY NEEDS

- **9** locations
- Down to **18A/2N**
- **250+** patents
- **250+** customers
- **400+** projects
- **10+** years
- **150** people
- **+1Bn** IPs deployed

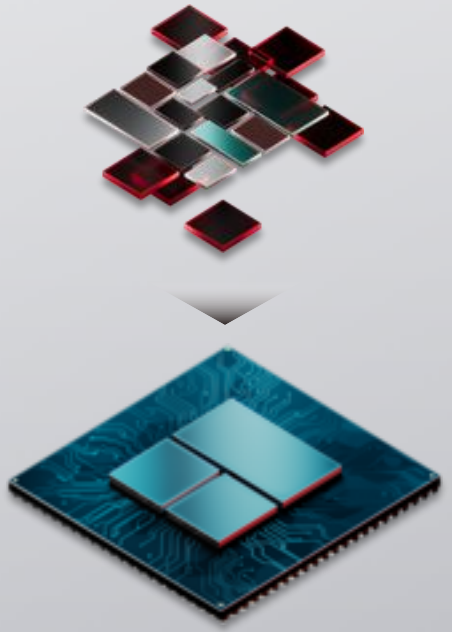


Industry Trends
Driving Growth in Semiconductor TAM

Disaggregation

2,4,6,8 CCD variant SKUs
(CCD – Core Chiplet Die)

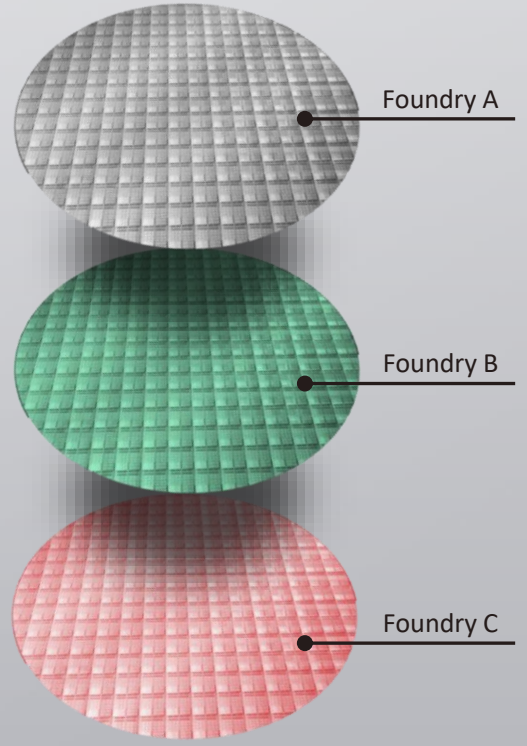
From IP to Solutions



Silicon Customization

TPUs | NPUs
DPUs | CPUs

Supply Chain Resilience



Physical AI Systems
The next evolution in the AI journey

Autonomous Vehicles

Drones

Robotics

Aerospace & Defense

What Customers Tell Us They Want in Their Next-Gen Designs

Cost efficiency – systems optimized for their needs

- Limited ability to optimize price efficiency in monolithic systems

Time to market speed for new solutions

- Today's distributed SoC model slows them down
- Using same process node for all IPs = long design/redesign cycles

Simplified software development

- Current distributed solutions lead to very complex SW development
- In some cases, each component has their dedicated SW

Reference Platform

- A chiplet framework to accelerate design efforts

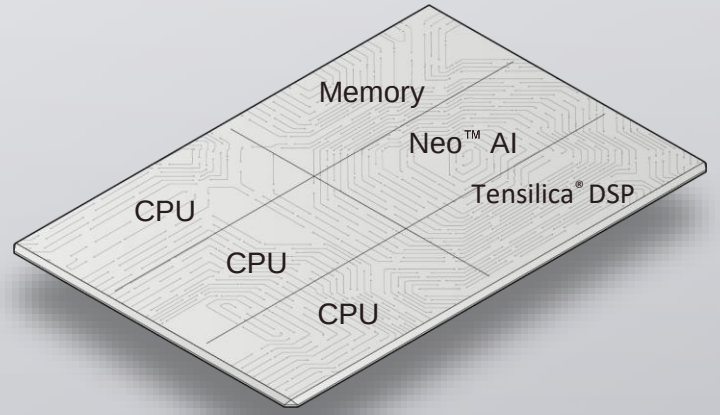
The Journey of an SoC Designer

Enginers seek to reduce development time and engineering costs

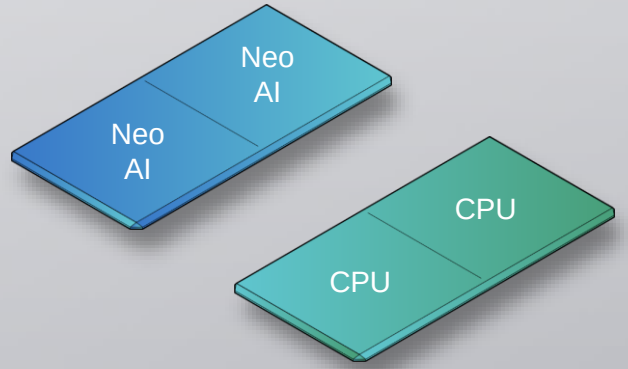
Heterogeneous SoCs:
IP Integration with some specialization

Designers look for ways to build bigger, faster, and cheaper

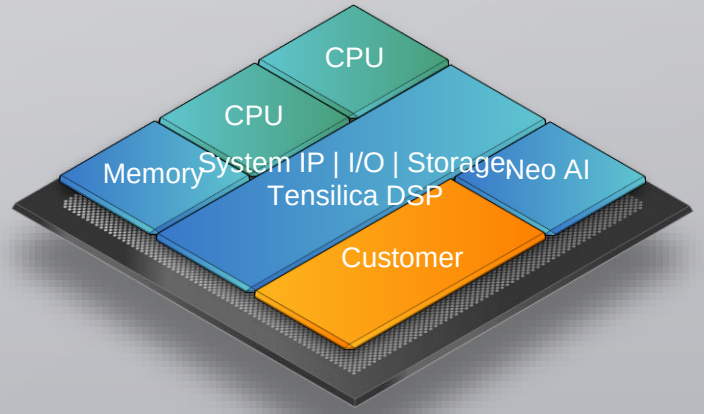
Monolithic Die SoC
Maximize Integration



Multi-Die SoC
Maximize Die Area



Heterogeneous Chiplet System
Extreme Specialization



Representative architectural diagrams. Not drawn to scale.

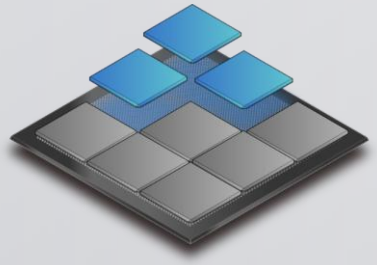
The 4 Cs of Chiplets

Addressing engineering and business challenges

Helping customers realize their chiplet ambitions

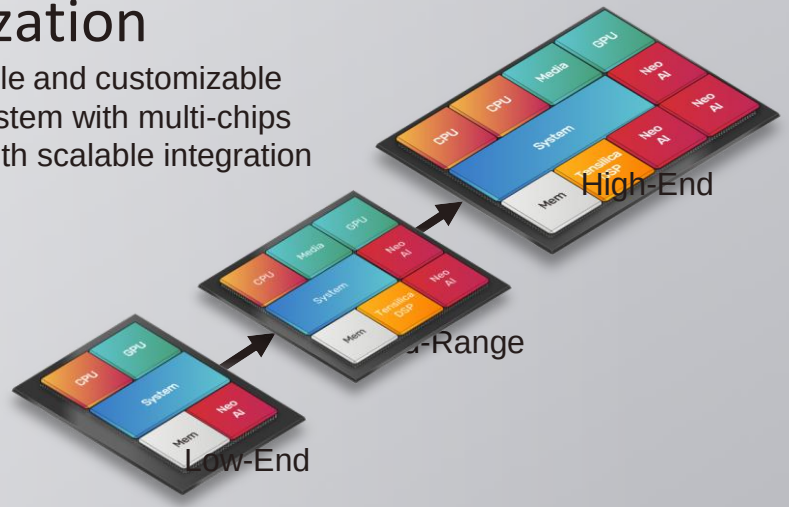
Cost Efficiency

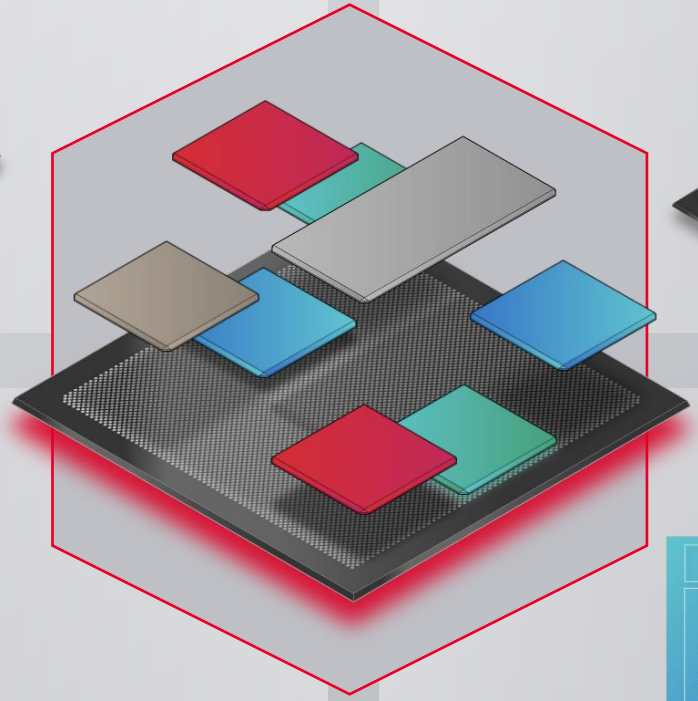
Reduced device design time and cost
Focus on your unique value-add
Leverage partners for other product complexities

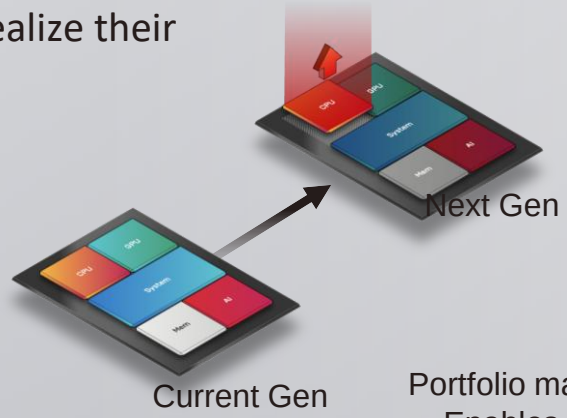


Customization

Modular, scalable and customizable
Enable large system with multi-chips
Chiplet reuse with scalable integration







Configurability

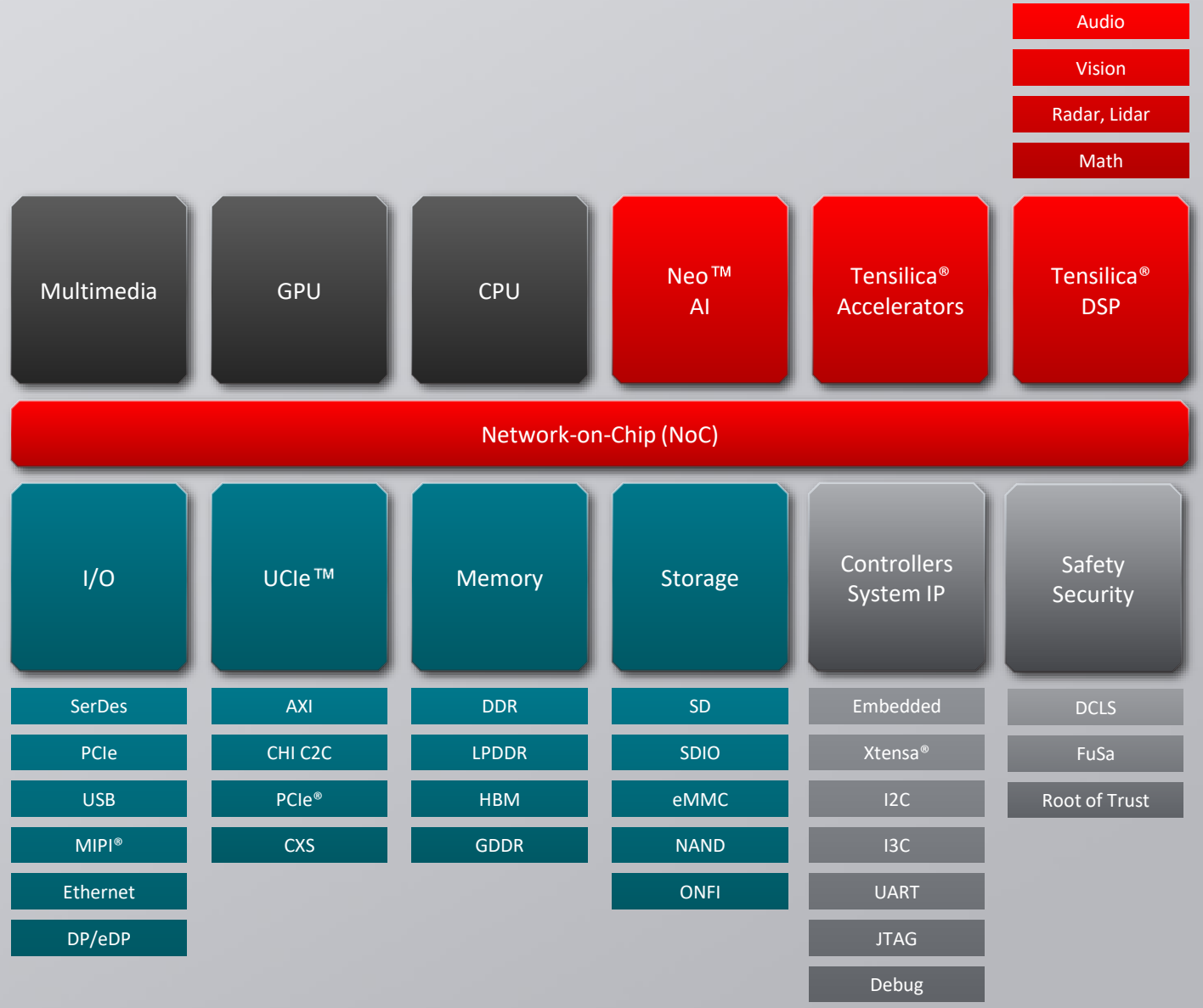
Portfolio management & diversification
Enables greater levels of integration
Chiplet reuse for next-gen products

Cadence Ecosystem

Proven and flexible engagement model
Arm® CSA and UCIe™ standardization
EDA, IP development and design services

Chiplets Require Architectural Sophistication

Delivering a scalable, extendable solution



3rd Party IP

Cadence Compute IP

Cadence Connectivity IP

Cadence System IP

SoC to Chiplet Decomposition

Physical AI Example

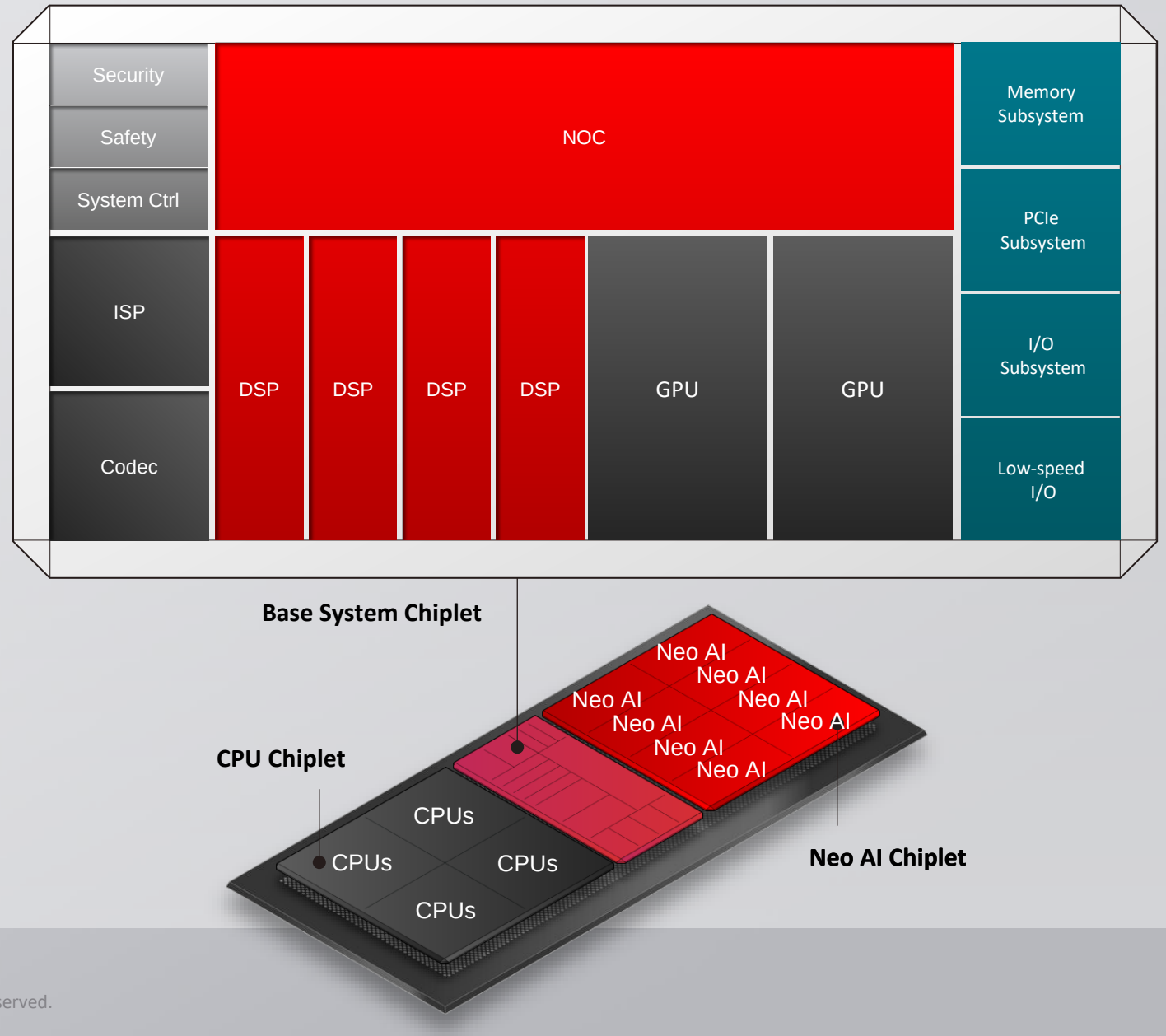
Scalable architecture to support a family of physical AI solutions

- Utilizing Arm® CPU solutions and Cadence® accelerators, memory, and I/O solutions

Using chiplet framework

- Maximizes component reuse
- Minimizes design effort
- Meets the breadth of customer requirements
- Supports Arm Chiplet System Architecture (CSA) and UCIe™ connectivity

Representative architectural diagrams. Not drawn to scale.



Supporting Chiplet Architectures

Chiplet frameworks

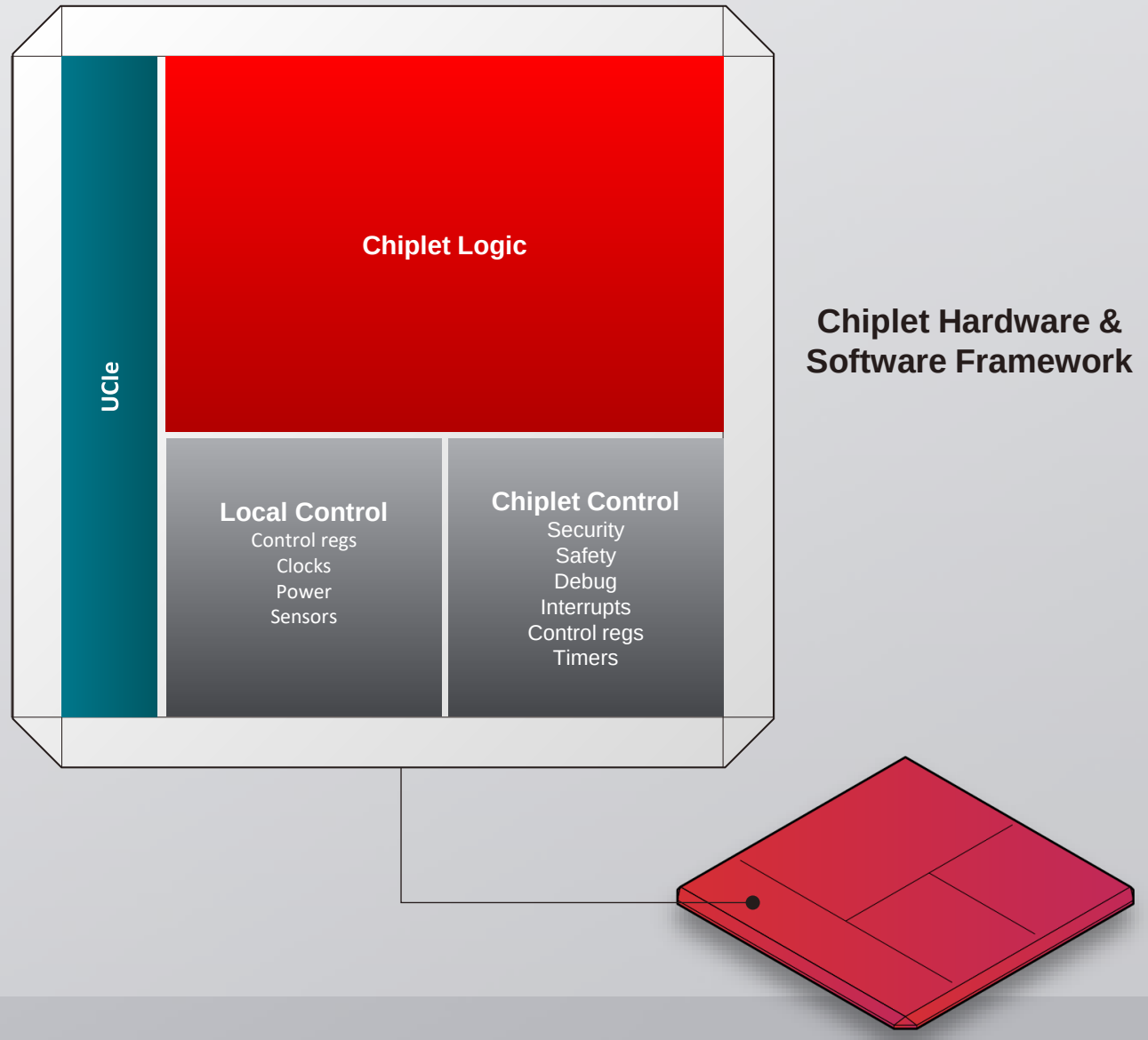
Supporting chip-to-chip behavior across chiplets

- Main interface based on UCIe™ IP
- Security/safety/control interface based on events and I3C interfaces

Spec-based framework to accelerate the design effort

Building out soft IP to enable quick and correct construction of chiplets

Representative architectural diagrams. Not drawn to scale.



Case Study

Focusing on Secure Boot and SiP Protection

Problem Statement

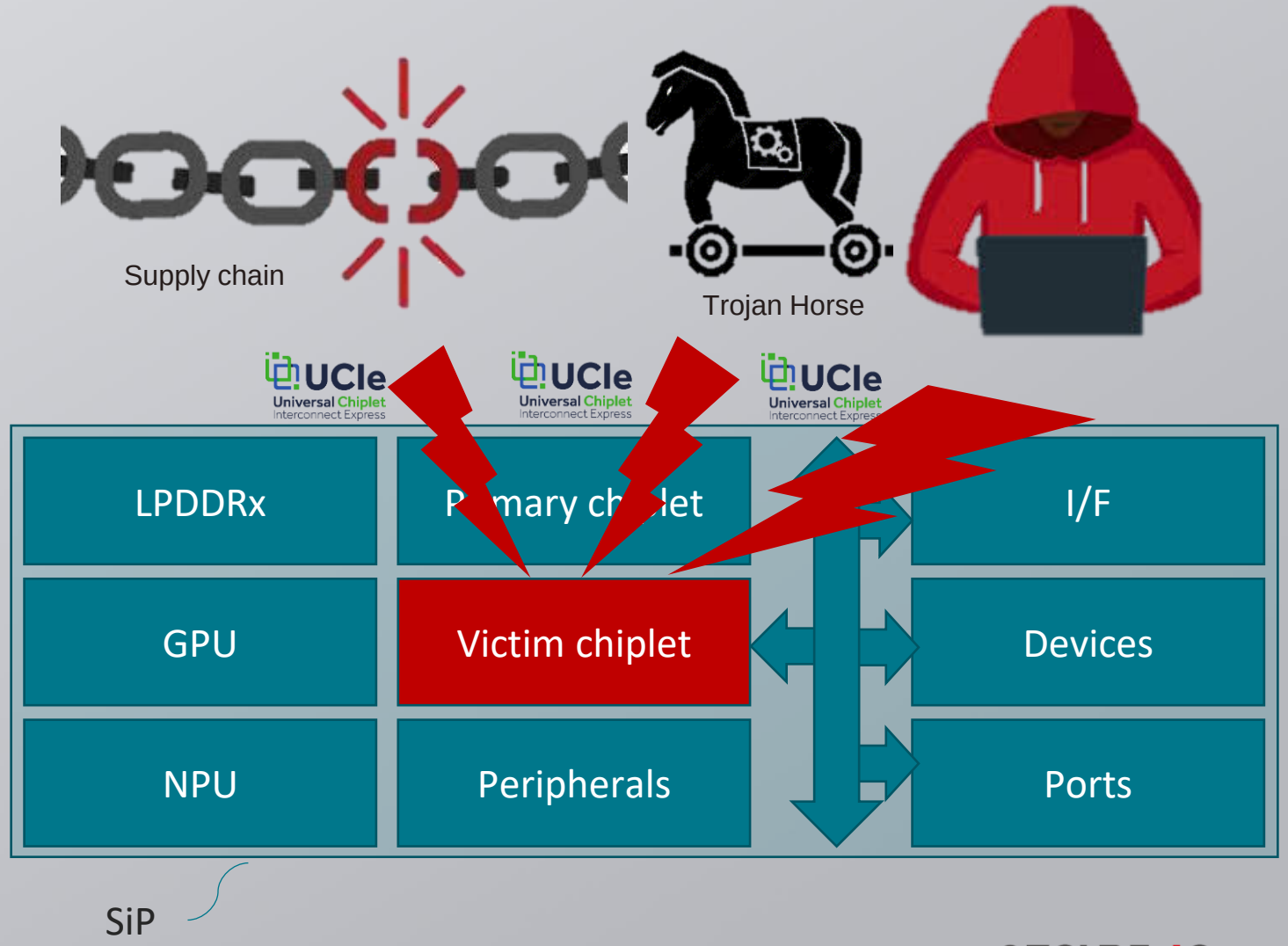
Assets:

- Chiplet integrity and authenticity
- Chiplet security assurance continuity

Threats:

- Rogue chiplet interfering with SiP expected behavior
- Manipulated chiplet through e.g., firmware corruption

Security along the full lifecycle is a prerequisite for chiplet business model



Case Study

Focusing on Secure Boot and SiP Protection

Constraints and requirements

Constraints:

- I/O are limited:
  - Accessibility for provisioning
  - FW loading speed
- **Individual chiplet FLASH-less or streaming boot**
- **SiP-level parallel boot to be orchestrated**
- **Hierarchical trust:**
  - Chiplets authenticate to a primary chiplet
  - Trust aggregation, from individual chiplet to the SiP assembly
  - Each chiplet keeps its independence

- **Security requirements (excerpt):**
  - Chiplets SHALL be secure by default
  - Chiplets SHOULD be owned by default
  - Chiplets SHALL have a trusted ID
  - Chiplets SHALL authenticate cryptographically and have a way to remain secure
  - Chiplets SHALL have an attestation mechanism
  - Chiplets SHALL be able to recover from an in-the-field attack

UCIe Universal Chiplet Interconnect Express

  - UCIe enables interoperability between chiplets
  - How to ensure chiplets are not used as an attack vector?

Case Study: Focusing on Secure Boot and SiP Protection

Leveraged security technologies (hardware + software)

Chiplet Minimum Functions:

Secure-boot:

- Measured firmware
- Trust propagation

Mutual authentication

- Cryptography and key management

Remote attestation – Various flavors:

- TPM (Trusted Platform Module) 2.0
- PSA (Platform Security Architecture)
- DICE (Device Identifier Composition Engine)
- IETF (Internet Engineering Task Force)

Matching with Protection Profile (PP)

Chiplet Configurable Functions:

Post-quantum cryptography

ISO/IEC 20897 PUF:

- For ID and unique per chiplet keys

Anti-tamper:

- To avoid physical hacking

Automotive-grade solution is readily available

- Functional safety (ISO 26262, ASIL B, and D)
- ISO/SAE 21434 to enable UN ECE R.155 and R.156 compliance

Case Study

Focusing on Secure Boot and SiP Protection

Lifecycle

Manufacturing → **Deployment** → **In-field update**

- Each chiplet is initialized.
- Chip & System Manufacturers serialize chiplets and injected their assets (like FW & credentials).
- The «Package Manufacturer» acts as a Certification Authority, and onboards the SiP leveraging a flat or levelled PKI.
- Primary chiplet receives orchestration FW; secondaries receive drivers.

- Upon boot, the primary authenticates secondary chiplets and aggregates their boot statuses.
- This info is certified by the primary chiplet.

- Upon remote request, the primary chiplet launches an attestation.
- It can span across multiple chiplets if the Chain of Trust (CoT) does so.

- Authorized manufacturers (chip, system, package) can push updates/patches leveraging role-based authentication.
- Those are verified upon next reboot.
- A golden imagine is retained, for rollback in case of failure.

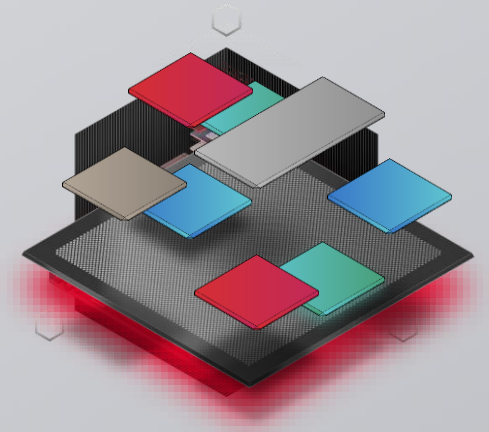
- Aggregated boot & distributed attestation services are back to normal.

Addressing Ever-Increasing Compute Demands in the Physical AI Era

Helping our customers realize their chiplet ambitions

Cadence collaboration with the industry

- arm
- Chiplet System Architecture (CSA)
- AMBA® Chip-to-chip protocols
- Standards Bodies: UCIe Universal Chiplet Interconnect Express, PCI SIG, ULTRA ACCELERATOR LINK, CXL Compute Express Link, Ultra Ethernet, JEDEC



cadence® SoC Design Cockpit

- Build on heritage of design automation
- Enabling Helium™ SW Dev frameworks
- Delivering improved efficiency and TTM

cadence® Implementation

- Arm® + Cadence® IP portfolio
- Cadence EDA tools and flows
- Cadence design and implementation
- Cadence chiplet Framework

Thank You

cadence® | SSG

SECURE-IC
THE SECURITY SCIENCE COMPANY