Cycuity

REQUIREMENTS DEFINITION WITH RADIX

Create comprehensive and verifiable hardware security requirements that surface both known and unknown risks

Most companies developing semiconductors – or products that incorporate them – have existing hardware security practices in place. But the security requirements that these activities are based on often have two key limitations:

1. They focus disproportionately on known risks and fail to account for the unexpected.
2. They aren't easily verifiable as the product development lifecycle advances.

As a result, product development can be derailed and delayed at any stage. Or worse, catastrophic hardware vulnerabilities can find their way into shipped products.

MAKE SECURITY REQUIREMENTS DEVELOPMENT SYSTEMATIC AND MEASURABLE

Cycuity's information flow analysis technology makes it possible to create abstract security requirements that are much more flexible, scalable, and verifiable than traditional approaches. We integrate with your existing design tools and provide a more holistic view of your hardware and software assets and how they interact – including any unexpected behavior.

This allows you to:

- Identify the locations and flows of the assets that need to be protected.
- State clear security objectives for each of these assets.
- Identify protection mechanisms that meet these objectives for each asset.
- Define methods of measuring the efficacy of each protection mechanism.

The output of this process is a compact set of requirements that can be verified in a scalable and automated manner during all phases of product design and development.

BUSINESS IMPACT

Simplify requirements development through abstraction.

Extend coverage to include unexpected risks and behavior.

Ensure that requirements are verifiable at every step of the product life cycle.

Create a foundation for automated requirements verification.

CYCUITY BRINGS SYSTEMATIC HARDWARE VULNERABILITY MANAGEMENT TO EVERY STEP OF THE PRODUCT LIFECYCLE

REQUIREMENTS	VERIFICATION	SIGNOFF
Define comprehensive and verifiable security requirements.	Automate security verification during all phases of chip development.	Make data-driven sign-off decisions backed by complete traceability.