Cycuity

# SECURITY VERIFICATION WITH RADIX

Verify semiconductor security requirements systematically at every stage of design and development

The attack surface of a semiconductor-based product evolves in unpredictable ways as design and development advance from block to system level. Creating comprehensive security requirements is an essential first step. But manual, point-in-time requirements verification is not practical with sophisticated products manufactured in collaboration with multiple supply chain partners. The only way to ensure that your security requirements are met at every step of design and development is by automating your security verification steps and performing them continuously throughout the product lifecycle.

TURN SECURITY REQUIREMENTS INTO ABSTRACT RULES THAT CAN BE VERIFIED THROUGH AUTOMATION

Cycuity's Radix takes the verifiable security requirements created using our information flow analysis technology and turns them into verifiable rules that work with your existing simulation and emulation tools.

Here's how it works:

1. Security requirements are translated into abstract rules that are understandable by stakeholders and easy to manage.
2. Abstract rules are instantiated with your design's register-transfer level (RTL) signals.
3. Radix generates a security monitor from the security rules and RTL signals.
4. The security monitor is added to your existing emulation or simulation workflow.
5. Security violations and information flows through your design are presented in an easy-to-understand interface.

This fully automated approach makes it possible to perform security verification at the block and system levels continuously as your product moves through its lifecycle, ensuring ongoing compliance with security requirements.

## BUSINESS IMPACT

Enhance the detail and accuracy of security verification.

Spot hidden security weaknesses at every stage of the lifecycle.

Visualize the information flows in your design.

Unlock additional value from your simulation and emulation tools.

**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. |

© Cycuity 2022

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. |

© Cycuity 2022

Cycuity

# SECURITY SIGNOFF WITH RADIX

Create a data-driven security signoff process that reduces risk and demonstrates rigor to customers and regulators

One of the most challenging tasks that semiconductor product stakeholders have is making informed decisions about when a design is ready to receive security signoff. Leaders are often forced to decide when a product can proceed to tape-out and chip manufacturing based on incomplete or outdated information – all while balancing competing pressures to meet release timelines and minimize risk. And the same information gaps that bring uncertainty to the signoff process later complicate efforts to demonstrate the completeness and effectiveness of security validation measures to customers, auditors, and regulatory bodies.

## DEMONSTRATE COMPLIANCE WITH INTERNAL AND INDUSTRY-LEVEL SECURITY REQUIREMENTS

Cycuity's Radix brings complete security requirements traceability to your product design and development processes. By establishing clear success metrics for security requirements and verification, Radix keeps stakeholders aligned on measurable success criteria – even as product designs evolve and unexpected developments occur. When signoff checkpoints are reached, decisions about whether security requirements have been satisfied are informed by quantifiable data instead of assumptions and guesswork.

Along with demonstrating fulfillment of internal security requirements, Cycuity's data-driven approach makes it easier to document alignment with industry security standards, such as:

- ISO/SAE 21434: Road vehicles – Cybersecurity engineering
- ISO/IEC 19790: Security requirements for cryptographic modules
- ISO/IEC 15408: Common Criteria

The clear security requirements verification audit trail that Radix provides also makes it easy to demonstrate to customers, partners, and regulators that security rigor has been applied to your product at every step of the design and development lifecycle.

## BUSINESS IMPACT

Remove risk and uncertainty from security signoff.

Ensure that internal security requirements are fulfilled.

Verify compliance with industry security standards.

Provide evidence of security rigor to customers and other interested parties.

**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. |

© Cycuity 2022