

# 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.