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Leaders are often forced to decide when a product can proceed to tape-out and chip manufacturing based on incomplete or outdated information – all while balancing competing pressures to meet release timelines and minimize risk.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.