RADIX

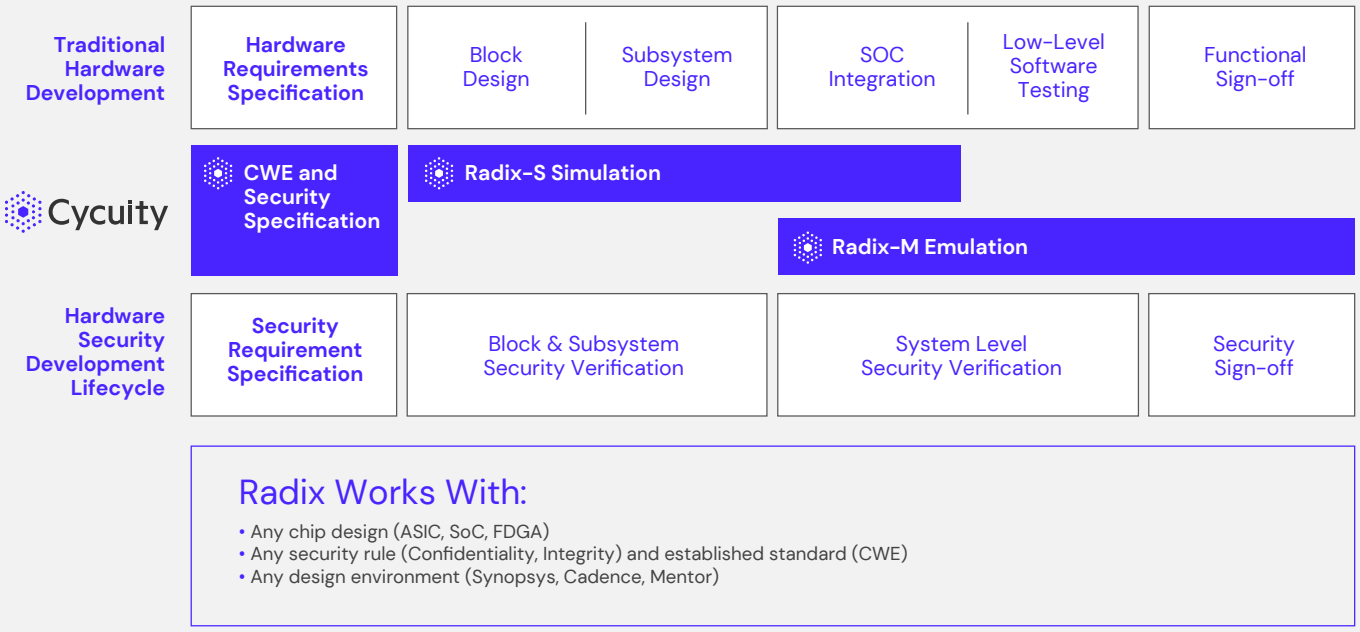
Automated Security Verification

Cycuity

Overview

Cycuity's Radix technology adds systematic hardware vulnerability detection and prevention to existing ASIC, SoC, and FPGA verification methodologies using its comprehensive information flow analysis technology. By bringing more precise and more systematic security practices to every step of the development process, Radix helps security and verification teams identify and isolate security vulnerabilities before the device is manufactured, dramatically improving the efficiency and completeness of the security review process.

SECURITY VERIFICATION IN LOCKSTEP WITH THE DEVELOPMENT LIFECYCLE



Radix Works With:

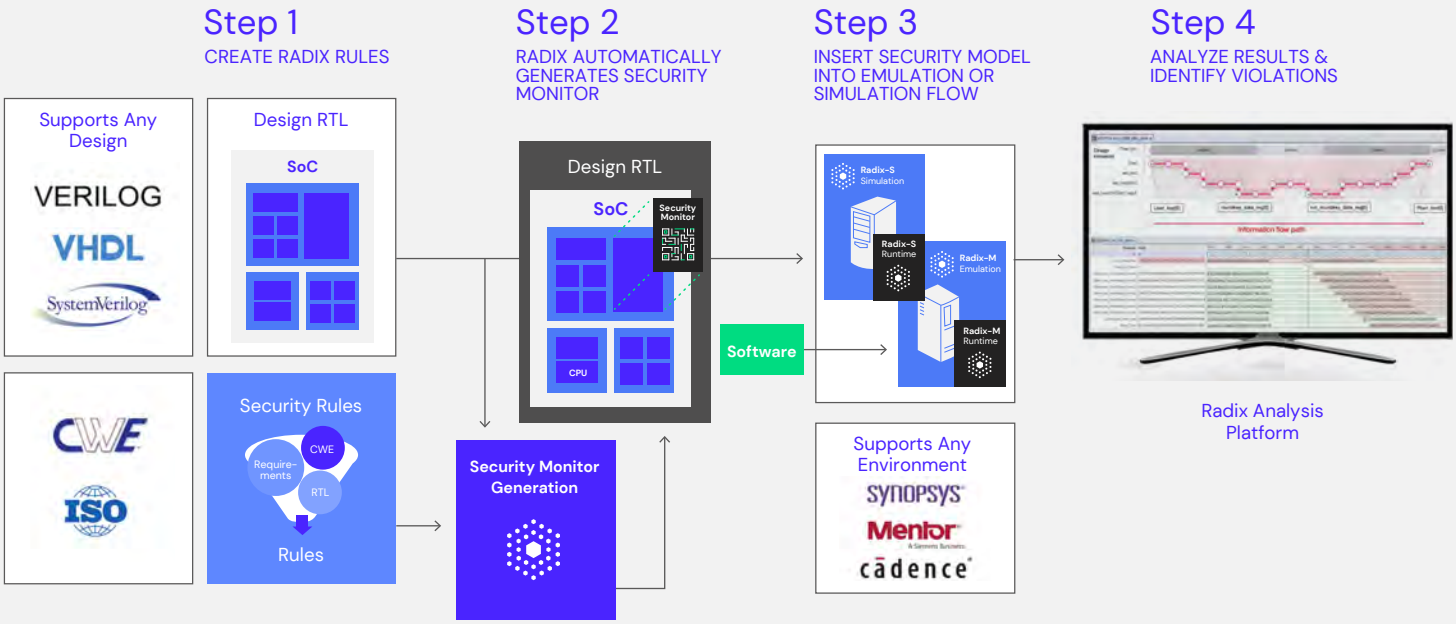
- Any chip design (ASIC, SoC, FDGA)
- Any security rule (Confidentiality, Integrity) and established standard (CWE)
- Any design environment (Synopsys, Cadence, Mentor)

Empower Your Team with Comprehensive Hardware Security Assurance

Radix provides a foundation for a comprehensive security program that fits seamlessly into existing workflows from Cadence, Synopsys, and Siemens EDA. Users have the flexibility to specify security verification rules that capture common security requirements efficiently and effectively. These rules are orders of magnitude more compact than traditional functional assertions and provide significantly broader security coverage. Moreover, their simplicity and expressiveness enable greater collaboration between security experts and hardware designers.

Radix's security rules are translated into a hardware security monitor using patented information flow technology that is added to the design and then run in standard commercial simulators. This unified approach provides scalable security verification covering the entire design lifecycle, from IP blocks to full SoCs running system software.

The inputs to Radix include the System IP or SoC's RTL files, the Radix security rules and the block or system-level testbench files that verification teams are already developing. Radix then creates and adds a hardware Security Monitor to the design. The Security Monitor is used to check **the validity of the security rules while running standard verification testbenches in your choice of simulator**. In addition, **Radix covers 80% of common hardware weaknesses in the Common Weakness Enumeration (CWE) database maintained by MITRE**.



Accelerate comprehension and remediation of security issues with guidance from an easy-to-use analysis engine.

If security vulnerabilities are found, analysis information including custom waveforms and leakage path information helps pinpoint the root cause. The Radix Analysis View displays both signal values and leakage information to identify the source of the vulnerability and the signal values that caused it, providing deeper understanding of security rule violations and assisting in remediation.

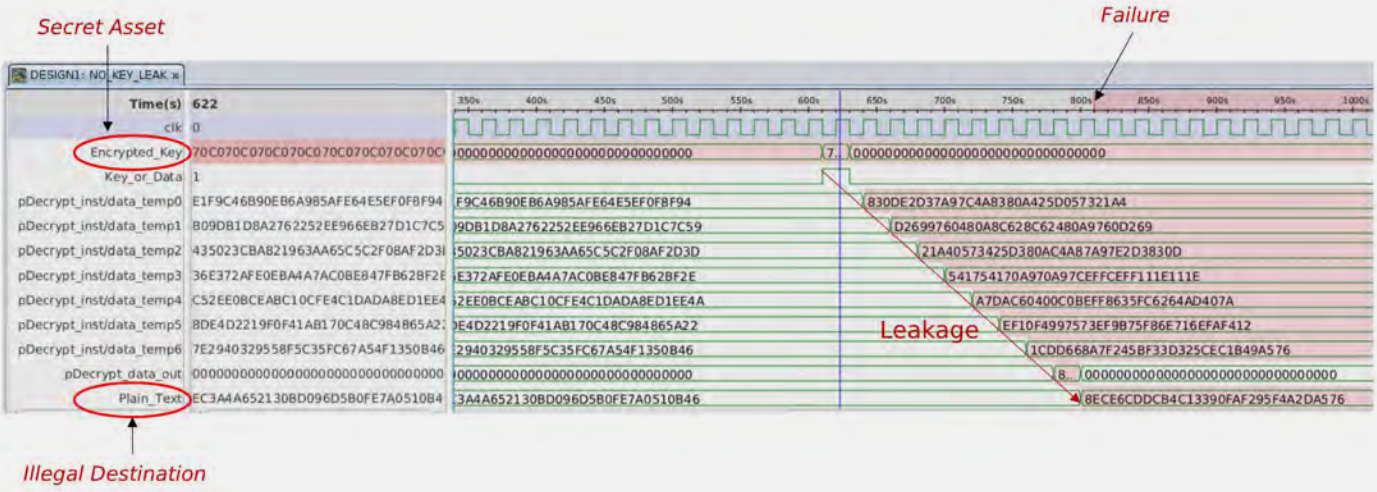


Figure 1: Waveform View illustrates data transformation of secure information leading to its leakage.

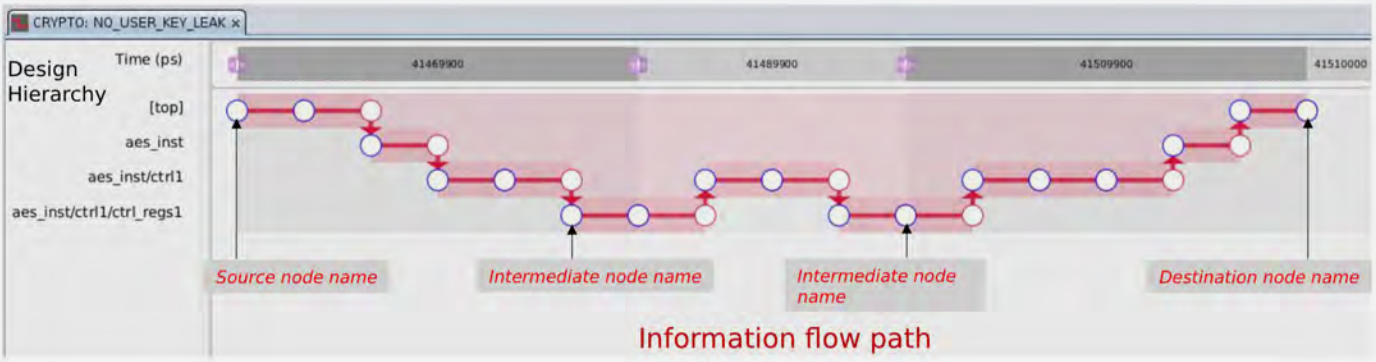


Figure 2: Path View visualizes hierarchical information flow leading to security rule violations.

Optimize hardware security with a repeatable and scalable process. Streamline security sign-off by using Radix for any of the following use cases.

EXAMPLE APPLICATIONS	BENEFITS
Hardware Root of Trust Security Verification	Ensures correct configuration for maximum security
SoC access control verification	**Prevents unauthorized access**
Security boot sequence verification	Verifies boot data and keys remain secure
Red/Black separation	**Checks for isolation of redundant systems**
Timing side channels	Detect and prevent Meltdown/Spectre variants of attacks
Configuration register read/write protection	**Ensures SoC access control is maintained**
Encryption key leakage	Ensures keys remain secure during and after usages
Verification of clearing secret content	**Ensure secure data is cleared prior to switching to non-secure modes**
External Debug disablement/analysis	Ensures JTAG does not access secure data or keys
3rd Party/vendor IP and interface security	**Verifies that vulnerabilities have not been introduced due to integration errors**

About Cycuity

Cycuity enables efficient and comprehensive security verification throughout the entire lifecycle of semiconductor chip development, so organizations can detect and mitigate hardware vulnerabilities before manufacturing. The company's Radix™ product line enables rigorous hardware security assurance for all silicon devices, helping companies that build or rely on semiconductors achieve security signoff faster and reduce risk. Founded in 2014, Cycuity is headquartered in San Jose, CA.

To Learn More: cycuity.com, info@cycuity.com