Ensuring Datapath Integrity and Adherence with Formal Security Verification in RISC-V Implementation

Sven Beyer, Keerthikumara Devarajegowda, Joerg Grosse, Nicolae Tusinschi
Siemens EDA, Germany

SIEMENS

Importance of Hardware Security

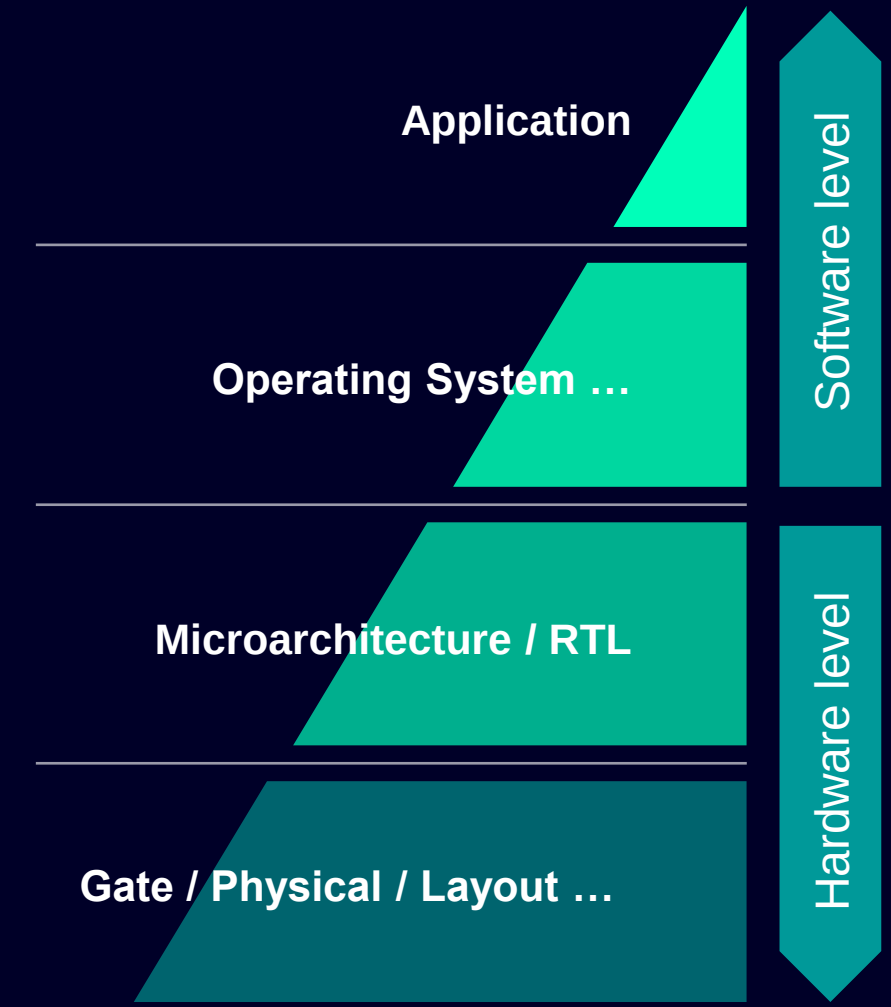
Crucial to thoroughly verify hardware security features

Designs containing security features that must be verified

58% Safety Critical ASIC	**+4%** since 2020
49% Safety Critical FPGA	**+5%** since 2020

Security is a topic at every layer of a system operation
Hardware is the foundation of all secure applications

- Hardware with vulnerabilities compromises the whole system
- Hardware must ensure the sanctity of secure operations



SIEMENS

Security Verification Challenges

Confidentiality
Internal data buses are vulnerable to external tampering

Integrity
Data sanctity is critical

Inversion
Secret data must not reach illegal points unencrypted

Sneak Path
Represent significant risk compromising control systems

Verification Methods
Simulation does not scale, traditional formal suffers from increased efforts and expertise

Difficulty
Highly complex and convoluted nature of designs rule out expert inspection of paths

SIEMENS

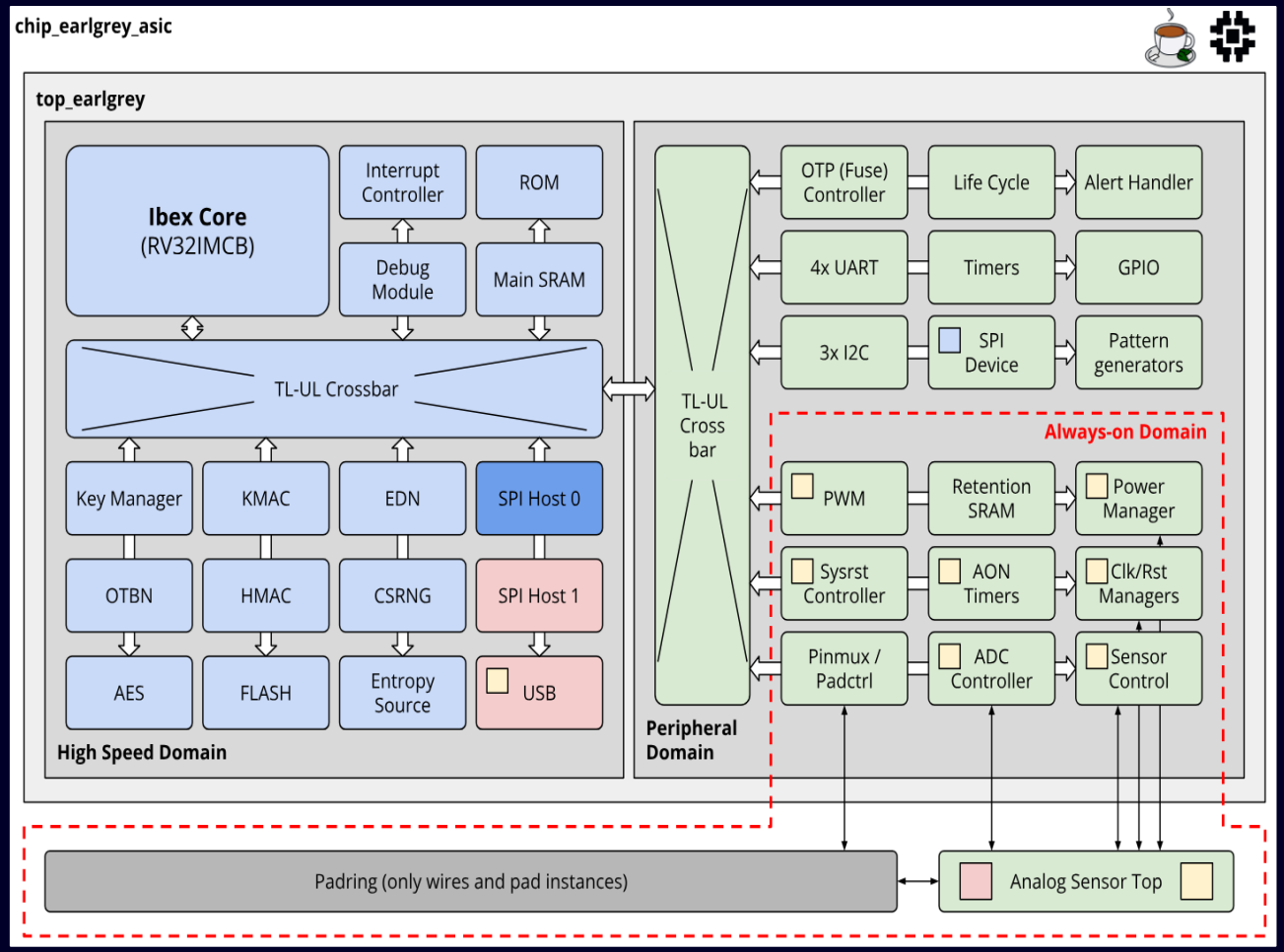
OpenTitan

- An open-source project aimed at creating a highly secure, transparent, and flexible Root of Trust (RoT) hardware design

- The design is scalable to meet the security needs of a wide range of applications, from small IoT devices to large data center hardware.

- Clean RTL implementation with several
  - Hardware Features for Security:

  Secure storage, Side-channel attack resistance, Secure boot, Cryptographic acceleration, Antitamper mechanisms, etc.

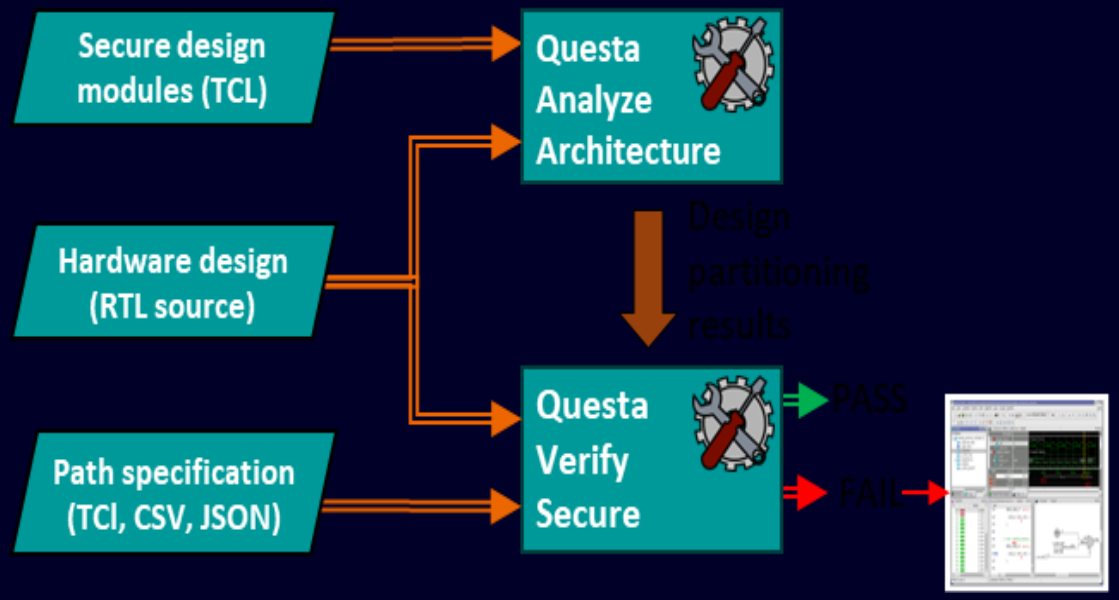


SIEMENS

Methodology Overview
Formal-based solution

- Formal Verification
  - Guarantees security requirements for datapaths through systematic and exhaustive analysis
  - High degree of automation speeds up the verification process

- Formal solutions applied
  - Questa Analyze Architecture (QAA) - For design partitioning
  - Questa Verify Secure (QVS) - For exhaustive datapath analyses

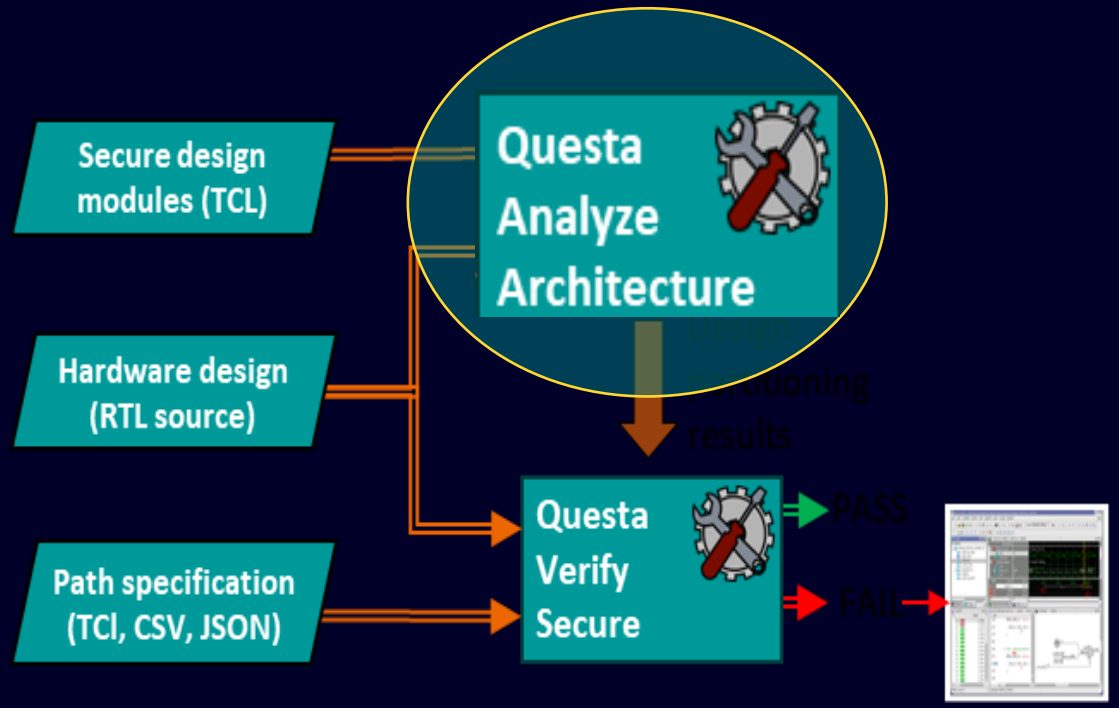


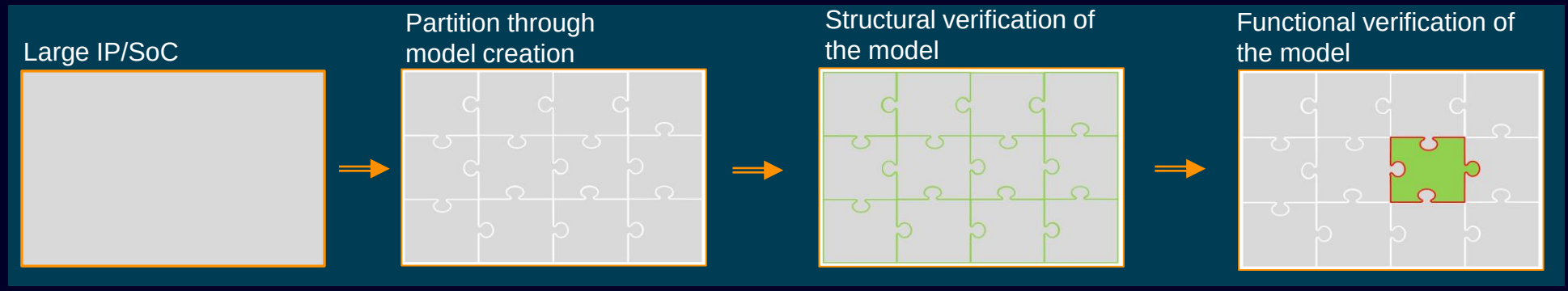
SIEMENS

Methodology Overview

Design partitioning through architecture exploration

- Crucial to understand/analyze the design architecture to extract the cluster of security sensitive modules
- Questa Analyze Architecture (QAA) enables architectural exploration
  - Simplifies understanding of complex designs
  - Isolates specific design instances for focused or targeted security analysis

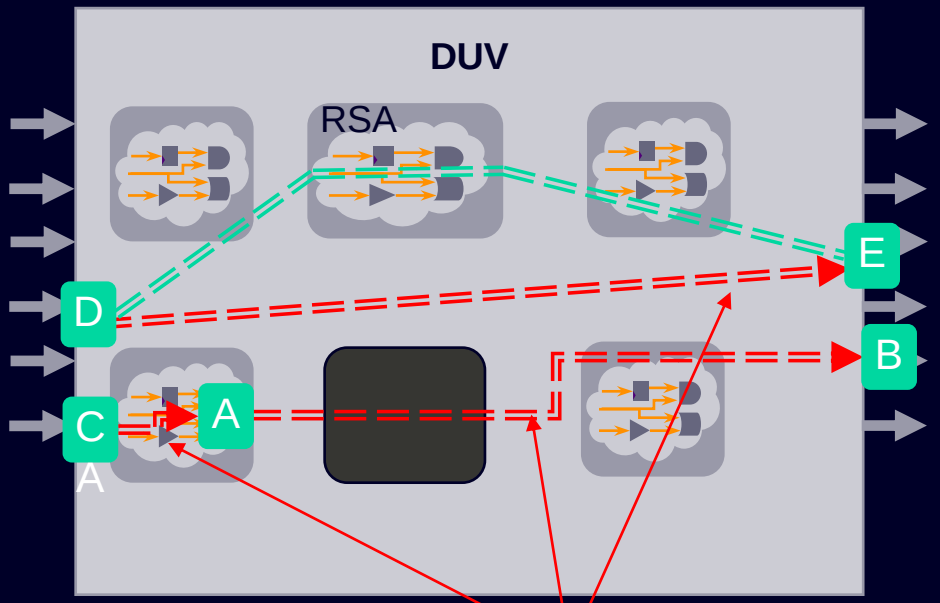




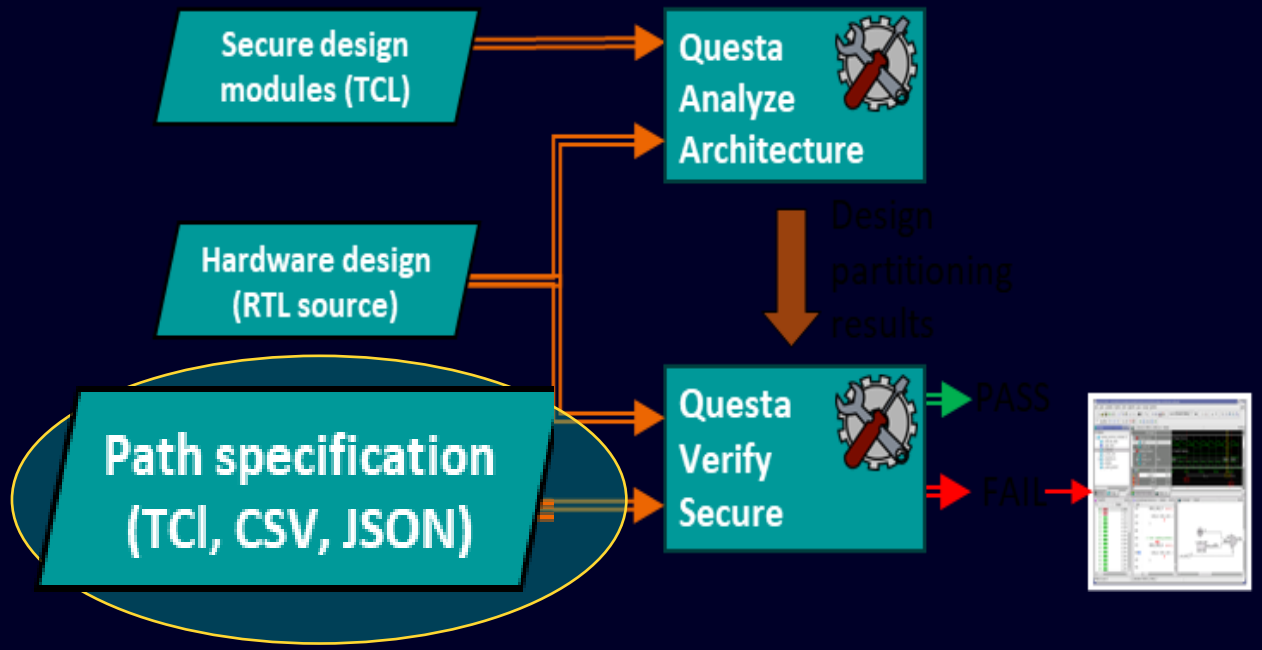
SIEMENS

Methodology Overview
Datapath specification

- Define paths that secure data should or should not traverse within certain design instances



do these paths exist, which violate the security datapath requirements?

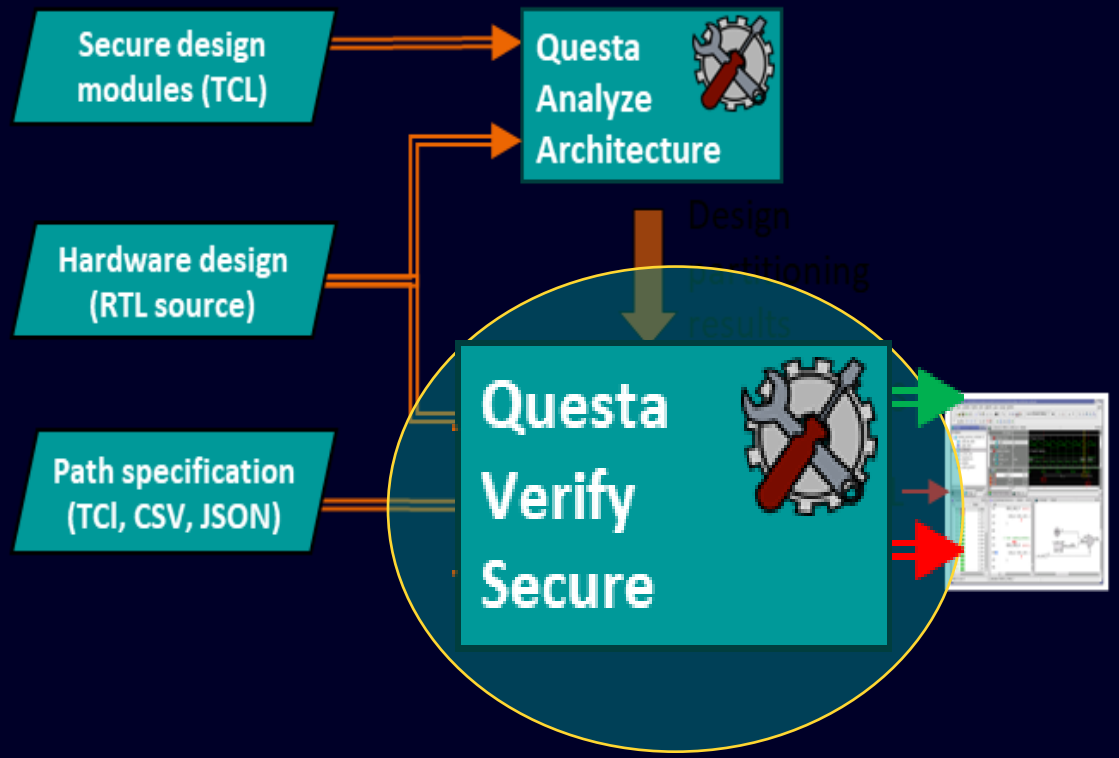


SIEMENS

Methodology Overview

Datapath analysis

Questa Verify Secure (QVS) is a formal app for running exhaustive datapath analyses



Automation

- Generate properties from high-level path specifications
- Identify ports and black box signals subject to potential security issues

Exhaustiveness

- Run path analysis with cutting-edge formal methods

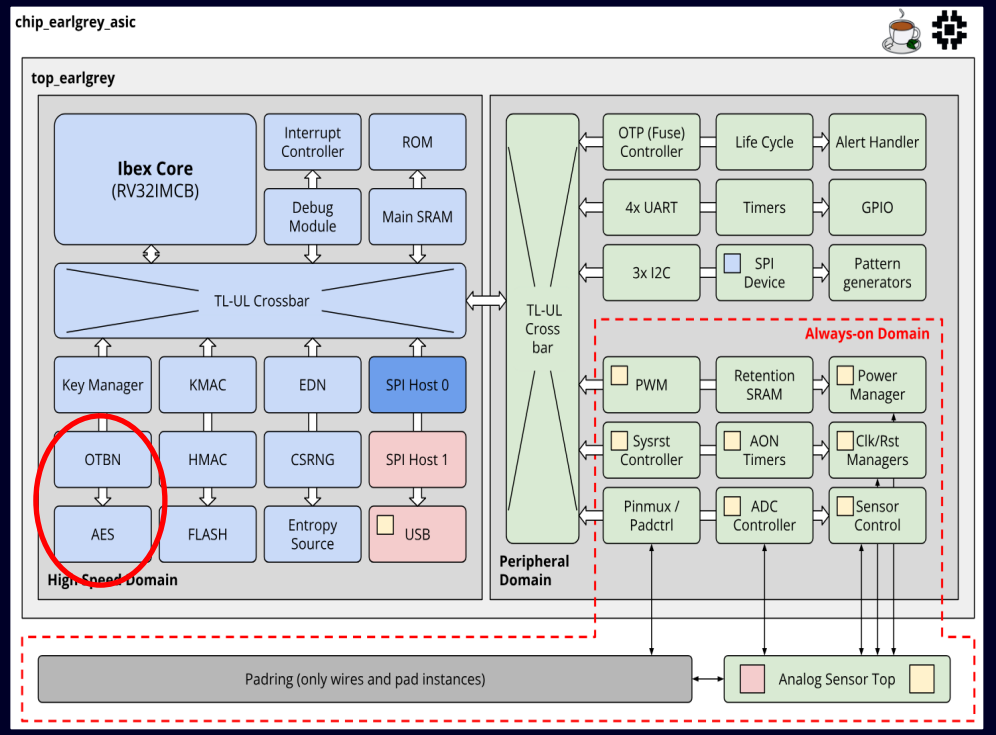
Debug

- Pinpoint debug of vulnerable paths
- Root cause identification with waveform analysis

SIEMENS

Application on OpenTitan

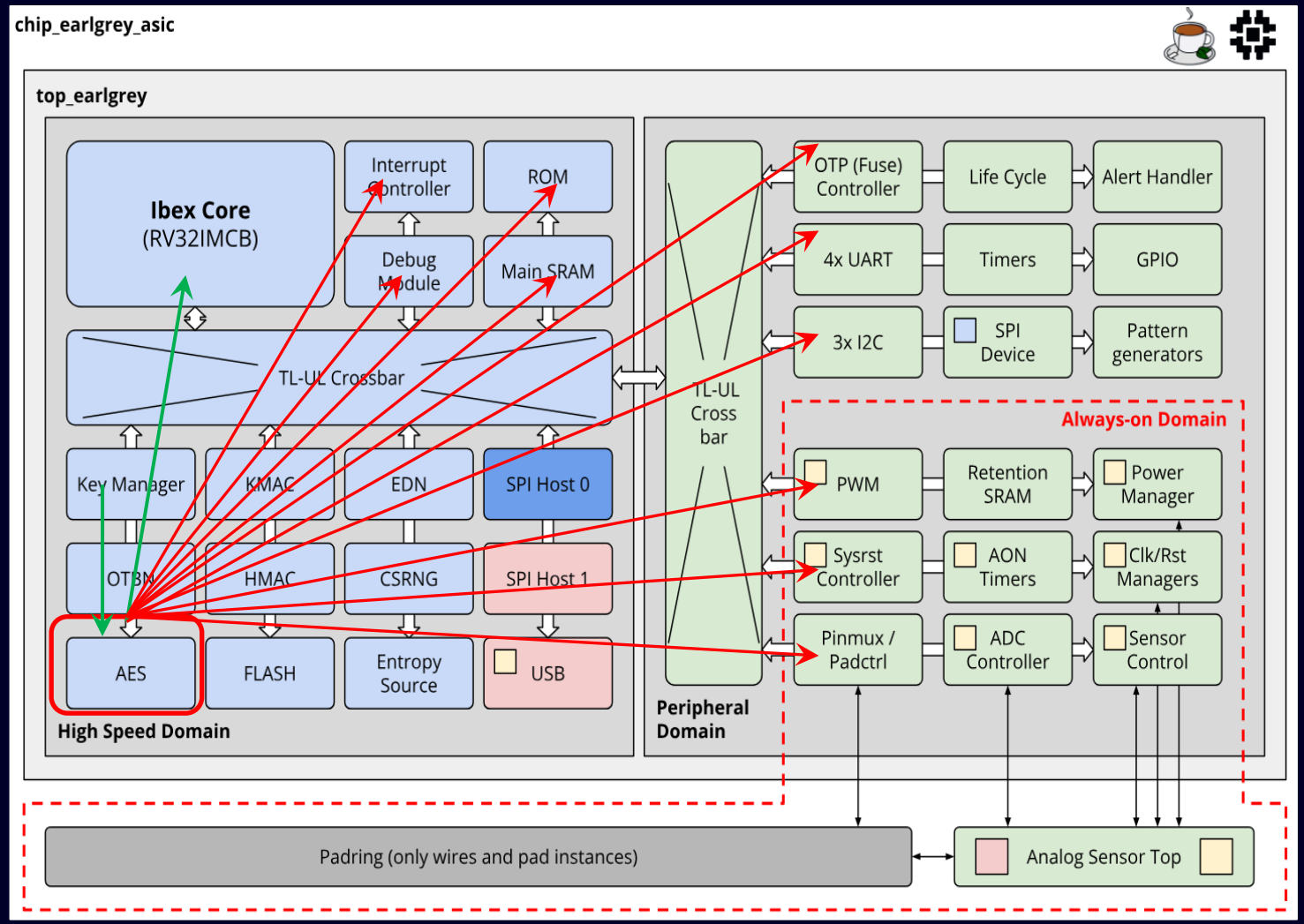
- RTL sources @ https://opentitan.org
- Focused on *chip_earlgrey_asic* version with *top_earlgrey* module
- Architecture exploration
  - Used Questa Analyze Architecture to explore the architecture of OpenTitan with a focus on AES and OTBN modules
  - Outcome is a list of design instances that have potential dependency on the data from AES and OTBN instances
- Path analysis
  - Specified paths from AES and OTBN secure data ports to all instances connected to the TL-UL Crossbar



SIEMENS

Application on OpenTitan: AES instance

- The AES unit is a cryptographic accelerator that accepts requests from the processor to encrypt or decrypt data
- Communication with the processor happens through a set of CSRs
- The AES unit includes a separate interface through which *KeyManager* can provide the key without exposing it to the processor or other hosts attached to the chip interconnect bus.



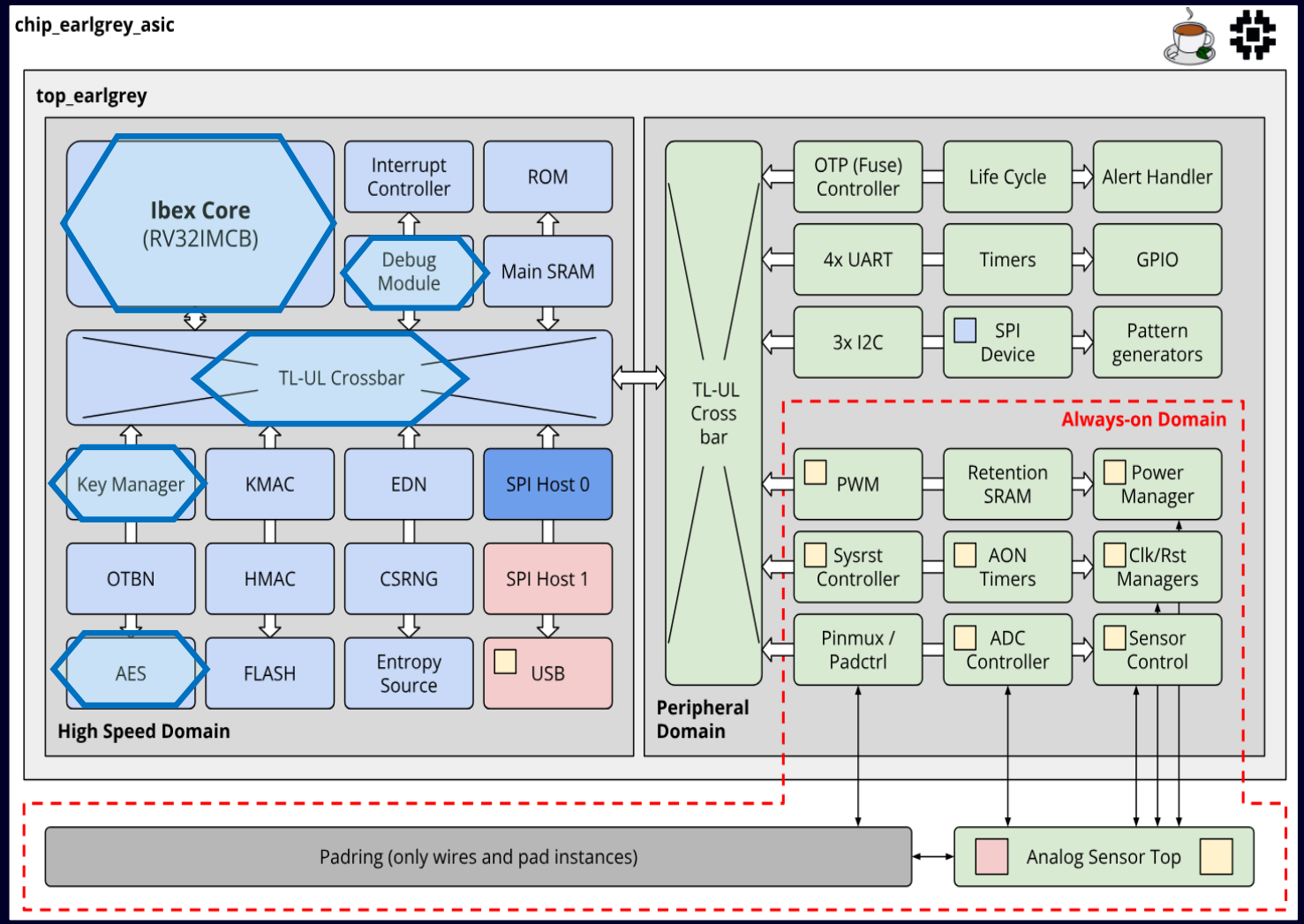
SIEMENS

Application on OpenTitan: AES instance

Data source	Data destination	Outcome	Runtime
AES instance	Ibex core data interface	Functional datapath present	152s
	Ibex core instr. interface	--	Timeout
	SPI	--	Timeout
	UART	--	Timeout
	RV-PLIC	--	Timeout
	Debug module	Functional datapath present	174s
	Main SRAM	--	Timeout
	ROM	--	Timeout

Application on OpenTitan: AES instance (with QAA)

- Application of QAA helped in creating a design cluster
- Ibex-core, debug module, Key manager, TL-UL Crossbar are the design instance that form a design cluster with the AES instance
- With this information, we could abstract away all other design instances for the formal path analysis



SIEMENS

Application on OpenTitan: AES instance (with QAA)

Data source	Data destination	Outcome	Runtime
AES instance	Ibex core data interface	Functional path present	62s
	Ibex core instr. interface	Functional path absent	25s
	SPI	Functional path absent	25s
	UART	Functional path absent	25s
	RV-PLIC	Functional path absent	25s
	Debug module	Functional path present	123s
	Main SRAM	Functional path absent	25s
	ROM	Functional path absent	25s

Summary

- Formal-based methodology effectively helps to safeguards complex digital systems
- Suitable for security verification in large SoCs
- Questa Analyze Architectures simplifies the application of formal methods
- Questa VerifySecure provides comprehensive path analysis
- Future Work
  - Further automation in the methodology
  - Refinement for increasingly larger System on Chips (SoCs)