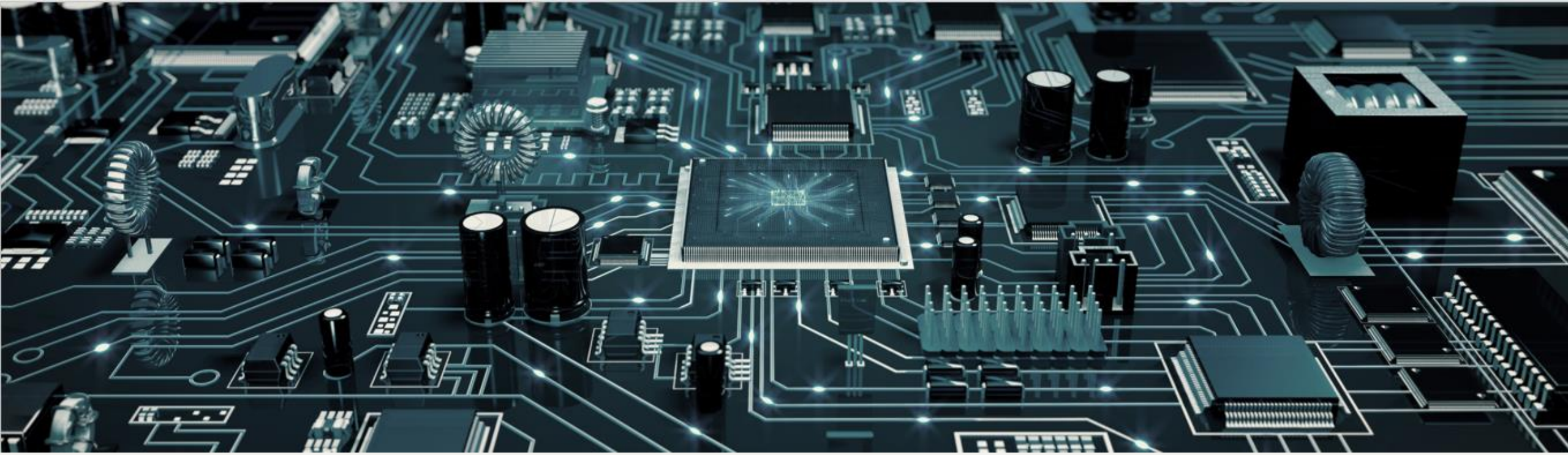


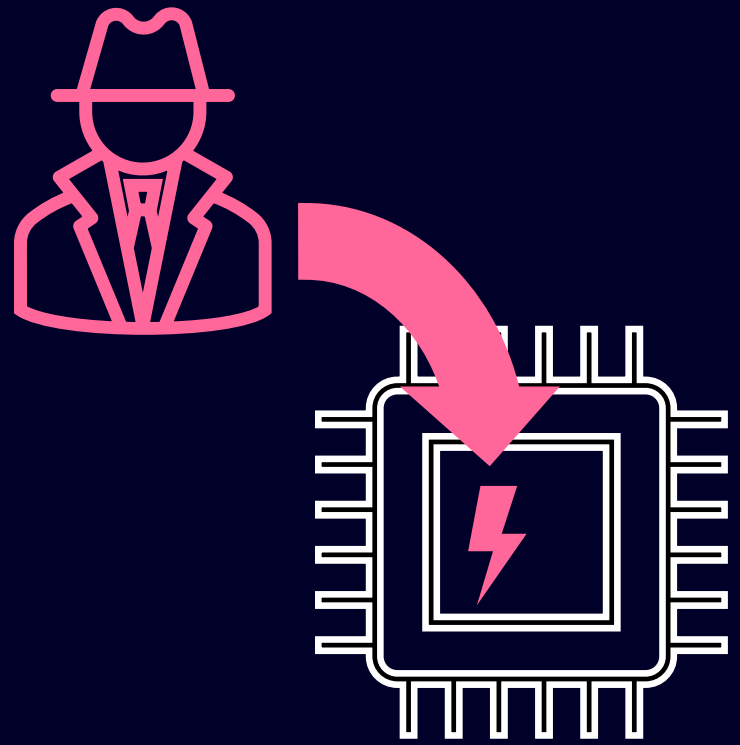
Formal Verification Tools for the Trustworthiness of RTL

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Joerg Bormann, PM Advanced Verification

SIEMENS

Teaser: Formal Verification & Trustworthiness



Example: Questa GapFree

- Verification of all functionality for all inputs (natural, but quite unique).

Every unusual I/O behavior will be detected.

- No matter how rare it is.
- ≠ Simulation
- Similar for Questa Processor and Questa Equivalence.

Formal is bad for the bad guys, because it identifies their trojans even if well hidden (i.e. very rarely activated).

To avoid a full GapFree verification just for the purpose of trustworthiness checking, please see the next slides.

SIEMENS

Tools for Trustworthiness

Confidentialiy, Integrity, Availability

1. Proper implementation of security architecture
   - **Questa Verify Secure**
   - Verifies data flow through the circuit
   - Cooperation partner Prof. Kunz (RPTU)
   - Research funded by Scale4Edge Phase 1

Scale4Edge

RPTU

FKZ 16ME0124

2. Detection of security-critical design bugs (= weaknesses)
   - **Questa Verify Trust**
   - Trust auto-checker
   - For 3rd party IP and inhouse RTL
   - Research funded by VE-VIDES

VE-VIDES

FKZ 16ME0248

SIEMENS

Questa Verify Secure

Verify Security Requirements

SIEMENS

Propagation path requirements in secure designs

Confidentiality

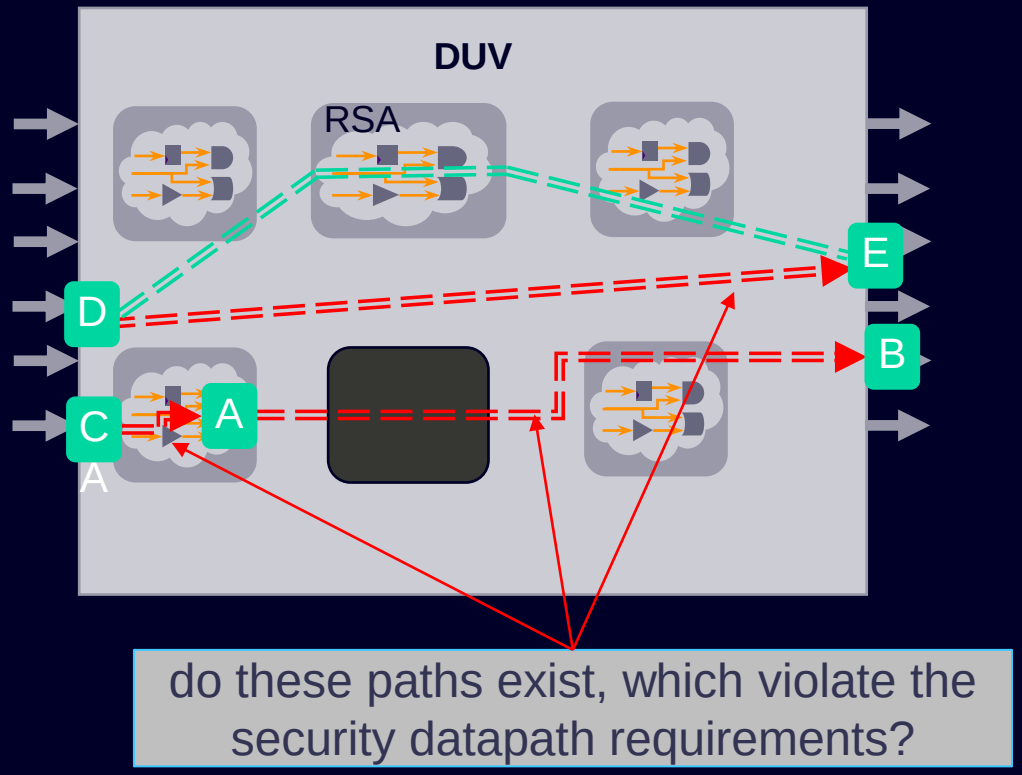
secret data from A should not leak to B

Integrity

data from C should not overwrite valuable data at A

Data inversion

secret at D should not reach port E without encryption



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

Formal verification of datapath security requirements

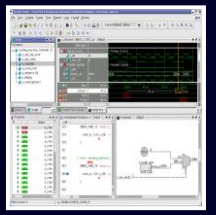
Exhaustive verification of datapath requirements from block to chip

1 Automation **2 Exhaustiveness** **3 Debug**

RTL

Secure storage and path specification

Verify Secure App



Focused debug

Exhaustive verification

User-friendly notations to specify interesting/illegal datapaths

Questa Verify Trust

Find security relevant design bugs

SIEMENS

Verify Trust
Automated formal detection of trust and security vulnerabilities

Feature	Benefit	CWE
Detects Trojans	Avoid extra logic that enables attacks	1242, 506, 507, 511
Identifies Unused Logic	Protects against physical side channels, fault insertion attacks & excess power consumption	561, 563, 1245
Detects Deadlocks	Protects against denial-of-service attacks	835, 1245
Detects Leakage & Corruption Paths	Exposes paths to break integrity or confidentiality of data assets	203, 1258, 1273, 1272, 1295; 1256, 1314
Checks Lock Bits	Formal verification of access protection	1224, 1231, 1233
Proves independence from reset states	Save production cost without compromising trust	1271
Extensible Platform	Add new detection methods and checks	

SIEMENS

Questa Verify Trust

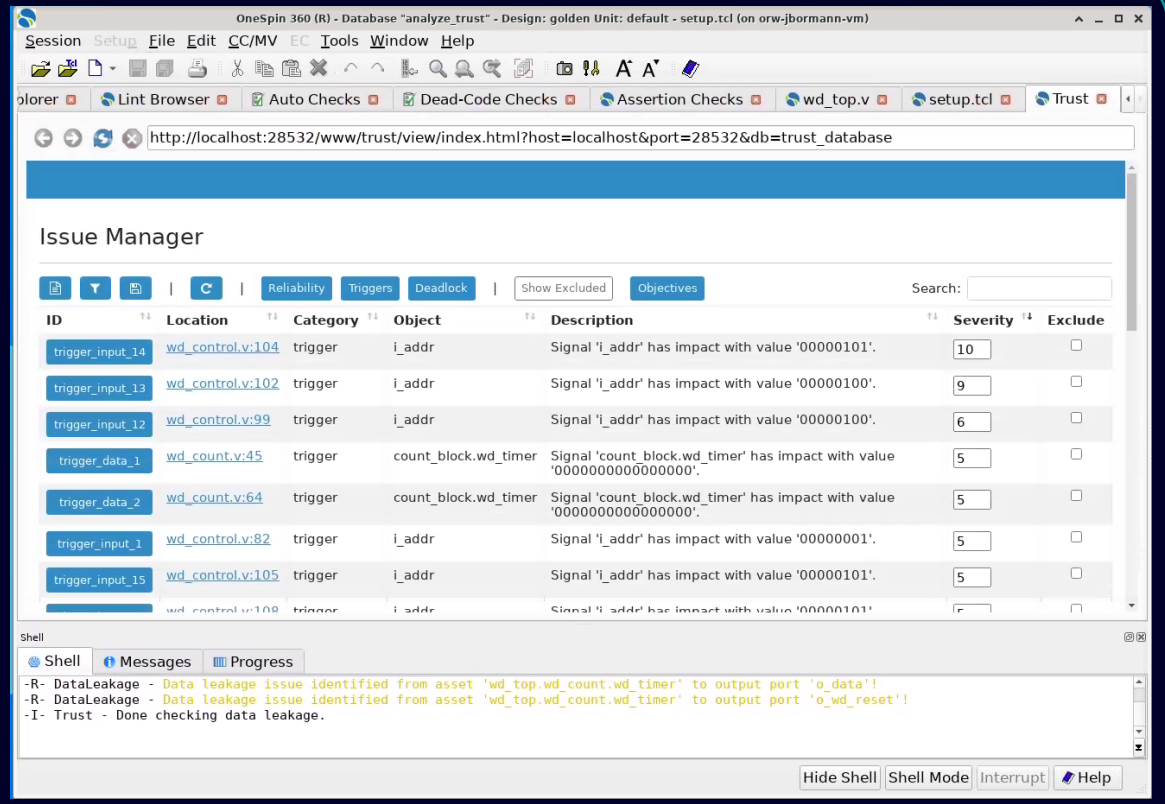
Use Case: Trust & Security Scan for 3rd party IP and own RTL, against CWE issues

RTL

Common Weakness Database
cwe.mitre.org

User selects Weakness Classes

Tool generates & executes formal checks to detect trust issues



Tool lists issues for deeper analysis.
User prioritizes, analyzes, and confirms or ticks off.

Report

SIEMENS

Summary

Formal Verification is well suited for Trust and Security verification.

Questa Verify Secure: Verification of Security Requirements

- User friendly path specification
- Exhaustive verification of propagation path requirements from block to chip.

Questa Verify Trust: Search for trust related design bugs

- Automation – no formal expertise required
- No design knowledge required
- Efficient analysis of suspicious locations

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Contact

Jörg Bormann
Program Manager Advanced Verification
Siemens EDA, München

Phone +49 1577 356 4108

E-mail joerg.bormann@siemens.com

SIEMENS