Pre-Silicon Formal Verification and Post-Silicon Assertion Checker on RISC-V Processor

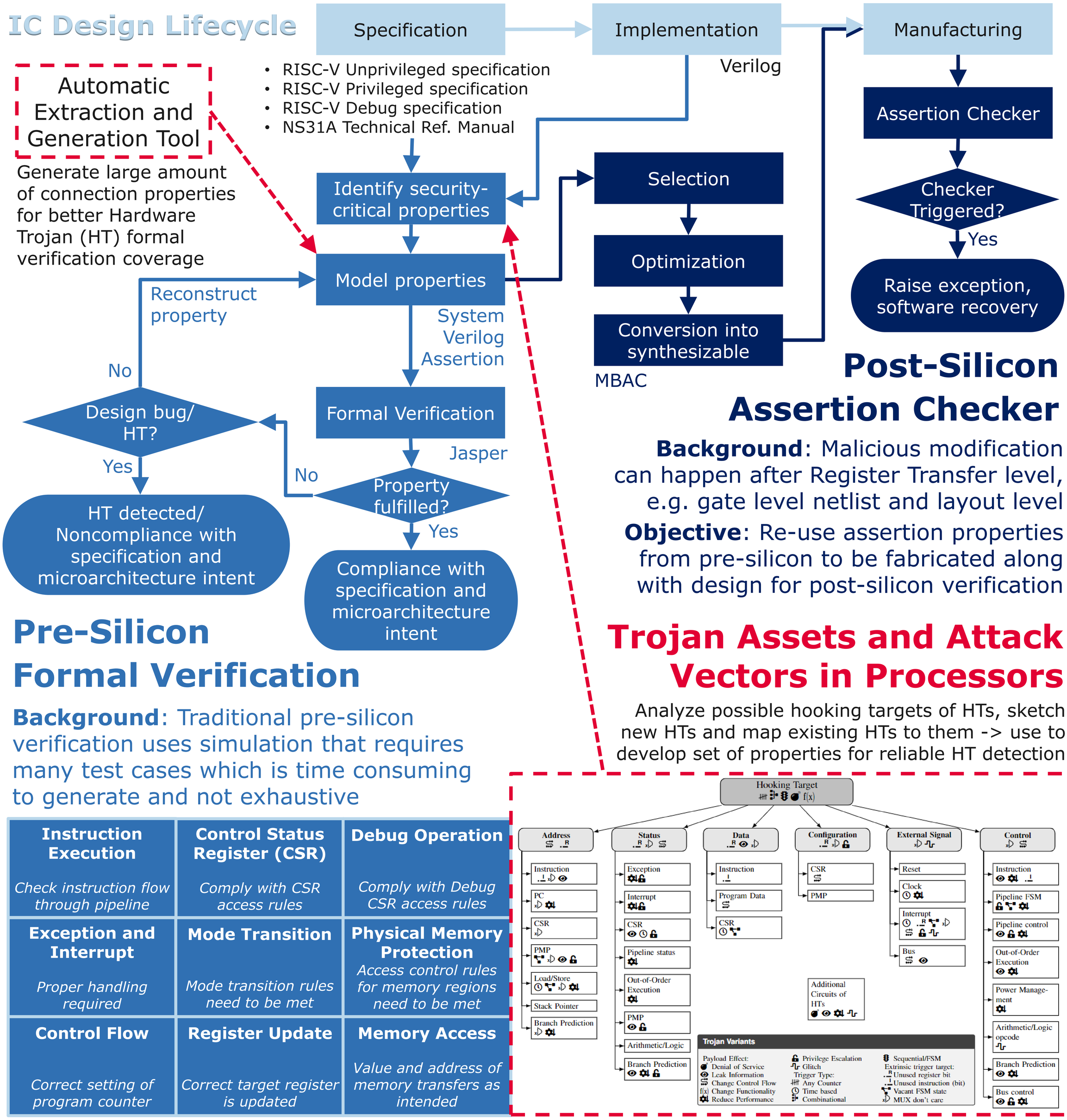
Czea Sie Chuah, Christian Appold

DENSO Crafting the Core

Technische Universität München

DIVA IC Vertrauenswürdige Elektronik

Motivation: High security demands of upcoming applications, several famous bugs and security-vulnerabilities in processors have been found in the past years, openness of RISC-V Instruction Set Architecture



Pre-Silicon Formal Verification

Background: Traditional pre-silicon verification uses simulation that requires many test cases which is time consuming to generate and not exhaustive

Instruction Execution *Check instruction flow through pipeline*	**Control Status Register (CSR)** *Comply with CSR access rules*	**Debug Operation** *Comply with Debug CSR access rules*
Exception and Interrupt *Proper handling required*	**Mode Transition** *Mode transition rules need to be met*	**Physical Memory Protection** *Access control rules for memory regions need to be met*
Control Flow *Correct setting of program counter*	**Register Update** *Correct target register is updated*	**Memory Access** *Value and address of memory transfers as intended*

Post-Silicon Assertion Checker

Background: Malicious modification can happen after Register Transfer level, e.g. gate level netlist and layout level

Objective: Re-use assertion properties from pre-silicon to be fabricated along with design for post-silicon verification

Trojan Assets and Attack Vectors in Processors

Analyze possible hooking targets of HTs, sketch new HTs and map existing HTs to them -> use to develop set of properties for reliable HT detection

Result:

- Identified 1146 properties and grouped them under 9 categories
- Achieved full-proof for passing properties
- Runtime: Control Flow < 24h, others < 4000s

C. S. Chuah, C. Appold and T. Leinmueller, "Formal Verification of Security Properties on RISC-V Processors," 2023 21st ACM-IEEE International Symposium on Formal Methods and Models for System Design (MEMOCODE), Hamburg, Germany, 2023, pp. 159-168.

C. S. Chuah, A. Hepp, C. Appold and T. Leinmueller, "Trojan Assets and Attack Vectors in Processors," 2024 25th International Symposium on Quality Electronic Design (ISQED), San Francisco, CA, USA, 2024, pp. 1-10, doi: 10.1109/ISQED60706.2024.10528700.