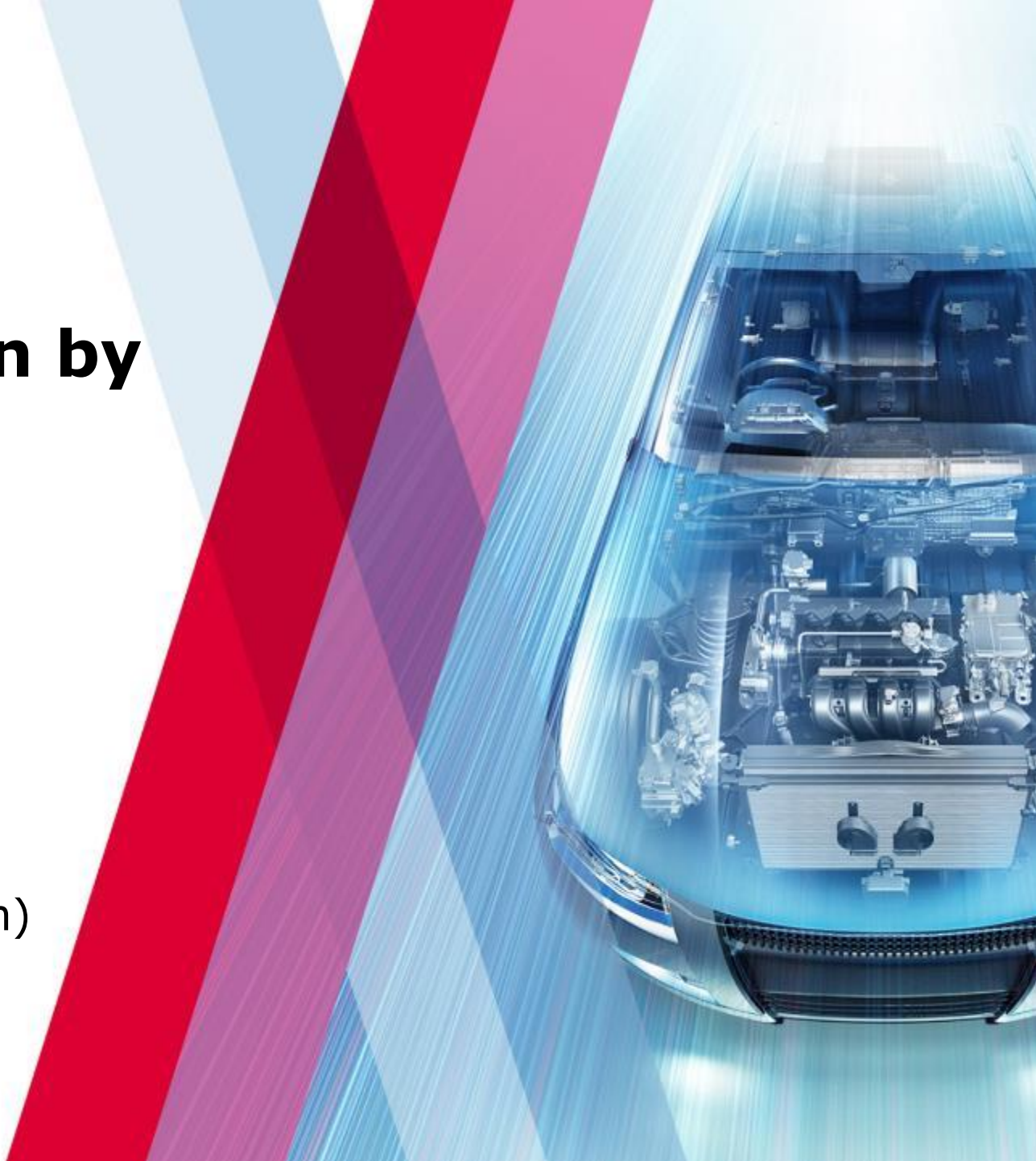
DENSO
Crafting the Core

Hardware Trojan Detection by using Formal Verification

Cybersecurity Vehicle Forum Munich



Christian Appold (c.appold@eu.denso.com)

2026/10/21

Outline

1. Introduction
2. Methodology
3. Complete PC HT Detection Property Set
4. Checking HT Detection Property Set Completeness
5. Experimental Results
6. Conclusion and Outlook

© DENSO CORPORATION All Rights Reserved.

Introduction

Christian Appold – Software R&D

© DENSO CORPORATION All Rights Reserved.

Introduction

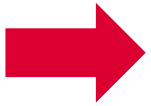
- Upcoming applications have very high security requirements, e.g. autonomous driving
- HTs are malicious modifications of hardware to change functionality or leak secret data
- Risk of HTs is increased through
  - Globalised semiconductor supply chains
  - Third-party IP
  - Outsourced design and manufacturing
  - Increasing hardware complexity
- HTs are a low-observability, potentially high-impact supply chain risk

Hardware Trust increasingly difficult to establish

© DENSO CORPORATION All Rights Reserved.

Introduction

- Approaches for HT detection have been developed, e.g.
  - Statistical analysis of side-channel information from chips
  - Reverse-Engineering
  - Formal Verification based approaches
- Most approaches
  - Lack automation and require significant manual effort
  - Target often specific HTs and offer low detection coverage



We developed a systematic Formal Verification approach reliably detecting each inserted HT - Focus of this talk

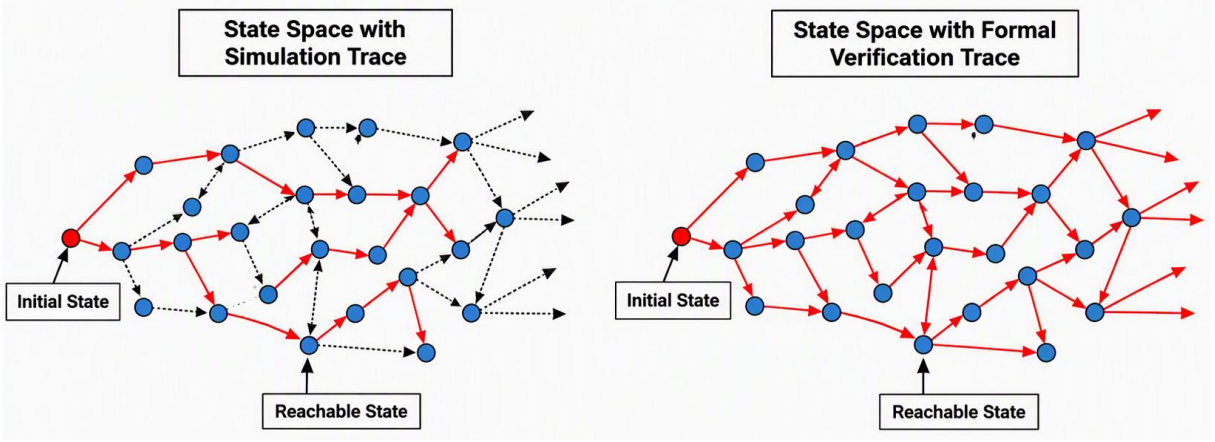
- **Speeding-up property writing by automation**

© DENSO CORPORATION All Rights Reserved.

Introduction

- Formal Verification:
  - Property-based methodology for exhaustive verification specified behaviour

Simulation: investigation selected traces



Formal Verification: exhaustive trace investigation

- Processors are ubiquitous and embedded in nearly every electronic device
  - Popularity and accessibility of open source RISC-V architecture further increases risk of inserted HTs

Approaches for reliable Hardware Trojan detection in processors urgently required

- **Developed complete Program Counter (PC) HT detection Formal Verification property set for RISC-V processors**

© DENSO CORPORATION All Rights Reserved.

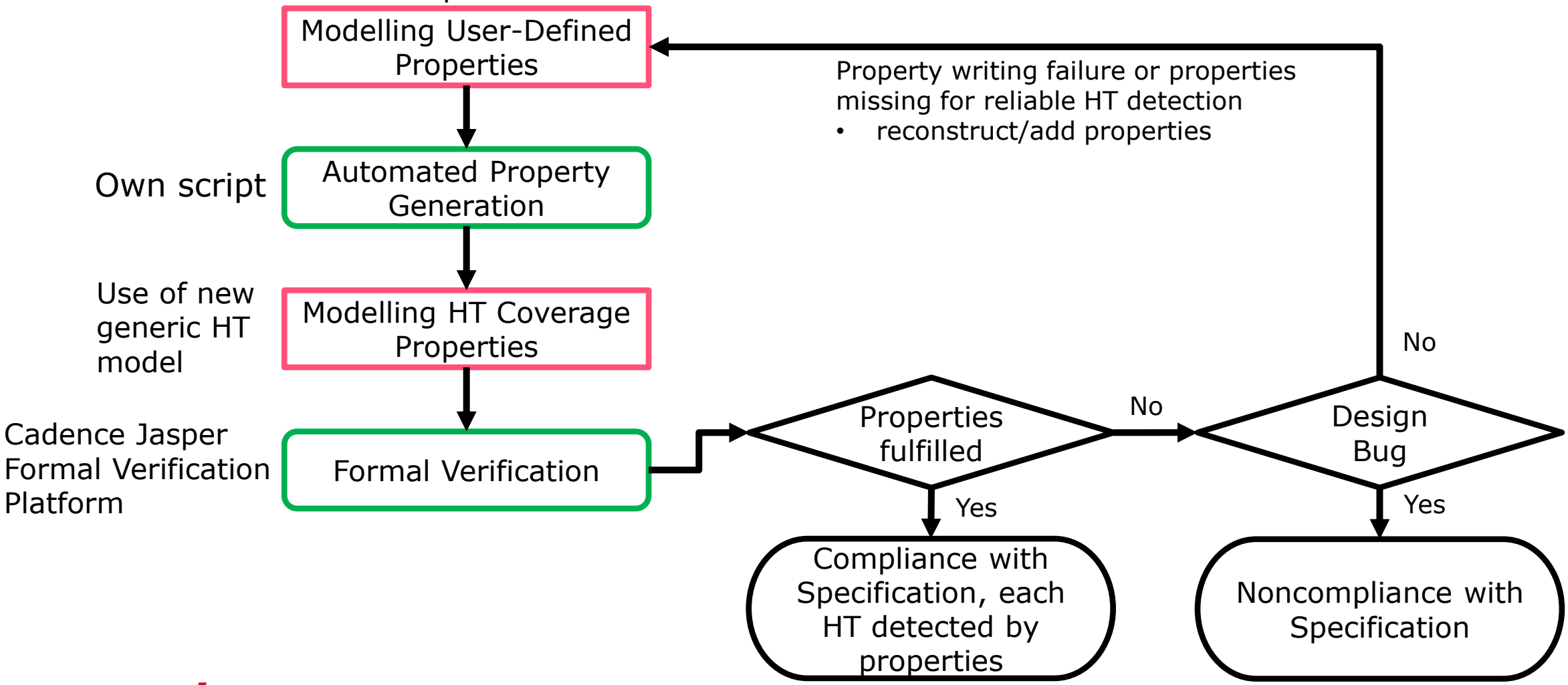
Methodology

© DENSO CORPORATION All Rights Reserved.

Methodology - Workflow

Manual
Automated

Two user-defined property types:
1. Design Intent Properties (from Specification or Microarchitecture intent)
2. Connection Properties



© DENSO CORPORATION All Rights Reserved.

Methodology

- Use of two property types for full HT detection coverage:

Design Intent Properties

1. Correct behaviour

Does the processor do what the specification says?

Example: Program Counter

If a branch is taken → Program Counter changes to the target address

Property: assert property (@(posedge clk) condition_PC_setting |-> ##1 InstPC==BranchPC)

Connection Properties

2. Correct data flow

Does information travel through the intended hardware path?

Example: Processor Pipeline

The Program Counter leaving one stage → must arrive correctly at the next stage

Property: assert property (@(posedge clk) TRUE ##1 !$stable(PipePC) |-> $past(PipeRegEn)==1'b1

Together: Check what processor does + how information moves

© DENSO CORPORATION All Rights Reserved.

Complete PC HT Detection Properties

© DENSO CORPORATION All Rights Reserved.

Complete PC HT Detection Properties

- Our complete PC HT detection property set for RISC-V processors consists of eight property categories (in total 296 properties):

PC Instruction Semantics (8) -e.g. for jal, branch, mret, PC standard increment, interrupt	**PC to Instruction Memory (5)** -e.g. fetch PC to memory and in IQ	**Instruction Code Flow (13)** -e.g. integrity in pipeline registers and IQ
General Purpose Register (GPR) change integrity (205) -e.g. for auipc, lui, jal, CSR insts or stable	**General Purpose Register (GPR) to Memory integrity (32)** - for store	**Integrity mtvec CSR writing (11)** - for CSR insts or stable
Integrity mepc CSR writing (20) - for CSR insts, interrupt, exception or stable	**NMI setting integrity (2)** - new NMI PC or stable	

- Property set able to detect each arbitrary HT compromising a PC signal
  - for whole PC flow through processor and each storing/reading of PC
- First focus on PC in this work as integrity of PC very important, e.g. to prohibit execution of attacker code
- Property set valid for each RISC-V processor, can be adapted for other ISAs with acceptable effort

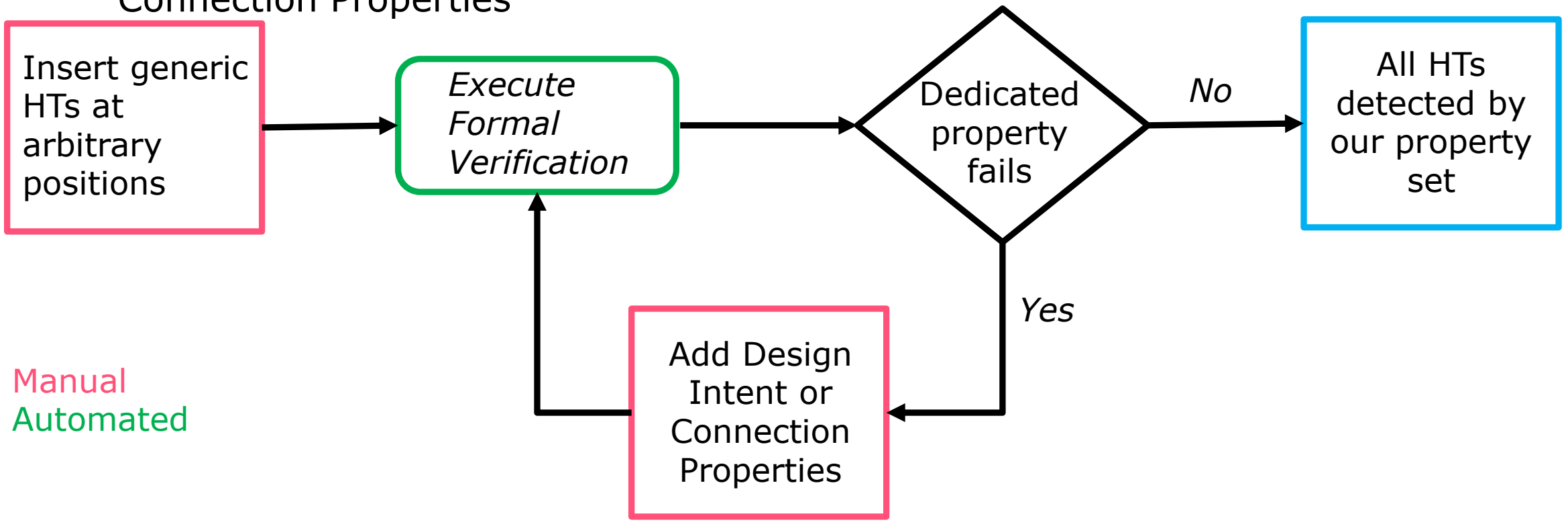
© DENSO CORPORATION All Rights Reserved.

Checking HT Detection Property Set Completeness

© DENSO CORPORATION All Rights Reserved.

Checking HT Detection Property Set Completeness

- We also use Formal Verification to check completeness of properties for HT detection
- Use of dedicated properties to prove each HT is detected by Design Intent and Connection Properties



Achieved goal: Every HT modification detected by at least on property

© DENSO CORPORATION All Rights Reserved.

Experimental Results

© DENSO CORPORATION All Rights Reserved.

Experimental Results

- Verification executed on 16-core AMD server with 2.2GHz each and 128 GB RAM
- Our work is executed on **DENSO 32-bit 4-stage pipeline RV32IMF ISA RISC-V processor**
- Use of Formal Verification tool **Cadence Jasper Formal Verification Platform**

© DENSO CORPORATION All Rights Reserved.

Experimental Results

- Achieved full-proof for all properties in < 24 hours

Formal Verification runs with subsets of category properties

Categories	# Properties	Runtime (Maximum runtime for a Formal Verification run)	Blackboxing
PC Instruction Semantics	8	<24h	Yes
PC to Instruction Memory	5	<1m	No
Instruction Code Flow	13	<1m	No
GPR change integrity	205	<15m	Yes
GPR to Memory integrity	32	<1.5h	Yes
Integrity mtvec CSR writing	11	<20m	No
Integrity mepc CSR writing	20	<10h	Yes
NMI setting integrity	2	<1m	No
Autogenerated connections	2973	<5m	No
Total	3269	<24h	

© DENSO CORPORATION All Rights Reserved.

Conclusion and Outlook

© DENSO CORPORATION All Rights Reserved.

Conclusion and Outlook

- We developed a systematic approach and property set for reliable HT detection using Formal Verification
  - Full property set to detect each inserted HT directly manipulating the PC
- We are first to propose generic HT model and approach to check HT detection property completeness by Formal Verification
- Experimental results confirm our approach is promising for scalable reliable HT detection
- Our work and properties provide a guideline for reliable HT detection in processors using Formal Verification and can be reused by processor vendors

Standardised property sets could be published
- **Besides this work we also published a comprehensive set of Security Properties for RISC-V processors**

© DENSO CORPORATION All Rights Reserved.

DENSO

Crafting the Core