Reliable Hardware Trojan Formal Verification

Czea Sie Chuah, Christian Appold, and Tim Leinmüller

Introduction

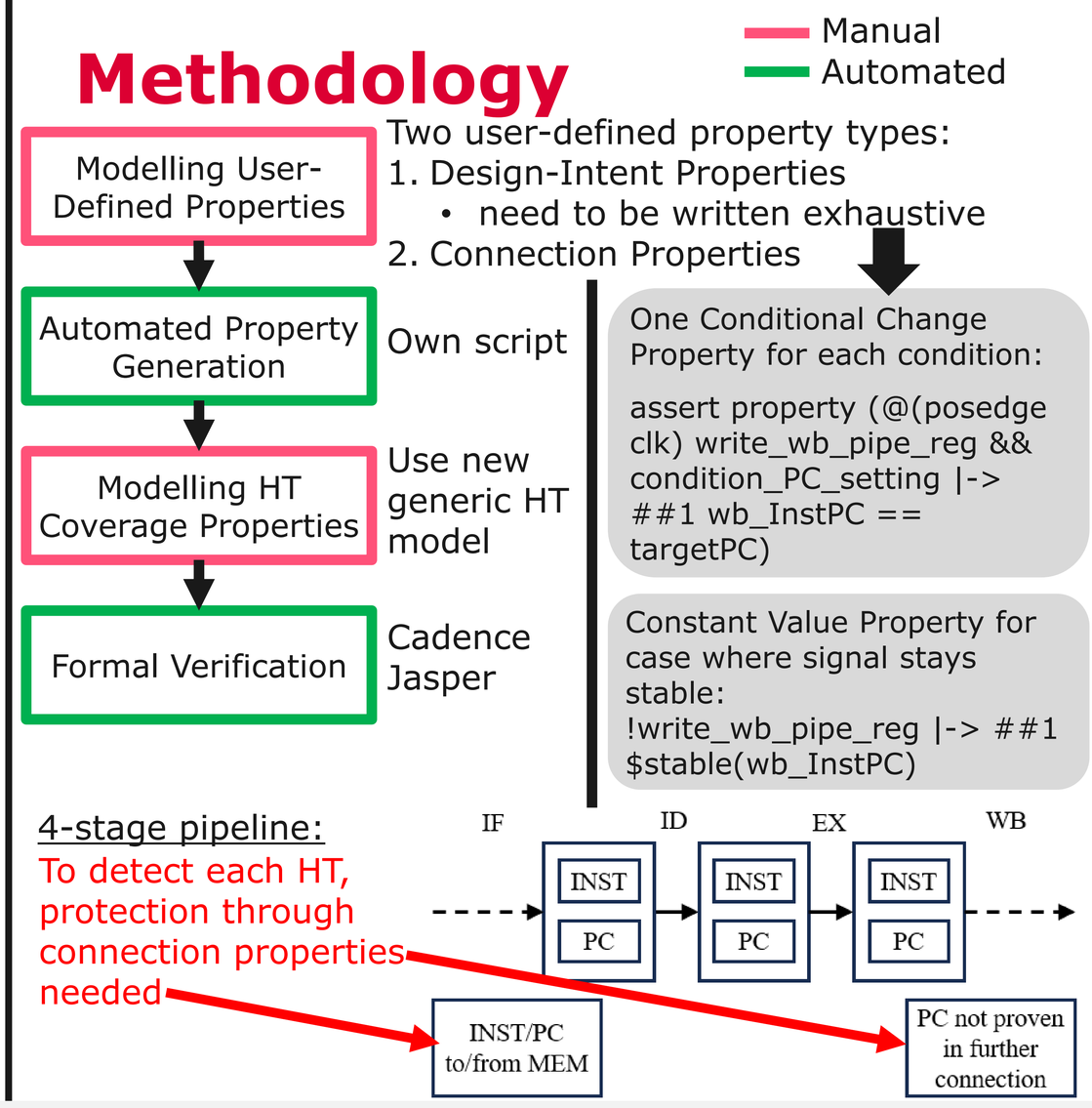
- High security requirements for upcoming applications, like e.g. autonomous driving
- Outsourcing of hardware design and manufacturing increases risk of HTs in processors
- Existing HT detection methods target only specific HT types or require high manual effort

We develop a systematic approach reliably detecting each inserted HT in processors:

- *Combination of two property types*
- *Automated and semi-automated property generation*
- *Properties reliable HT detection for important design parts, e.g. for PC*
- *Generic HT model and approach for property completeness check*

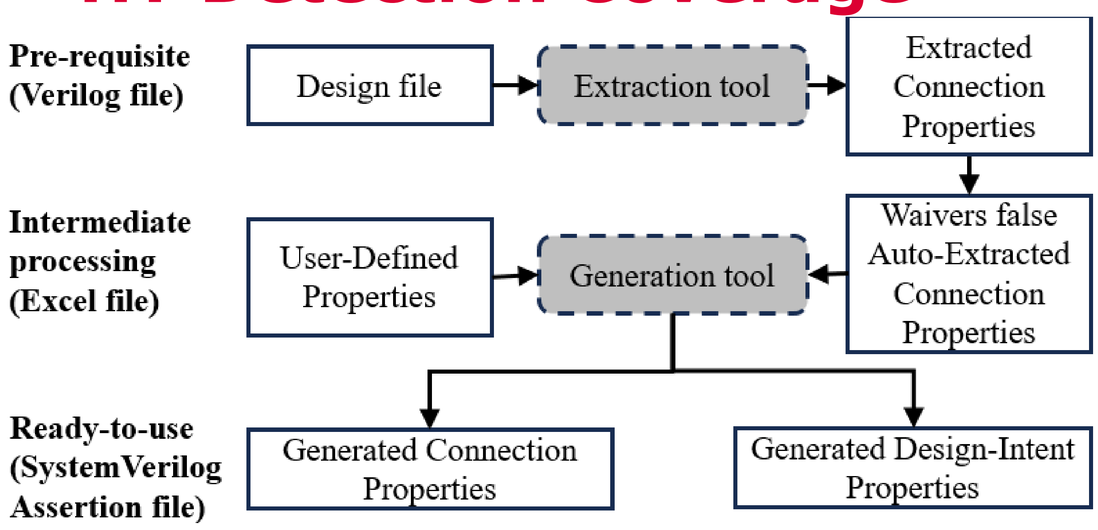
- **Collaboration with TUM Chair of Security in Information Technology**

Methodology



Work presents systematic approach for reliable Hardware Trojan detection

Property Automation and HT Detection Coverage



- Direct signal connection properties between modules generated fully automated
- User-defined properties semi-automated

- HT detection coverage check with generic HT:

```
assign sig1_mod = sig1 XOR TROJ_INPUT     //HT modelling using
                                          //free input TROJ_INPUT
assign conn1 = instQueuePC==memPC  //check property fulfilled
                                   //example for one connection property
trojanTriggered |-> !conn1    //property proves if HT is triggered,
                              //one HT detection property fails

assign trojanTriggered = TROJ_INPUT!=0 //indicates HT triggered
```

Results and Conclusion

- Experimental Results
  - DENSO develops/sells own RISC-V processors
    - Work executed on own DENSO 32-bit, 4 pipeline stages RISC-V processor
  - Cadence Jasper Formal Verification Platform
  - Property generation tool generates ~1500 connection properties fully automatically
  - Achieved full-proof for passing properties

Property Type	Runtime
Used PC Design-Intent Properties	< 24h
Connection Properties	< 3 sec

- Target of work and current state:
  - Approach enables HT detection during RTL design up to generated netlist
  - IP vendors can deliver corresponding HT detection property set with their IP
  - Completed property auto generation tool
  - Completed significant portion of properties reliable HT detection for PC, privilege mode
  - Work will develop comprehensive property set and guidelines to reliably protect key processor constituents from HT insertion

HT: Hardware Trojan, PC: Program Counter, IF: Instruction Fetch, ID: Instruction Decode, EX: Execute, WB: Write Back

DENSO
Crafting the Core

c.appold@eu.denso.com