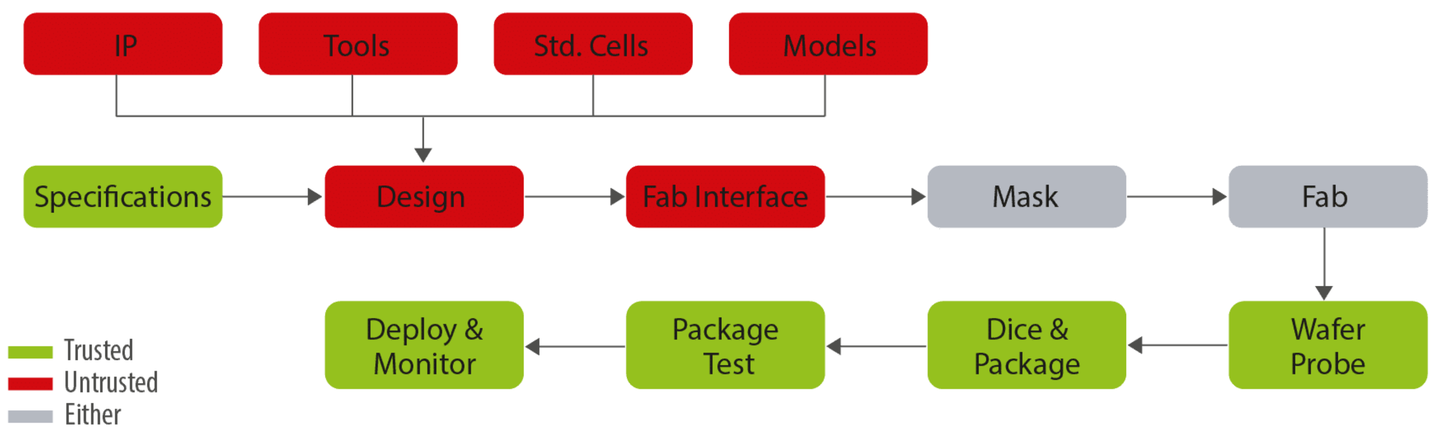
A microarchitectural signals analysis platform to craft Hardware Security Counters

Lucas Georget[1-2], Vincent Migliore[1], Vincent Nicomette[1], Frédéric Silvi[2], Arthur Villard[2]
1: LAAS-CNRS | 2: EDF R&D

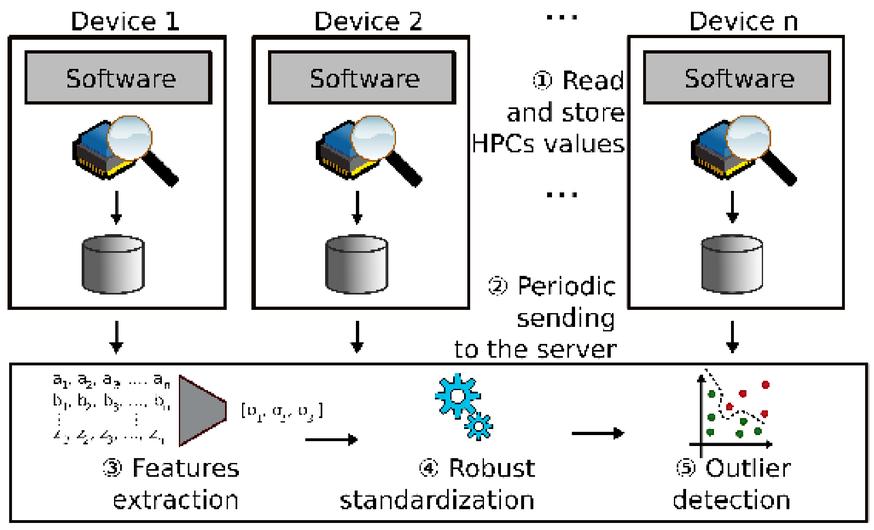
Context: IC supply-chain security [1]



➢ Critical attacks exploit hardware features -> overcome classical security countermeasures

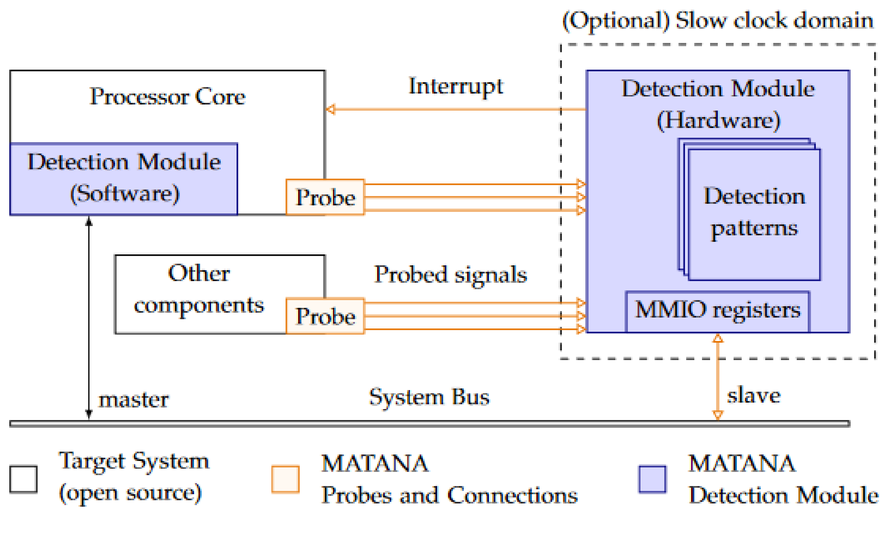
Related work: Low-level intrusion detection systems

Hardware Performance Counters [2]



High detection efficiency with:
- low overhead
- low execution time

Hardware Signal Probing [3]



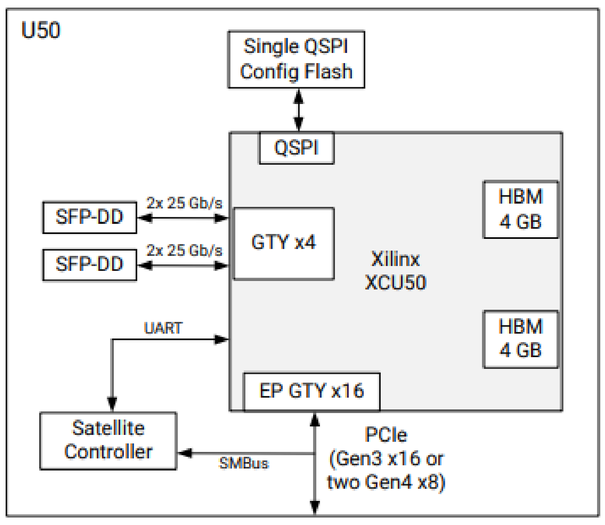
Detection of different classes of attacks:
- cache side-channel attacks
- ROP attacks

➢ Literature solutions: 1) software IDS running on the system 2) active hardware hardening -> both not adapted to ICS context

Contribution: A generic platform to design Hardware Security Counters

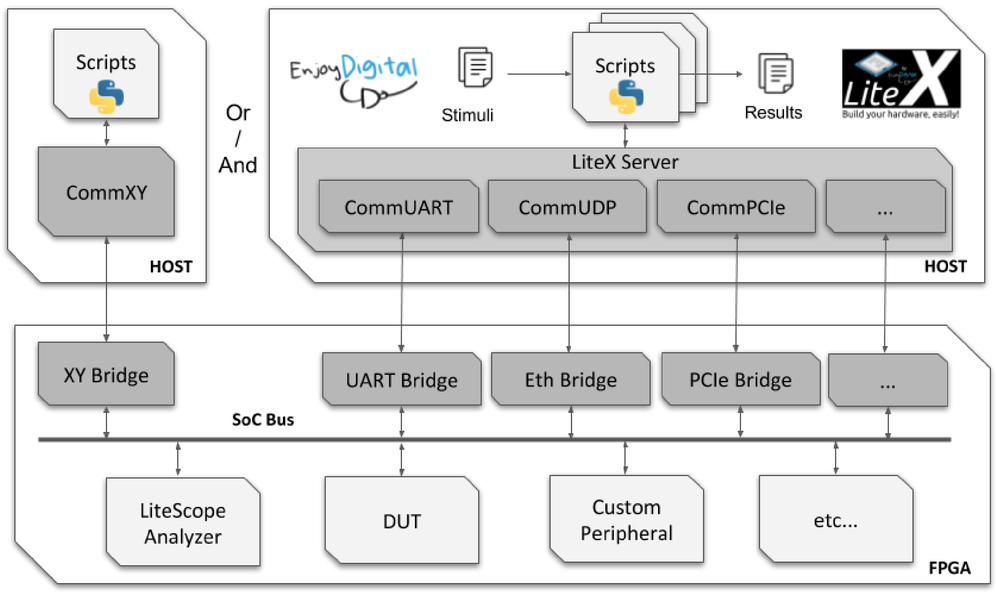
Xilinx Alveo U50-DD [4]

HBM Memory Capacity
8 GB
HBM Bandwidth
316 GB/s[1]
Internal SRAM Capacity
28 MB
Internal SRAM Bandwidth
24 TB/s



Signals must be captured:
- in real time
- without perturbing the system
- with the limited resources available

LiteX / LiteScope [5]



LiteX Remote Control/Debug Infrastructure

Two main components:
- Host Computer
- FPGA with Logic Analyzer

New possible use-cases

- Side-channel attacks: Spectre, Meltdown, Rowhammer
- Hardware Trojans: processor and peripheral levels
- Reverse engineering of CPUs behavior

[1] Secure-IC. “Hardware Trojans’ threat in IC supply chain.”
[2] Bourdon, Malcolm et al. “Hardware-Performance-Counters-based anomaly detection in massively deployed smart industrial devices.” IEEE 19th International Symposium on Network Computing and Applications (NCA) (2020).
[3] Mao, Yuxiao et al. “MATANA: A Reconfigurable Framework for Runtime Attack Detection Based on the Analysis of Microarchitectural Signals.” Applied Sciences (2022).
[4] AMD Alveo™ U50 Data Center Accelerator Card
[5] Florent Kermarrec et al. “LiteX: an open-source SoC builder and library based on Migen Python DSL.”