Hardware security counters built from microarchitectural signals analysis

HARRIS workshop - 03/17/2025

Lucas Georget

EDF R&D / LAAS-CNRS

LAAS-CNRS
/ Laboratoire d'analyse et d'architecture des systèmes du CNRS

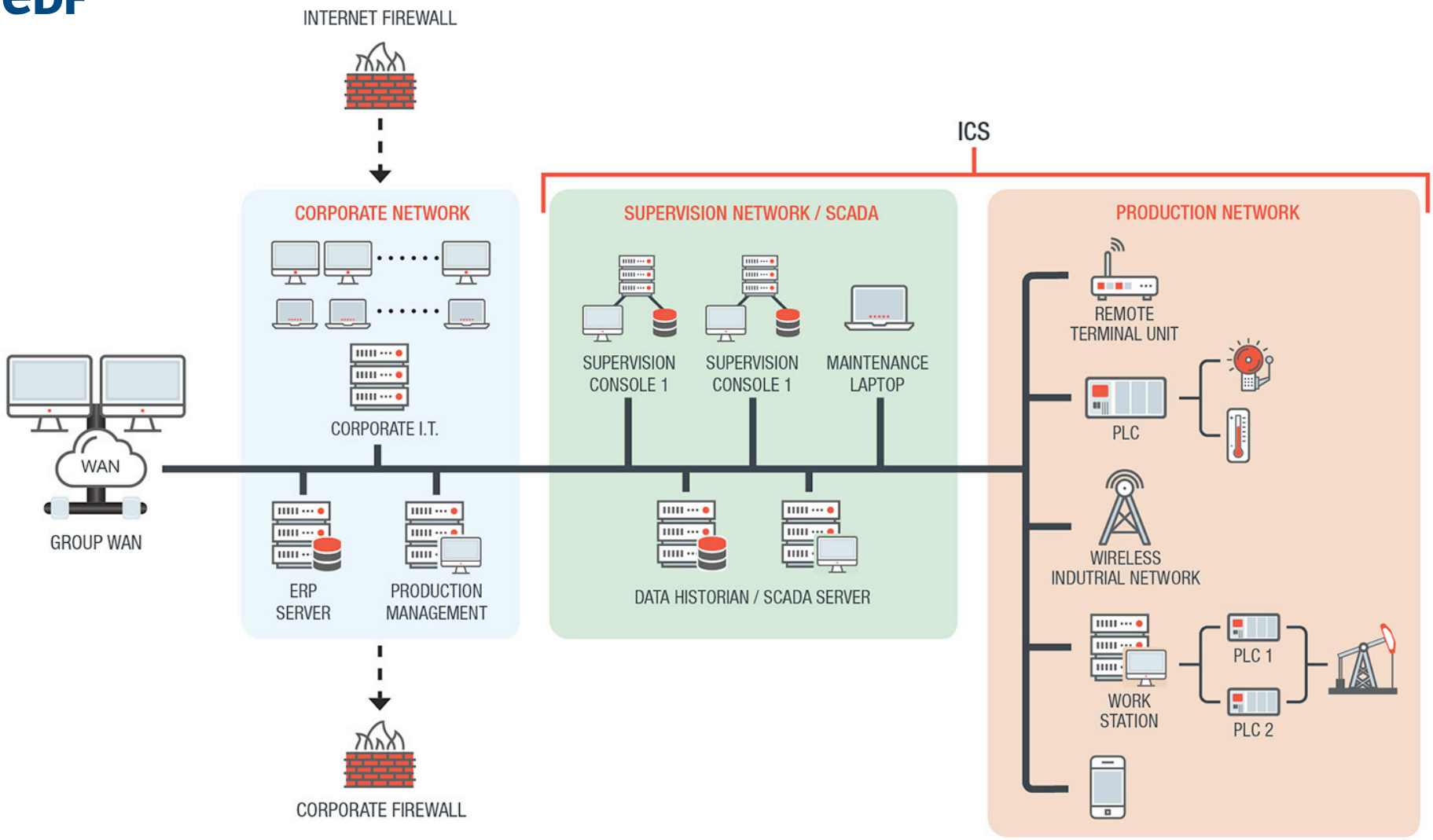
Laboratoire conventionné avec
Université de Toulouse

CIFRE PhD environment

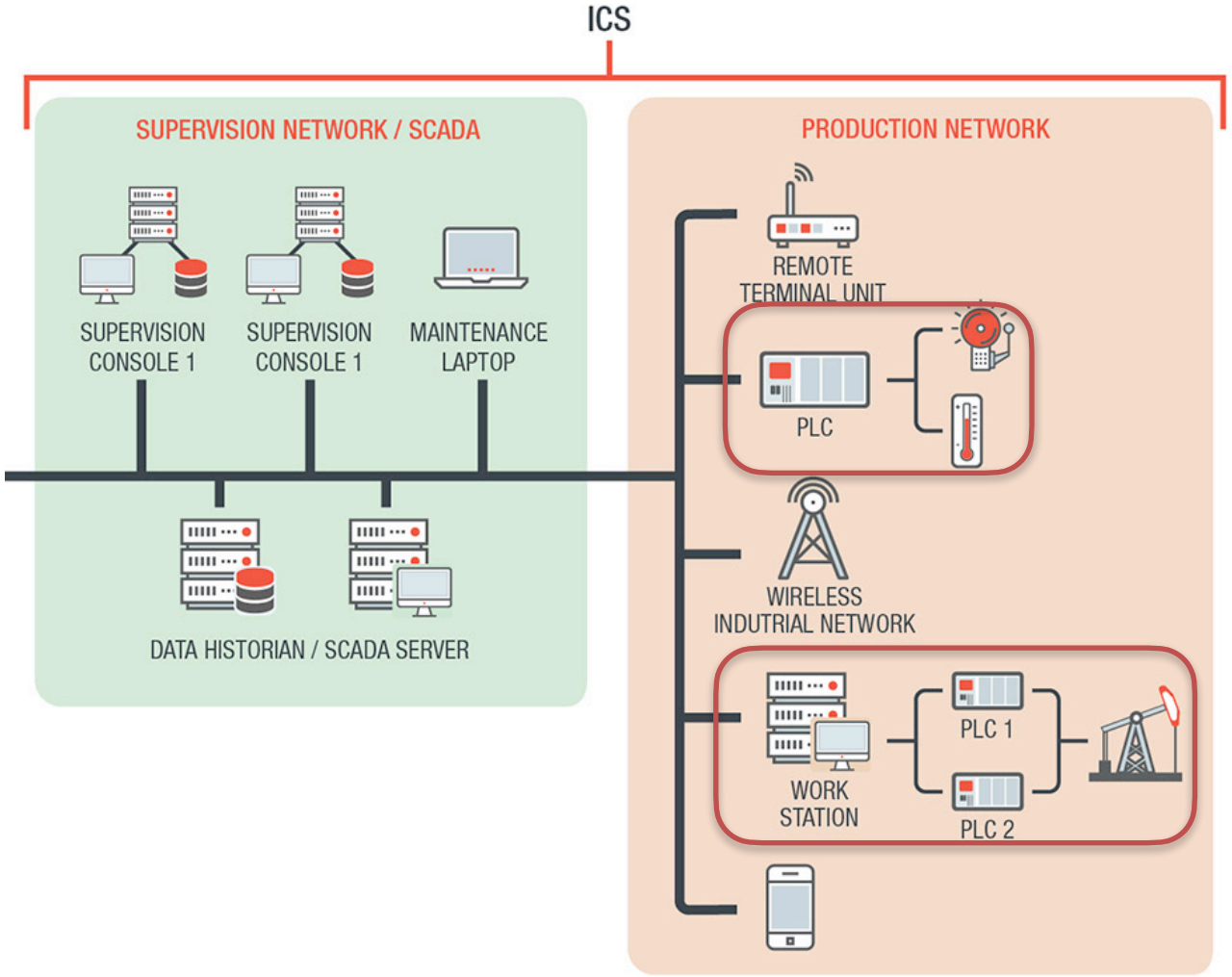
- EDF R&D (Paris-Saclay)
  - Industrial company
  - Electricity producer & provider
  - Frédéric Silvi & Arthur Villard

- LAAS-CNRS (Toulouse)
  - Academic laboratory
  - System architecture & analysis
  - Vincent Migliore & Vincent Nicomette

Context: Industrial Control System

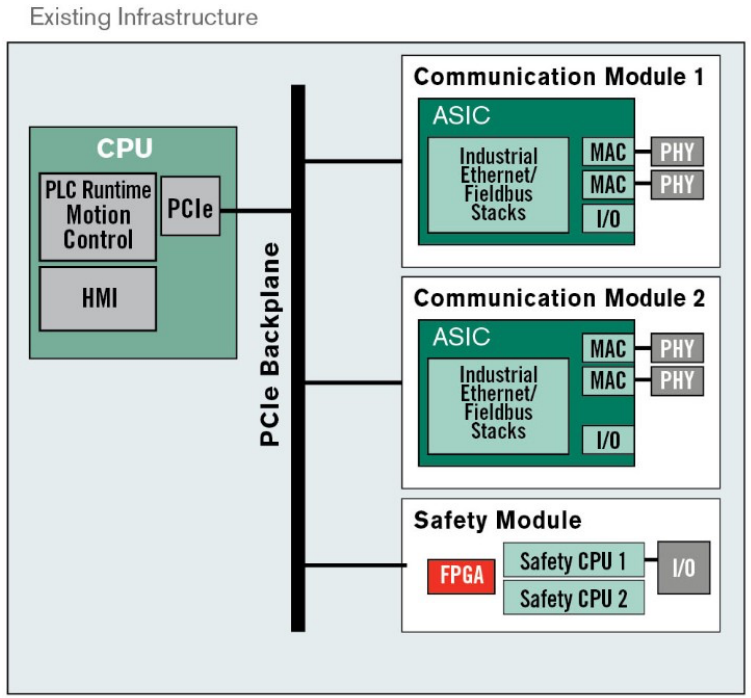


Context: Industrial Control System



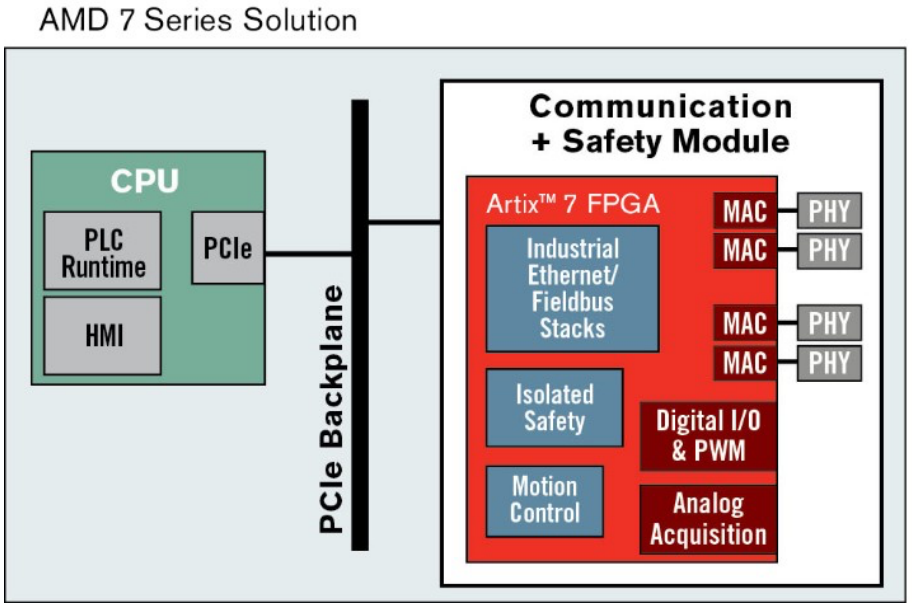
Context: Command & Control Systems

- Programmable Logic Controller
  - Deterministic behavior
  - Real-Time constraints
- Critical systems
  - Safety functions
  - Qualification



Context: Command & Control Systems

- COTS PLCs
  - Legacy
  - Strict needs
- Industrial FPGAs
  - Low-Power
  - Reliable
  - Reconfigurable



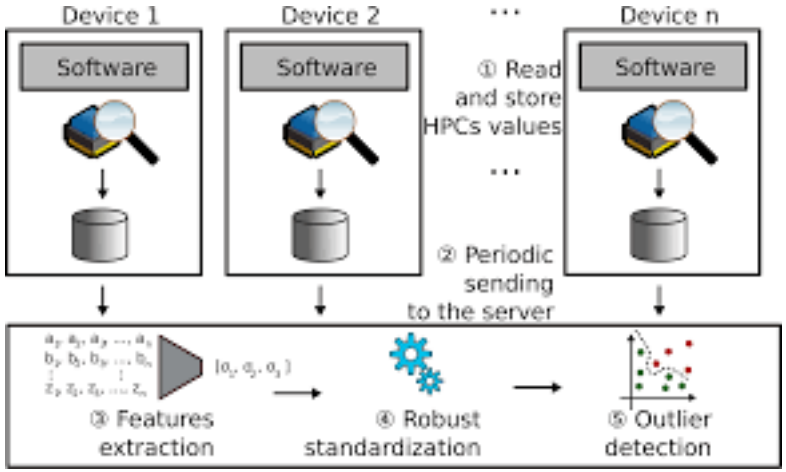
Research problem: Attack detection

- **Threat scenario**
- Low-level attacks
  - Close to hardware
  - Ex: Microarchitectural malwares, trojan horses

- **Proposed solution**
- Low-level detection metrics for:
  - Anomalies (light systems)
  - Signatures (known attacks)

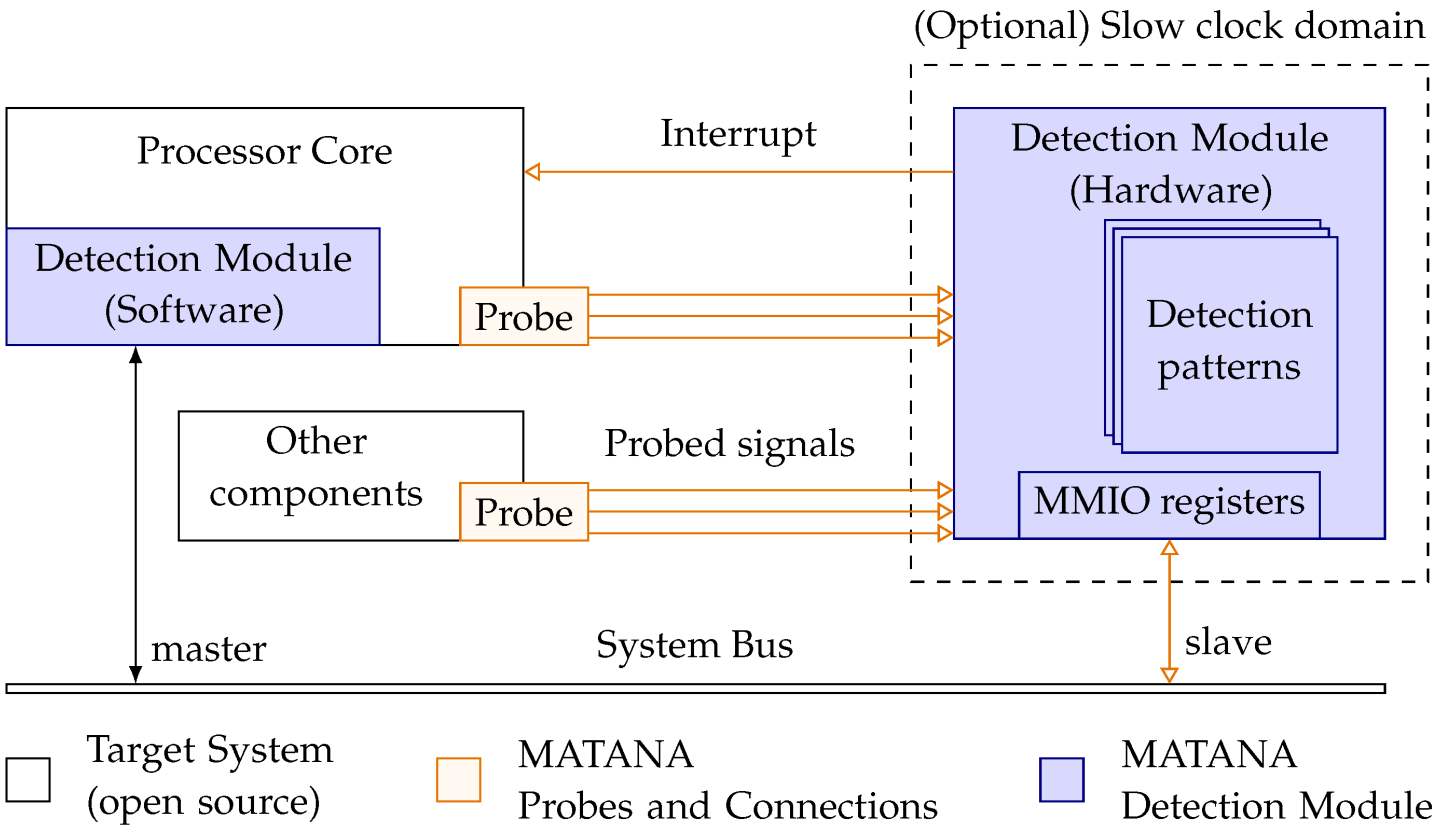
SotA: Hardware Performance Counters

- High detection efficiency with
  - Low overhead
  - Low execution time



- But… events from a
  - small and predefined list
  - Let's create that for security!

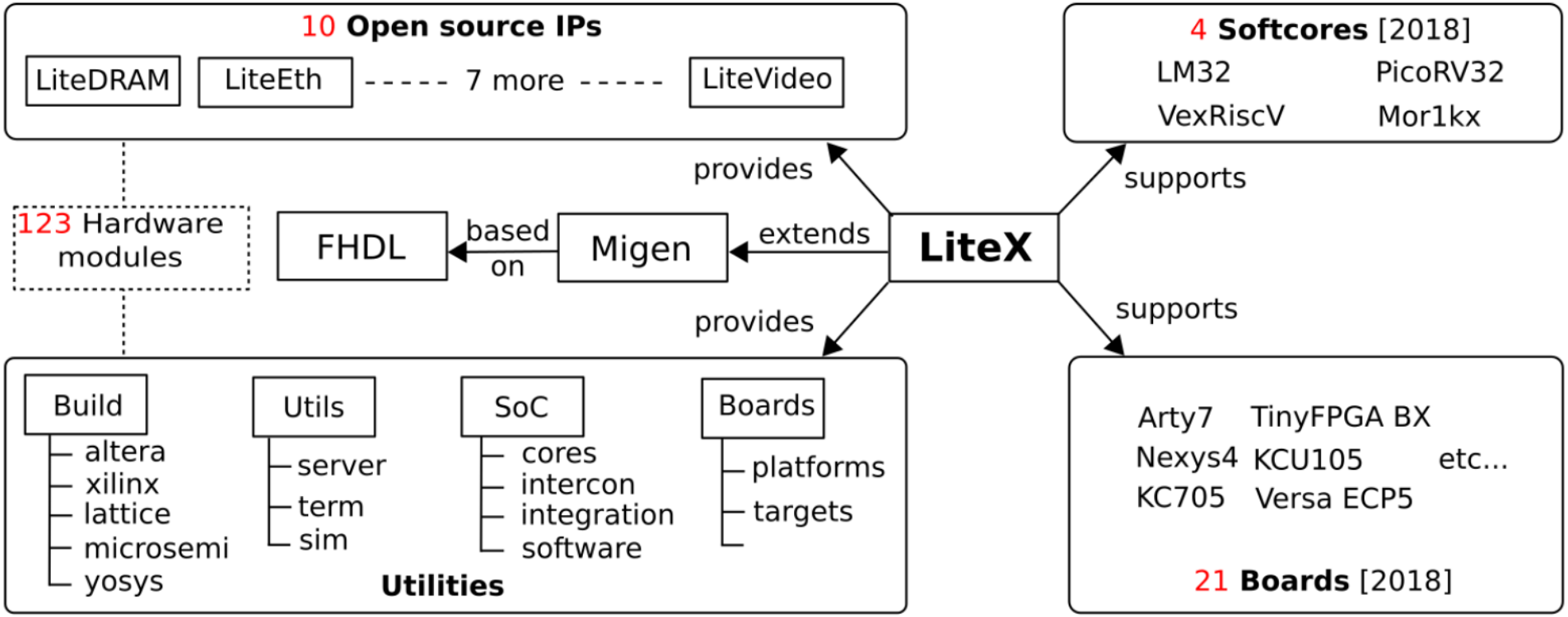
SotA: MATANA Reconfigurable Framework



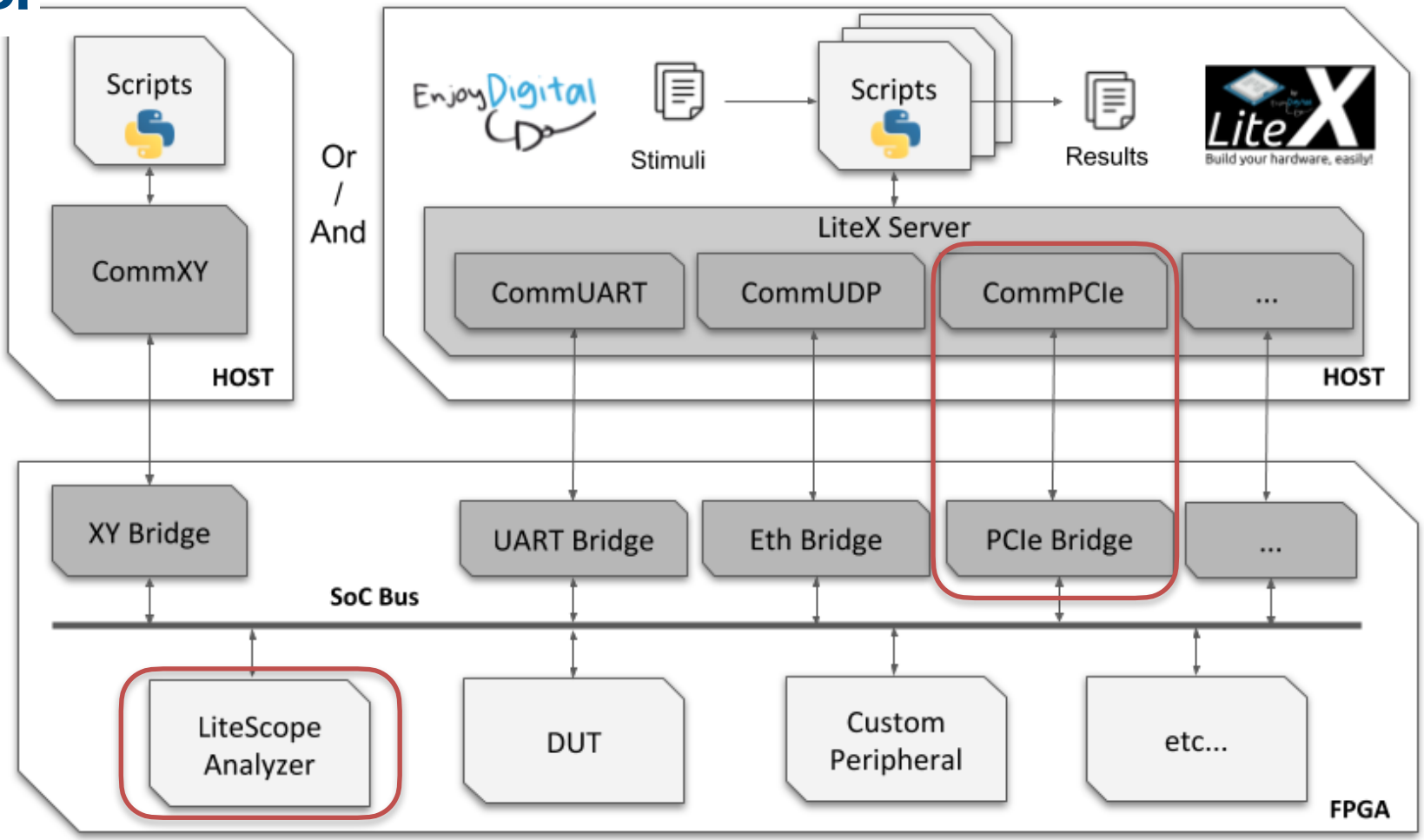
Microarchitectural signals analysis

- Contributions
  - A generic platform to monitor a large variety of microarchitectural signals
  - An experiment-based methodology on this platform to craft Hardware Security Counters

Migen/LiteX framework extension



Use LiteScope to monitor a SoC

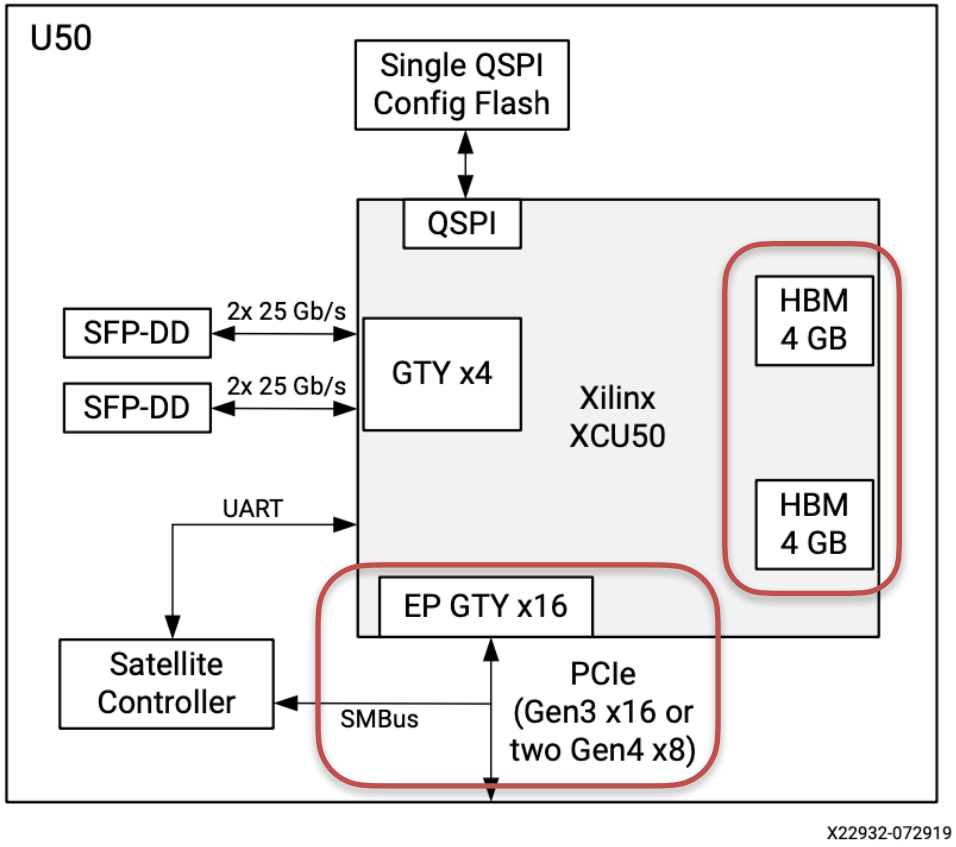


LiteX Remote Control/Debug Infrastructure

Alveo U50DD monitoring system

- HBM Memory Capacity
  - 8 GB
- HBM Total Bandwidth
  - 316 GB/s

Figure 2: **Card Block Diagram with SFP-DD Interface**



LiteScope Analyzer modifications

- Sizing (number of clock cycles)
- Signals length: 204 bits
- Depth: 6.4e10 bits
- Clk Cyc = 3.21e8

```
analyzer_signals = [
    # IBus (could also just added as self.cpu.ibus)
    self.cpu.ibus.stb,
    self.cpu.ibus.cyc,
    self.cpu.ibus.adr,
    self.cpu.ibus.we,
    self.cpu.ibus.ack,
    self.cpu.ibus.sel,
    self.cpu.ibus.dat_w,
    self.cpu.ibus.dat_r,

    # DBus (could also just added as self.cpu.dbus)
    self.cpu.dbus.stb,
    self.cpu.dbus.cyc,
    self.cpu.dbus.adr,
    self.cpu.dbus.we,
    self.cpu.dbus.ack,
    self.cpu.dbus.sel,
    self.cpu.dbus.dat_w,
    self.cpu.dbus.dat_r,
]
```

Two system configurations

- OT: Operational Technology (Industrial machines)
  - Lite/no CPU
  - RT/no OS

- IT: Information Technology (Computer systems)
  - Medium/complex CPU
  - Lite/full OS

Experiments: data labels and ML

- Data collected from
  - Benin benchmarks: Coremark, Embench, MiBench
  - Malicious ones: CSCA + ROP + …
  - With or without trojans

- Then use Machine Learning models to determine the main relevant signals

Three possible use-cases on the platform

- 1) Microarchitectural and control-flow attacks
  - Software
- 2) Hardware Trojan Horses
  - Gateware
- 3) Reverse-Engineering / Forensic

1) Software attacks

- Prime + Probe
  - Instruction signals, memory access (addresses), HPCs (cache events)
- Return-Oriented Programming
  - 32-bit instruction signal (jump), 1-bit instruction valid signal
- RISC-V Spectre, Rowhammer, Meltdown
  - To be determined…

2) Gateware attacks

- Design inserted trojans (HDL)
  - RTL and gates levels (user or CAD/EDA tools)
- Bitstream modifications
  - Netlist RE (HAL Hardware Analyzer)
  - Corrupted synthesis (trusting trust)
- Multiple impacts/effects
  - Processor core, peripherals, …

3) Reverse-engineering / Forensic

- Black-box component, characterization of
  - Platform (board)
  - SoC (cores)
  - RISC-V Soft-CPU
  - Firmware / OS

- Keeping logs for future investigation
  - Inside a TEE?
  - External extraction?

Bibliography (slides)

- 3/4: Industrial Control System (TrendMicro)
- 5/6: Industrial PLC FPGA (Xilinx)
- 8: Hardware-Performance-Counters-based anomaly detection in massively deployed smart industrial devices
- 9: MATANA: A Reconfigurable Framework for Runtime Attack Detection Based on the Analysis of Microarchitectural Signals
- 11: LiteX: an open-source SoC builder and library based on Migen Python DSL
- 12: Use Host Bridge to control debug a SoC
- 13: Alveo U50 Data Center Accelerator Card (Xilinx)
- 14: Use LiteScope To Debug A SoC

Questions?

- MATANA Framework
  - https://gitlab.laas.fr/matana
- RISC-V ROP Generator
  - https://gitlab.laas.fr/matana/bench/rop-generator
- Contact: lucas.georget@laas.fr (or edf.fr)