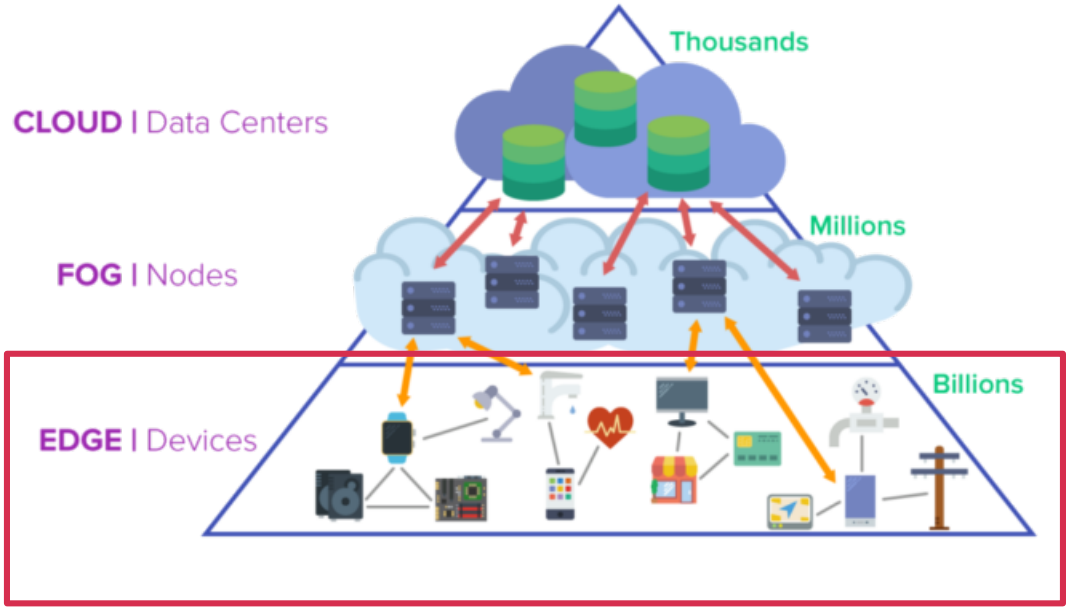
– Power monitoring at the edge – is this opening a new door to side-channel attacks?

Prof. William Fornaciari
william.fornaciari@polimi.it

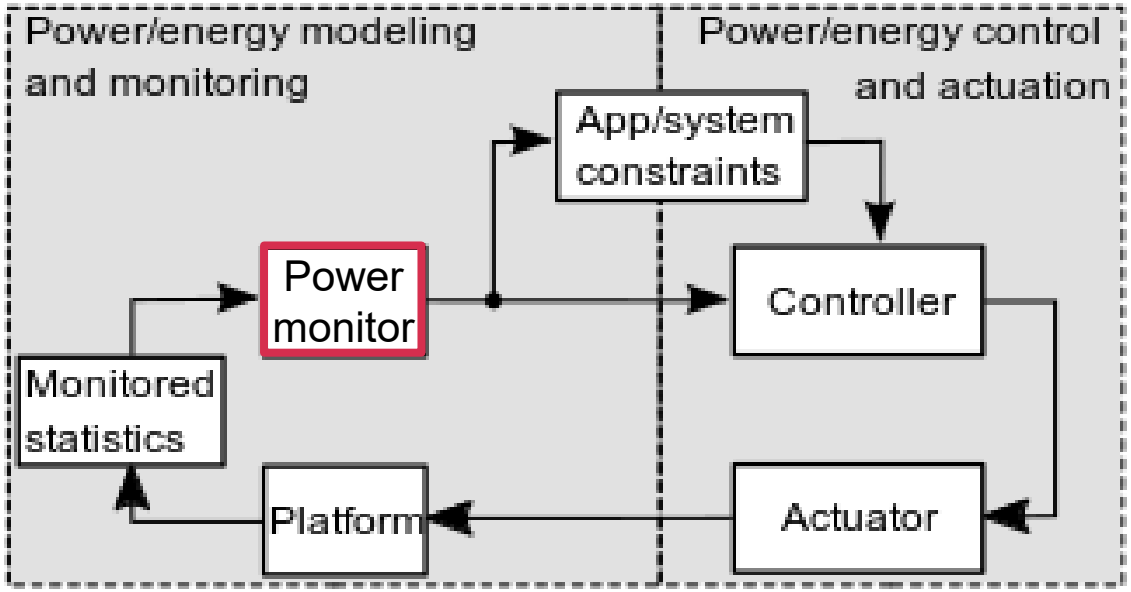
Edge computing (contrasting) requirements



Efficiency (Run-time)
- battery powered
- general-purpose computing platforms + accelerators

Security
- process private data
- execute critical tasks

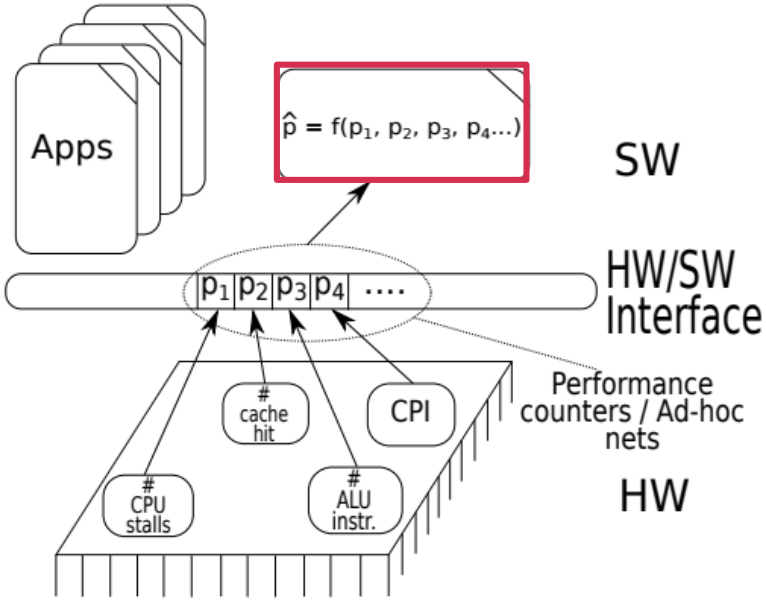
Run-time efficiency: run-time power optimizations



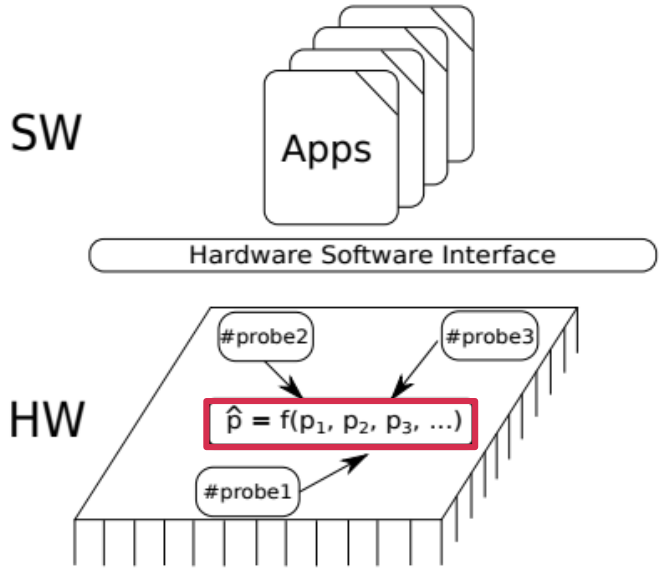
The run-time power monitoring is at the core of any run-time optimization methodology

Power monitors: hardware or software?

Software power monitors
- statistics from performance counters
- less efficient (than hw pwr monitors)
- more flexible (implementation as software application or kernel module)



Hardware power monitors
- statistics from switching activity of selected wires
- high accuracy and efficiency
- invasive (modify the RTL)

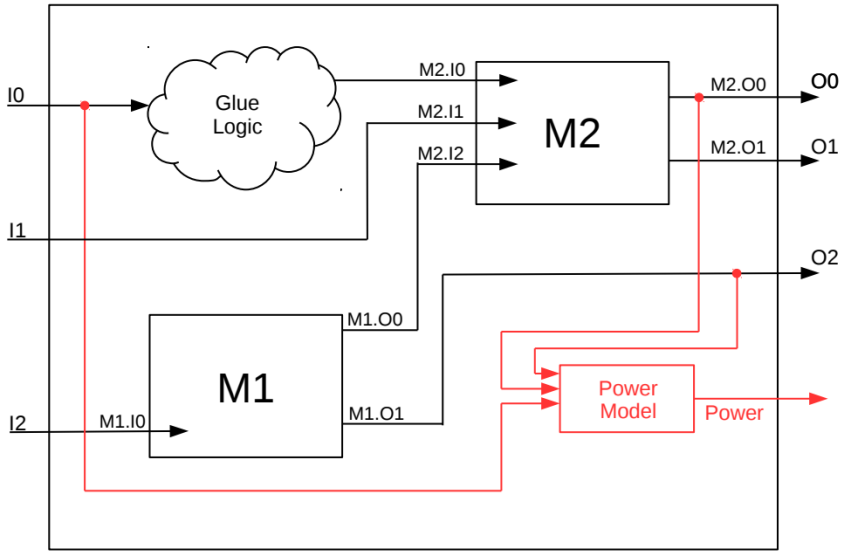


Implementation of the hardware power monitors

The two step methodology

1) Power model identification - relationship between a subset of physical signals and the power consumption

2) Power model instrumentation – add the RTL structures to implement the identified power model into the computing platform



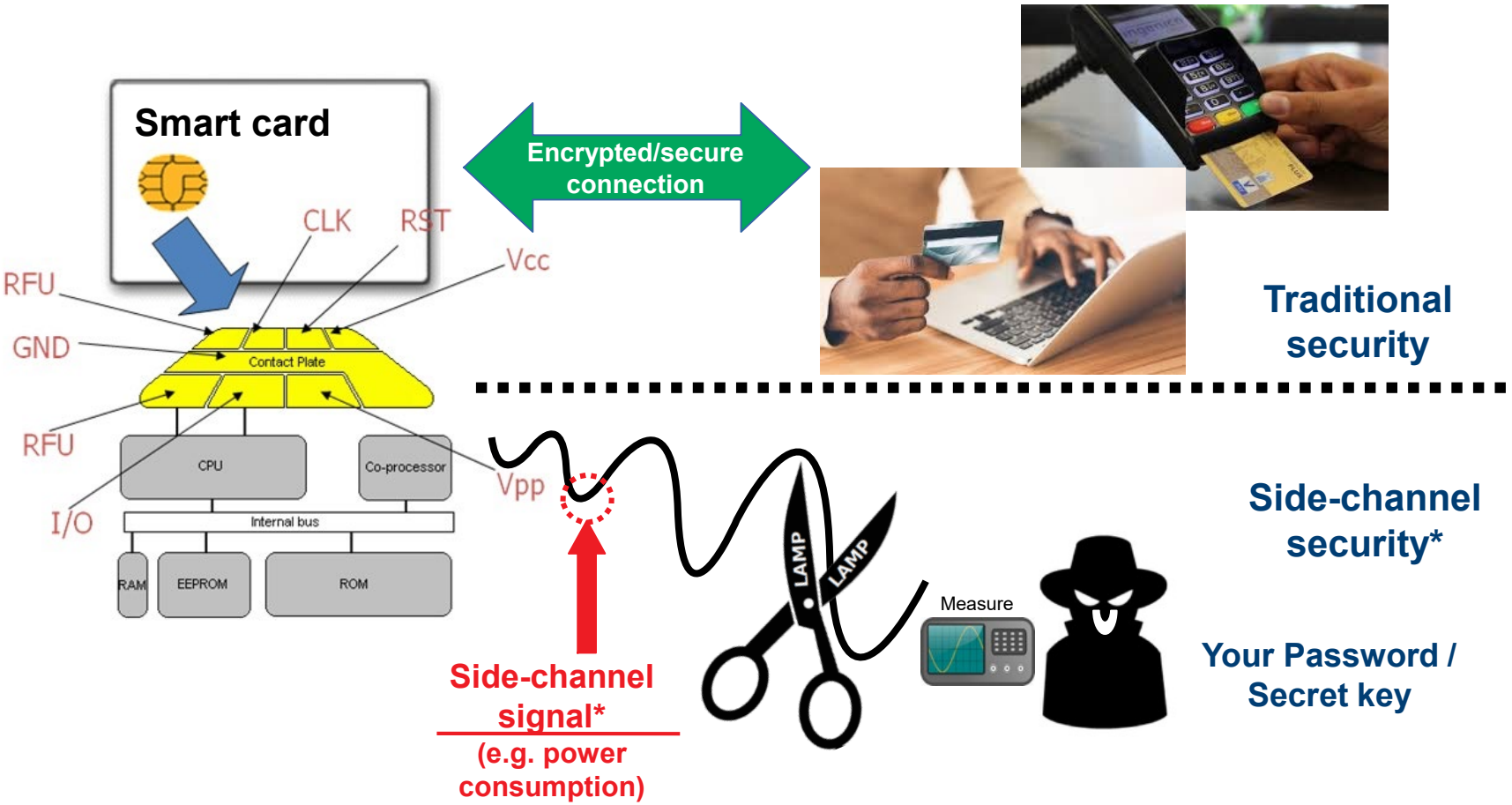
Accuracy and overhead tunable

Stress test using RISC-V platform and 8 accelerators generated via HLS

- Max avg accuracy 5% @20us resolution
- Max avg accuracy 1% @hundreds of microseconds
- Overhead is tunable, typ +5% area

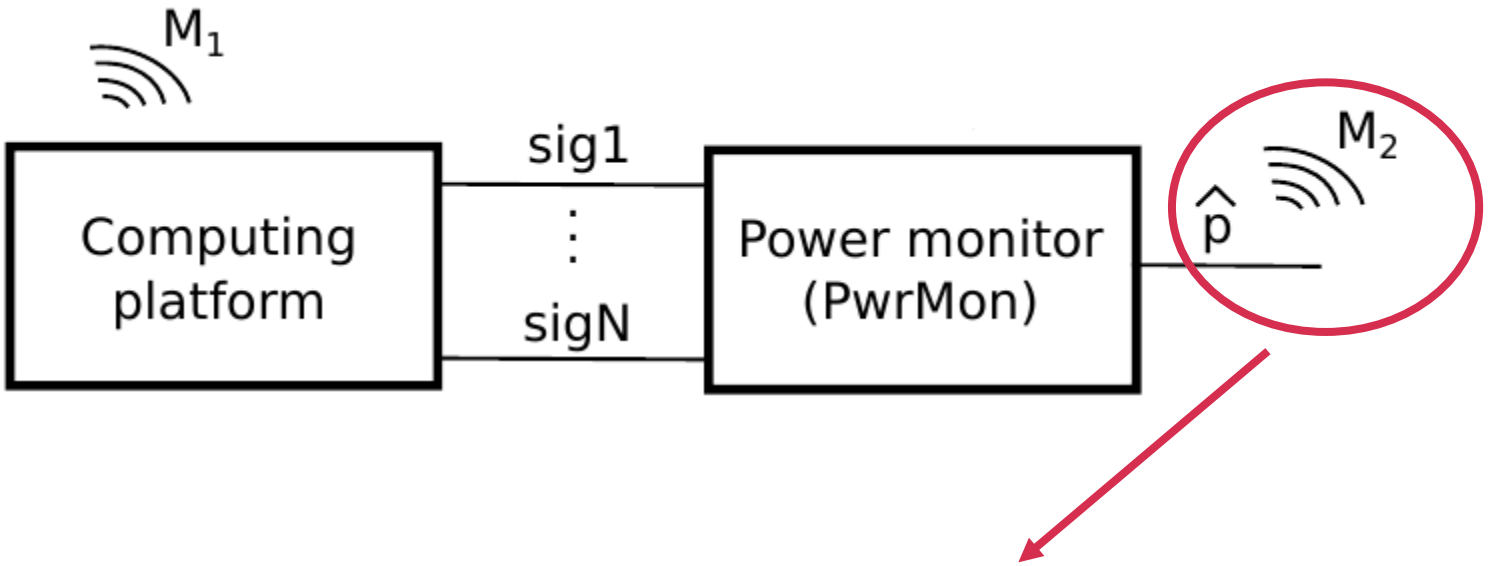
L.Cremona, W.Fornaciari, D.Zoni, Automatic identification and hardware implementation of a resource-constrained power model for embedded systems. Sustainable Computing: Informatics and Systems, Vol. 29, Part B, 2021, https://doi.org/10.1016/j.suscom.2020.100467.

Power estimates and side-channel attacks



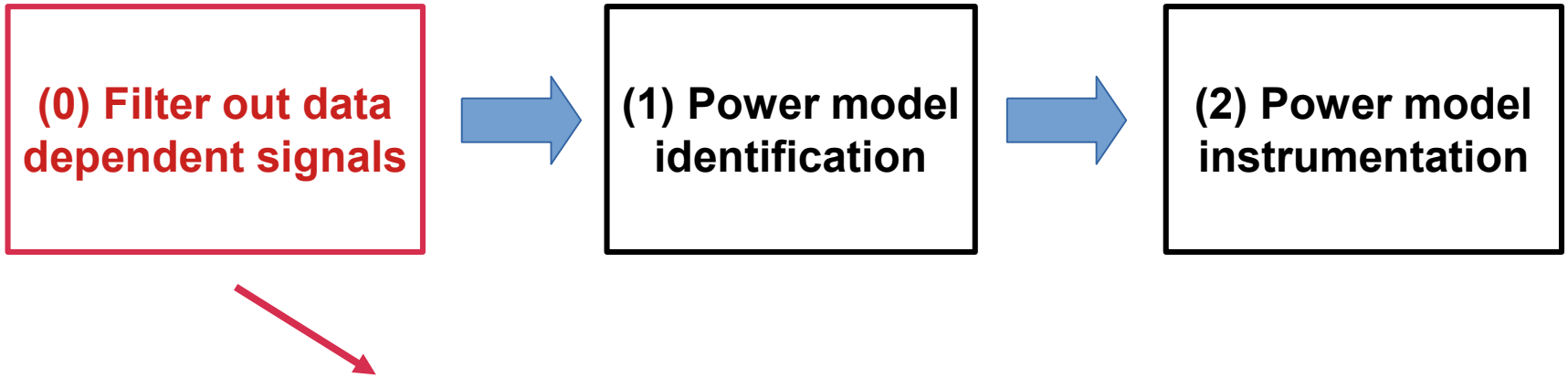
* correlate the side-channel signal with program data to retrieve the secret key

Design of secure power monitors: threat model

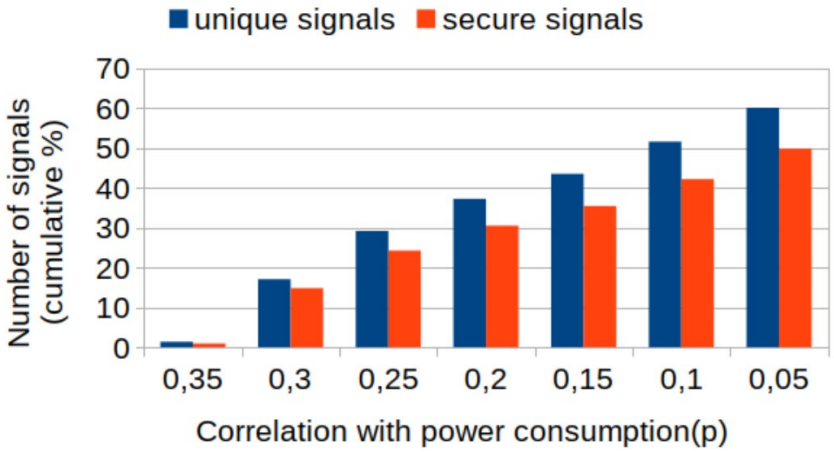


The power estimates are an information source to setup up successful side-channel attacks

Design of secure power monitors: methodology



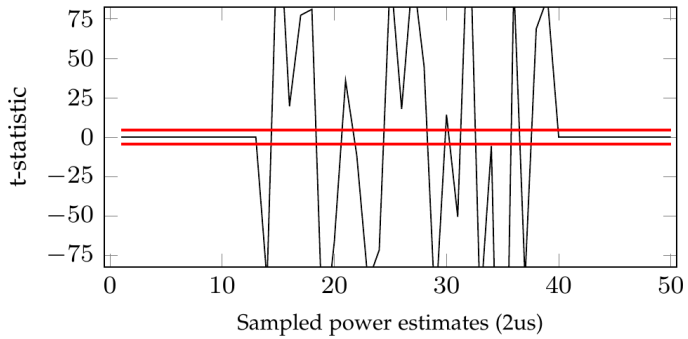
Design of secure power monitors: results [1]



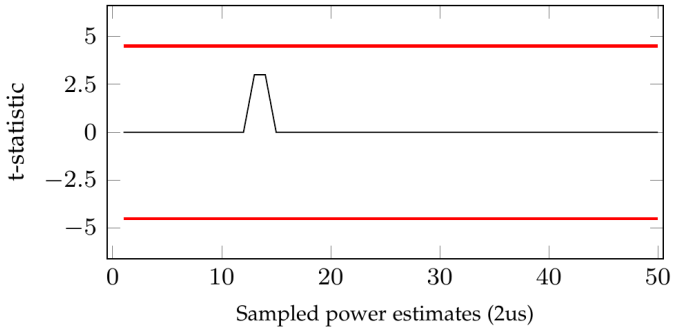
- Data dependent signals are a low fraction of the total signals

- We can design secure and accurate run-time power monitors

Secure power monitors do not show any leak via the power estimates



T-test (unprotected) power monitor



T-test secure power monitor

[1] D. Zoni, L. Cremona and W. Fornaciari, "Design of side-channel resistant power monitors," in IEEE TCAD, 2021. doi: 10.1109/TCAD.2021.3088781.

– The bigger problem –
Design secure and efficient devices at the edge

Trends in the hardware security market

Custom HW devices | process private data | execute critical tasks | time-to-market

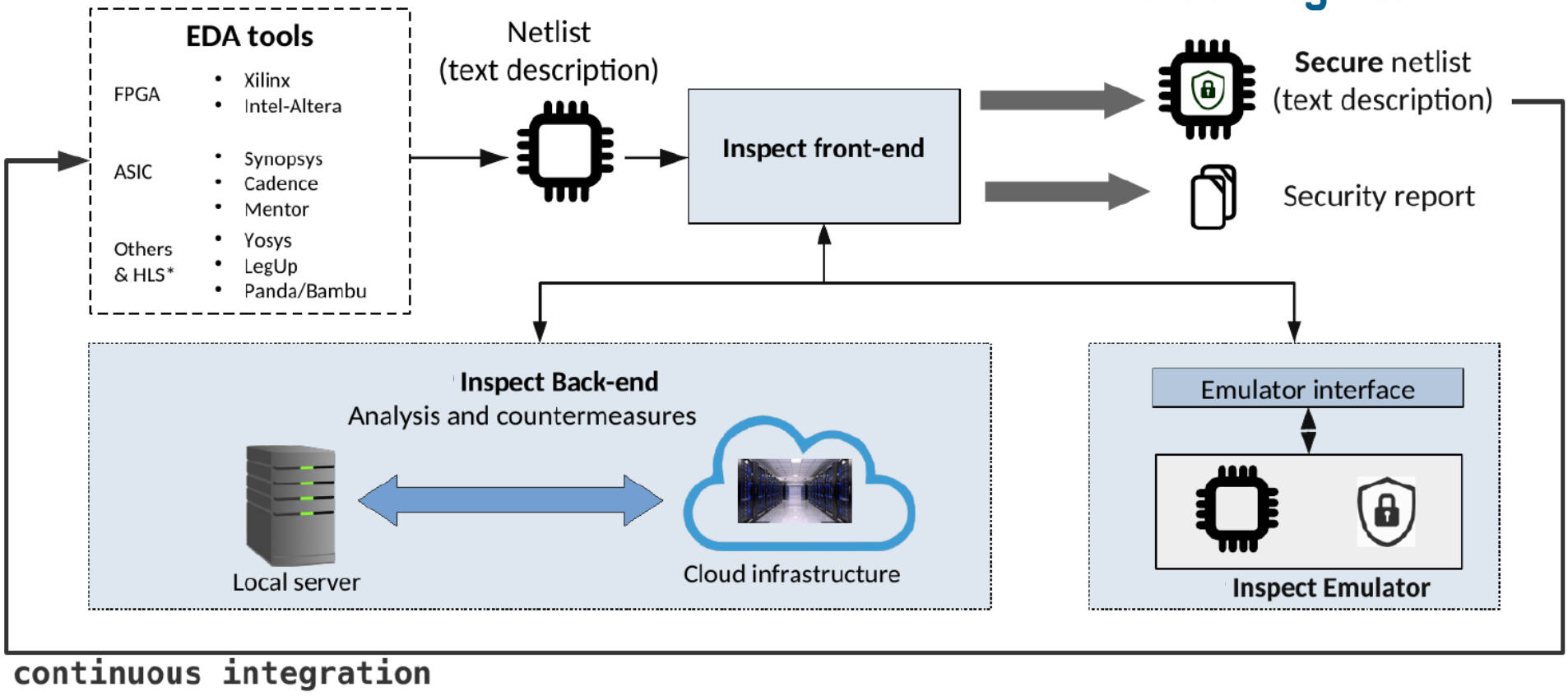
Pervasive

Trust

Anything
Anywhere
Anytime

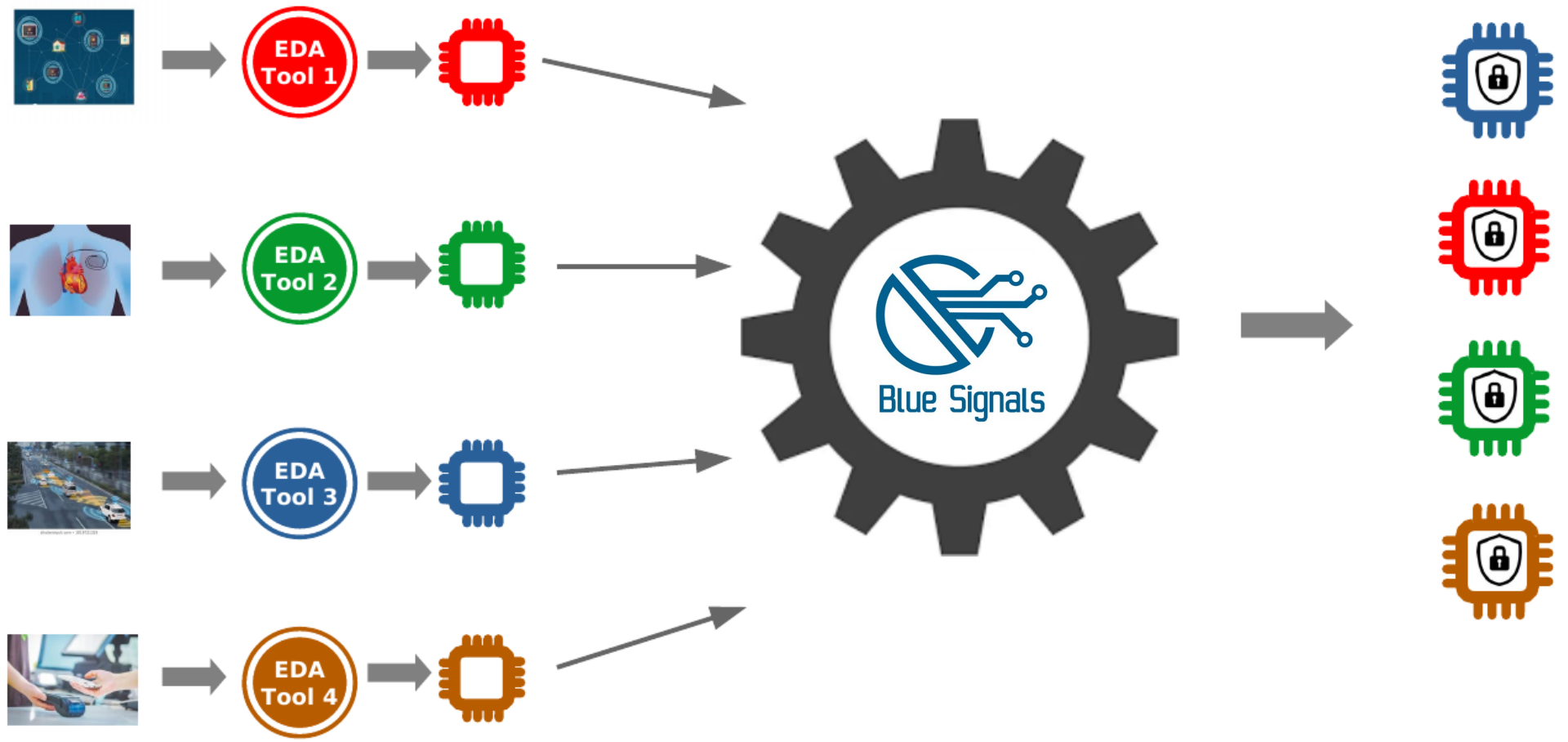
Mission Critical

Blue Signals Srl: Automatic design of secure hardware at the edge



[1] Blue Signals Srl – an innovative startup and a Politecnico di Milano spin-off – https://bluesignals.it | https://bluesignals.eu

Results – Automatic security analysis and fix of generic computing platforms at the edge



Thank you and visit https://www.bluesignals.it/

Blue Signals

Formally created as innovative academic spinoff in 2021
Winner of Switch to Product challenge in 2019 as LAMP
Collected one PoC and one industrial grant in 2020
2 Italian patents pending in 2020 and 2 PTC filed in 2021
Winner of the 2021 HiPEAC Technology Transfer Award

William Fornaciari
william.fornaciari@polimi.it

Davide Zoni
davide.zoni@polimi.it