Design of secure power monitors for hardware accelerators

AA 2023 - 2024

prof. **William FORNACIARI**
william.fornaciari@polimi.it
https://fornaciari.faculty.polimi.it/
Politecnico di Milano – DEIB

https://textarossa.eu/

Outline

- EuroHPC in a nutshell
- General information on the TEXTAROSSA project
    - Project Objectives, Technical Goals, Strategic Goals
- The vertical co-design approach
- Main technologies developed in TEXTAROSSA
- Applications used for validation
- From power monitoring to secure power monitoring
- Conclusions

EuroHPC JU (EU commission + Member states + private partners) https://eurohpc-ju.europa.eu/

EuroHPC Budget is 7 billion € for the period 2021-2027

- EUR 1,9 billion from the Digital European Programme (DEP) to support the acquisition, deployment, upgrading and operation of the infrastructures, the federation of supercomputing services, and the widening of HPC usage and skills
- EUR 900 million from Horizon Europe (H-E) to support research and innovation activities for developing a world-class, competitive and innovative supercomputing ecosystem across Europe
- EUR 200 million from Connecting Europe Facility-2 (CEF 2) to improve the interconnection of HPC, quantum computing, and data resources, as well as the interconnection with the Union's common European data spaces and secure cloud infrastructures

The EU contribution is matched by a similar amount from the participating countries. Additionally, private members are contributing an amount of EUR 900 million

#EuroHPC
Joint Undertaking

The European High Performance Computing Joint Undertaking (EuroHPC JU) will pool European resources to develop top-of-the range exascale supercomputers for processing big data, based on competitive European technology.

Member countries are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and Turkey.

EuroHPC

The JU provides financial support in the form of procurement or research and innovation grants to participants following open and competitive calls. **TEXTAROSSA is one of the accepted projects**

The TEXTAROSSA project

- Project coordinator: Massimo CELINO, ENEA
- Project Tech. Manager: William FORNACIARI, POLIMI
- Partners from 5 countries: ENEA, Fraunhofer, INRIA, ATOS, E4, BSC, PSNC, INFN, CNR, IN QUATTRO, CINI (Politecnico di Milano, Università di Torino, Università di Pisa), LTP: Universitat Politecnica de Catalunya (UPC), Université de Bordeaux
- EuroHPC Joint Undertaking, H2020 G.A. 956831
- Duration: 36 months (April 2021 – March 2024)
- Budget 6 M€
- Web site TEXTAROSSA: https://textarossa.eu/
- Website CINI lab on HPC: Key Technologies and Tools
    - https://www.consorzio-cini.it/index.php/it/laboratori-nazionali/hpc-key-technologies-and-tools
- ETP4HPC Handbook on ISSU:
    - https://issuu.com/etp4hpc/docs/european_hpc_handbook_2021_final

Long – term project objectives

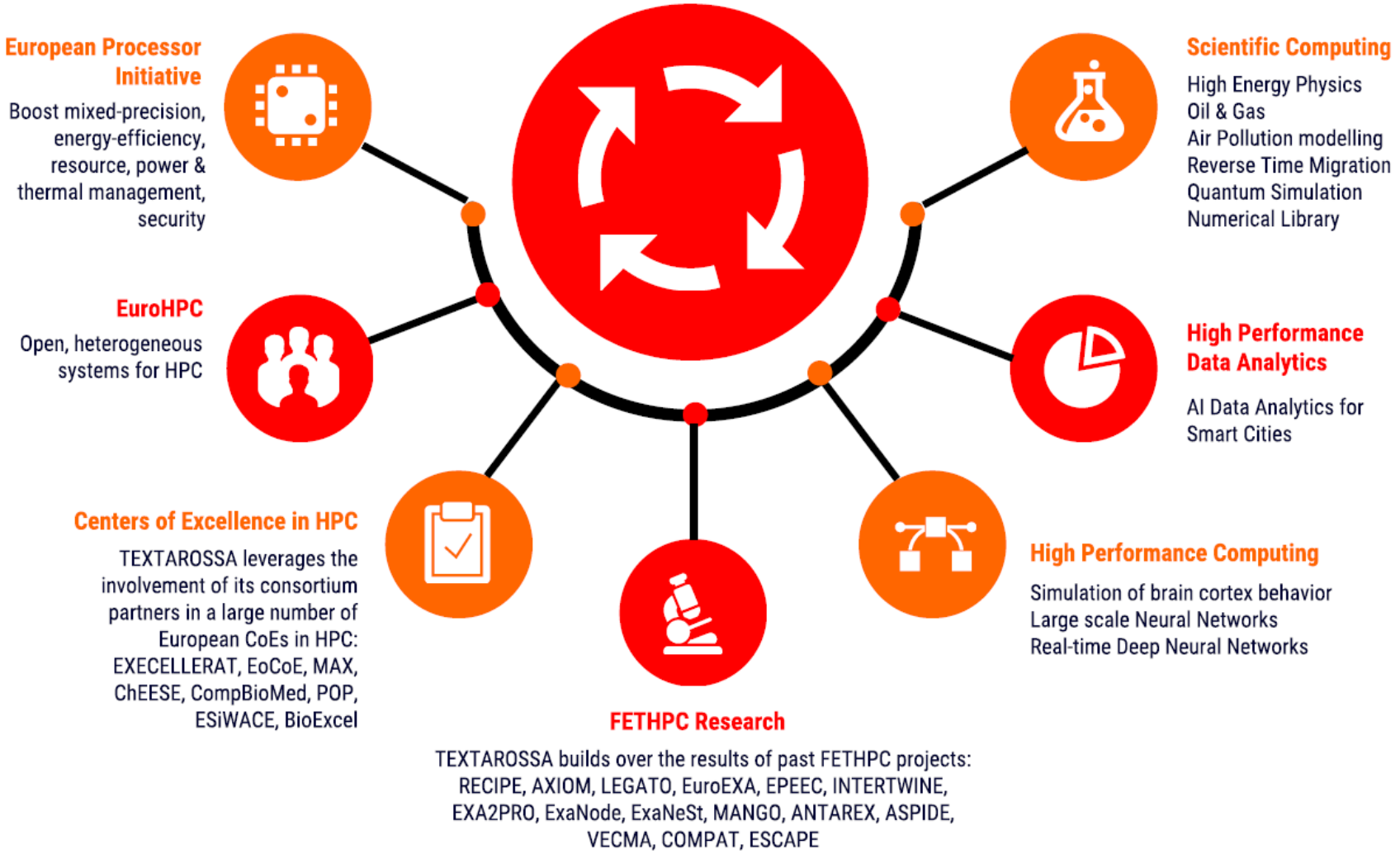
- HPC is vital infrastructure for industry and social actors
- *Heterogeneous* computing architectures and *Green HPC* are pillars for both research and industry
- Need for a holistic approach for the Hardware/Software stack design
    - Development of application-specific hw accelerators
    - Run-time resource management
    - Data management and software development
    - Thermal/power management and cooling systems
- TEXTAROSSA provides technology advances and key technologies
    - Validated on new platforms representative of HPC nodes
    - Covering several application domains (traditional and emerging)

Main technical goals

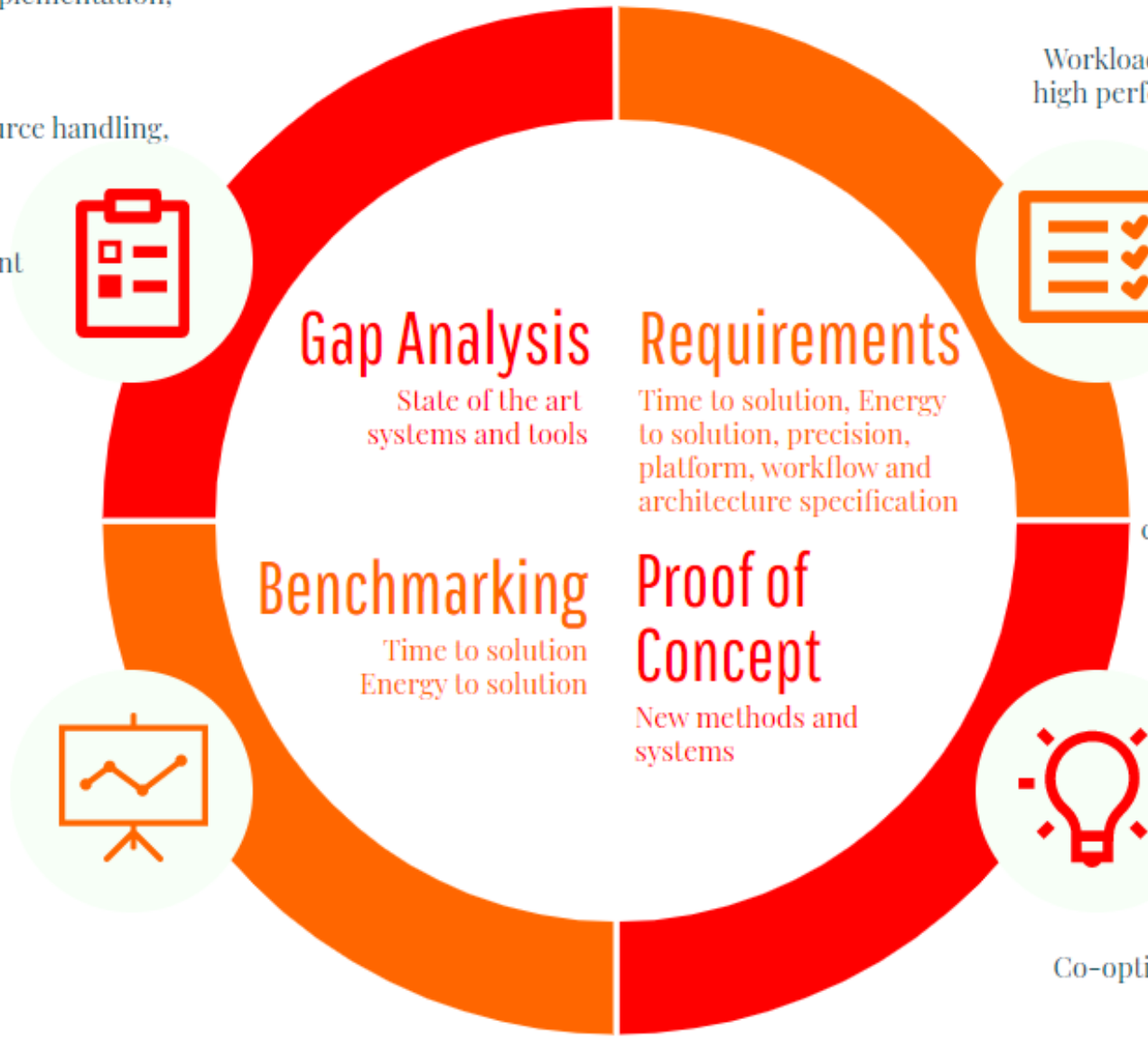
1. **Energy efficiency and thermal control**
   - innovative two-phase cooling technology at node and rack level, fully integrated in an optimized multi-level runtime resource management
2. **Sustained application performance**
   - efficient exploitation of highly concurrent accelerators (GPUs and FPGAs) by focusing on data/stream locality, efficient algorithms and programming models, tuned libraries and innovative IPs
3. **Seamless integration of reconfigurable accelerators**
   - by extending field-proven tools for the design and implementation such as Vitis and OmpSs@FPGA to support new IPs and methodologies such as mixed-precision computing and power monitoring and control
4. **Development of new IPs**
   - for mixed-precision AI computing, data compression, security, power monitoring and control, and scheduling
5. **Integrated Development Platforms**
   - by developing two architecturally different, heterogeneous Integrated Development Vehicles (IDVs), one as a dedicated testbed for two-phase cooling technology, and one supporting the wider range of project technical goals

Main strategic goals

- Alignment with the European Processor Initiative (EPI)
- Supporting the objectives of EuroHPC: Strategic Research Agenda (SRA) for open HW and SW architectures
- Building over European expertise
- Opening of new usage domains (HPDA, HPC-AI) + traditional HPC domains



- # A vertical 4-stage Co-Design-centric process workflow



User Applications
Computing models, implementation, algorithms, AI, HPDA

Runtime Services
Execution model, resource handling, fault tolerance, I/O

Programming Models
Toolchains, development tools

System Architectures
CPU, GPU, FPGA, Transprecision, memory, I/O, network

Hardware Platforms
Node and rack

User Applications
Time/Energy to solution, Precision, Data locality

Runtime Services
Workload-specific, parallel workflow, high performance I/O, time to solution

Programming Models
Design, verification, IP integration, emulation debugging, optimization

System Architecture
IP/SoC, low power, ARM SVE, RISC-V, bandwidth/latency

Hardware Platform
Power supply/management cooling, thermal management

User Application
New methods and algorithms

Runtime Services
Energy-aware management

Programming models
Toolkits for heterogeneous architectures

System Architectures
Co-optimized with toolchain and API

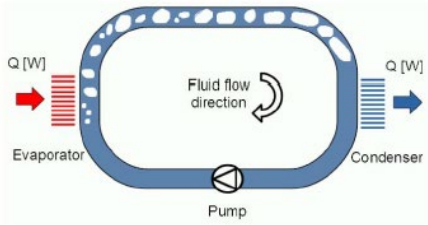
Hardware Platforms
Energy efficient and heterogeneous

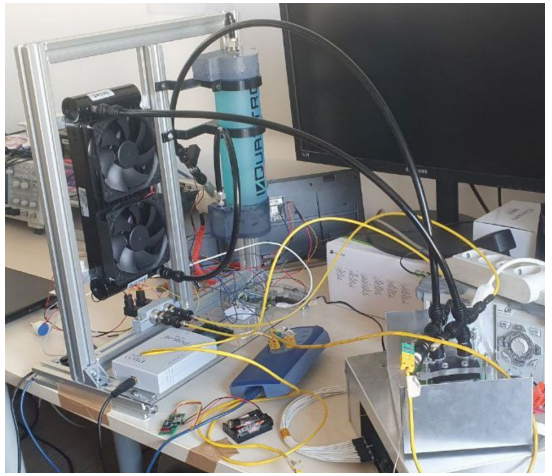
Technologies - Programming Models & Toolchains

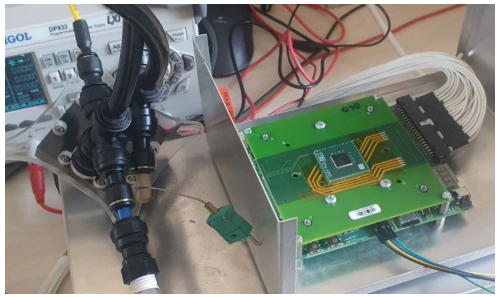
- **Vitis based HLS flow** to define the interface APIs for new accelerators
- **StarPU, OmpSs.** Task based programming models extended to simplify the management of heterogeneous resources
- **FastFlow**. Library to support low-latency and high-throughput data-flow streaming networks
- **Streamflow**. Container-native Workflow Management System (WMS) written in Python 3 and based on the Common Workflow Language (CWL)
- **Compiler Technology for Mixed-Precision Support.** Support to the exploitation of new data types (e.g. Bfloat, Posit) whose FPUs are developed

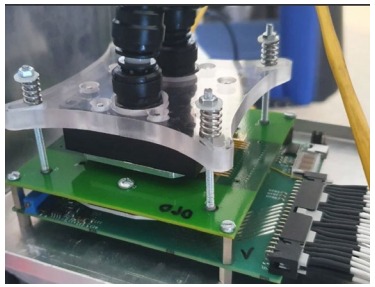
Technologies – Thermal Management

- Innovative two-phase cooling system for node(s) with the objective to serve an entire rack
- Improvement of the cooling efficiency up to 70% compared to air cooling, up to 30% compared to liquid cooling. It will be tested on both ATOS and E4 infrastructures
- Design and validation of thermal models taking advantage of equation-based object-oriented modeling languages to easily account for two phase liquid cooling
- Model validation uses a thermal test chip to capture accurate thermal maps of chips connected to the proposed heat dissipation solution
- Multilevel control allows to partition the system level control problem into multiple interacting control loops, each optimized for the specific thermal dynamics to control









Technologies - Low-latency Communication (FPGAs)

- Users have full control of the platform, allowing the implementation of custom processing tasks on FPGAs, still maintaining ease of usage by supplying a set of interfaces to integrate with the HLS tools developed in the project
- TEXTAROSSA will develop a communication IP and its SW stack, providing the implementation of a direct network that allows low-latency communication between processing tasks deployed on FPGAs, even hosted in different computing nodes
- The direct communication between tasks deployed on FPGAs will avoid the involvement of the CPUs and system bus resources in the data transfers, improving the platform's energy efficiency and reducing communication latency

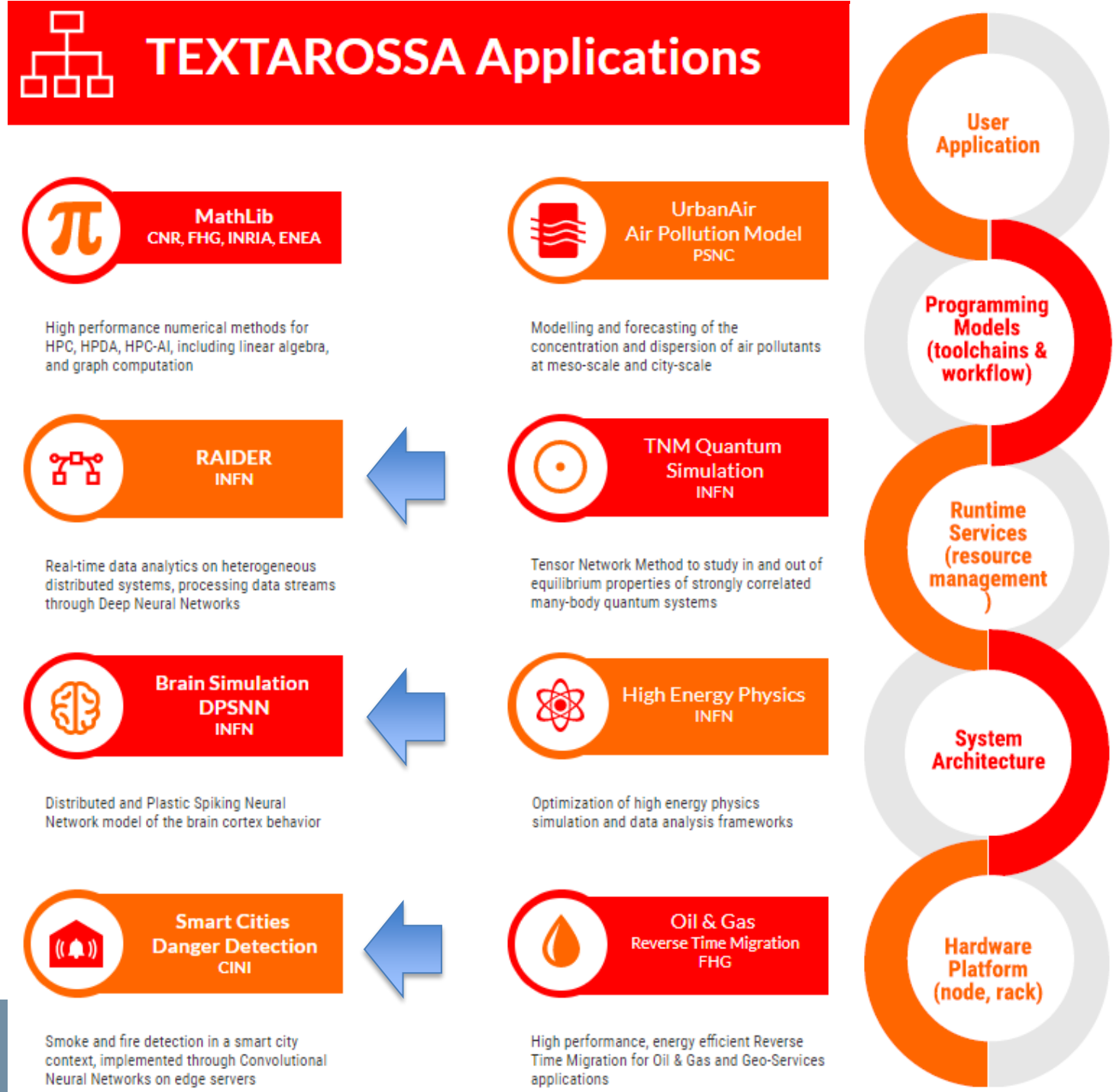
HPC-DA and HPC-AI

- RAIDER
- DPSNN
- DANGER DETECTION

Traditional HPC apps

- Urban air
- TNM
- HEP
- HPC-Drugs
- RTM

Mini-apps to test specific features

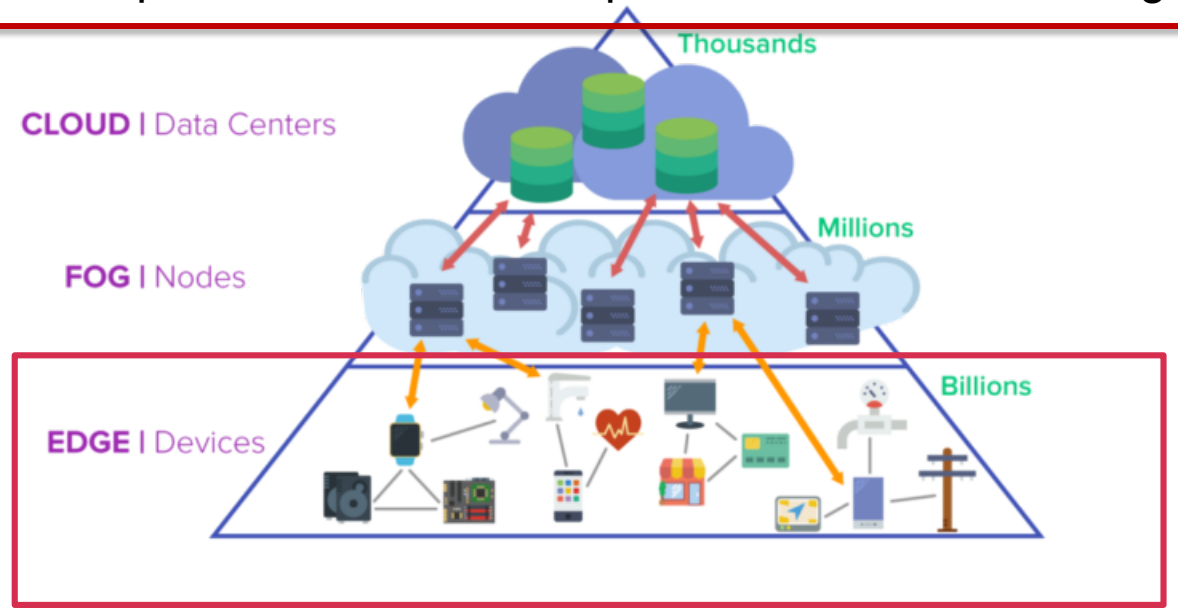


Who needs of power monitoring?

- TEXTAROSSA target computing platforms are heterogeneous
- Off the shelf CPUs and GPUs have some consolidated approaches for power monitoring
    - The architecture is stable
    - The workload can be variable
- FPGA-based hardware accelerators
    - Hardware is an ad-hoc design
    - During system lifetime the uploaded bitstream can vary significantly
    - Variable workload
    - Designers focus on the functionality and area constraints, power monitoring is out of the scope
- Our goal is to provide a methodology and a tool for automatically augment an RTL design with a power monitor

From edge to cloud to HPC – a flow of competing requirements

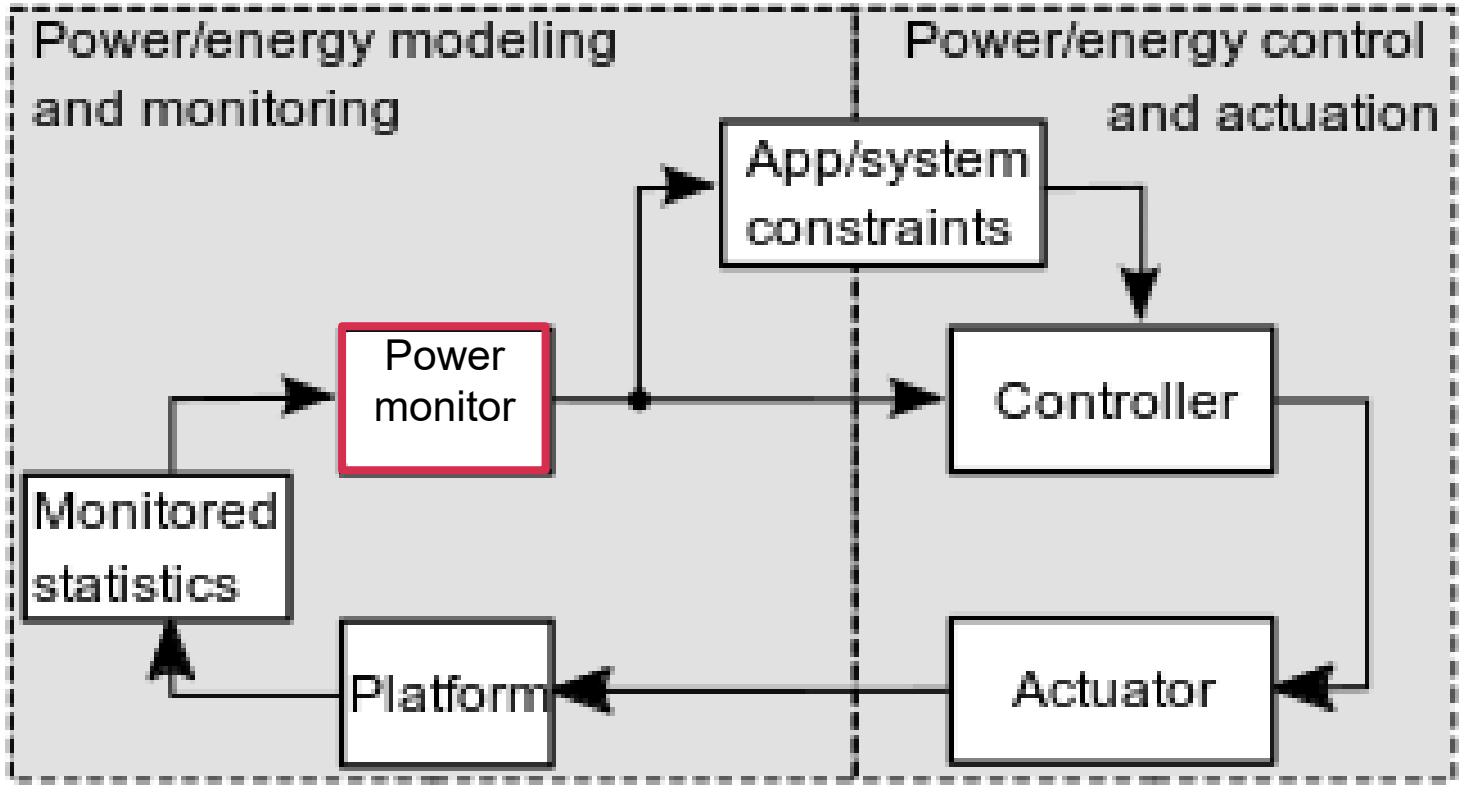
Power management of heterogeneous HPC architectures
- power and thermal walls are “real”
- need for power estimation and power control at variable granularity



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

Security
- process private data
- execute critical tasks

Run-time power optimizations need on-the-fly estimation and control

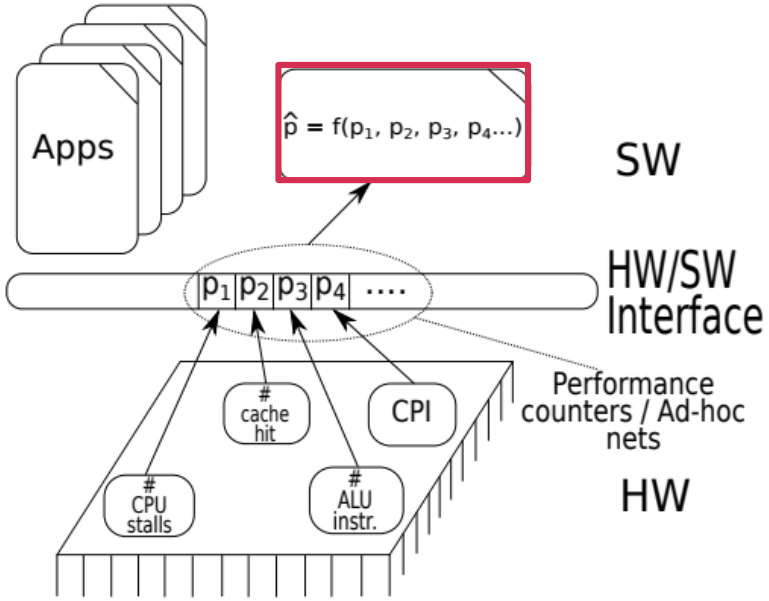


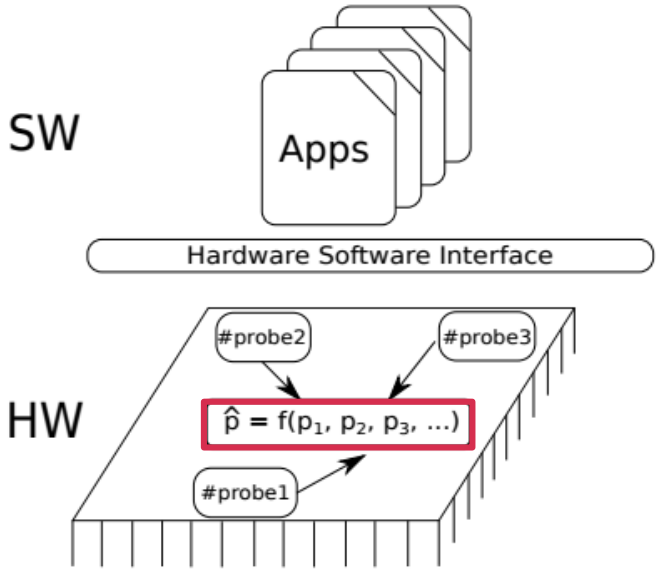
The run-time power monitoring is
at the core of any run-time optimization methodology

Power monitoring: better 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)





On the SoTA on power monitors and controllers

Power controllers: managed in software by a dedicated module of the operating system or by a resource manager

- Computations and communication latency
- Performance overhead especially in small embedded systems
- Extensions easy to implement, for example, new power allocation policies

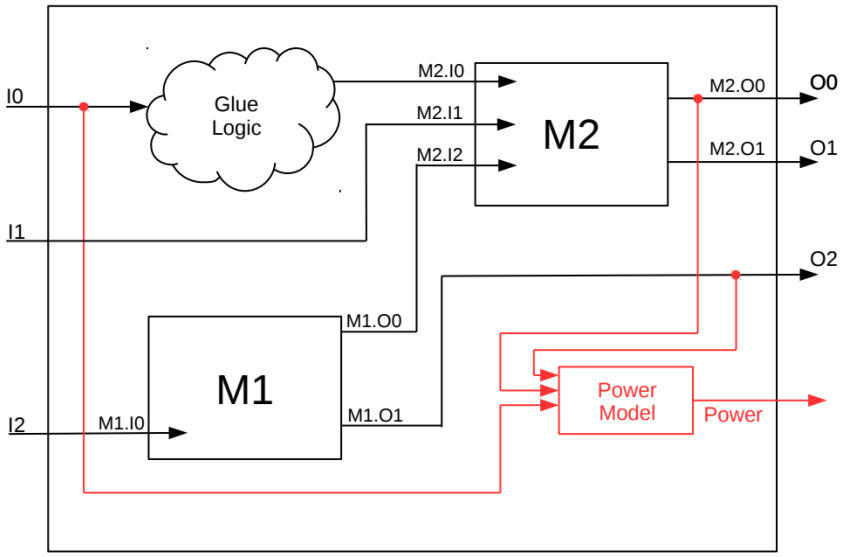
Actuators: traditionally DVFS

- Limited scalability of the voltage at current technology nodes
- Voltage scaling not available in FPGAs
- Low dynamics, not able to face high power consumption changes

Missing aspects

- Study of a systematic methodology to build a power monitor based on switching activity information
- Consider the power monitor power/resource overhead from the model identification stage
- Automatic implementation of the power monitoring infrastructure into a generic RTL design
- Study of a run-time power control methodology able to perform power/energy cupping on multi-cores systems
- Analysis of possible security issues introduced by these new power meters

Implementation of the hardware power monitors



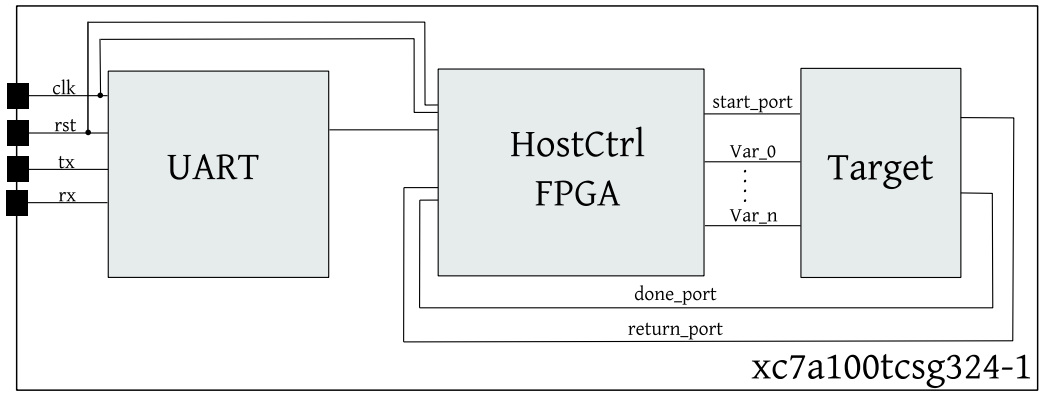
A two-step methodology

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

- Selection of the signals to reduce the implementation cost while ensuring a good accuracy
- Plug-in approach
  - No modification of the critical path to maintain original performance
  - Automatic generation of the power estimator
- Low latency in providing estimates is a boost for thermal and power management
  - Both monitor and control could move from software to hardware under sever energy/response time constraints

Online power monitoring: experimental setup



FPGA wrapper

- UART module implementing communications between PC and FPGA
- Host controller to forward the variables to the hardware accelerator
- Target accelerator implementing the algorithm

Benchmark	DSP	LUT	FF
fibonacci	0	185	101
crc	0	438	297
aes-Enc	0	491	233
aes-Dec	0	1037	137
expint	2	1361	1334
sqrt	2	2299	1682
qsort	0	2775	1323
fft	78	14974	10776
RISC-V	10	7868	5606
average	10.2	3492	2378.7

Benchmark table

- Eight benchmarks coming from WCET benchsuite
- A fully compliant RISC-V CPU

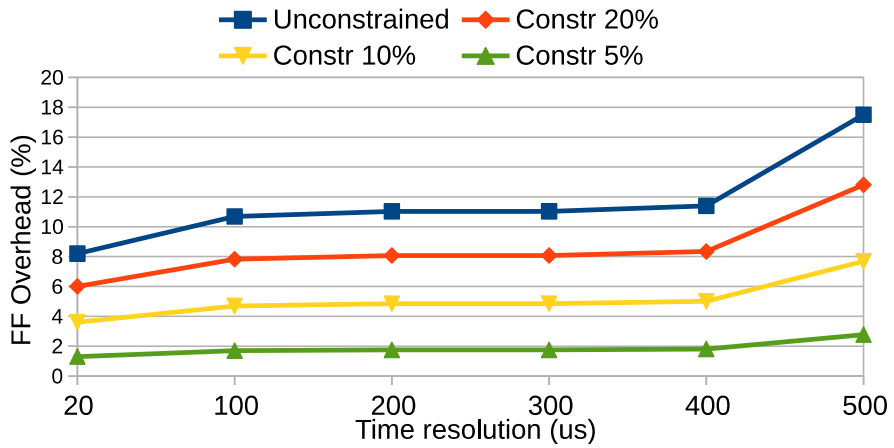
Regression was the key…

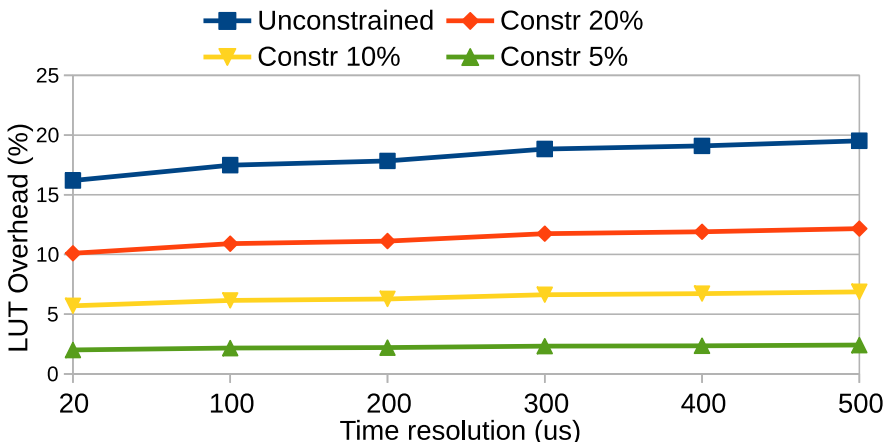
Accuracy and overhead tunable

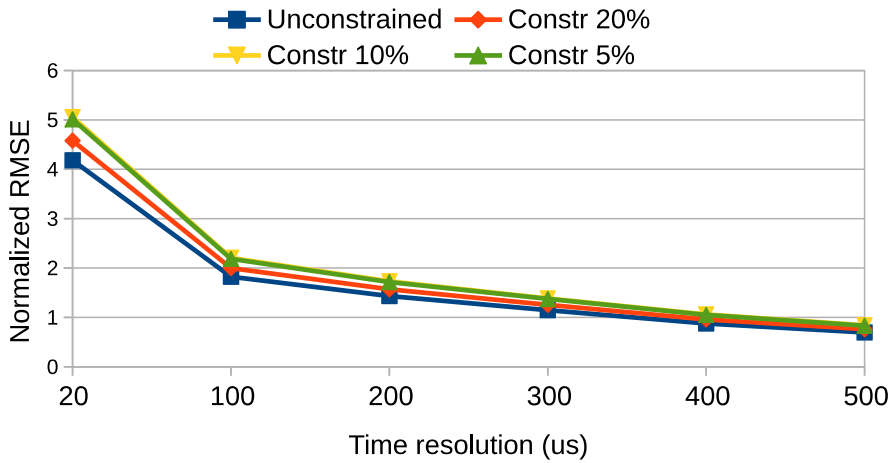
Stress test using RISC-V platform and 8 accelerators generated via HLS

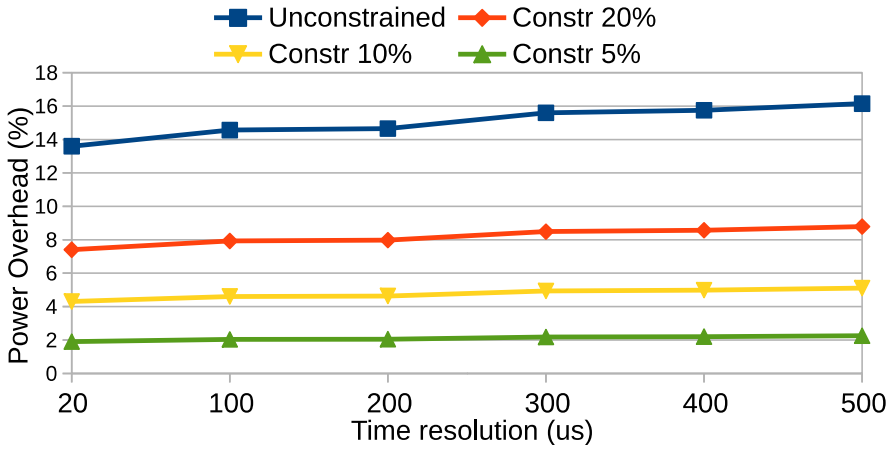
- Max avg accuracy 5% @20us resolution
- Max avg accuracy 1% @hundreds of microseconds
- Overhead is tunable, typ +5% in area

On-line power monitoring: experimental results and tradeoffs







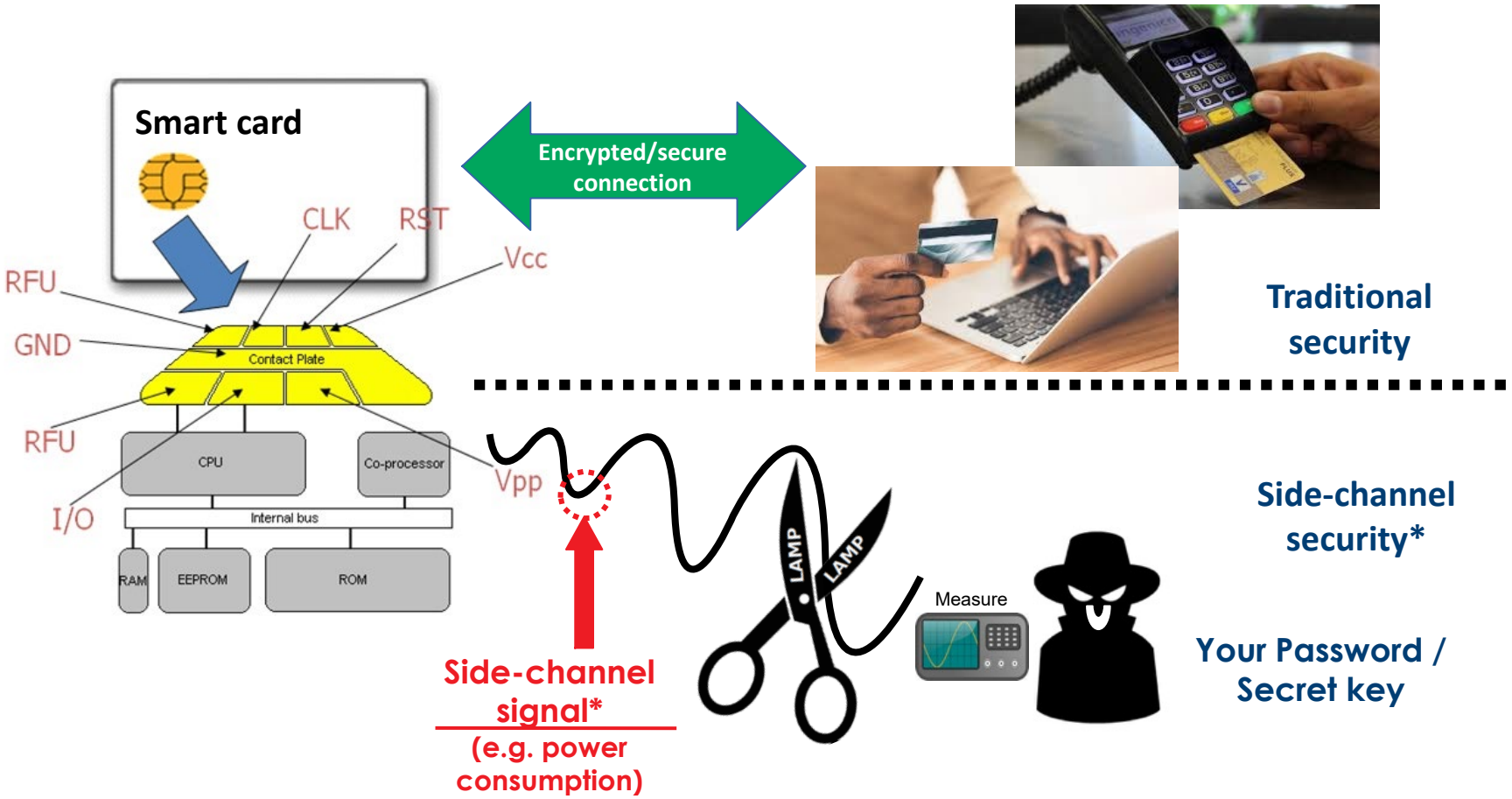


Winner of the 2020 edition of Eurolab4HPC Business Prototyping Project: GreenHLS

Luca Cremona, William Fornaciari, and Davide 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.

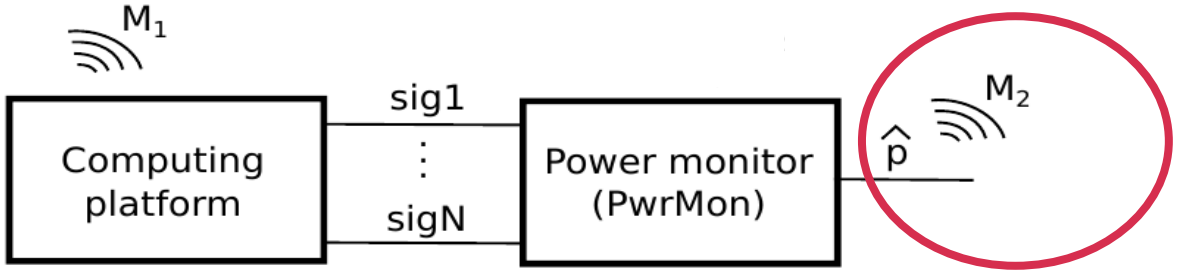
Power estimates and side-channel attacks

Perfect for closed systems, …but…
accurate power monitoring is opening the door to side-channel attacks



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

Design of secure power monitors: threat model and design methodology



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

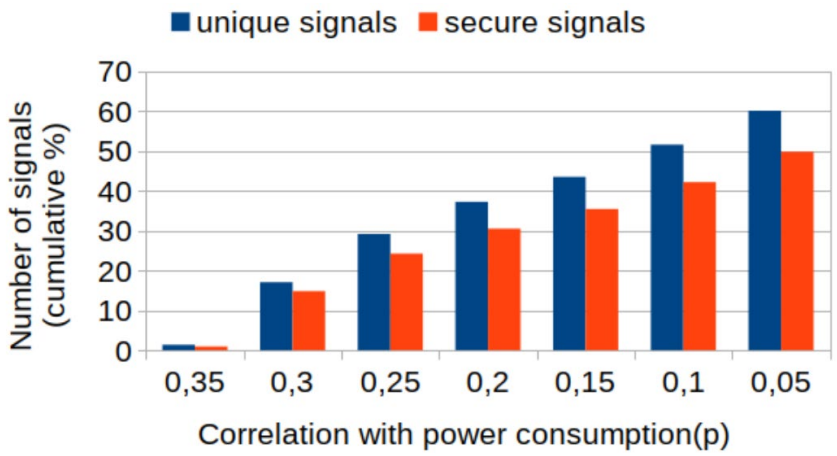
(0) Filter out data dependent signals → (1) Power model identification → (2) Power model instrumentation

Avoid using signals for which the statistics depends on the processed data

The values of the power estimates will be independent from the data being computed

The power estimates are no longer a valid side-channel signal

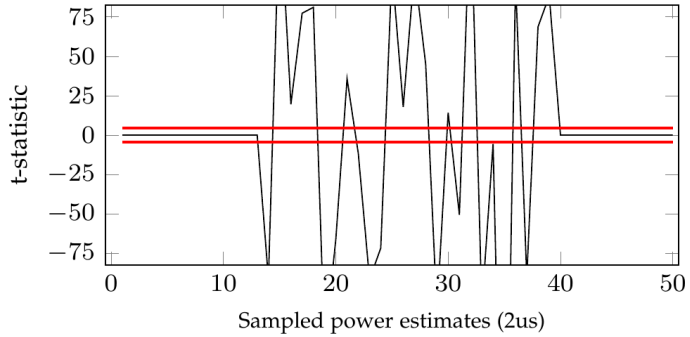
Design of secure power monitors: results [1]



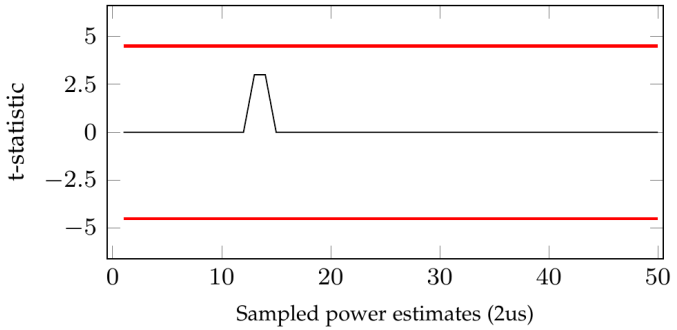
- Data dependent signals are a low fraction of the total signals

- 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.

T-test useful for clustering of signals

- Design secure and accurate run-time power monitors with overhead comparable to that of un-protected power monitors

- Possibility of automation of the entire design process
  - to provide a tool for TEXTAROSSA designers of accelerators or, in general, of any hardware blocks, to include their sub-systems in the global power management
  - Usable outside the scope of TEXTAROSSA, especially for EDGE computing

Conclusions

- The TEXTAROSSA project aims to achieve a broad impact on the HPC field both in pre-exascale and exascale Scenarios
- The TEXTAROSSA consortium will develop new IPs, algorithms, methods and software components for HPC-AI, HPC and HPDA applications, mostly Open Source and able to be adopted as standalone building blocks or to interoperate with other Exascale-ready components
- Through the participation of three supercomputing centers in the consortium, the proposed technologies will be tested by and known to the HPC community
- **The development of secure power estimators for any piece of hardware allows to create a system with a truly usable global power management**
- **WiP: validation with two partners, working on Hw blocks for security and on Hw2Hw communication templates. A third partner will be involved later with apps to be accelerated in Hw**

Thanks for your attention – POLIMI research group

Politecnico di Milano – DEIB main staff for TEXTAROSSA
Prof. William FORNACIARI, Giovanni AGOSTA
william.fornaciari@polimi.it, agosta@acm.org
Prof. Davide ZONI, Dr Federico TERRANEO, Dr Federico REGHENZANI. Dr Andrea Galimberti
Name.surname@polimi.it

Our Lab on Embedded and HPC computing
HEAPLab: http://heaplab.deib.polimi.it/

Active Projects on HPC

- **Textarossa (Euro-HPC, 2021-2024): https://textarossa.eu/**
- ITN «Apropos» – ITN on Approximate computing: https://projects.tuni.fi/apropos/

Other EURO-HPC projects started in early 2022 (technology and application Pilots)

- **The European Pilot - EuroHPC**
- **Eupex –EuroHPC**
- KDT-ISOLDE