Barcelona Supercomputing Center
Centro Nacional de Supercomputación

EXCELENCIA SEVERO OCHOA

4 Birds with 1 Stone:

On the use of time-randomized processors to address the time-predictability, reliability, energy and security challenges of real-time autonomous systems

David Trilla, Carles Hernandez, Jaume Abella, Francisco J. Cazorla

10/05/2019

ESSA 2019 | McLean, VA

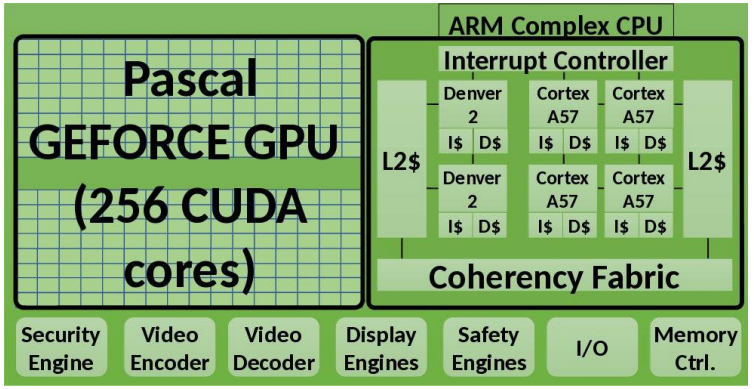
Critical Real-Time Embedded Systems (CRTES)

- Require validation and verification of functional & non-functional aspects:
  - Amongst the non-functional aspects there is timing verification:
    - Tasks must execute within their assigned budgeted time.
    - Worst-Case Execution Time estimates are used to provide an schedule of all system functionalities.
- Historically, CRTES processors and software have been kept very simple:
  - Simplify Validation and Verification of its requirements.
  - Reduces Validation and Verification costs.

Autonomous Driving (AD) is a game changer in CRTES

- New ML and AI techniques are enabling vehicles to operate autonomously.
  - They have huge performance requirements.
  - Can only be reasonably provided using high-performance hardware features in HPC and mainstream domains.

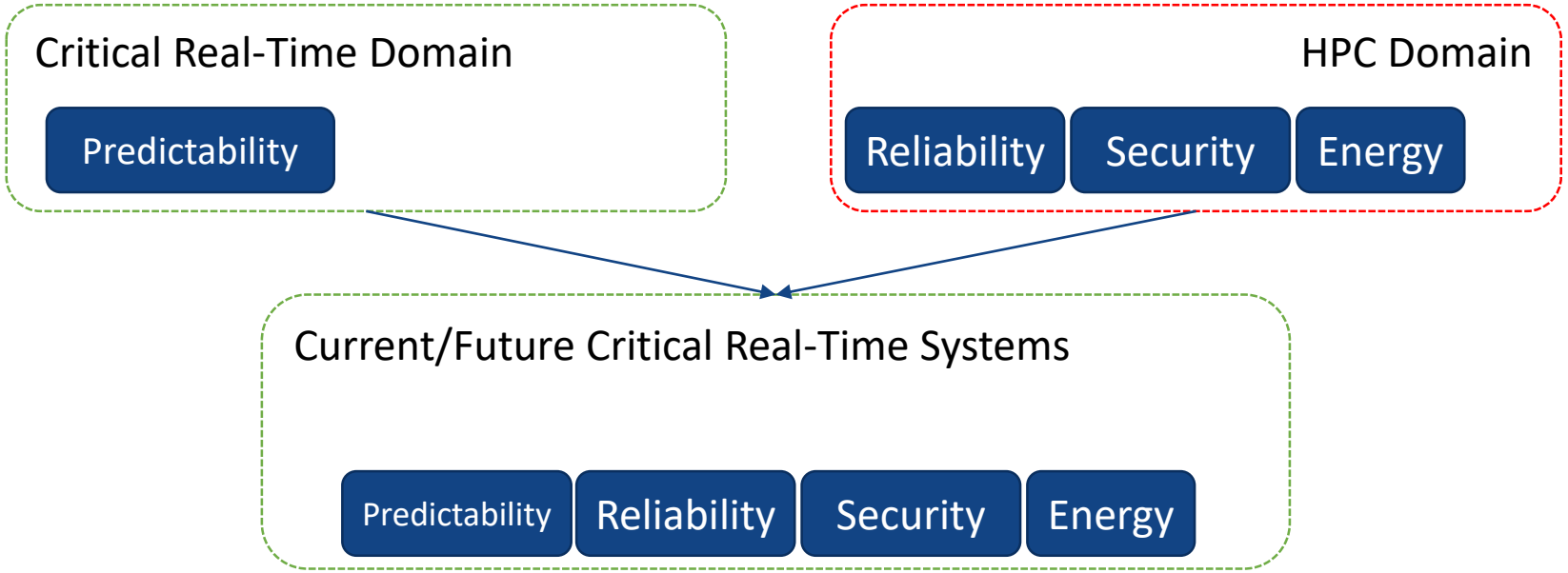
Current architecture for highly critical applications: lock-step ECU



Future devised platform for Autonomous Driving

The Autonomous Vehicle Breakthrough

- New requirements → New design principles



- Manufacturers in the real-time domain are racing to solve all these complex problems at once.

The Conundrum

- Intrinsically opposing design principles
  - Security and Predictability.
- Timing
  - Complexity of hardware (well) beyond what can be analyzed by static timing analysis techniques.
  - Measurement-based techniques incapable of providing evidence in covering processor states.
- Security
  - New security threats appear when devices are connected.
- Reliability
  - Aging problems appear when processor feature size decreases.
- Energy
  - Accurate models needed for precise accountability of energy are not feasible processor granularity.
- Without renouncing high performance

Randomization: Light at the end of the Tunnel

- Randomization in CRTES has emerged as a way to get the necessary high-performance without losing time-predictability capabilities.

- Randomization properties solve problems way further the time-predictability domain:
  - Reliability
  - Energy
  - Security

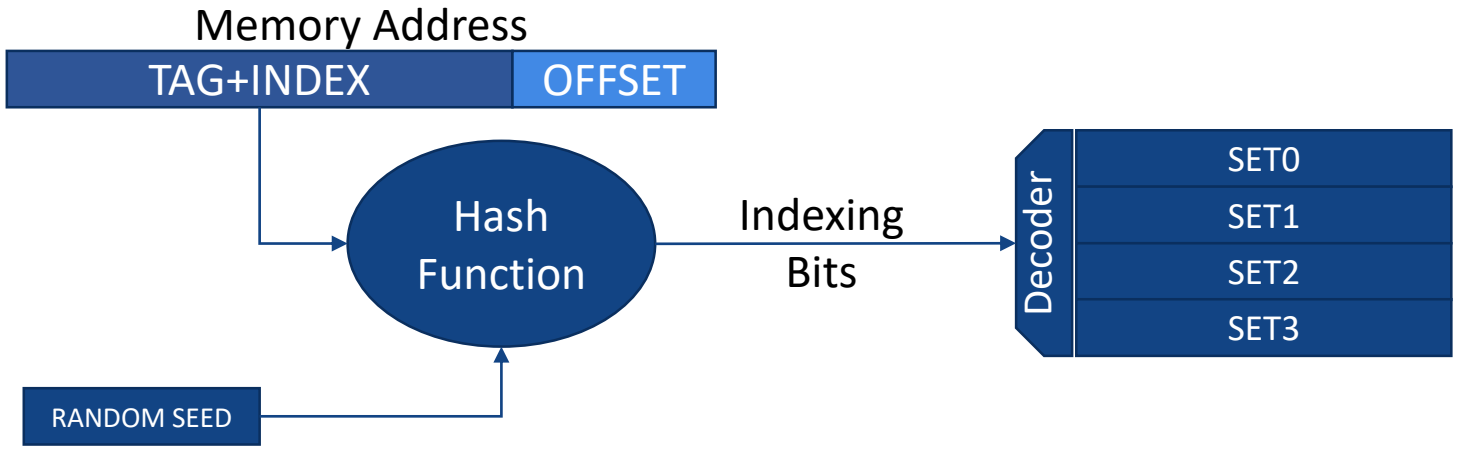
- Randomization can be implemented in:
  - Software [1]
  - Hardware

[1]L. Kosmidis et al. ICCAD 2016

Time Randomized Processors: Hardware

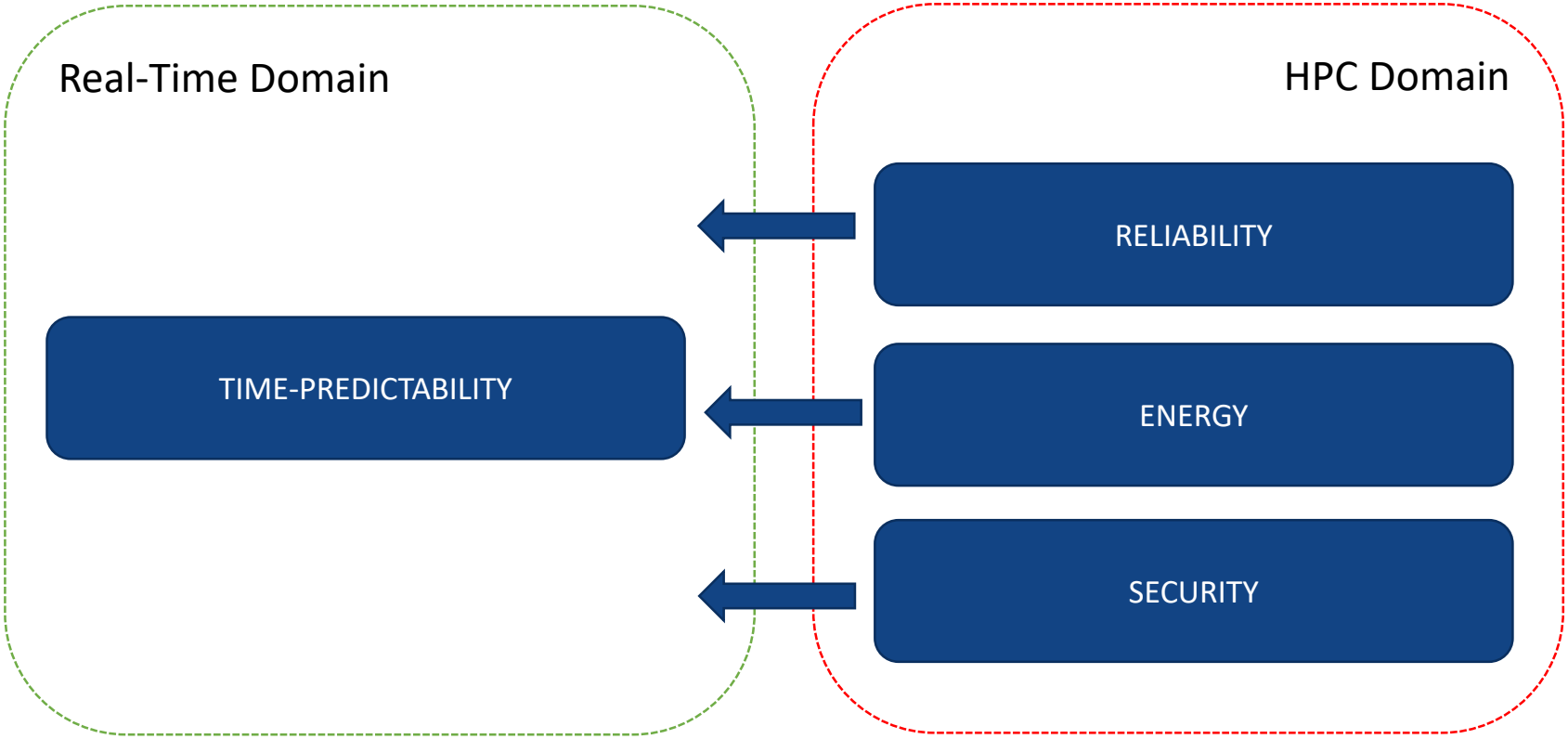
- TRP goal is to control and bound processor features that exhibit time jitter:
  - Upper-bound (Use maximum latency always).
  - Randomize (Randomize source of time jitter).

- e.g. Cache Placement Randomizaiton



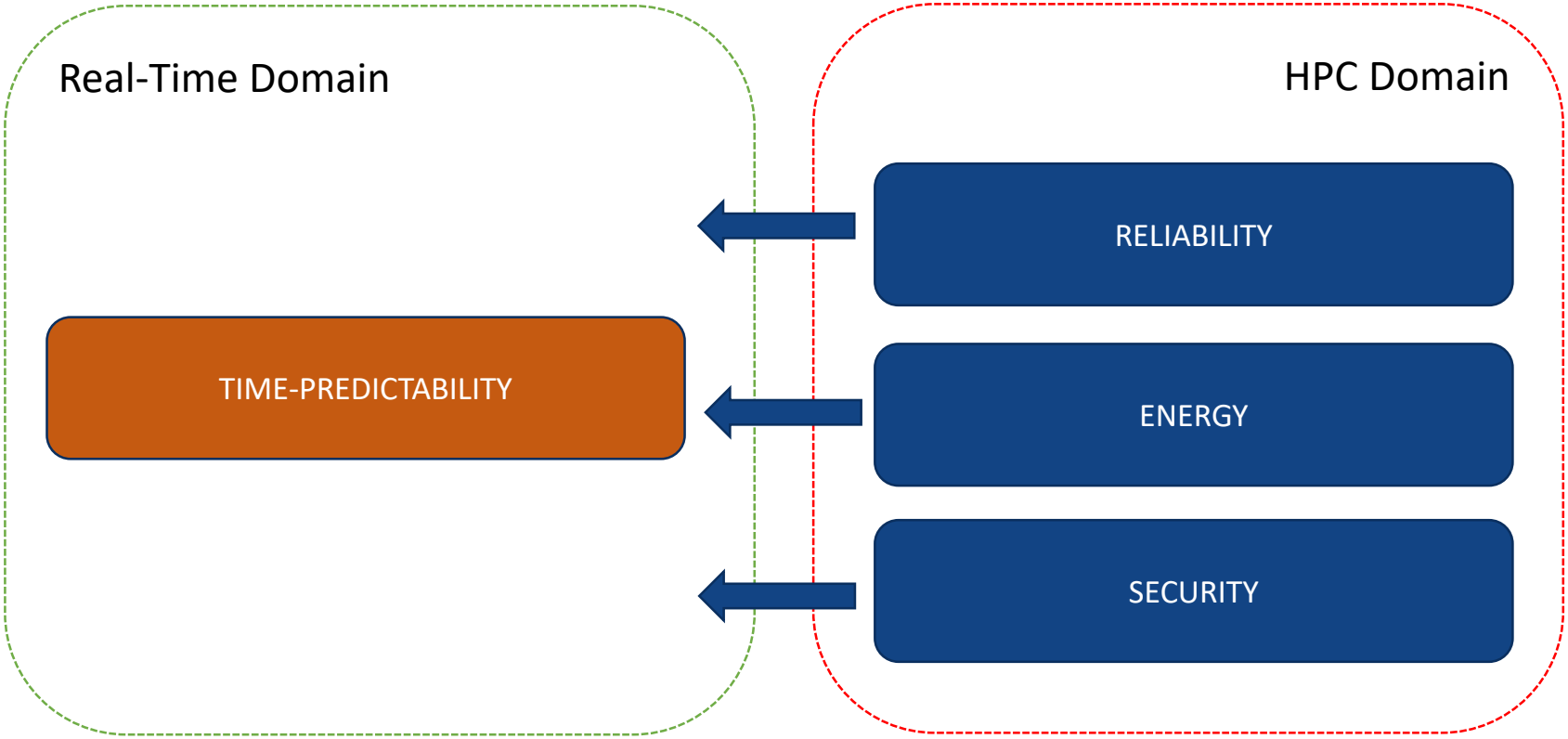
4 Birds

- How to tackle all this domains with TRP



4 Birds

- How to tackle all this domains with TRP

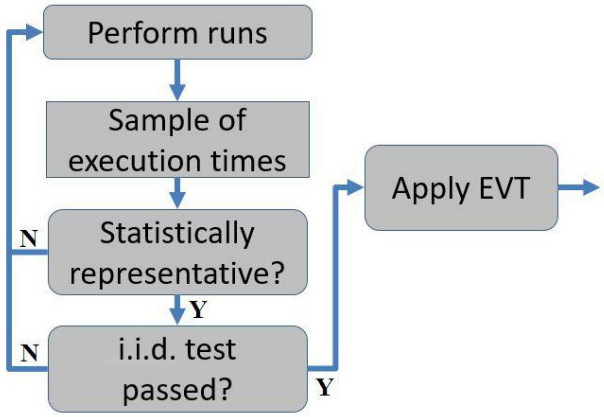


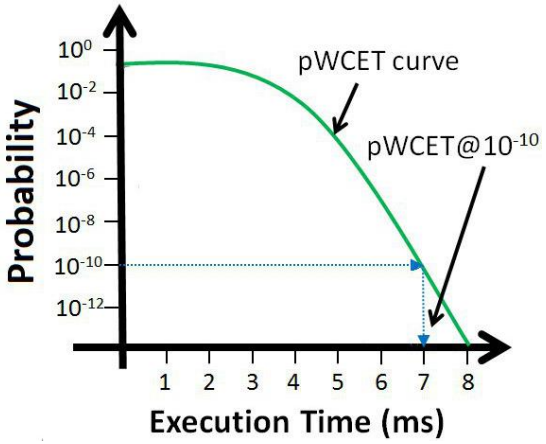
Randomization: Benefits for Time Predictability

- Timing Analysis is an important requirement of process of validating Non-functional properties of CRTES:
  - Critical tasks are required to execute in their demanded time budgets
  - The goal is to predict the worst-case execution time (WCET) of critical tasks.
- Each execution on a TRP becomes a random experiment/sample over all the possible execution times.
  - Observation of execution times gains statistical properties
- This allows the use of statistical techniques (Extreme Value Theory) to provide with guarantees upper-bounds on the execution time of tasks.

Time Predictability

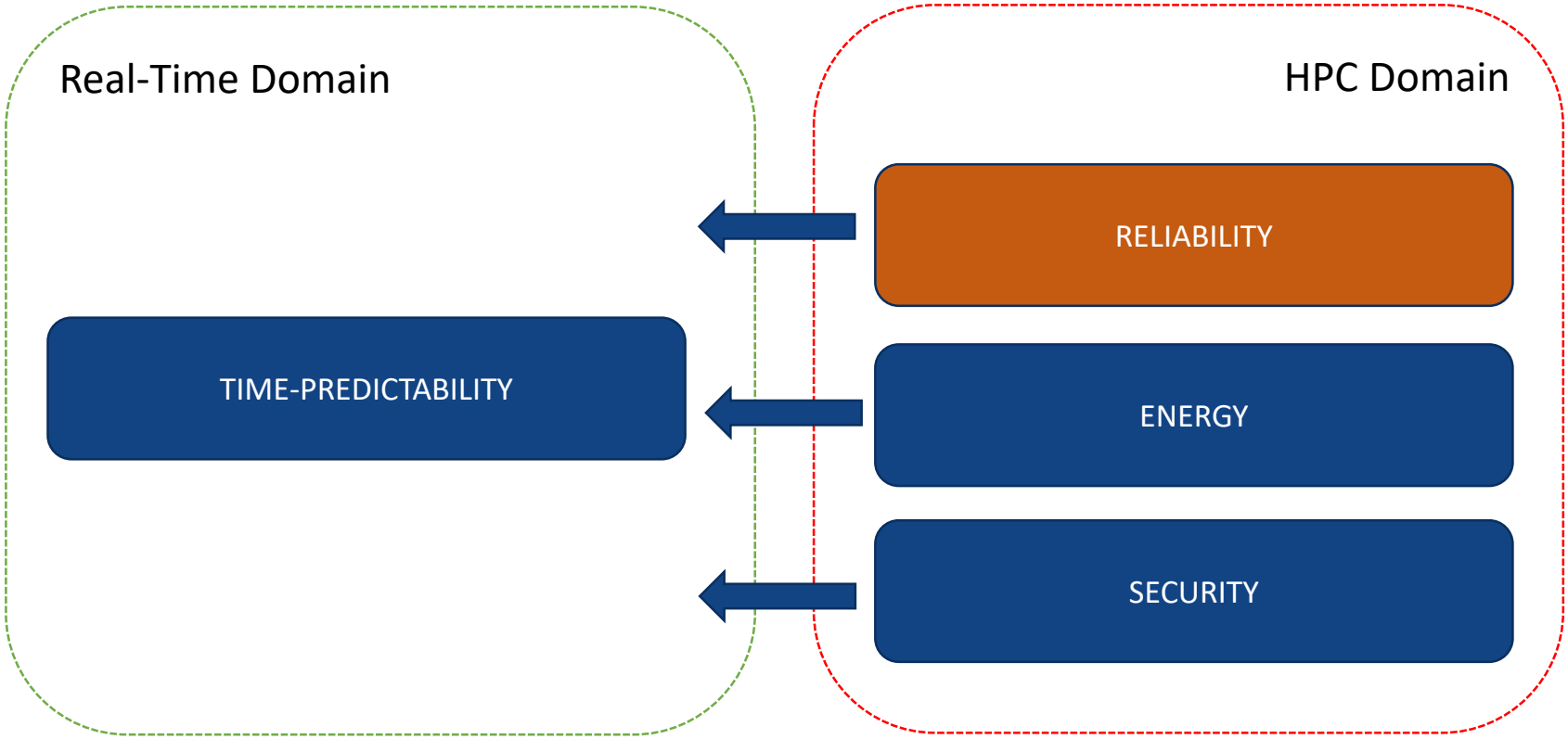
- Measurement-Based Probabilistic Timing Analysis(MBPTA): Methodology used to extract probabilistic Worst-Case Execution Times.
  - Collect execution time measurements.
  - Apply EVT.
  - Getp pobabilistic WCET





4 Birds

- How to tackle all this domains with TRP



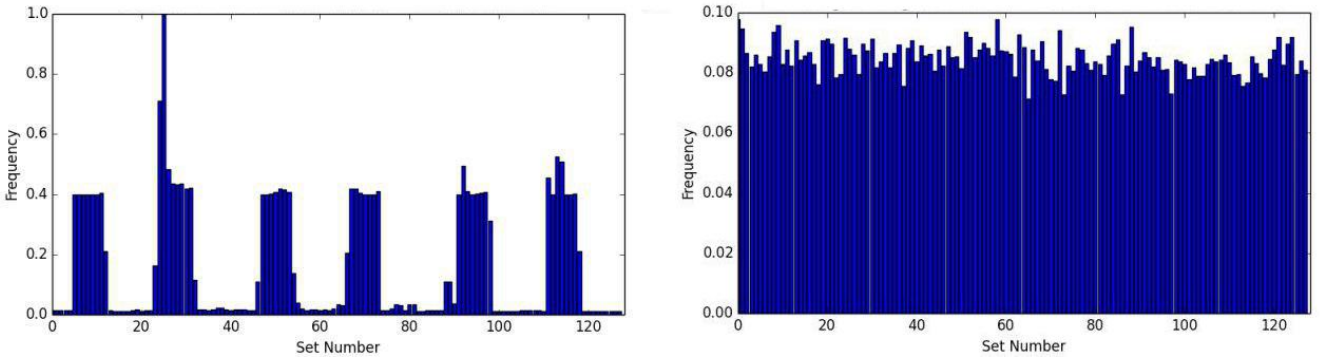
Randomization: Benefits for Reliability

- Compared to other types of devices, Critical Real-Time Systems are demanded continuous reliable operation for time spans in the decades.
- As processor feature size diminishes, aging effects make a bigger impact in overall performance and reliability.
- Aging effects such as:
  - Hot Carrier Injection (HCI)
  - Negative-bias temperature instability (NBTI)
  - Electromigration
- Are directly related to the utilization/activity of the hardware

Reliability

- Time-Randomized Processors use random placement and replacement to distribute cache accesses randomly.

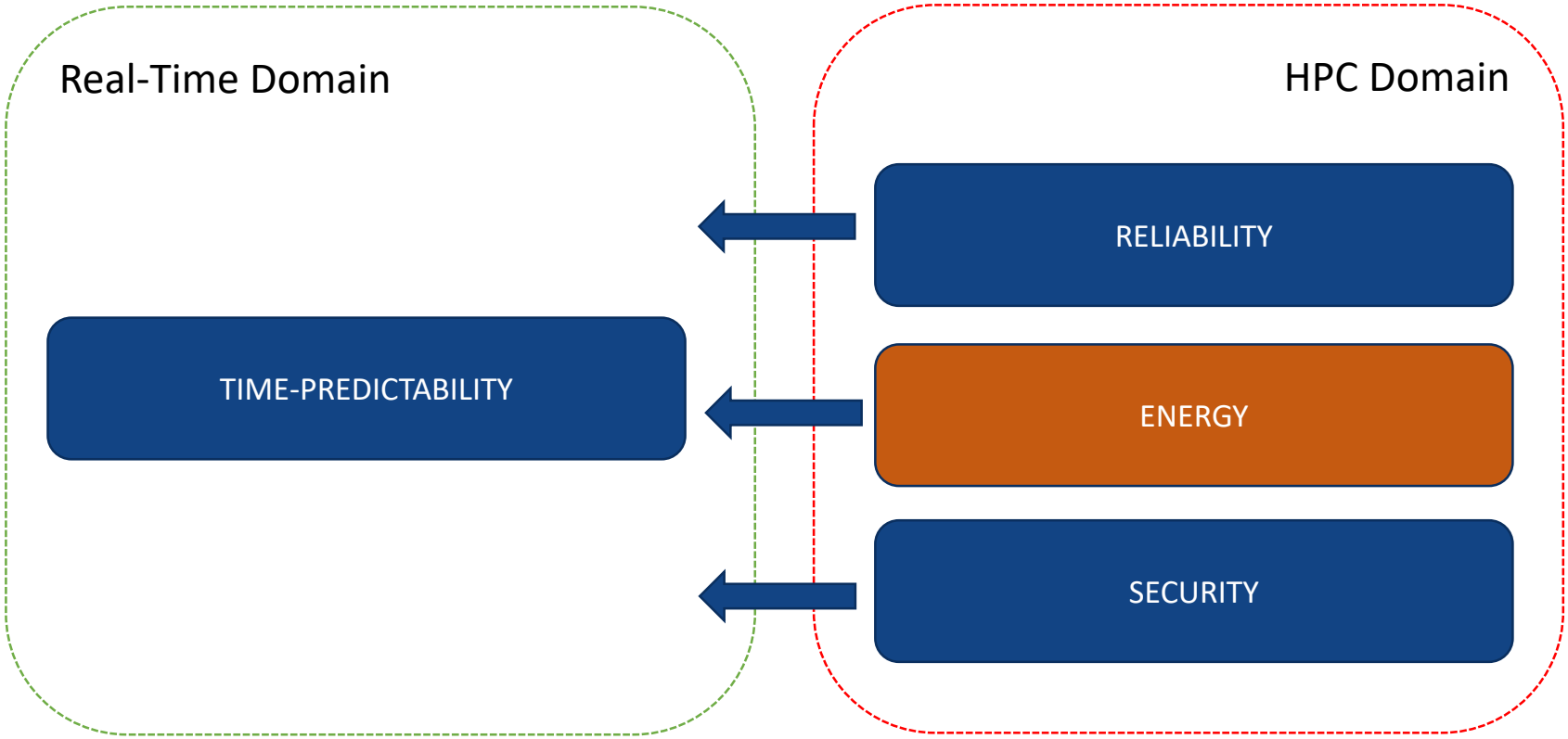
- A more even distribution of the accesses improves overall lifetime by eliminating biased usage of the cache.



Normalized distribution of instruction cache accesses across sets in Deterministic Hardware (left) and Randomized Hardware (right). Note the difference in Y-axis scales.

4 Birds

- How to tackle all this domains with TRP



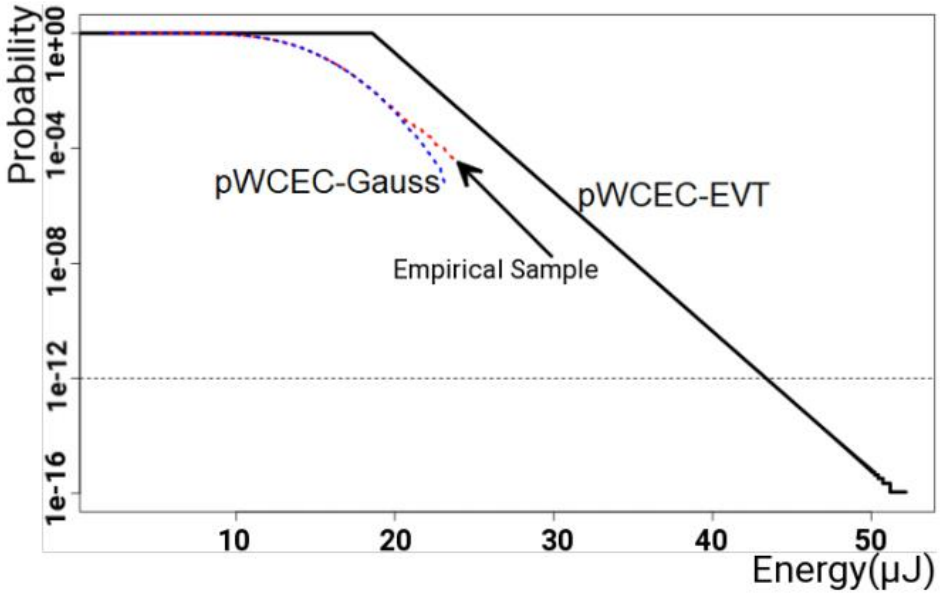
Randomization: Benefits for Energy

- Continuous rise in the use of electric vehicles and battery powered devices.
- The autonomous revolution is leading some of this battery powered devices to perform critical-real time tasks.
- As processors increase in complexity, exposing the power dissipation scenarios requires extensive levels of detail about the inner workings and interferences of the hardware.
- This demands for a stringent validation and verification of the energy availability of devices.

Energy: Probabilistic Energy Estimation

- Energy models are limited for their low accuracy when modeling processor hierarchies, and computationally unfeasible for full processor estimation when modeling at the circuit level.

- Similarly to obtain Time-Predictability, we can use the MBPTA methodology to extract energy measurements and apply statistical techniques to obtain mathematically sound estimates.



Energy: Detection and Mitigation of Power Peaks

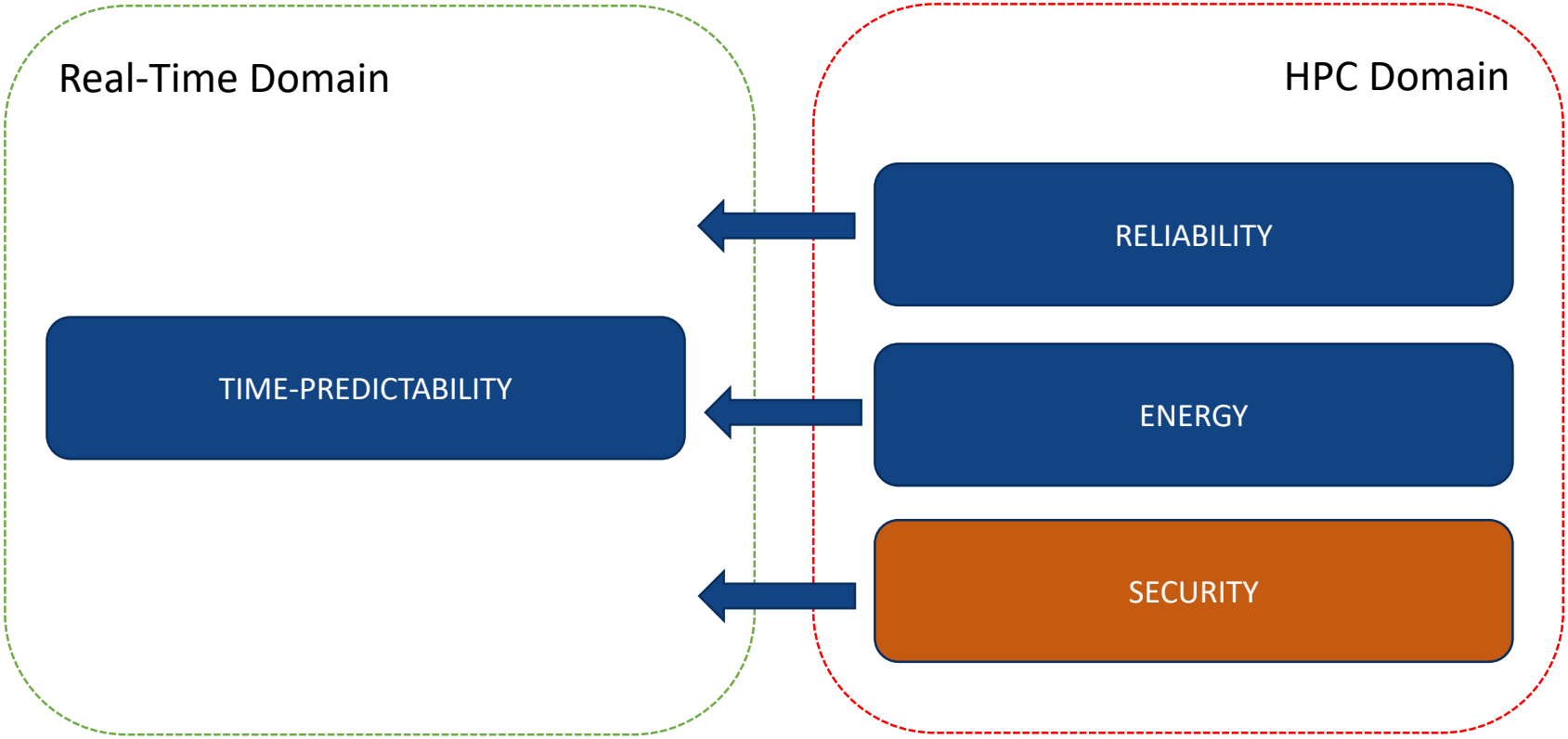
- Generating the precise power virus to expose worst-cases requires deep knowledge on the architecture and even in that case, taking into account all the interference patterns might be unfeasible.

- TRP naturally expose corner patterns by producing event sequences that might escape typical power virus designs.

- At the same time, any pathological behavior that occurs systematically on a deterministic processor is neutralized on randomized hardware.

4 Birds

- How to tackle all this domains with TRP

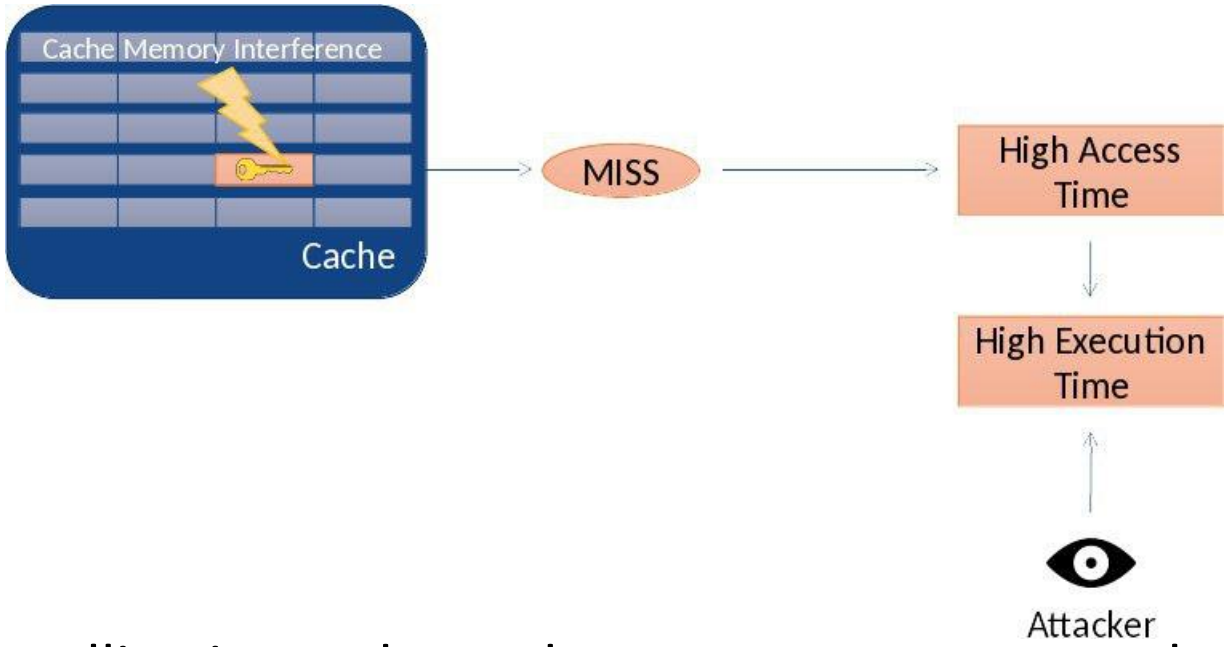


Randomization: Benefits for Security

- New autonomous systems will have the ability to integrate tasks from different actors being executed in the same hardware.
  - Software updates from third parties will become usual in the future.
  - Connected vehicles will be sharing information between them.
- The activation or deactivation of specific hardware features is dependent on the execution of any given task.
  - This creates a channel of information that could be used for malicious actors.
- Tasks that share processor resources can also use them to recover sensitive information enabling Side-Channel Attacks.

Security

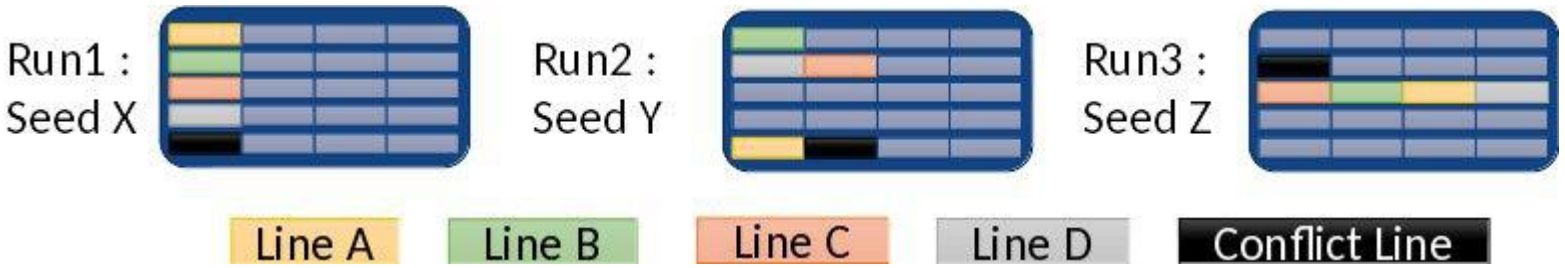
- In a Cache Contention-Based Side-Channel Attacks an attacker tries to recover encryption keys by establishing a correlation between cache conflicts and key values:



- By controlling input dependent memory accesses, the attacker can deterministically evict victim's data.

Security

- TRP nullify the information channel by decorrelating the cache placement from the input data and the attackers influence [1].



- Different executions and tasks, will have different random seeds, therefore the mapping of an attacker line (Conflict Line) will contend with different victim lines on each execution.

[1] D. Trilla et al. DAC18 (Best paper award nominee)

Performance Penalties of Randomized Caches

- Implementing TRP also comes with some drawbacks.
- Increase in Cache Misses.
- Depending on the implementation of randomization and the workload, performance is penalized between 2% and 10%.
- Coherence limitation.
  - Cache flush impacts performance.
- Increased Energy consumption.

Conclusion

- TRP provide mathematical properties to it's execution time measurement
  - Allowing for Probabilistic predictions of the Worst-Case Execution Time and enabling HPC hardware to be time-analyzed.
- TRP distribute randomly the usage of processor features.
  - Increasing the lifetime against usage dependent hardware aging effects.
- TRP naturally expose pathologic energy consumption behaviors and help in quantizing the amount of energy that a task consumes in extreme cases.
- TRP decorrelate conflicts in the data cache from memory layout.
  - Disabling some types of cache side-channel attacks.
- TRP look to be an integrated solution to tackle the challenges where autonomous systems meet real-time embedded systems.


Barcelona
Supercomputing
Center
Centro Nacional de Supercomputación
BSC
EXCELENCIA
SEVERO
OCHOA
THANK YOU!
dtrilla@bsc.es
www.bsc.es