PROXIMA

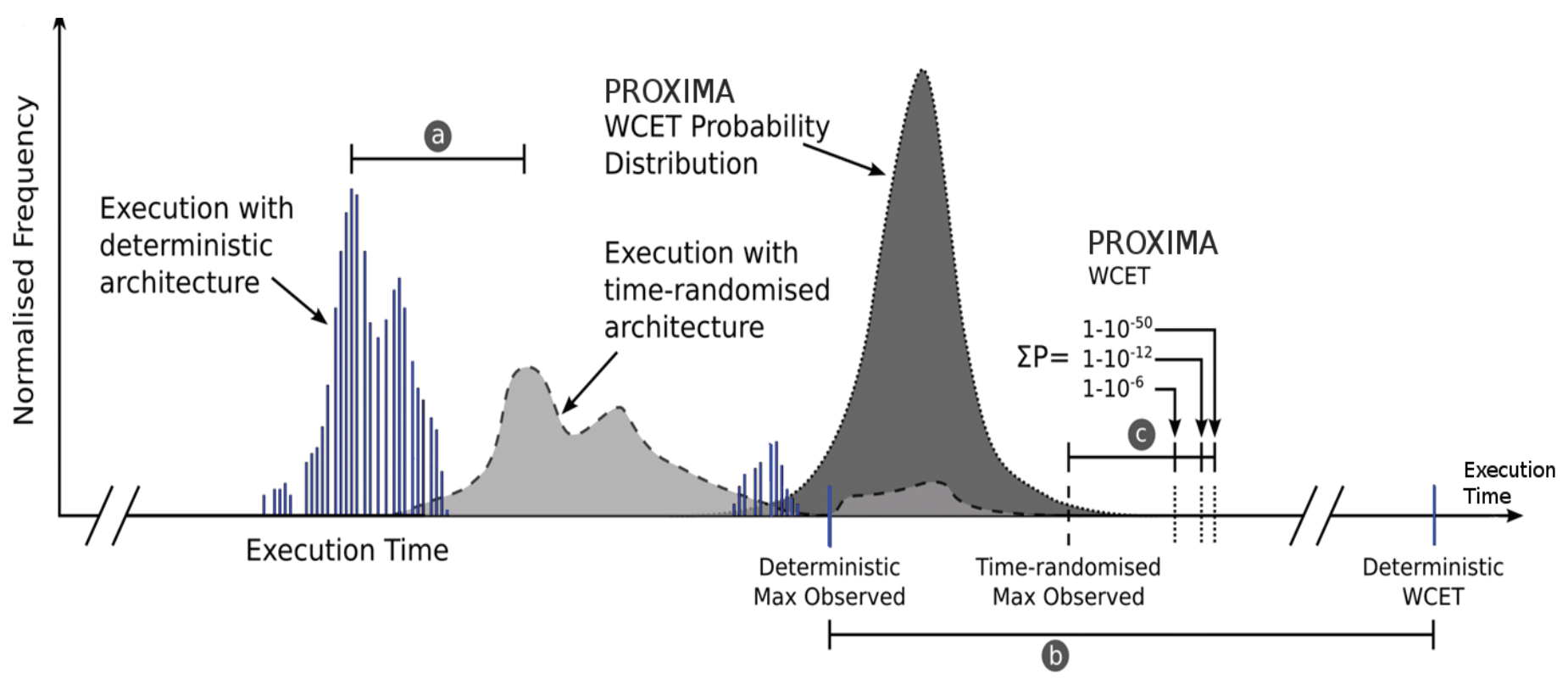
www.proxima-project.eu

Probabilistic real-time mixed-criticality multi-core and many-core systems

PROXIMA is providing industry ready tools, hardware and software support for the latest probabilistic software timing analysis techniques on multi-core and many-core architectures.

Benefits

- Increase real-time performance of mixed criticality systems
- Reduce cost of software design, verification, validation and certification
- Enable new multi-core hardware in critical systems



Key Achievements:

- Initial hardware and software **randomisation mechanisms implemented** for FPGA, Compiler and RTOS
- Prototype probabilistic **timing analysis techniques implemented** in Rapita Verification Suite
- **Industrial case studies** underway
- Initial proof of concept for **safety and certification approval**
- Initial results soon... **Stay Tuned!**

By Project Finish:

- Industry-ready probabilistic **timing analysis tools**
- **Certification arguments** for the use of probabilistic timing analysis in high integrity domains
- Design **guidelines for new hardware** and support for COTS hardware

Supported Platforms for Industrial Case Studies

- Multi-core processors: Leon 3 (FPGA), Freescale P4080, Infineon Aurix
- Many-core processors: PowerPC Simulator

PROXIMA Consortium

Barcelona Supercomputing Center – Centro Nacional de Supercomputación · AIRBUS · Inria · Università degli Studi di Padova · RAPITA Systems Ltd · AIRBUS Defence & Space · Infineon · IK4 IKERLAN Research Alliance · COBHAM · SYSGO Embedding Innovations · University of York

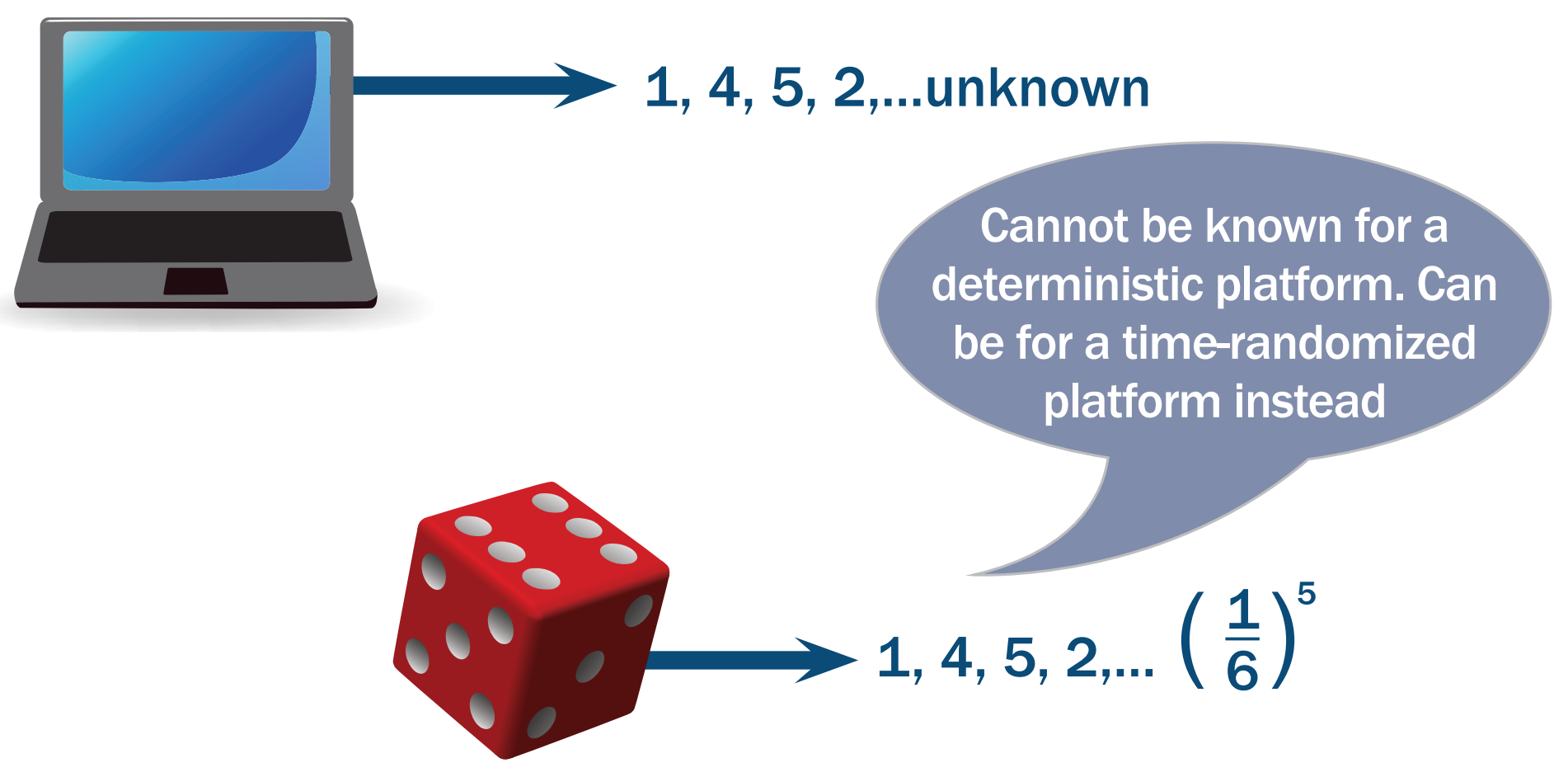
PROXIMA Industrial Advisory Board

Continental · DENSO EUROPE · EUROCOPTER an EADS company · AdaCore The GNAT Pro Company · IBM · CAF · Audi · ARM · KALRAY · BMW Group · ETAS · esa

Probabilistic-timing Platforms

- PROXIMA uses time-randomized hardware and software techniques and advanced statistical methods to accurately predict timing behaviour to quantify the probability of software timing failures in critical real-time embedded systems for the aerospace, automotive, rail and space industries
- PROXIMA modifies hardware components that have complex timing behaviour (which make timing analysis pessimistic) so that they have probabilistically characterizable timing behaviour. This allows new forms of software timing analysis with less pessimism. If the timing behaviour is actually truly random, then we can use probabilities to predict the overall behaviour of the software and its likelihood of failure

What is the probability of 1, 1, 1, 1, 1?

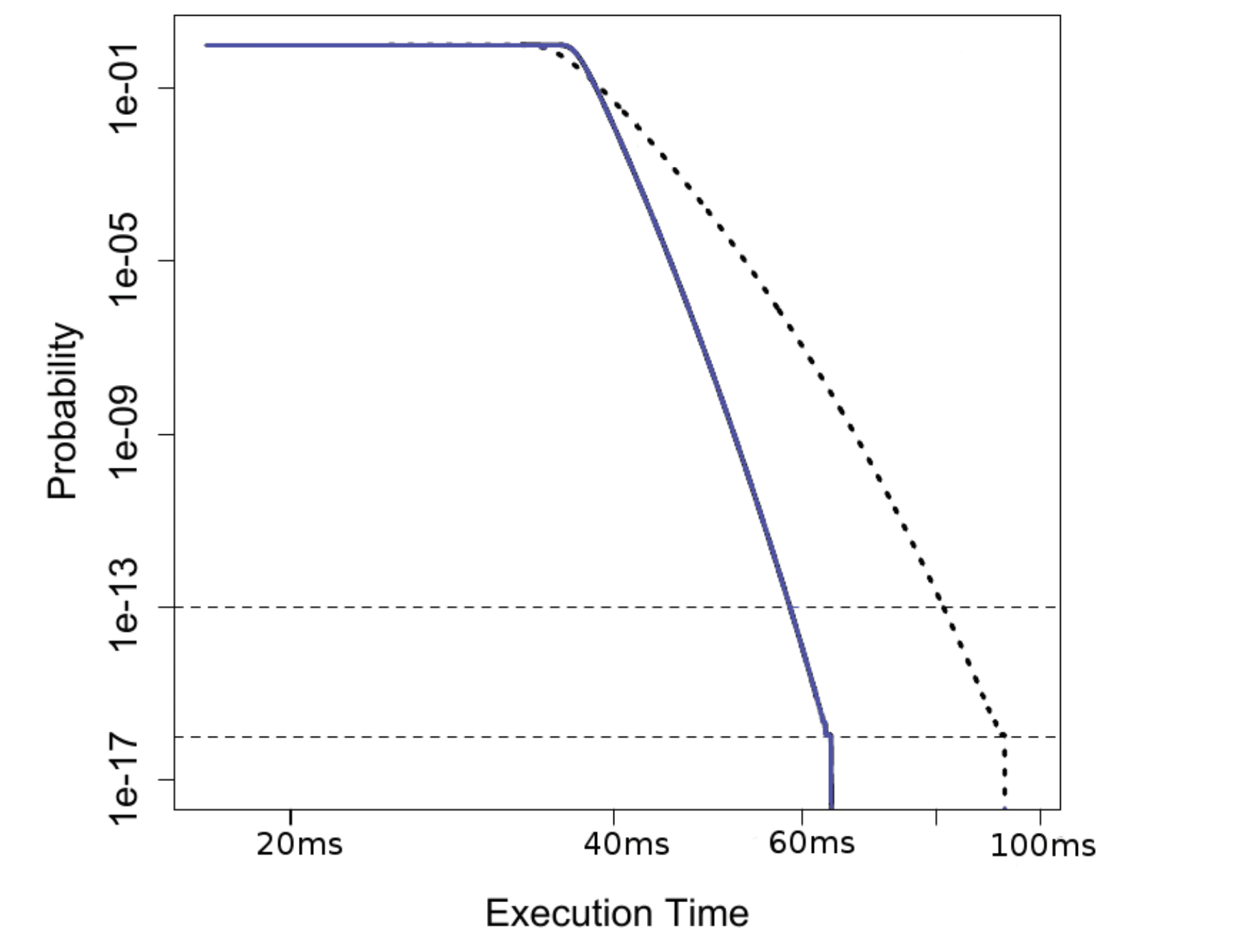

1, 4, 5, 2,...unknown
Cannot be known for a deterministic platform. Can be for a time-randomized platform instead
1, 4, 5, 2,... $\left(\frac{1}{6}\right)^5$

Execution history

By removing dependency on execution history (or making it probabilistically analysable), new simpler timing analysis techniques are possible and systems become much more composable.

Hardware and software time-randomization techniques support:

- Cache replacement and placement
- Network on chip design
- Memory allocation
- Bus arbitration



Example Execution Time Profiles for a Random-replacement Cache Policy

The project and the research leading to these results received funding from the European Community's Seventh Framework Programme [FP7/2007-2013] under grant agreement number 611085