PROBABILISTICALLY ANALYZABLE REAL-TIME SYSTEMS

PROARTIS

Key Innovation

Reliable computer systems such as aircraft flight control systems and engine control systems are of ever growing importance in the operation of aircraft and cars. These systems need to be developed to an exceptional level of reliability, yet their increasing complexity leads to enormous development cost, including the cost and time to test and analyze the system performance. PROARTIS will develop new tools, hardware and software architectures that will allow faster computer hardware features to be used and analyzed more easily in reliable systems. The project will reduce the cost of performance analysis for new systems by 40% and help support the growth in complexity.

Technical Approach

The project will demonstrate how using probabilities can help to analyze software. Deliberately adding randomness to the timing behaviour allows *new forms of software timing analysis* that are not currently possible. If the system behaviour is actually *true random* behaviour, then we can start using probabilities to predict the overall behaviour of the software and its likelihood of failure. PROARTIS will introduce timing randomization properties that are responsive to probabilistic analysis and propose novel and effective probabilistic timing analysis methods. To achieve these aims the project will focus on three key areas.

Architectural Design Principles. Defining hardware and software design guidelines that allow critical real-time embedded systems designers to benefit from randomization.

Probabilistic Timing Analysis. Creating a new analysis model that exploits the randomization capabilities of any new architectural designs, leading to effective timing analysis of new high performance hardware features and more complex software systems.

Contract number

249100

Project coordinator

Barcelona Supercomputing Center

Contact person

Francisco J. Cazorla

CAOS Group

Barcelona Supercomputing Center

Jordi Girona, 29. Nexus II.

08034

Barcelona, Spain

Tel: +34 93413 7173

Fax: +34 93413 7721

proartis-coordinator@bsc.es

Project website

www.proartis-project.eu

Community contribution to the project

1.800.000 Euro

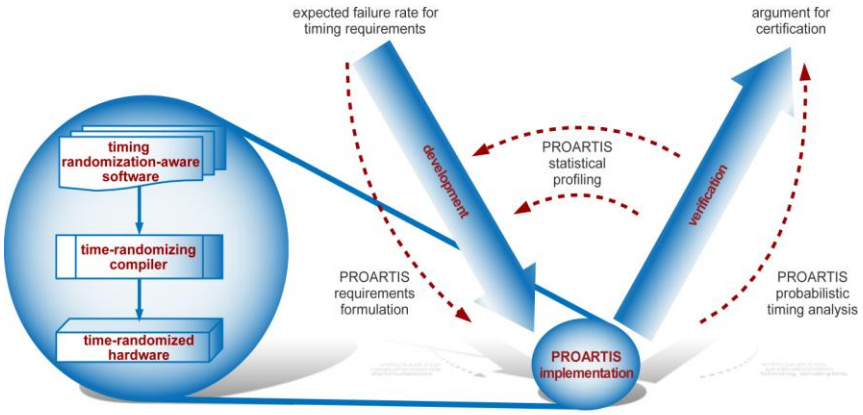
Project start date

01 February 2010

Duration

36 months

Verification and Certification. Developing arguments that can be used in the verification and certification of critical real-time embedded systems using probabilities.



Applying PROARTIS to the V-Cycle development model for certified systems

Demonstration and Use

The software timing will be measured and analyzed in a real Airbus application using modified versions of RapiTime, a timing analysis tool, which will be enhanced with new mathematical analysis techniques developed in the project. The hardware architecture will be simulated using software simulation techniques to show that the randomness introduced is truly beneficial to the reliability and analyzability of timing. Further demonstration opportunities are available via the Industrial Advisory Board, which has several representatives of the aerospace and automotive electronics industries.

Scientific, Economic and Societal Impact

As PROARTIS results will reduce the development costs of reliable systems in the avionics, automotive and space industries, partner Airbus will have a strong competitive advantage in developing new products. The project will position Rapita Systems as the company for viable on-target verification solutions as complex hardware and software architectures of the future are developed. The three academic partners, key European research centres, will all strengthen their core reputation and capability for further research opportunities in reliable systems because of their association with this groundbreaking project.

Second, PROARTIS techniques will enable the increased use of modern hardware features such as cache-memory and multi-core processors in high reliability systems. The amount of testing and analysis required for timing analysis of new software will be significantly reduced. More functionality can be put safely into one computer, which leads to opportunities to reduce the cost, weight and power consumption of embedded systems. This will have an impact on the fuel economy of aircraft and motor vehicles. Benefits to consumers will include improved safety in planes and cars and enable more advanced safety systems to be used.

Project partners	**Country**
Barcelona Supercomputing Center – Centro Nacional de Supercomputación	ES
Rapita Systems Ltd.	UK
Università degli Studi di Padova	IT
Institut National de Recherche en Informatique et Automatique	FR
Airbus France SAS	FR

First Achievements

- Introduced randomness into hardware and software design
- Generated mathematical foundation for probabilistic timing analysis
- Demonstrated timing analysis of random hardware on simple code
- Created the framework for research, testing and evaluation
- Incorporated knowledge and data from the safety-critical industry
- Established strategy for exploitation of new analysis technology