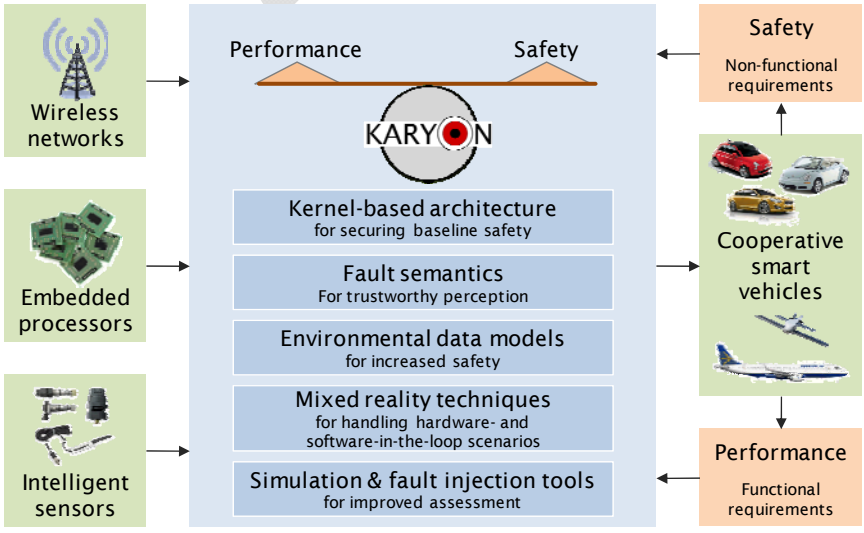
KERNEL-BASED ARCHITECTURE FOR SAFETY-CRITICAL CONTROL

KARYON

Mission Statement

The use of autonomous mobile systems as unmanned aerial vehicles (UAVs) or cooperative smart cars is desirable, for example, for environmental surveillance like the monitoring of ash clouds emitted by volcano eruptions as seen in 2010. Likewise, smart cars co-ordinating behaviours to improve vehicle density without driver involvement, will be a means of increasing traffic throughput to maintain mobility without the need to build new traffic infrastructures. Sharing the same air- or ground space with other systems, these systems need to communicate and cooperate in their environment. However, in the current state of the art, these systems are not allowed to operate in the public air space or on public roads, because the risk of causing severe damage cannot be excluded with sufficient certainty.

The key objective of KARYON is to provide **system solutions for predictable and safe coordination of smart vehicles that autonomously cooperate and interact in an open and inherently uncertain environment**. This is a challenging objective since the same increasingly complex control components and wireless communication, which would allow improving performance, end up introducing new safety risks, which have to be mitigated or neutralized. Addressing this challenge requires innovative solutions in two major problem areas. The first one is to achieve a high availability of the complex control system investigating **new ways of achieving fault-tolerant distributed control** that allow maintaining a high performance level in the presence of uncertainties and failures. The second is the **provision of a safety kernel to constraining system operation in order to avoid hazardous situations**.



Contract number

288195

Project coordinator

FFCUL

Contact person

António Casimiro

Dep. Informática, FCUL

Campo Grande, Ed C6, Piso 3

1749-016 Lisboa

Tel: +351 217500612

Fax: +351 217500084

casim@di.fc.ul.pt

Project website

www.karyon-project.eu

Community contribution to the project

2.74 Mio Euro

Project start date

01 10 2011

Duration

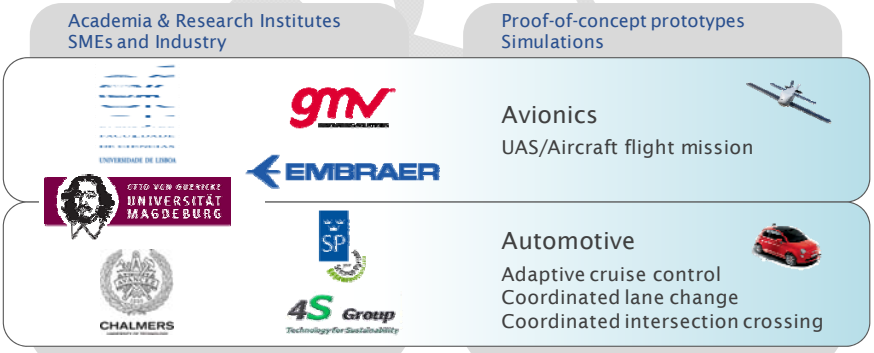
36 months

The technical approach

KARYON will define a **safety architecture for sensor-based cooperative systems**, which is based on a small local **safety kernel**, which will allow adaptive and dynamic behaviour whilst preventing dangerous behaviour. Because this is a very small subsystem compared to the overall complex control system, its predictability can be justified. This is essential for guaranteeing overall safety along a set of safety rules. The project will further investigate the relevant **fault detection concepts**, particularly for the sensor systems, needed to show fulfilment of dependability attributes and argue about safety according to safety standards. **Simulation and mixed reality techniques** will be developed to validate the approach. KARYON will integrate concepts in advanced **event dissemination middleware** and in improved **simulation and fault-injection tools** for assessing the behaviour of autonomous, mobile systems under failure conditions.

Demonstration and Use

KARYON will explore the elaborated concepts and results in the context of two major use cases from the avionics and automotive areas. Application expertise provided by the respective industrial beneficiaries from the avionics and automotive fields, will ensure that scenarios and evaluation will always be aligned with industrial needs. The first use case is related to a **monitoring mission performed by an Unmanned Aerial System (UAS)** scheduled to execute a flight plan previously agreed with UAS Ground Control and Air Traffic Control and entering an air traffic space shared with piloted aircrafts. The second use case is related to **Advanced Driver Assistance Systems (ADASs) for coordinating vehicles**. In particular, KARYON will examine scenarios in which vehicles cooperate while: (1) Going on the road and keeping their distance from other vehicles, (2) Cursing in their lanes and coordinating when lane changes are needed, and (3) Crossing intersections in a coordinated way.



Scientific, Economic and societal Impact

In terms of **impact**, KARYON opens new perspectives by enabling the use of available technology for **safe cooperative systems** and for **increased efficiency**. Project results will be exploited by two large-scale companies in the aeronautics domain (GMV and EMBRAER) in a multi Billion EURO market and by one SME in the automotive market (4S Group). It is expected that their respective position in the worldwide competition will be strengthened by the project and a high return on their investment is envisaged. Academic partners will stay at the forefront of worldwide research with the knowledge and prestige gained in the project. Also, by realizing the various safety classes defined in the standard ISO 26262 on functional safety for road vehicles, **safety standards in the car industry will benefit** and citizens in Europe will profit from **safer mobility**.

Project partners	Country
Univ. of Lisbon	Portugal
Magdeburg Univ.	Germany
Chalmers Univ. Tech.	Sweden
GMVIS SKYSOFT	Portugal
EMBRAER S.A.	Brazil
SP	Sweden
4S srl	Italy

Key features

- Improve interaction in cooperative scenarios whilst preserving safety
- Assessment of safety according to standards
- Efficient use of resources for sustainable transportation