KERNEL-BASED ARCHITECTURE FOR SAFETY-CRITICAL CONTROL

KARYON

We use our senses in everything we do. Our brains keep track of where we are, our body postures, and the position of others. We employ this awareness for avoiding running into others. We keep eye contact with anybody that approaches us, we try to anticipate their actions, we use our voices to make ourselves noticeable, and we estimate whether we need to slow down or we can just “pass through”. In fact, our capabilities are not limited to obvious cases; we change our behaviour when we are uncertain about the attention of others. It is expected that in the future vehicles will also deal with uncertainties when anticipating the behaviour of approaching vehicles. KARYON shows that is not science fiction anymore to expect vehicles to deal with their uncertainties.

All major automakers are developing vehicles with on-board sensors for alerting the driver about road hazards, such as approaching vehicles. Vehicle-to-vehicle communications can amplify this awareness by sharing these alerts and sensor information in a process that is called distributed sensor fusion. However, vehicle-to-vehicle communication is interference prone; it may unexpectedly fail at any time. Thus, automakers are uncertain about the level of information quality that the distributed sensor fusion provides. When it comes to safety-critical systems, the current practice pessimistically avoids any car-to-car communication dependencies. KARYON studies the limits of prospective safety-critical services with respect to dealing with the uncertainties that depend on the level of information quality.

Let us consider soon-to-be cooperative safety-critical services, such as supervised intersection crossing and lane-change assistance; each has its own set of requirements about the level of information quality. Insufficient information quality can cause the vehicles to reduce their level of service, and the cooperative services, in turn, change their operation mode from cooperative to autonomous. For example, when two vehicles are approaching each other in an intersection, the underlying communication systems as well as relevant local sensors must be producing information with good enough quality to allow vehicles to first have a common knowledge about their trajectories before they can coherently decide on their actions; one should yield to the other that is coming on the right. However, in the presence of communication interferences, the level of information quality is insufficient, and they cannot safely anticipate their joint behaviour, i.e., lower their level of service for a safer operation. Thus, they must both reduce their speed so that they can each autonomously decide whether crossing is safe. In other words, the cooperative system changes its operation mode to meet the current service abilities. Once the service abilities recover, the operation mode can return to normal and by that regain a higher traffic throughput.

KARYON proposes solutions for avionic and automotive systems that are based on safety kernel architectures for adapting the level of service according to the changing level of information quality. The safety kernel architecture can be seen as the system’s (i) self-perception of the ability to know how well it

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

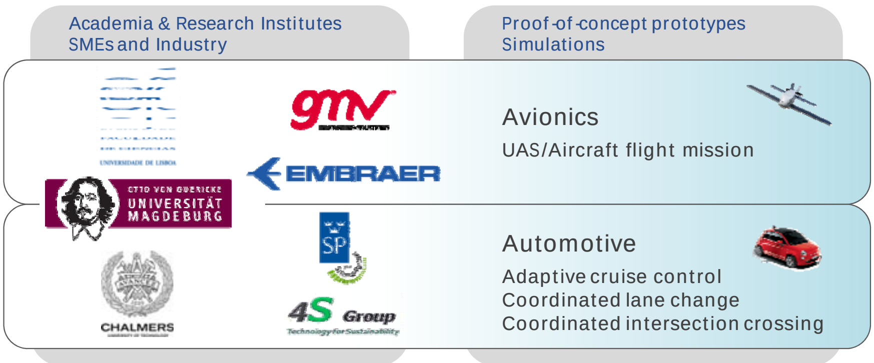
Duration

36 months

perceives information from its senses; and (ii) mechanism for tuning into different levels of cautious behaviour accordingly. Unlike the common practice that takes the pessimistic approach, according to which one can merely trust its own senses, KARYON facilitates safe cooperation when possible by introducing forever-vigilant self-perception abilities. This project introduces the concept of a safety kernel architecture that reduces the level of service in the presence of system failures or communication interferences, and then regains highest level of service when the level of information quality recovers. In addition to contributions in the area of distributed sensor fusion and complex system control, we expect the safety kernel architecture to open new opportunities for safety-critical cooperative systems to adaptively deal with uncertainties.

Another approach that KARYON follows is to increase the predictability of the communications system and its networks. The current practice mainly considers the use of communication protocols that do not provide predictable bounds on the communication delays or dealing effectively with message contention. As a result, the system experiences arbitrary long periods of communication delays. In order to increase the degree communication predictability, dedicated radio bands were allocated for traffic communication. However, the current practice in these dedicated bands is to use communication protocols that have no predictable delay and no effective mechanism for message contention control. The result is that soon the dedicated communication channel will become clattered. KARYON research aims at developing new protocols that can increase the communication timeliness and decrease the degree of communication uncertainty.

By providing solutions that enable the use of cooperative functions in a way that safety is not jeopardized, KARYON will create new opportunities for the design of increasingly complex cooperative functionalities, which will be fundamental in the future to achieve improved vehicle density without driver involvement and increased traffic throughput to maintain mobility without a need to build new traffic infrastructures.



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