Brief Announcement: KARYON: Towards Safety Kernels for Cooperative Vehicular Systems*

António Casimiro[1], Jörg Kaiser[2], Johan Karlsson[3], Elad Michael Schiller[3], Philippas Tsigas[3], Pedro Costa[4], José Parizi[5], Rolf Johansson[6], and Renato Librino[7]

[1] Univ. Lisboa
casim@di.fc.ul.pt
[2] Otto-von-Guericke Univ. Magdeburg
kaiser@ivs.cs.uni-magdeburg.de
[3] Chalmers Univ. Tech.
{johan,elad,tsigas}@chalmers.se
[4] GMVIS SKYSOFT
pedro.costa@gmv.com
[5] EMBRAER SA
parizi@embraer.com.br
[6] SP AB
rolf.johansson@sp.se
[7] 4S SRL
renato.librino@4sgroup.it

KARYON, a kernel-based architecture for safety-critical control, is a European project that proposes a new perspective to improve performance of smart vehicle coordination focusing on Advanced Driver Assistance Systems (ADASs) and Unmanned Aerial Systems (UAS). The key objective 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. Currently, these systems are not allowed to operate on the public roads or in the air space, as the risk of causing severe damage cannot be excluded with sufficient certainty. The impact of the project is two-fold; it will provide improved vehicle density without driver involvement and increased traffic throughput to maintain mobility without a need to build new traffic infrastructures. The results will improve interaction in cooperation scenarios while preserving safety and assessing it according to standards. The prospective project results include self-stabilizing algorithms for vehicle coordination, communication and synchronization. In addition, we aim at showing that the safety kernel can be designed to be a self-stabilizing one.

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

* This work was partially supported by the EC, through project FP7-STREP-288195, KARYON (Kernel-based ARchitecture for safetY-critical cONtrol).

A.W. Richa and C. Scheideler (Eds.): SSS 2012, LNCS 7596, pp. 232–235, 2012.

objective since the same increasingly complex control components and wireless communication, which would allow improved performance, end up introducing new safety risks, which have to be mitigated or neutralized. Addressing this challenge requires innovative solutions for: (1) 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, and (2) Provision of a safety kernel for constraining system operation in order to avoid hazardous situations.

Thus far, vehicular application safety is typically based on worst-case analysis and pessimistic allocation of resources to achieve the intended functionality. This has a strong impact on the final cost of the solutions. Often, when considering automotive systems, even a slight cost increment is not affordable.

Architectural Support for Safety-Critical Systems. Safety-critical systems call for predictability, i.e., real-time operation. Traditionally, safety-critical solutions have been based on synchronous system models. These are well understood, both in terms of distributed systems theory and in the design of real-time systems and solutions, in areas such as real-time communication [5,7,2] and real-time scheduling [3,6]. However, when moving to distributed, large-scale, wireless and possibly complex infrastructures, these infrastructures do not provide the timeliness guarantees required. Therefore, designing applications using the synchronous model would cause incorrect system behavior due to assumption violation, and would defeat any safety requirements.

Supporting Services for Sensor-Based Safe Coordination. Advanced control systems rely on a correct perception of the environment and system state, e.g., consistent view on the system state in the presence of faults and concurrency [8]. Results in this field address synchrony and replication issues but often assume correct information at its origin, and same state replicas. If reliable operation of sensors and actuators are required dealing with the environment perception and actuation on it, these methods have to be extended. Reliable operation has to cope with continuous data where replication is not always possible and redundancy mechanisms have to be different. One can find control models for fault detection of the sensor-to-actuator chain, such as fault detection and isolation (FDI) [4] or analytical redundancy methods [1]. Currently there is no consideration for system impact on largely varying network latencies or dynamically varying sensor information beyond mere statistical effects.

The Technical Approach. KARYON will define a safety architecture for sensor-based cooperative systems, which is based on a small local safety kernel, that will allow adaptive and dynamic behaviour whilst preventing dangerous behaviour. Because this is a tiny subsystem compared to the overall complex control system, and its design is guided by concepts of fault independence from the rest of the system, possession of it's own resources, highest reliability of operation and autonomy of control decisions, its predictability can be justified. This is essential for guaranteeing overall safety along a set of safety rules. The architecture will be defined in a generic way, like an architectural pattern,

without restricting the concrete faults to be considered and the fault-tolerance mechanisms to be deployed. In fact, since KARYON focuses on functional safety, the safety kernel should guarantee that the specified functionality should not fail in a hazardous way. To build a safe product, the integrity of the implementation should be high enough to ensure acceptable risks, where the risks are derived from an analysis of the potential hazards. Therefore, a set of safety rules will have to be derived from each specific application, and will be guarded by the safety kernel. The safety kernel will thus control the adaptive and dynamic behavior of the system, based on information about the integrity of system components and quality of perception (sensor data), and safeguard the system against unsafe control commands, by checking them against the derived 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. At the same time, the idea is to achieve improvements in the reliable and trustworthy environment perception, based on adequate fault models for complex sensor faults, on solutions for increased communication predictability and on environment monitoring components. Simulation and mixed reality techniques will be developed to validate the approach. Furthermore, 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 and to evaluate safety assurance according to the ISO 26262 safety standard.

Demonstration and Use. KARYON will explore the elaborated concepts and results in the context of two major use cases from the automotive and avionics areas. Application expertise provided by the respective industrial beneficiaries from the automotive and avionics fields, will ensure that scenarios and evaluation will always be aligned with industrial needs. The automotive 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.

Conclusions. KARYON opens new perspectives by enabling the use of available technology for safe cooperative systems and for increased efficiency. Global safety predicates are powerful abstractions for describing the intended safe behaviour of systems as a whole. Since that behaviour must be guaranteed at run-time, KARYON will conduct research on the problem of deriving safety monitors from the global safety predicates. We aim at providing a safety kernel and mechanisms for detecting unsafe states and trigger appropriate responses. We expect that KARYON's impact will include benefits of overall increased traffic throughput, safer roads and sustainable transportation.

References

1. Blanke, M., Kinnaert, M., Lunze, J., Staroswiecki, M.: Diagnosis and Fault-Tolerant Control, 2nd edn. Springer (2006)
2. Davis, R.I., Burns, A., Bril, R.J., Lukkien, J.J.: Controller Area Network (CAN) schedulability analysis: Refuted, revisited and revised. Real-Time Systems 35, 239–272
3. Deng, Z., Liu, J.W.-S.: Scheduling real-time applications in an open environment. In: IEEE Real-Time Systems Symposium, pp. 308–319 (1997)
4. Frank, P.M.: Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy- A survey and some new results. Automatica 26, 459–474 (1990)
5. Kopetz, H.: Real-Time Systems. Kluwer Academic (1997)
6. Ramamritham, K., Stankovic, J.: Scheduling algorithms and operating systems support for real-time systems. Proceedings IEEE 82(1), 55–67 (1994)
7. Tindell, K., Burns, A., Wellings, A.J.: Analysis of hard real-time communications. Real-Time Systems 9(2), 147–171 (1995)
8. Verissimo, P., Rodrigues, L.: Distributed Systems for System Architects. Kluwer Academic (2001)