KARYON: Kernel-Based Architecture for safetY-critical cOntrol

Overview of main results

KARYON Workshop, Borås, Sweden, Dec 11, 2014

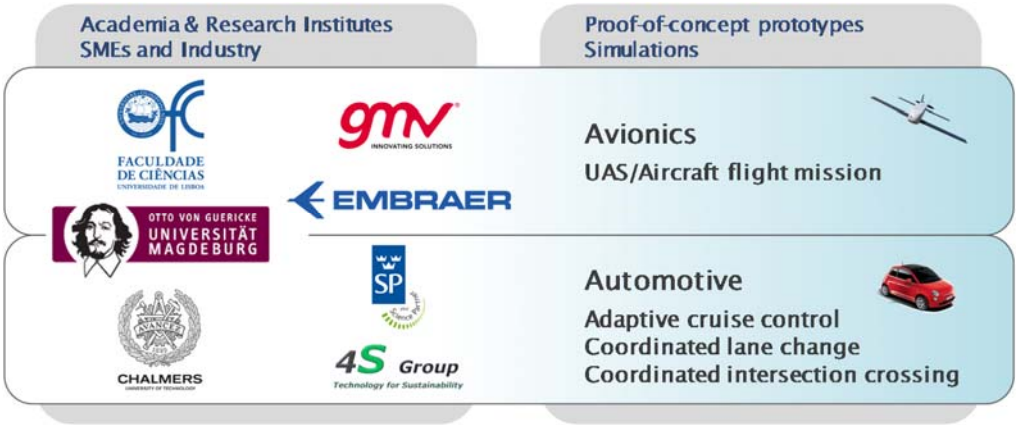
KARYON

Kernel-Based ARchitecture for safetY-critical cONtrol

Consortium

KARYON

- 7 partners from 5 countries (one from Brazil)
- Covering diverse areas
  - Dependability, distributed systems, sensors, modelling and simulation, middleware, communication



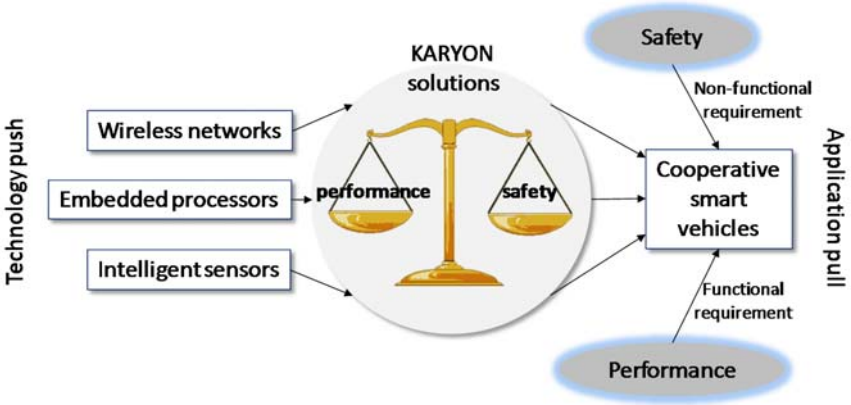
KARYON goals

- Provide system solutions for **predictable and safe coordination** of smart vehicles that autonomously cooperate and interact in an open and inherently **uncertain environment**

- In particular:
  - Specify a safety architecture for sensor-based cooperative systems
  - Define a fault semantics for complex sensor faults
  - Define methodologies for environmental data models
  - Validate and assess the feasibility and impact of the KARYON results

Main challenge

- Solve the apparent paradox between achieving all the following objectives at the same time:
  - Improve performance
  - Assure safety goals
  - Employ low-cost technologies



Application domains

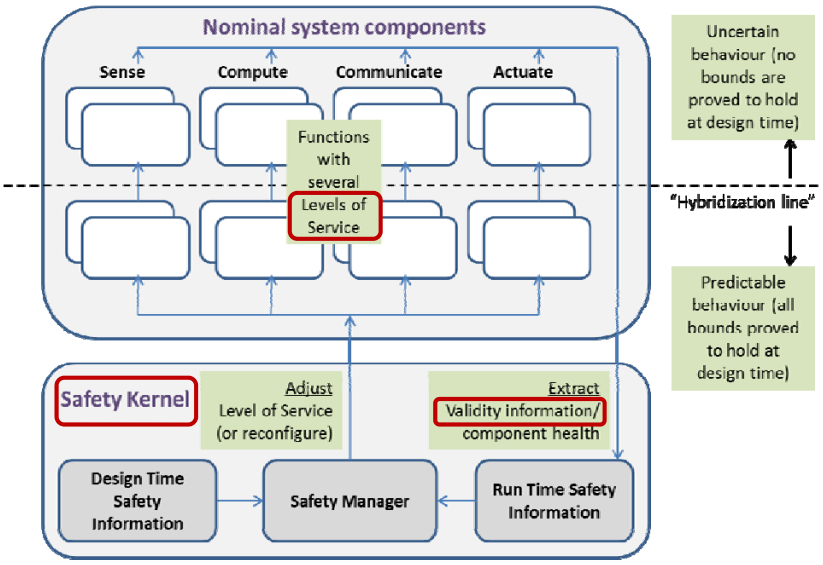
- Automotive domain
  - Adaptive Cruise Control Systems
  - Coordinated lane change manoeuvres
  - Coordinated intersection crossing
- Next:
  - Automotive domain promotional video

Application domains

- Avionics domain
  - UAS/Aircraft manoeuvres in shared air space
- Next:
  - Avionics domain promotional video

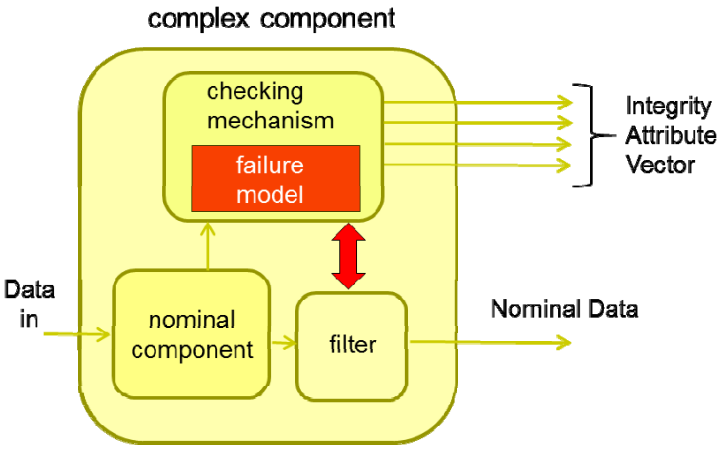
Main achievements

- KARYON architectural pattern
- Concepts:
  - Level of Service
  - Data validity
  - Safety kernel
- KARYON work was developed around this pattern



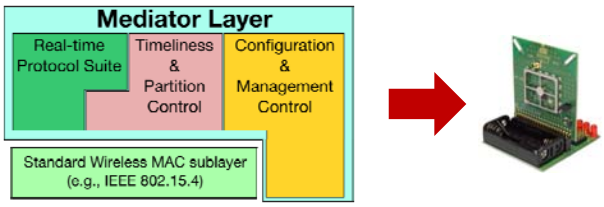
Main achievements

- Abstract sensor model
  - Sensor data with attached data validity attribute
- Separation of concerns:
  - Correctness criteria only based on data validity

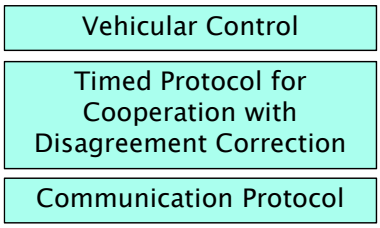


Main achievements

- Solutions for predictable communication
- Abstract network properties
  - Reduced communication uncertainty in wireless networks

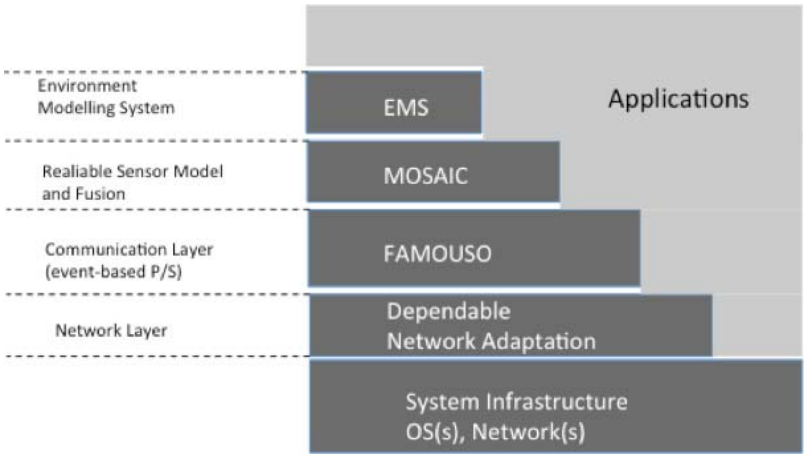


  - Cooperative systems and agreement



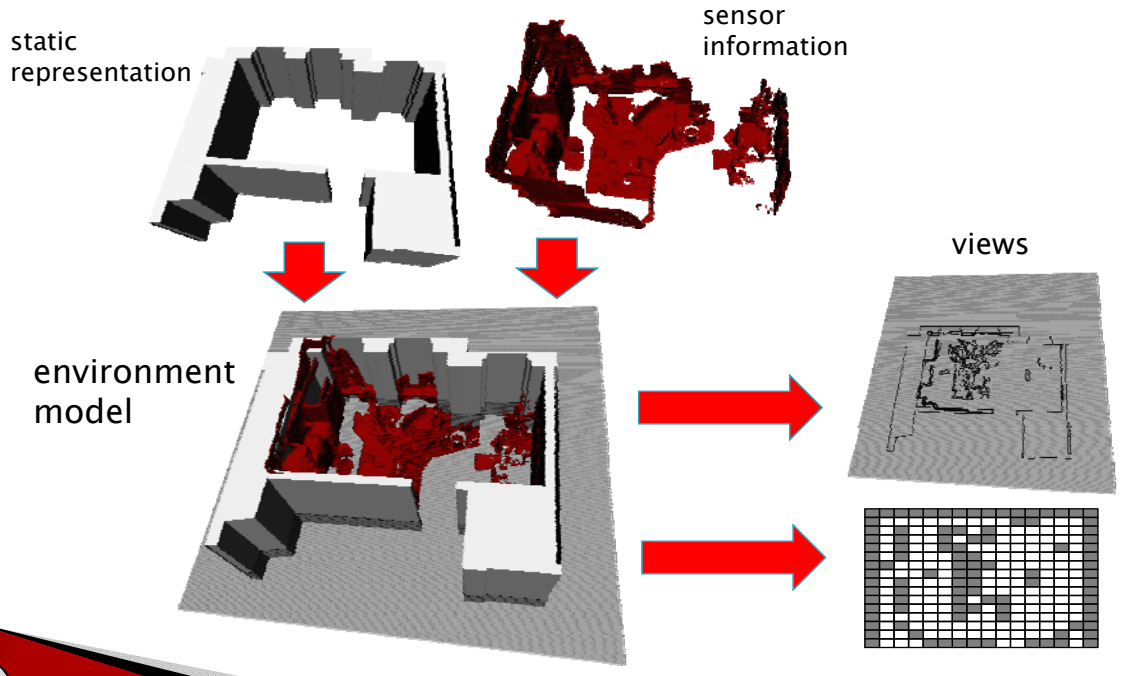
Main achievements

- Middleware for mixed-reality systems
  - FAMOUSO publish/subscribe middleware for event-based communication



Main achievements

- Environment models



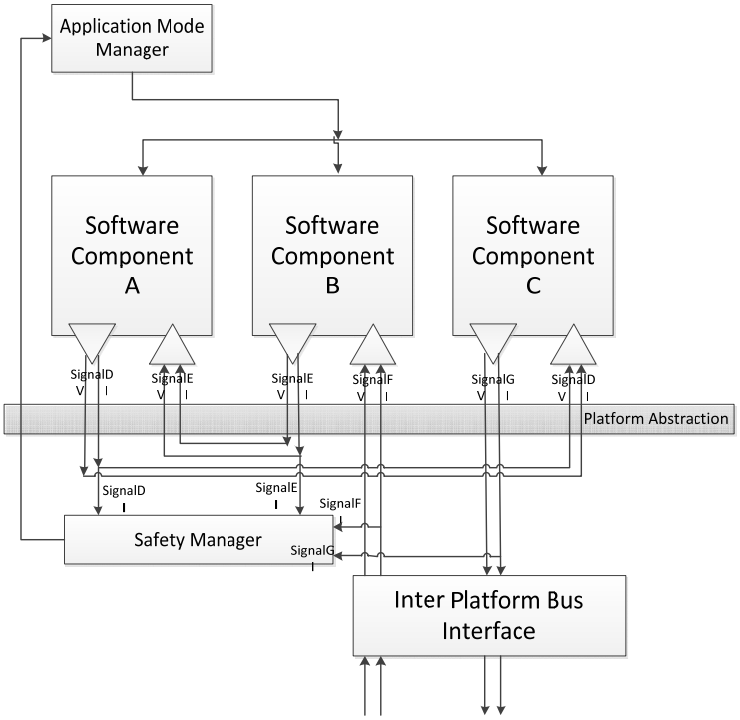
Main achievements

- Standards analysis
  - Similarities between ISO 26262 and ARP4754A
  - ASIL vs DAL
    - Conceptually the same

- Automotive domain:
  - ISO 26262
  - ETSI EN 302 665
  - ETSI TR 102 638
  - ETSI TS 102 637-2
  - ETSI TS 102 868-1
  - ETSI TR 102 863
  - ETSI TR 102 893
  - ETSI TR 102 862 V1.1.1 (2011-12)
- Avionics domain:
  - DO-178B/ED-12B
  - DO-254/ED-80
  - ARINC 653
  - ARP4754A
  - ARP4761

Main achievements

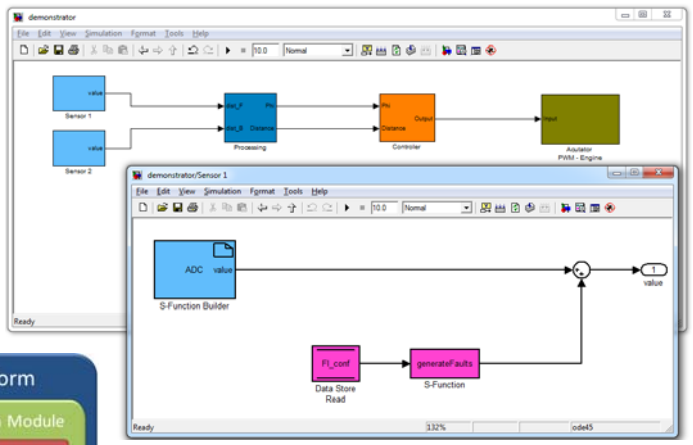
- **Deployment of architectural pattern**
  - To AUTOSAR
  - To IMA (ARINC 653)

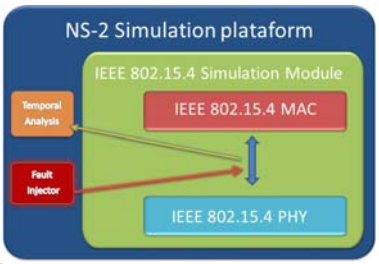


Main achievements

- **Fault injection tools**

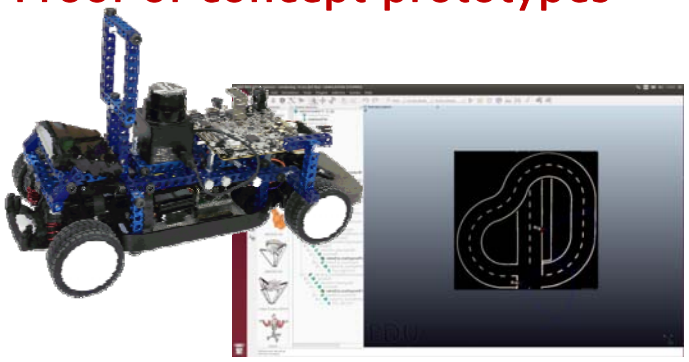
Fault injection node

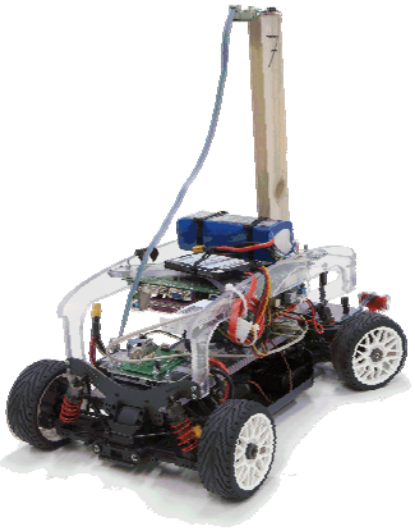




Main achievements

- Proof of concept prototypes





Main achievements

- Publications
  - About 40 papers in conferences and workshops
  - Two promotional videos
- ASCoMS workshop
  - Organized in conjunction with SAFECOMP
  - 3 editions (to be continued)
- Prizes
  - 2 best paper awards