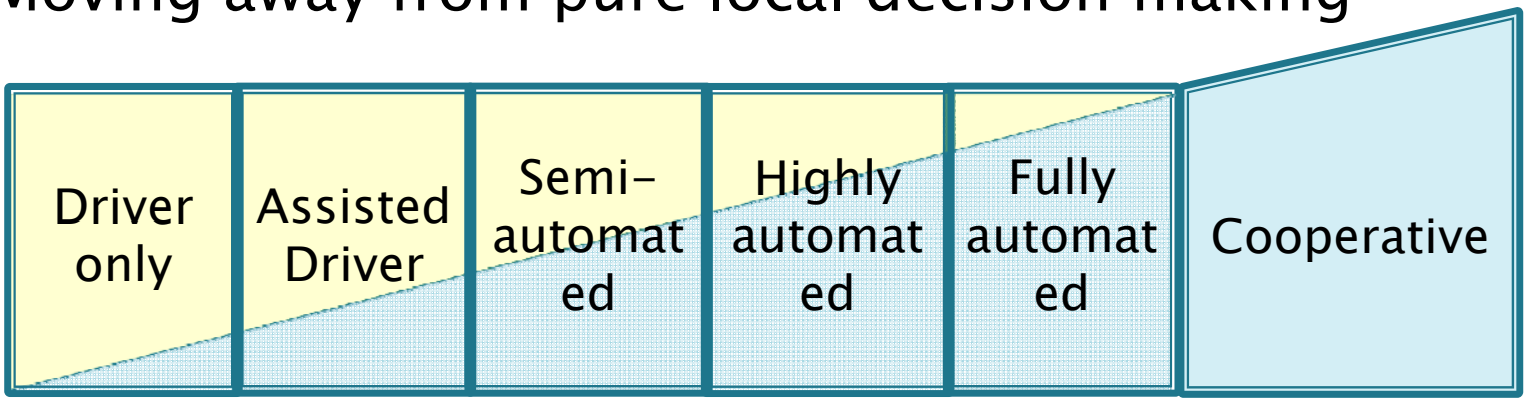
The KARYON approach for Safe Coordination in Cooperative Vehicular Systems

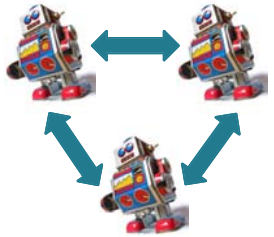
Presented by António Casimiro, FCUL

Kernel-Based ARchitecture for safetY-critical cONtrol

Autonomy and cooperation

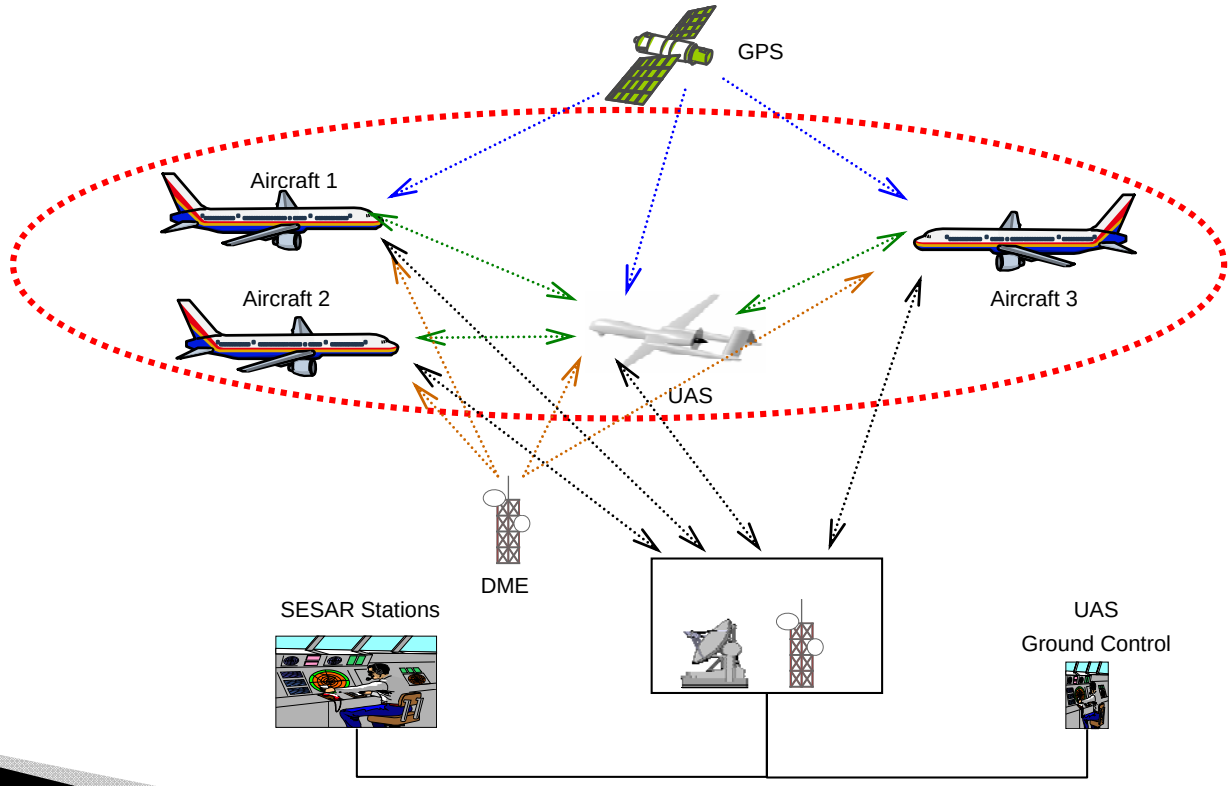
- Automotive and avionic application domains
  - Still very limited use of automated control functions
  - **No cooperation**
- Cooperative control, cooperative functionality
  - Moving away from pure local decision making





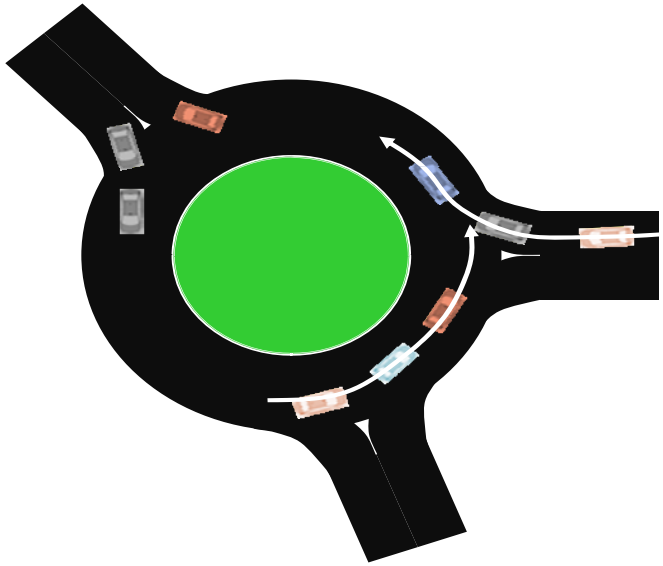
Example in the avionics domain

- From segregated to shared airspace
  - UAVs coordinating with airplanes
- Optimized use of air space

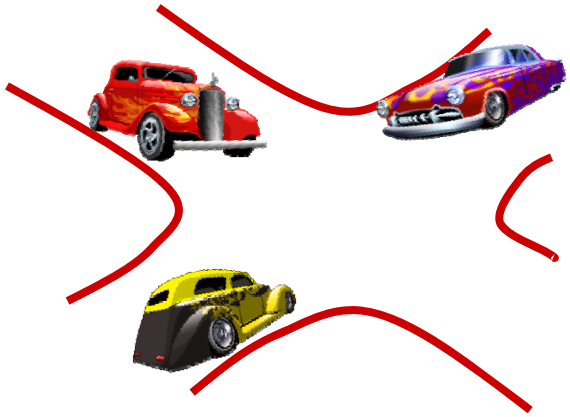


Example in automotive domain

- Cooperative ‘X’ functions
  - Cooperative lane change
  - Cooperative collision warning
  - Cooperative roundabout
  - Etc.
- Optimized traffic flows



Cooperative roundabout



Virtual traffic light

Are we ready to cooperate?

- Availability of sensor technology
  - GPS, Video, Radar, Infra-red, inertial, etc
- Availability of wireless communication solutions
  - ADS-B, 802.11p, 802.15.4, C2CC solutions, etc.
- Availability of processing technology
  - Large number of ECUs in vehicles
  - Powerful embedded processors

- **But there are still many challenges…**

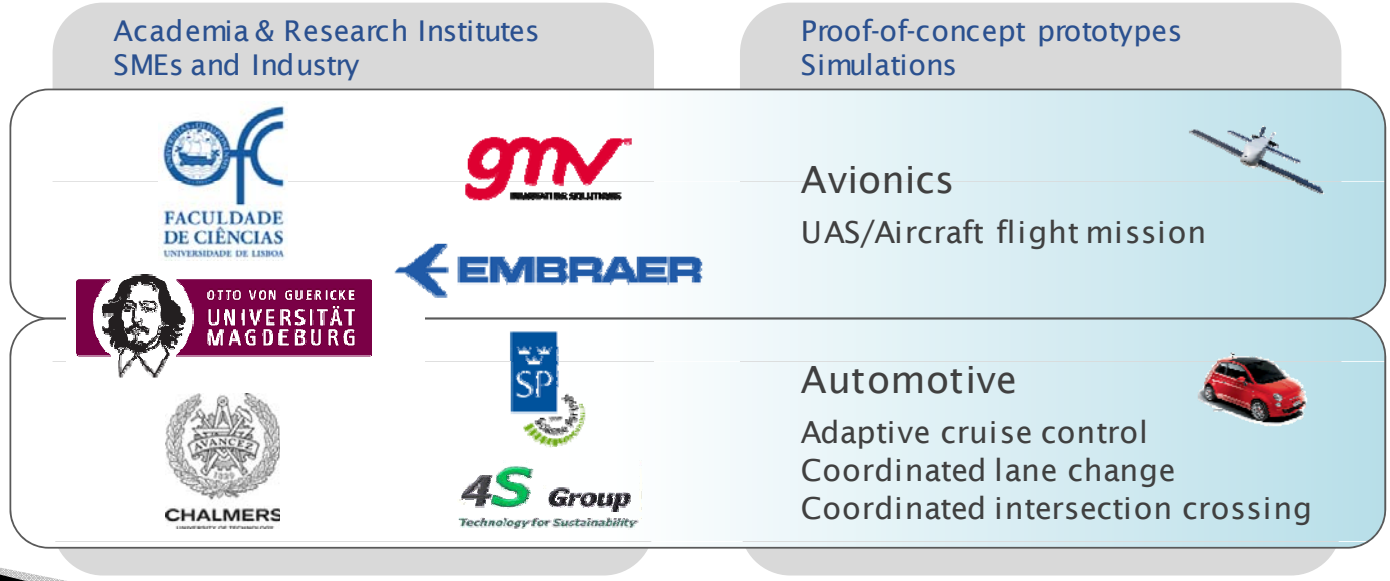
Challenges

- **Uncertainty, uncertainty, uncertainty**
  - Sensor faults
  - Wireless communication faults
  - Timing faults due to complex processing
- On the other hand, **safety requirements are very, very high**

How to achieve improved functionality, exploiting coordination and using more complex control solutions, without sacrificing cost and/or safety?

KARYON partners

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



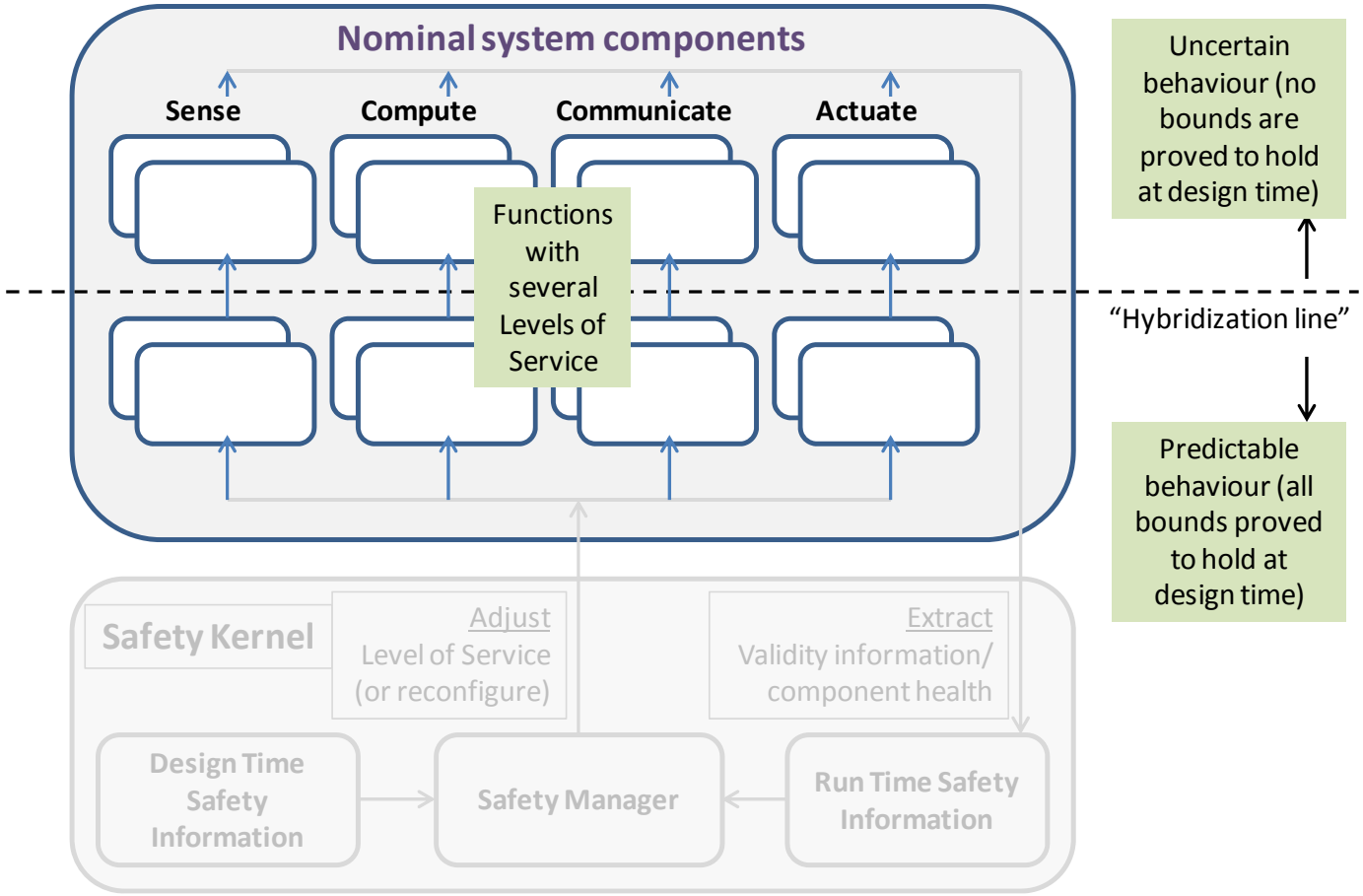
KARYON highlights

- **Architectural solution**
  - Hybrid system model [*Wormholes*]
  - Complex and simple control components [*Simplex*]
  - Safety Kernel: runtime safety manager
- **Abstract sensor model**
  - Sensor data with attached validity attribute
- **Mechanisms for improved perception**
  - Reduce uncertainty in wireless communication
- **Proof of concept prototypes**
  - Demonstration with small vehicles
  - Simulation with airplanes and RPVs

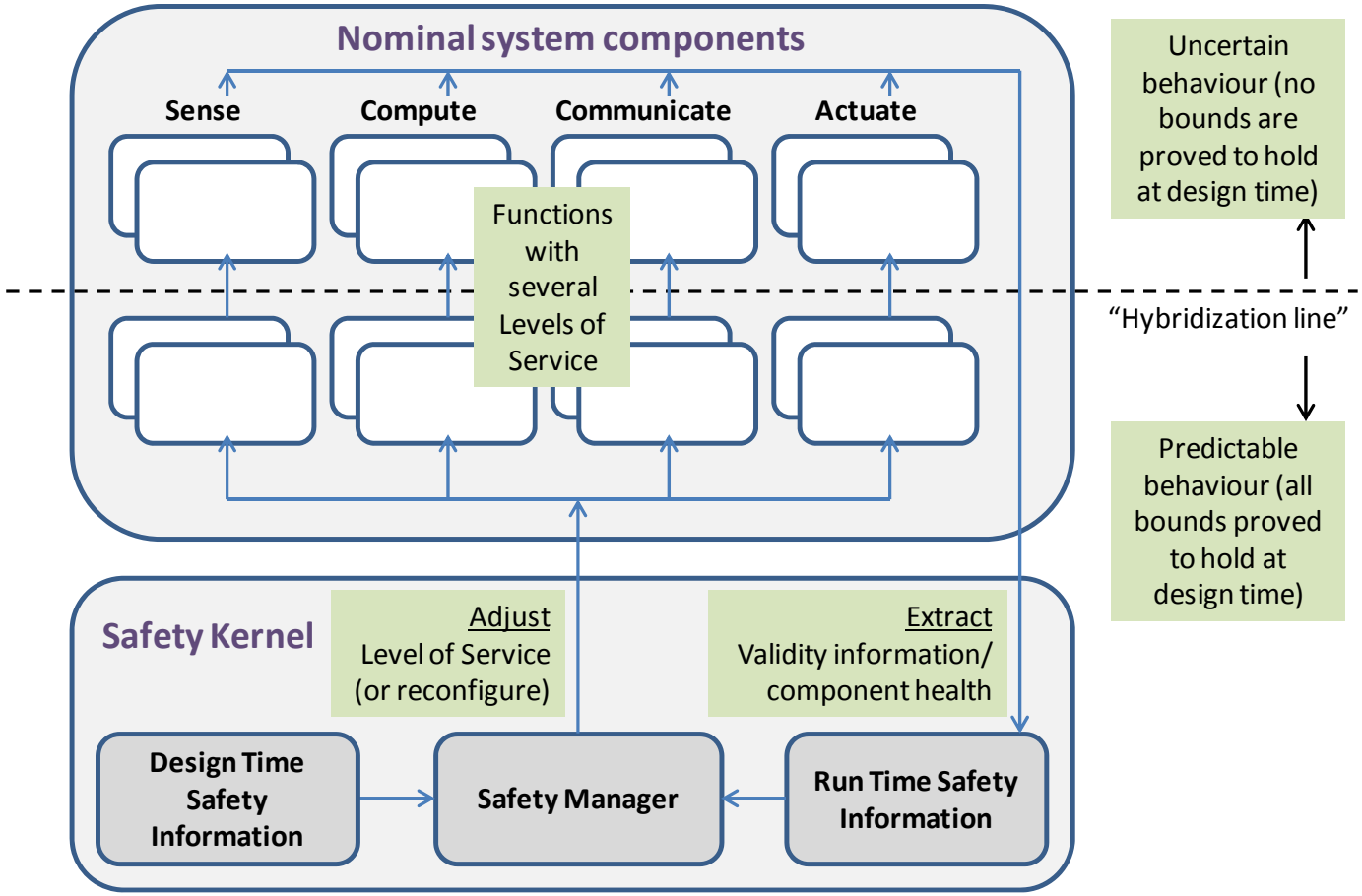
Fundamental concepts

- **Hybrid system architecture**
  - Different properties in different parts of the system
    - Predictable part – Timeliness proved to hold in design time
    - Non-predictable part – Uncertain timeliness
  - Improved performance when complex components in non-predictable part execute timely
  - Reduced performance (but safe behavior) when complex component become untimely
- **Level of Service**
  - Functionality can be provided with different levels of service
  - Each level of service has different safety requirements
  - When the integrity of some component or data becomes smaller, switch functionality to lower level of service

KARYON architecture



KARYON architecture

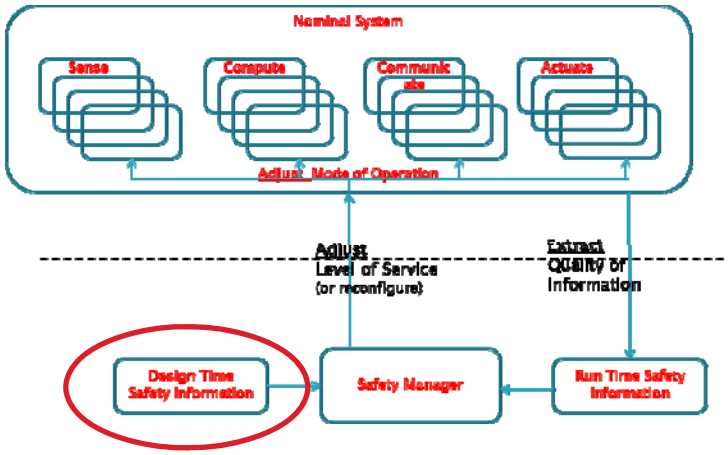


Safety control loop

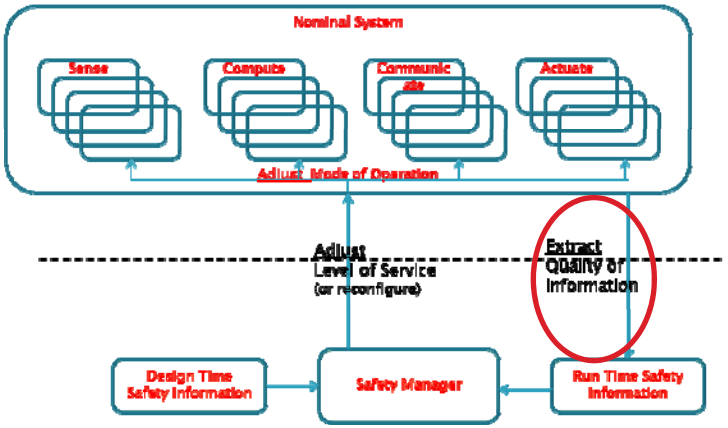
- **Decisions on mode of operation are based on:**
  - Observed **validity** of sensor data
  - Observed **timeliness** of complex components
- **The LoS must be changed in bounded time:**
  - Requires real-time LoS management control loop
  - The lowest LoS can be provided only with components below the hybridization line, which are timely (by design)
- **Safety rules are derived at design time:**
  - As a result of hazard analysis, for each LoS…
  - …and setting safety bounds (on data validity and execution time) for each LoS

Design Time Safety Information

- What Safety Requirements (or Contracts) apply for each LoS of each service and where they are allocated?
- For each architectural block in the system
  - What modes of operation relate to what LoS for all the different services?



Safety Requirements on a Component



Complex Component

Nominal data

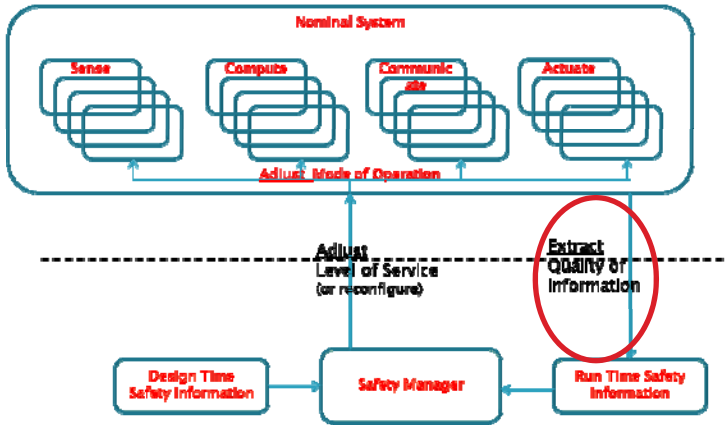
Safety Requirement

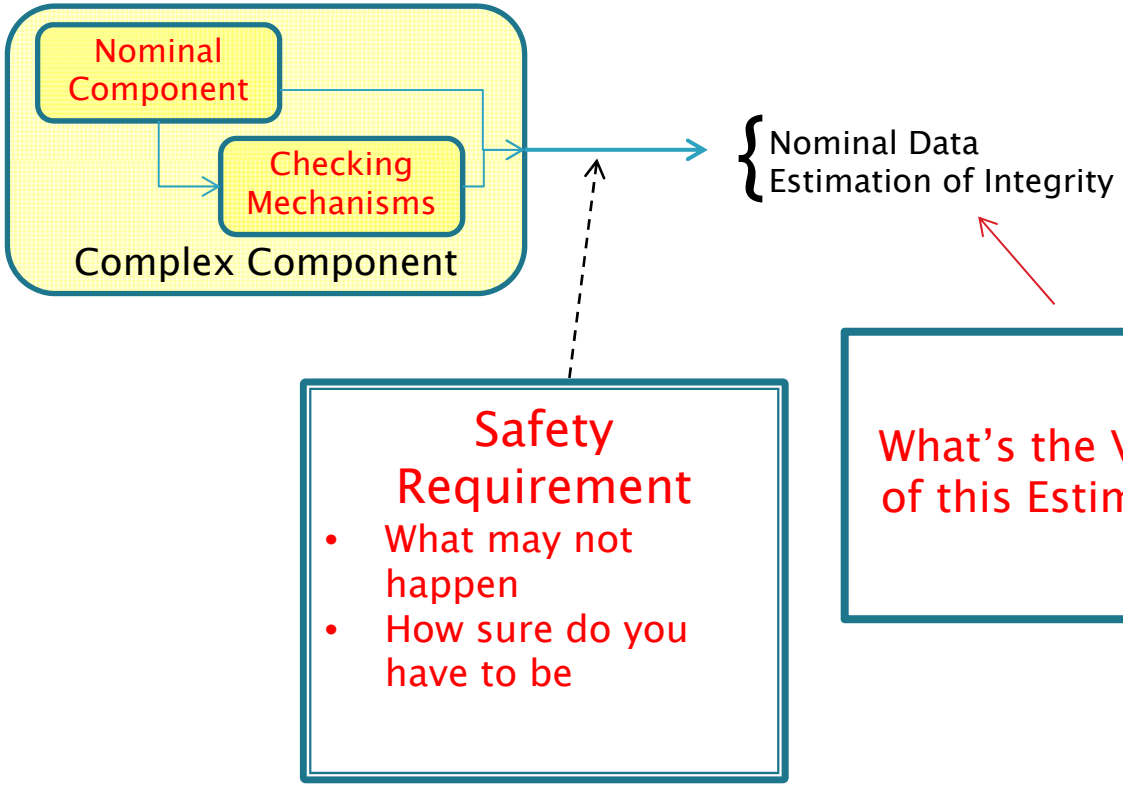
- What may not happen
- How sure do you have to be

Failure model

Safety Integrity Level

Estimate in run time fulfilment of safety requirement

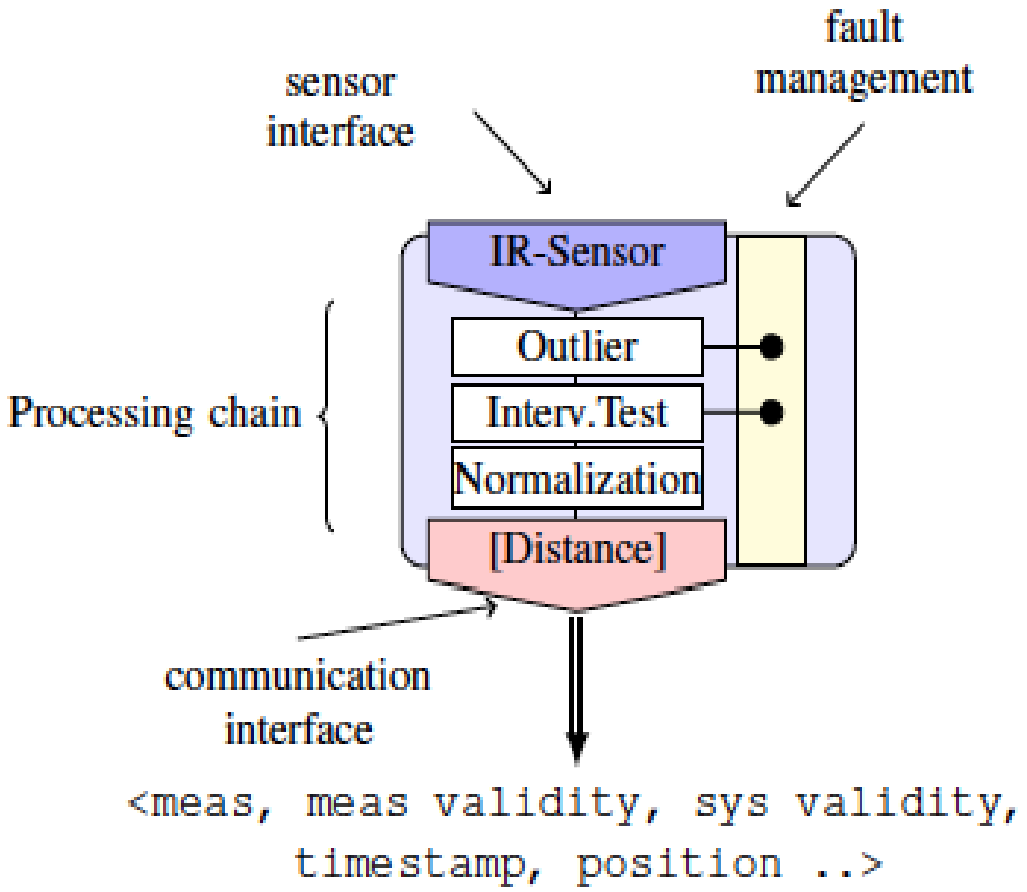




How are validity estimates propagated?

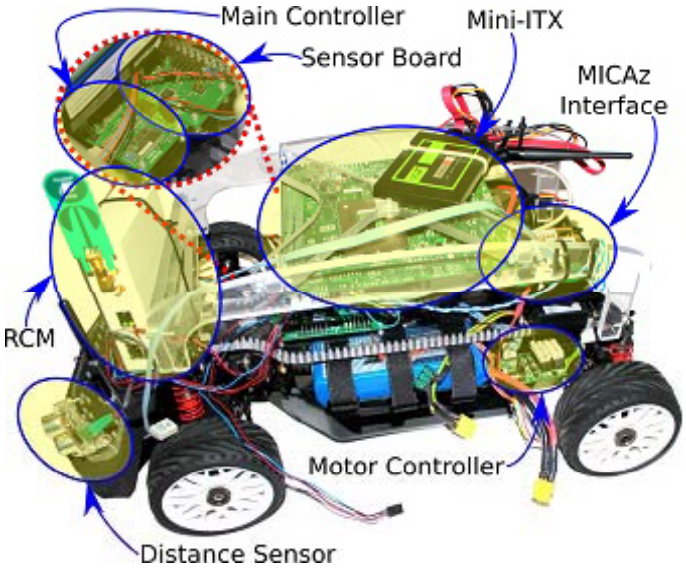
How does redundancy affect validity estimates?

Abstract sensor model



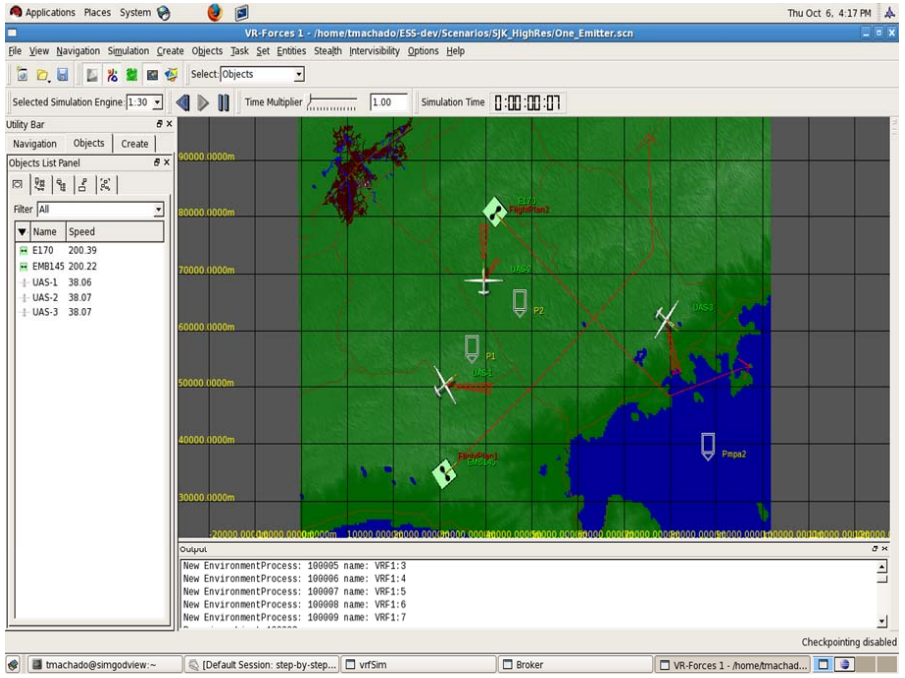
Automotive Scenarios

- Adaptive Cruise Control Systems
  - More efficient Platooning capabilities should improve fuel consumption
- Crossing road intersections
  - Improved safety measures should help avoid collisions
- Coordinated lane change
  - One of the key collision reasons is the changing of lanes with other vehicles in the driver “blind spot”



Avionics Scenarios

- Common trajectory traffic in the same direction
  - Increased usage of air corridors
- Levelled crossing trajectories
  - Improved safety measures should help avoid collisions
- Coordinated flight level change
  - Improved safety measures should help avoid collisions



Final remarks

- Other topics not covered in this talk
  - Environment models
  - How to bridge avionics and automotive standards concerning functional safety (e.g. DAL vs ASIL)
  - Network inaccessibility for 802.15.4
  - Fault injection tool for experimental evaluation of safety according to ISO 26262
  - Reliable cooperation and assessment of global state

- A lot of work ahead of us !!!!

Questions?

Thank you!

Visit us at

http://www.karyon-project.eu

or

http://www.navigators.di.fc.ul.pt