Summary from Session 5:
Autonomous Vehicles

Alysson Bessani

FCUL

Two presentations

- Safety in Cooperative Autonomous Systems
  (Emilia Cioroaica, Fraunhofer IESE)

- An Architectural Approach for Safe Cooperative Autonomous Vehicles
  (Antonio Casimiro, FCUL)

Safety in Cooperative Autonomous Systems

- Vision of Dynamic Safety Management
  - Uncertainties must be explicit at design time
  - Uncertainties lead to adaptive models
  - And then we have dynamic dependability management
- This vision was applied in a modular way, using contract-based development
- Method for building trust in dynamic systems
  - Digital twin (of a smart agent) runs in a simulated world
  - A digital twin is verified and generates constraints for its smart agent behavior

An Architectural Approach for Safe Cooperative Autonomous Vehicles

- For safety, autonomous cars work on restricted environments, use expensive hardware, and sacrifice functional performance (e.g., Google car is too slow)
  - Challenge is to achieve high performance, safety and low cost
- Vehicle cooperation might be a way to achieve that
- But there are many challenges…
  - No business model, new safety risks due to the use of external data, interoperability, lots of data being collected
- The KARYON project focused on improving functional performance
  - In design time it is proved that the service works under certain assumptions
  - In runtime, these assumptions need to be monitored by a safety kernel
  - System requires agreement on the cooperative level of service

Takeaways

- Main theme: monitoring for safe autonomous adaptation
  - But, monitoring what?
  - The monitor must be trusted & trustworthy

- (Some) open questions:
  - What is the cost of writing a digital twin for a component? Can they be generated automatically (from the component code)?
  - How can one ensure that the constraints generated by a digital twin ensures the component operates safely?
  - What kind of assumptions the safety kernel can monitor?
  - How to agree on the safety level under harsh conditions?