ATRIUM - Architecting Under Uncertainty

Naveen Mohan et al.;
5th Scandinavian Conference on SYSTEM & SOFTWARE SAFETY
Who am I? My “Priors”

➔ 1 year; Defence Industry; Communication, Networks

➔ 3 years; **Volvo Cars/ QRTECH**; SW/ System Designer

➔ The **ARCHER** project

➔ PhD candidate at Mechatronics, KTH and Scania CV;
Introduction to automotive architecting

i.e. What does ATRIUM help with?
Architects make safety critical decisions every day!
How would you enable automation in this platform?
How would you enable automation in this platform?

- Type of sensor?
- “smartness”
- Reliance on other functions?
- Failure modes?
- Redundancy?
- Design diversity?

- Reliability?
- Cost?
- Aftermarket repairs?
ATRIUM provides

- a framework to systematically trace decisions to assumptions and uncertain information
- a work product required by the ISO 26262
- Rationale management and traceability
Why autonomy: Heavy Commercial Vehicles

- **Logistics.** Trucks currently limited in speed.
- **Environmental.** Air resistance – convoying - Fuel savings
- **Chauffer related.** Shortage of qualified drivers Truck driver >30% in cost
- **Simplification (eventual)** Stressful job and environment regulations to help drivers Design to help the driver: ergonomics,
- **New business models** possible if “C” drivers license is not essential. Lower cost of entry for more people.

Source: Sveriges Åkeriföretag
What we are trying to do?

ADI – Autonomous Driving Intelligence

SAE L4 and L5

Source: IEEE Xplore: article on self driving vehicles.

By Veronica538 (Own work) [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0) or GFDL (http://www.gnu.org/copyleft/fdl.html)], via Wikimedia Commons
Human influences in automotive systems design

- Sensitive, critical
- The ultimate fallback
- A simple warning away
- Detectability vs robustness
Legacy: Boon or Bane?

ADI Platform

Source: AutoDrive project consortium
1500 logical nodes
100,000 Vehicles

A Scania production vehicle from 2013
14000 connections

A Scania production vehicle from 2013
What should an architect do?
How do we (Scania) plan to deal with the increased complexity?
Extracting legacy information
SAE WCX 17
Detroit, USA

Using Legacy information for PAA design
This paper: IEEE SysCon 17

Validating the design
(Near) Future work
Using Legacy information for PAA design

This paper:
IEEE SysCon 17
Architectural Refinement using Uncertainty Management - ATRIUM
Architecture and Safety are linked, and inseparable!
Uncertainty must be explicitly managed.

Contradicting viewpoints
Architecting and especially regarding automation => increase in complexity and more uncertainty
Safety requires more formalization to reduce burden on argumentation

And yet, so different
Scope and delimitations

➔ ATRIUM *does not* guarantee safety;

➔ Safety depends highly on use cases and functional requirements.

➔ ATRIUM *does* help extracting relevant information to help design the future architecture for *safety-critical systems*
Risks to the selection

Traceability & Rationale management

INPUTS

Architectural knowledge
Operational Scenarios
Functional Requirements
Components
Failure modes

Clarifications
Tasks

Assumptions

CFA
DA

DG
SDG

DECOMES
DECOMES

Risks
Selection

UNCERTAIN DOMAIN
PERCEIVED CERTAIN DOMAIN

L3...
L4?
What are the assumptions we should make?

How smart should your sensors be for safe L5 vehicles?

Billion miles of driving?

Fuses? Mechanical handovers? Out of scope for safety?

HD Maps:
What happens to the first car in the chain. Delay to update.

Tactical safety vs operational safety. How would your safety case be designed?

View on ATRIUM?
Practicalities in your domain?

Limitations on actuators: where will the redundancy come from?!