# ATRIUM - Architecting Under Uncertainty

**Naveen Mohan et al.;**

**5th Scandinavian Conference on SYSTEM & SOFTWARE SAFETY**

# Who am I? My “Priors”

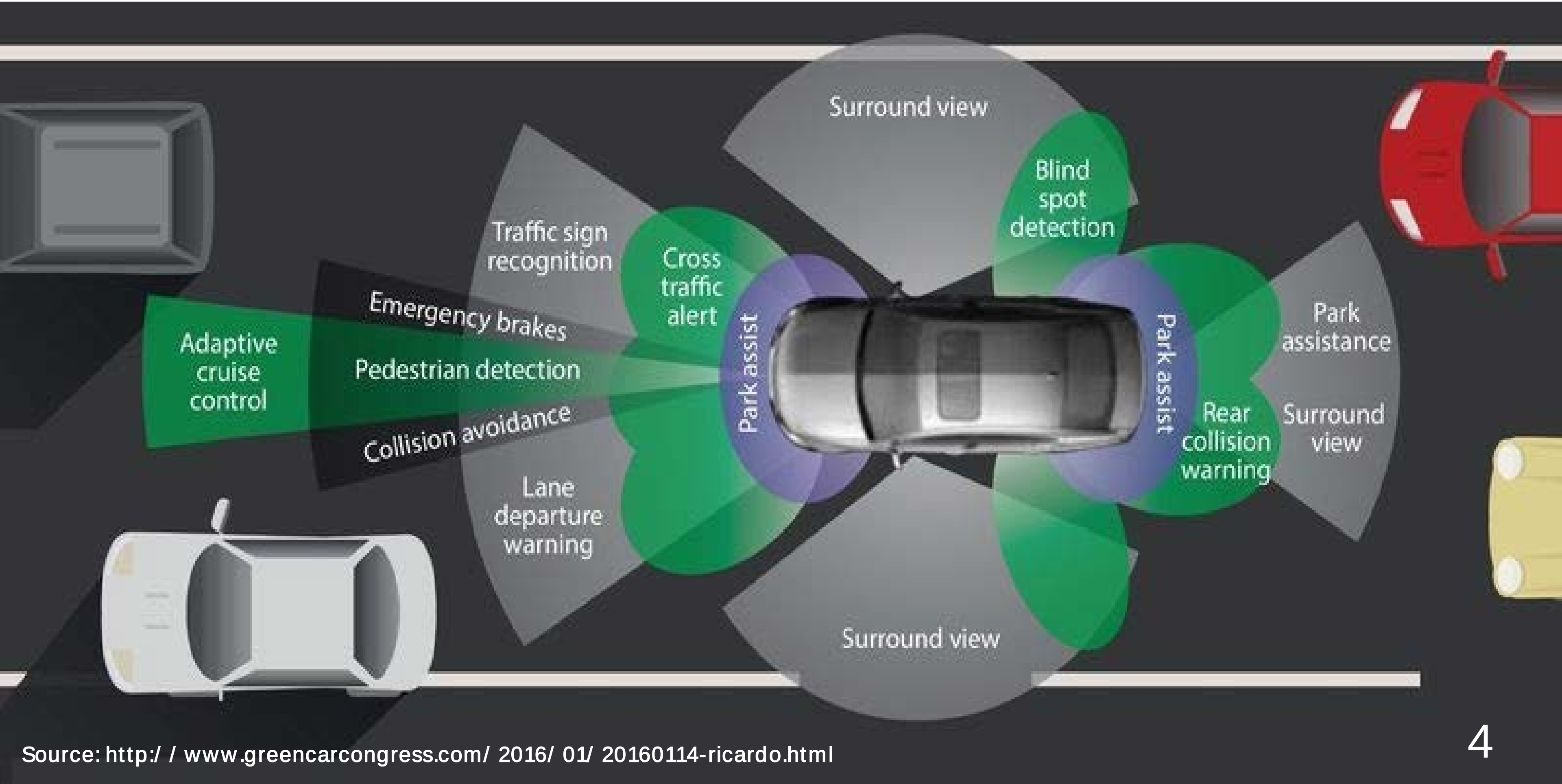
- ➔ 1 year; Defence Industry; Communication, Networks
- ➔ 3 years; **Volvo Cars/ QRTECH;** SW/ System Designer
- ➔ The ARCHER project
- ➔ **PhD candidate at Mechatronics, KTH and Scania CV;**

# Introduction to automotive architecting

i.e. What does ATRIUM help with?

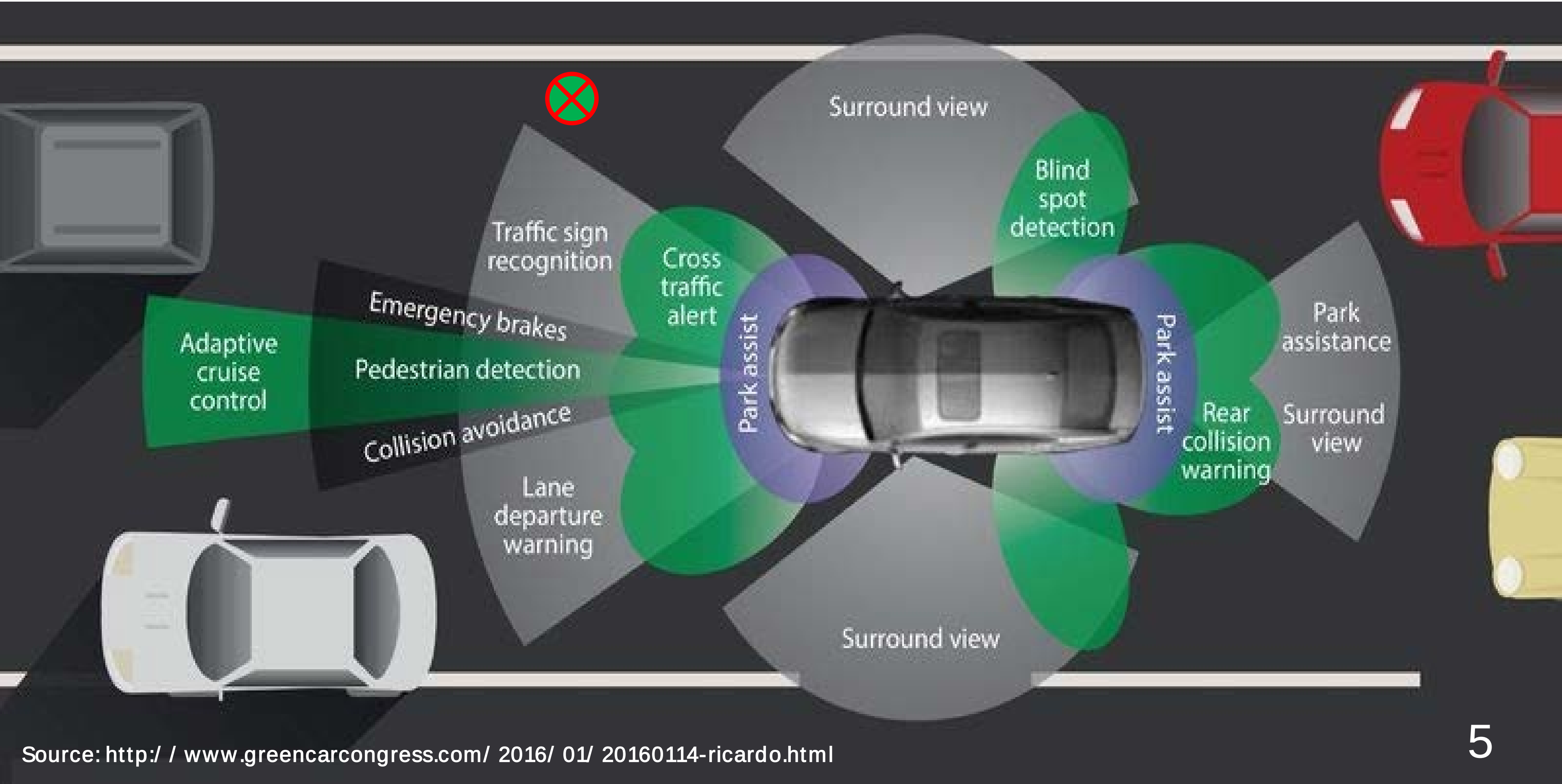
Source: http:/ / www.greencarcongress.com/ 2016/ 01/ 20160114-ricardo.html

# Architects make safety critical decisions every day!



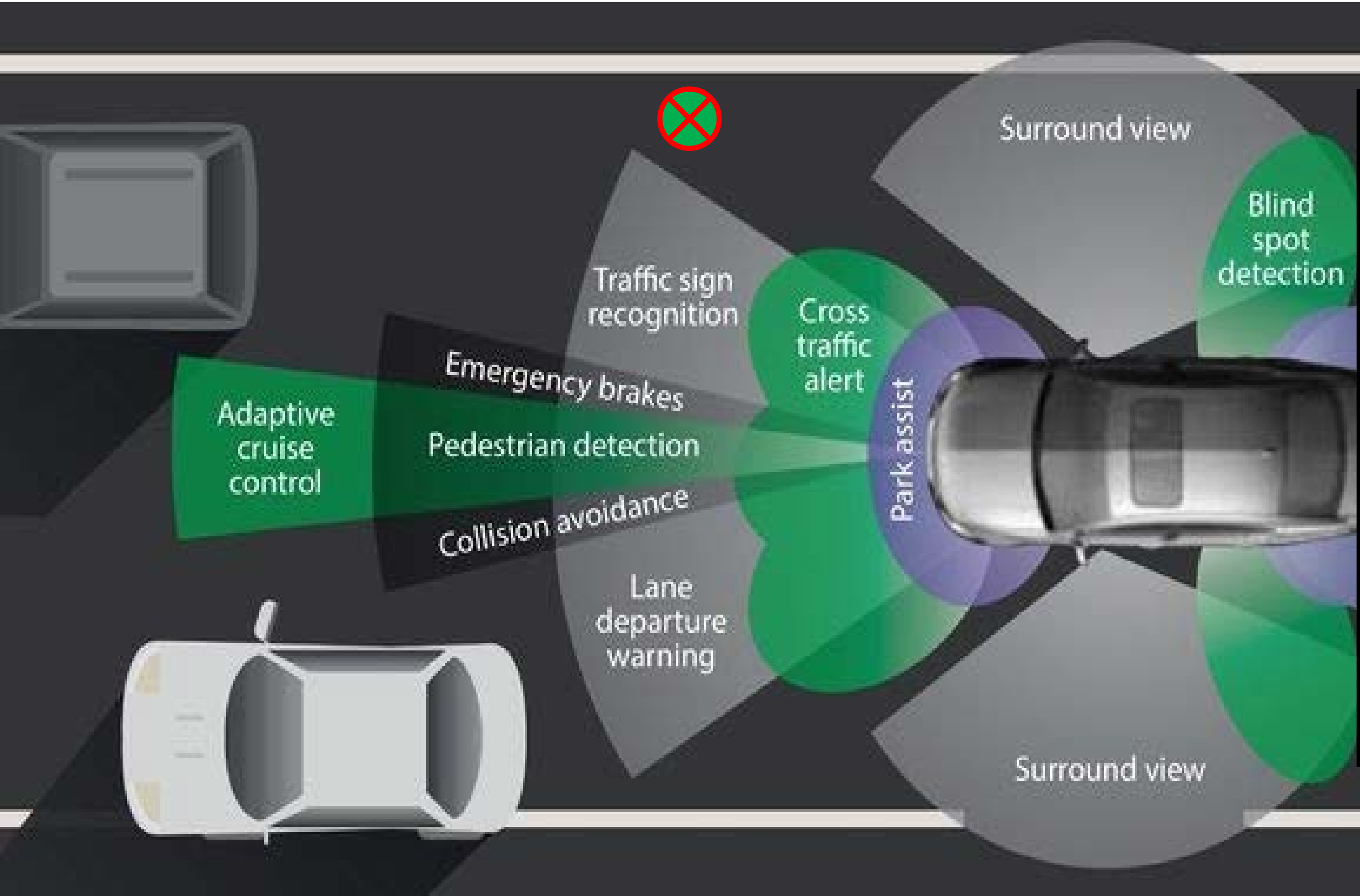
Source: http:/ / www.greencarcongress.com/ 2016/ 01/ 20160114-ricardo.html

# How would you enable automation in this platform?



Source: http:/ / www.greencarcongress.com/ 2016/ 01/ 20160114-ricardo.html

# How would you enable automation in this platform?



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

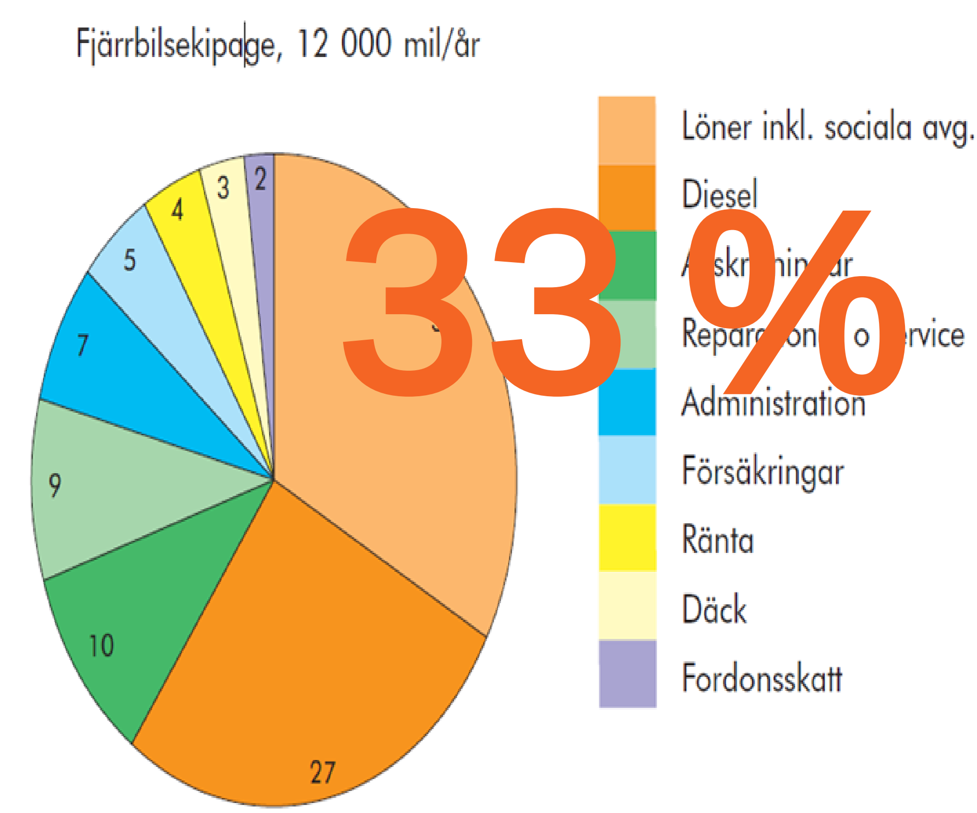
- Reliability?
- Cost?
- Aftermarket repairs?

Source: http:/ / www.greencarcongress.com/ 2016/ 01/ 20160114-ricardo.html

# 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



33%

→ **Logistics.**
Trucks currently limited in speed.

→ **Environmental.**
Air resistance – convoying - Fuel savings

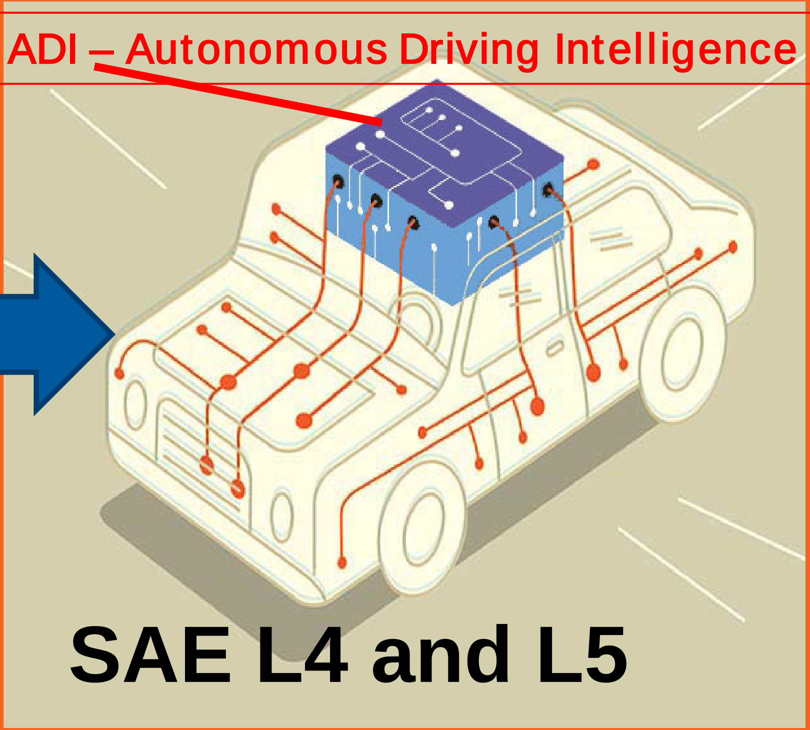
→ **Chauffer related.**
Shortage of qualified drivers
Truck driver >30% in cost

→ **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?

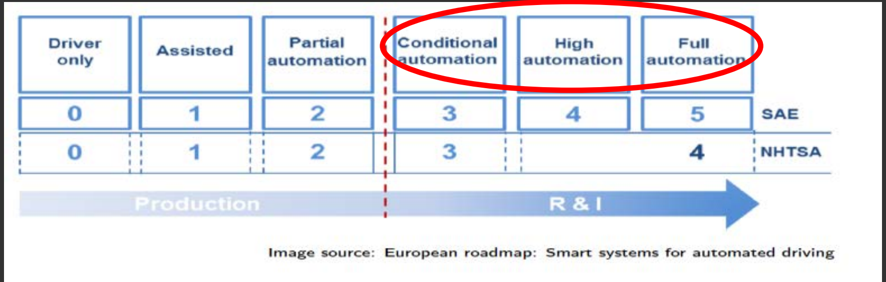


ADI – Autonomous Driving Intelligence

SAE L4 and L5

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

Source: IEEE Xplore: article on self driving vehicles.



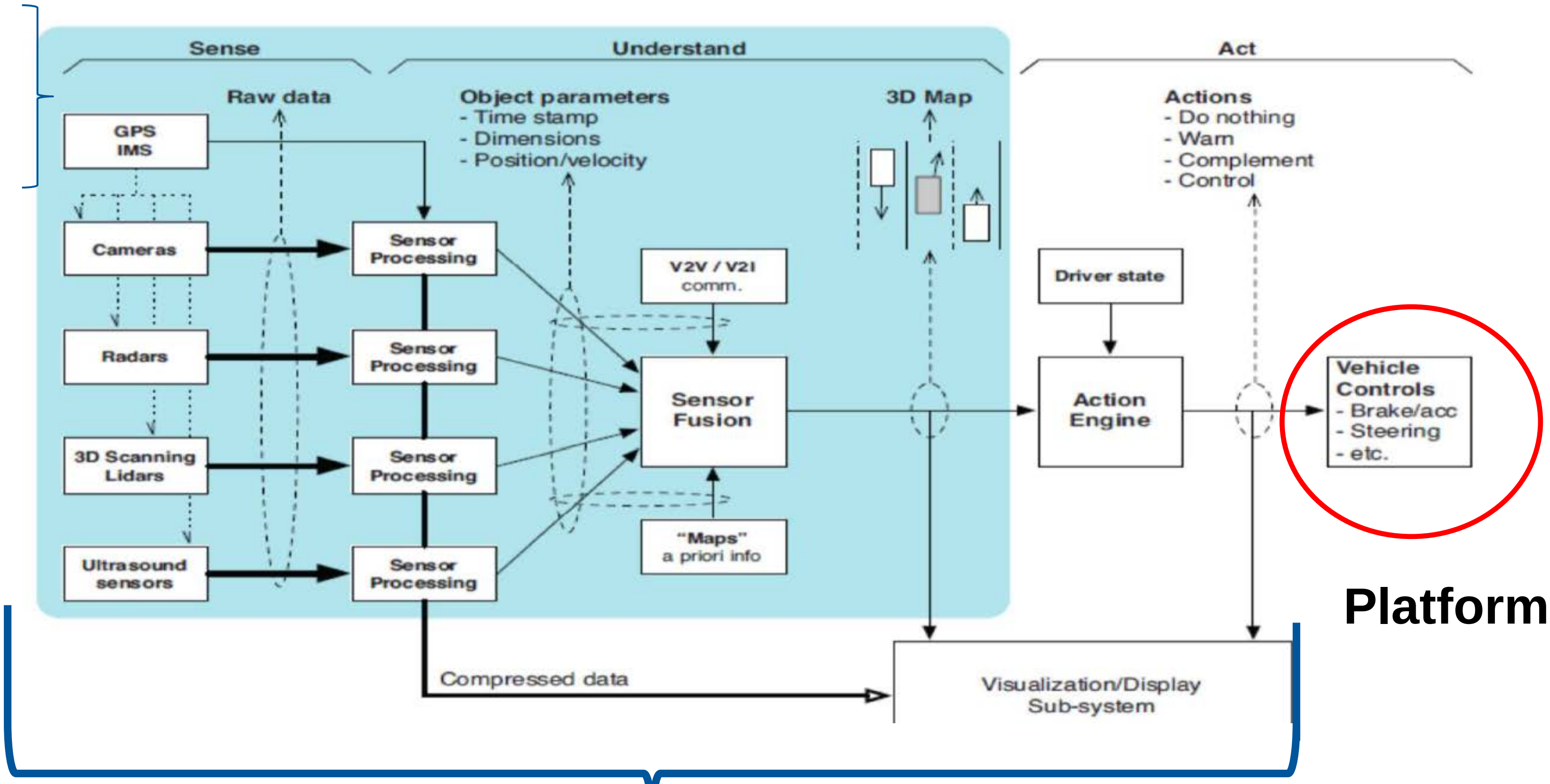
| Driver only | Assisted | Partial automation | Conditional automation | High automation | Full automation | |
|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | SAE |
| 0 | 1 | 2 | 3 | 4 | | NHTSA |

Image source: European roadmap: Smart systems for automated driving

# Human influences in automotive systems design

- Sensitive, critical
- The ultimate fallback
- A simple warning away
- Detectability vs robustness

# Legacy: Boon or Bane?

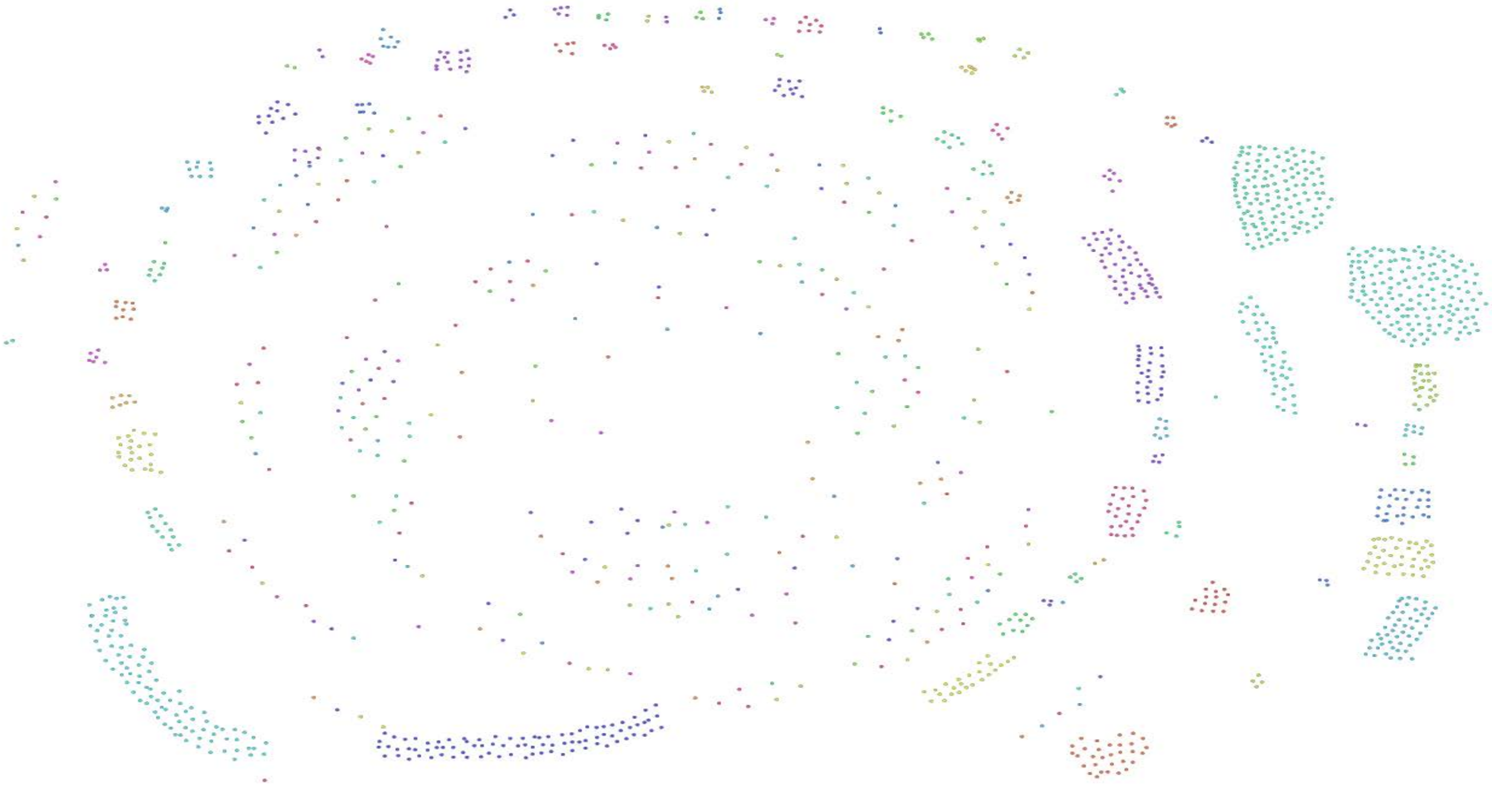


Platform

ADI

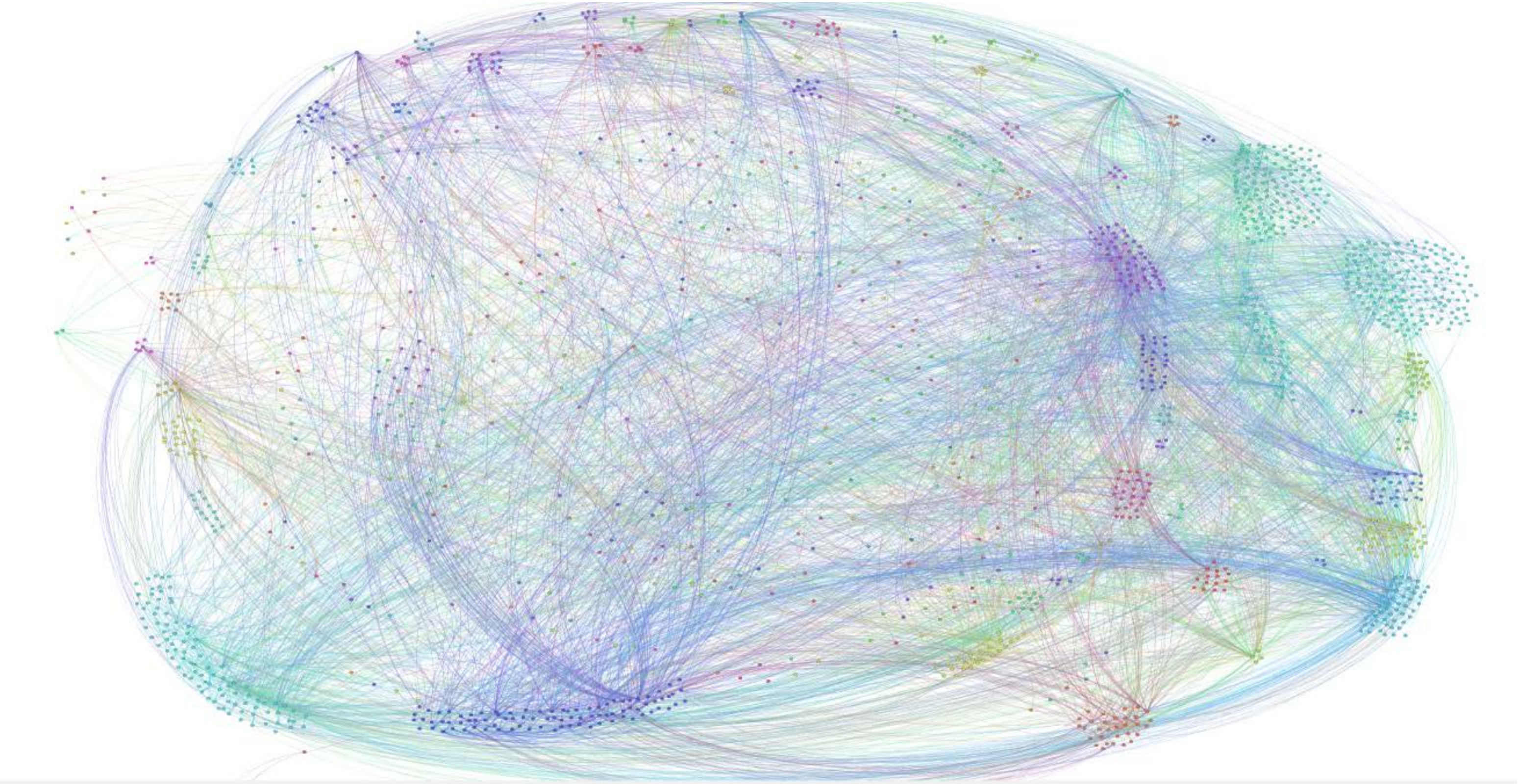
Source: AutoDrive project consortium

# 1500 logical nodes 100,000 Vehicles



A Scania **production vehicle** from 2013

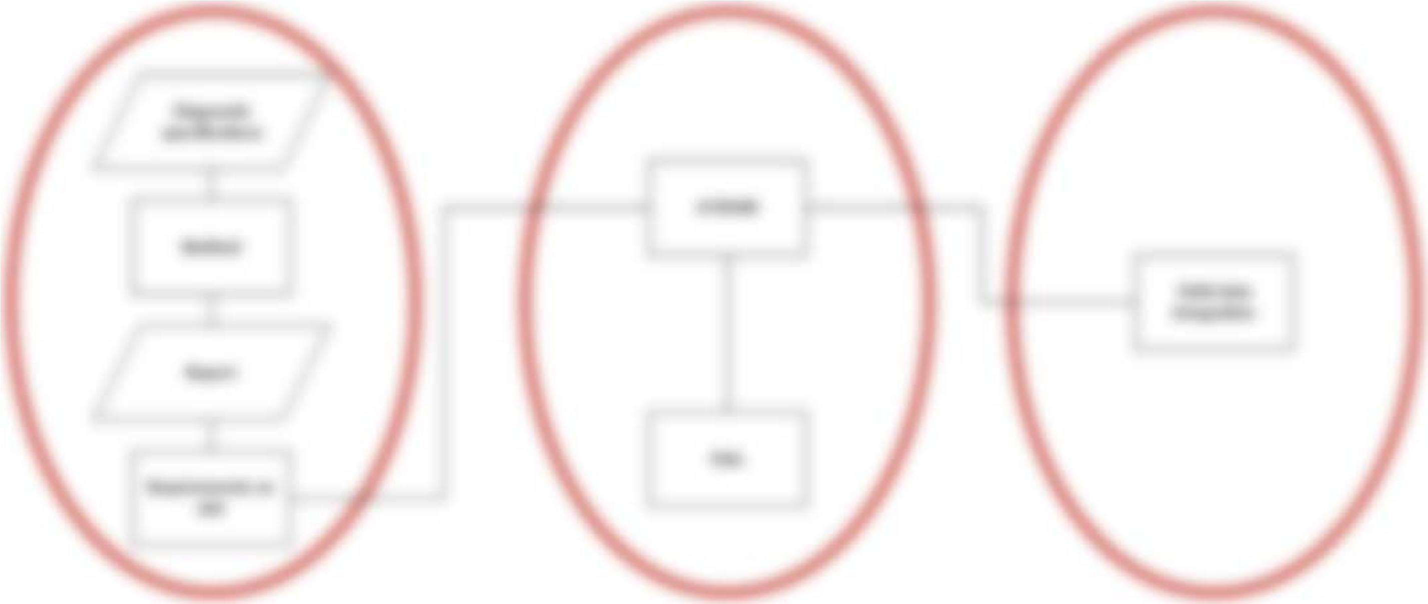
# 14000 connections



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

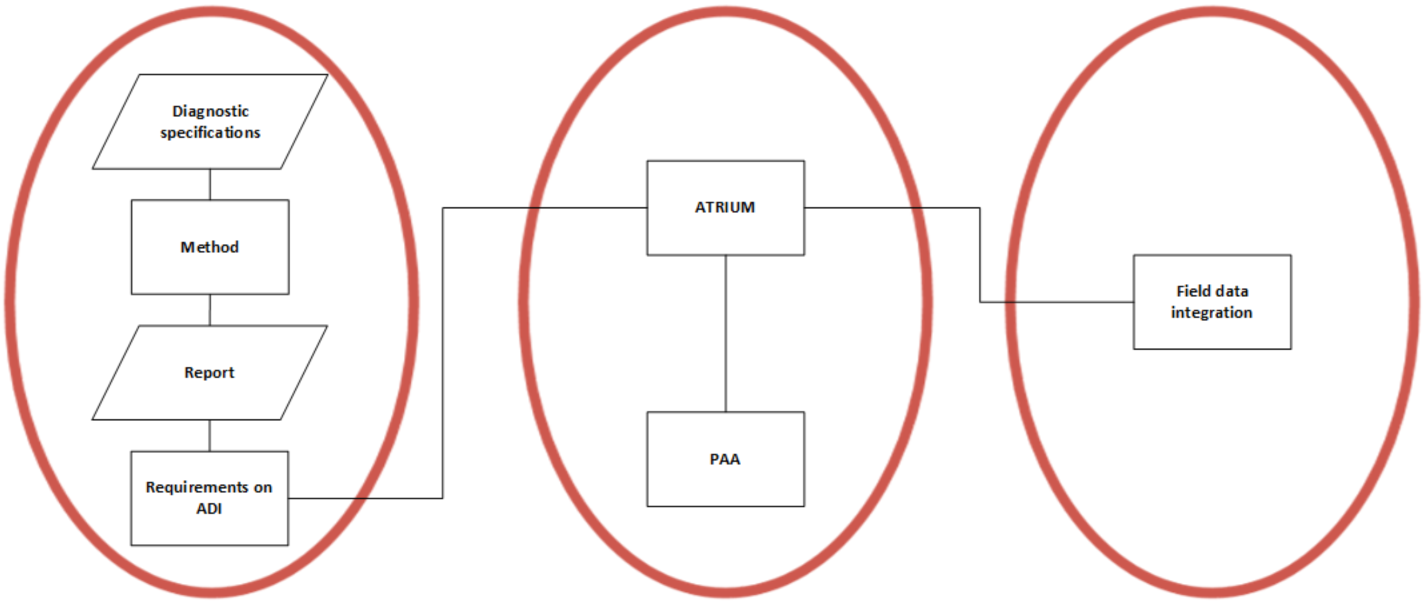
SAE WCX 17
Detroit, USA

Using legacy information for FSA design

This paper:
IEEE SysCon 17

Validating the design

(Next)Future work



Diagnostic specifications

Method

Report

Requirements on ADI

ATRIUM

PAA

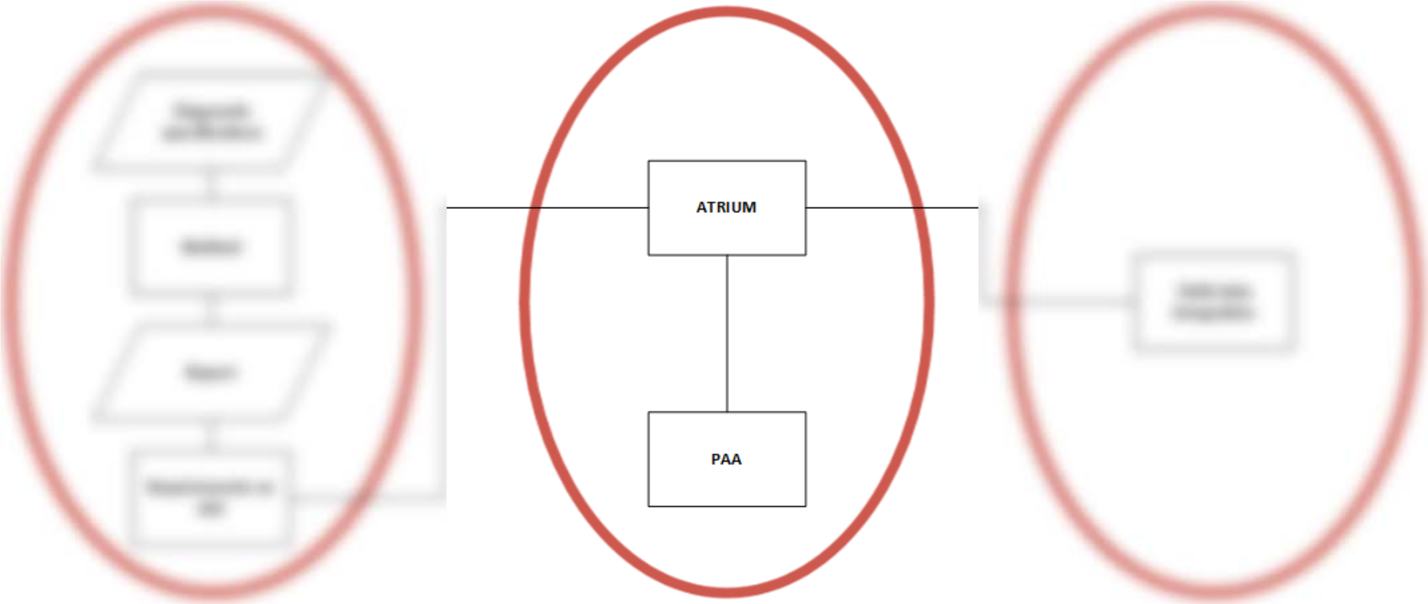
Field data integration

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



Extracting legacy information

SAE WCX 17
Detroit, USA

Using Legacy information for PAA design

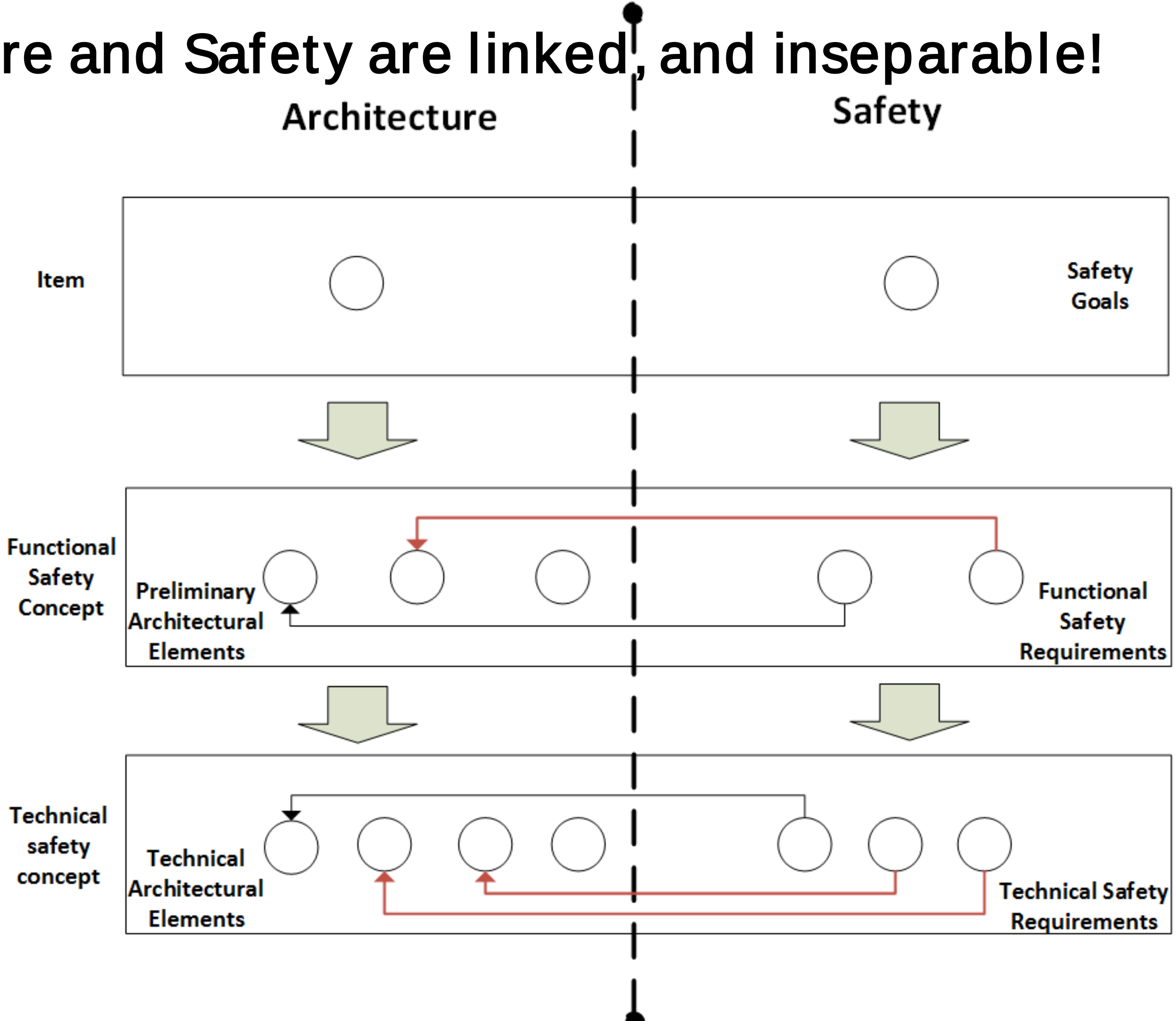
**This paper:**
**IEEE SysCon 17**

Validating the design

(Next/Future work)

# ArchiTectural RefInement using Uncertainty Management - *ATRIUM*

# Architecture and Safety are linked, and inseparable!

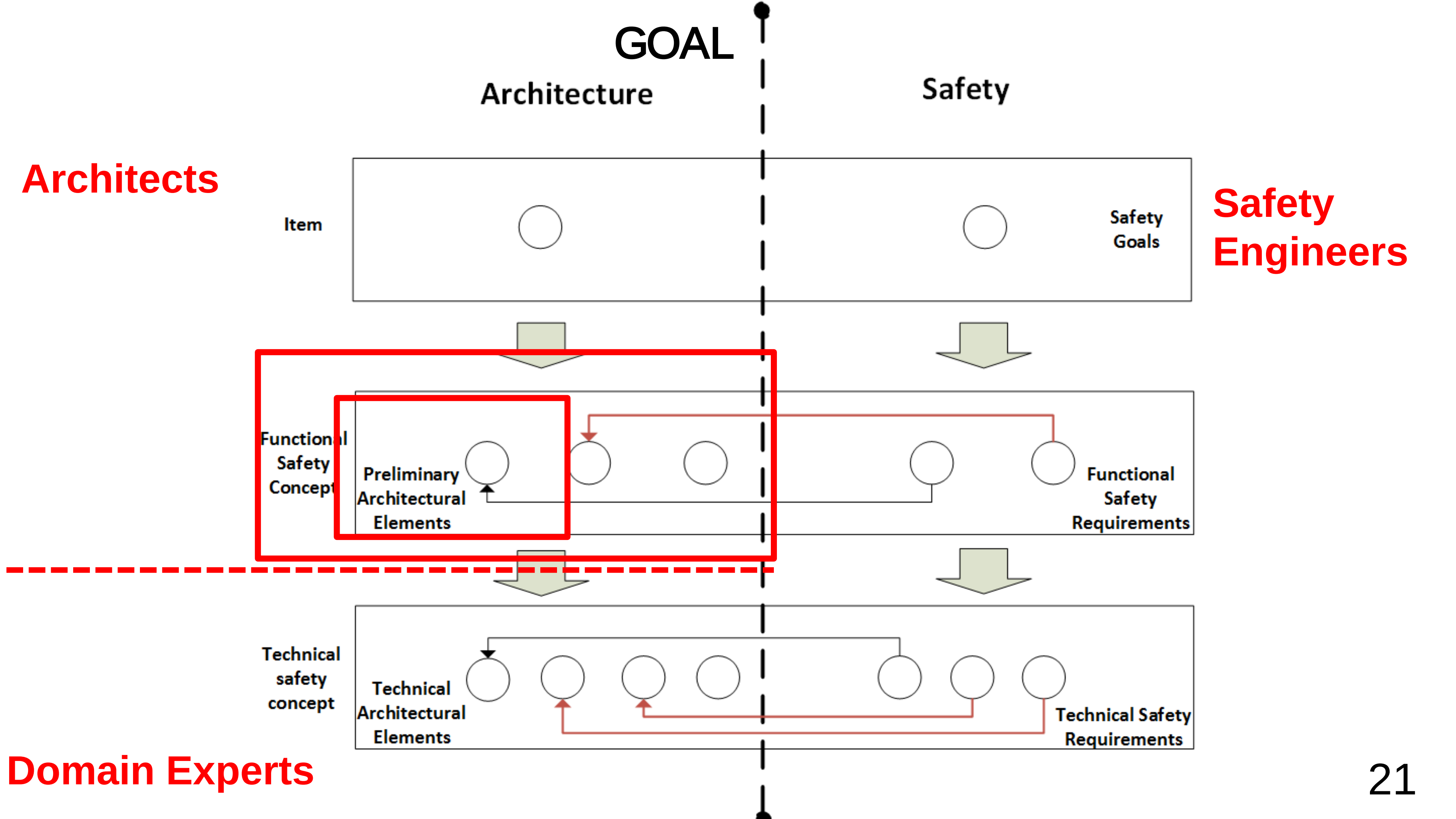

Architecture
Safety
Item
Safety Goals
Functional Safety Concept
Preliminary Architectural Elements
Functional Safety Requirements
Technical safety concept
Technical Architectural Elements
Technical Safety Requirements

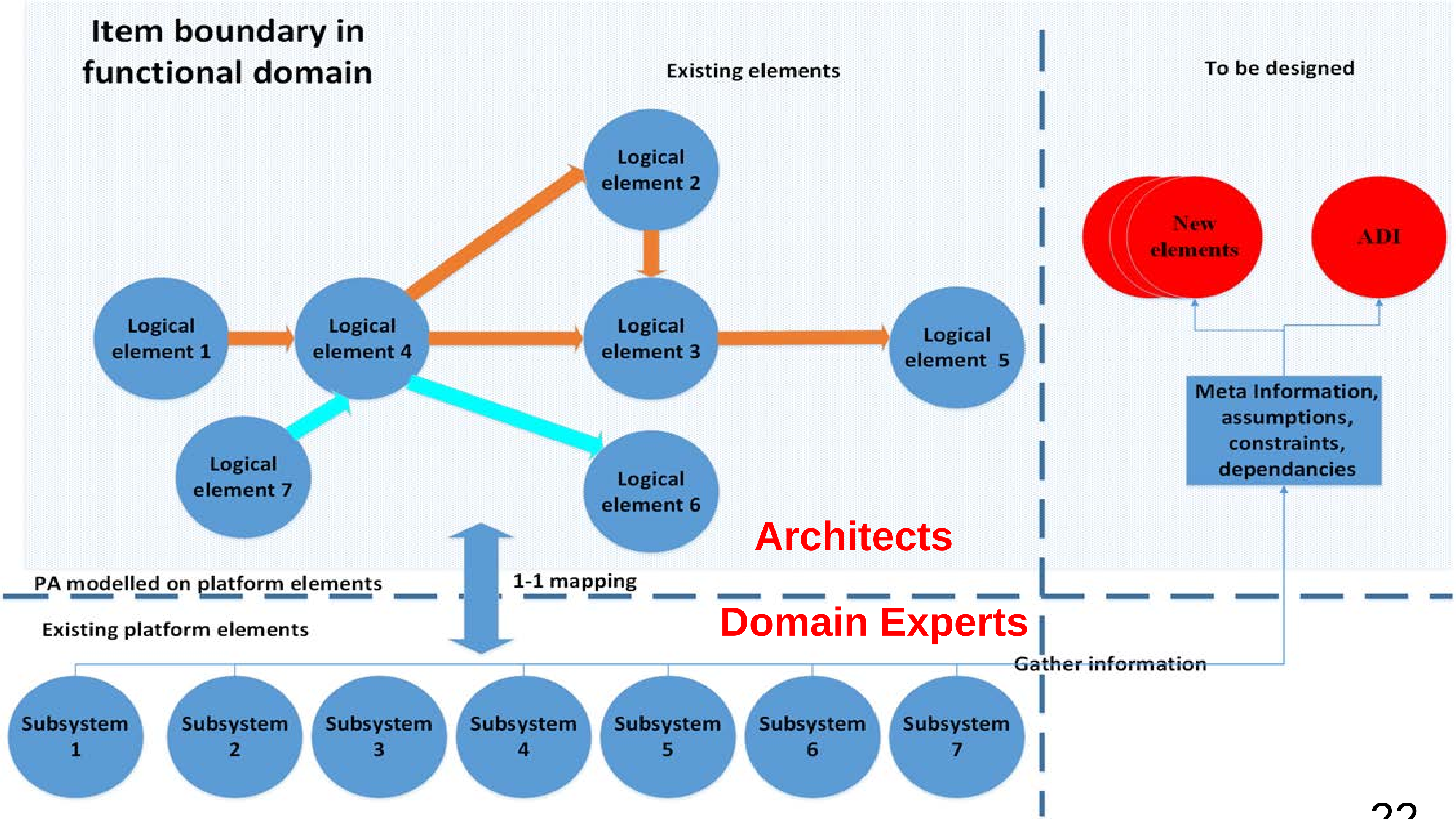
# And yet, so different

## Contradicting viewpoints

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

# Uncertainty must be explicitly managed.


GOAL
Architecture
Safety
Architects
Item
Safety Goals
Safety Engineers
Functional Safety Concept
Preliminary Architectural Elements
Functional Safety Requirements
Technical safety concept
Technical Architectural Elements
Technical Safety Requirements
Domain Experts



Item boundary in functional domain

Existing elements

To be designed

Logical element 1

Logical element 2

Logical element 3

Logical element 4

Logical element 5

Logical element 6

Logical element 7

New elements

ADI

Meta Information, assumptions, constraints, dependancies

Architects

PA modelled on platform elements

1-1 mapping

Domain Experts

Existing platform elements

Gather information

Subsystem 1

Subsystem 2

Subsystem 3

Subsystem 4

Subsystem 5

Subsystem 6

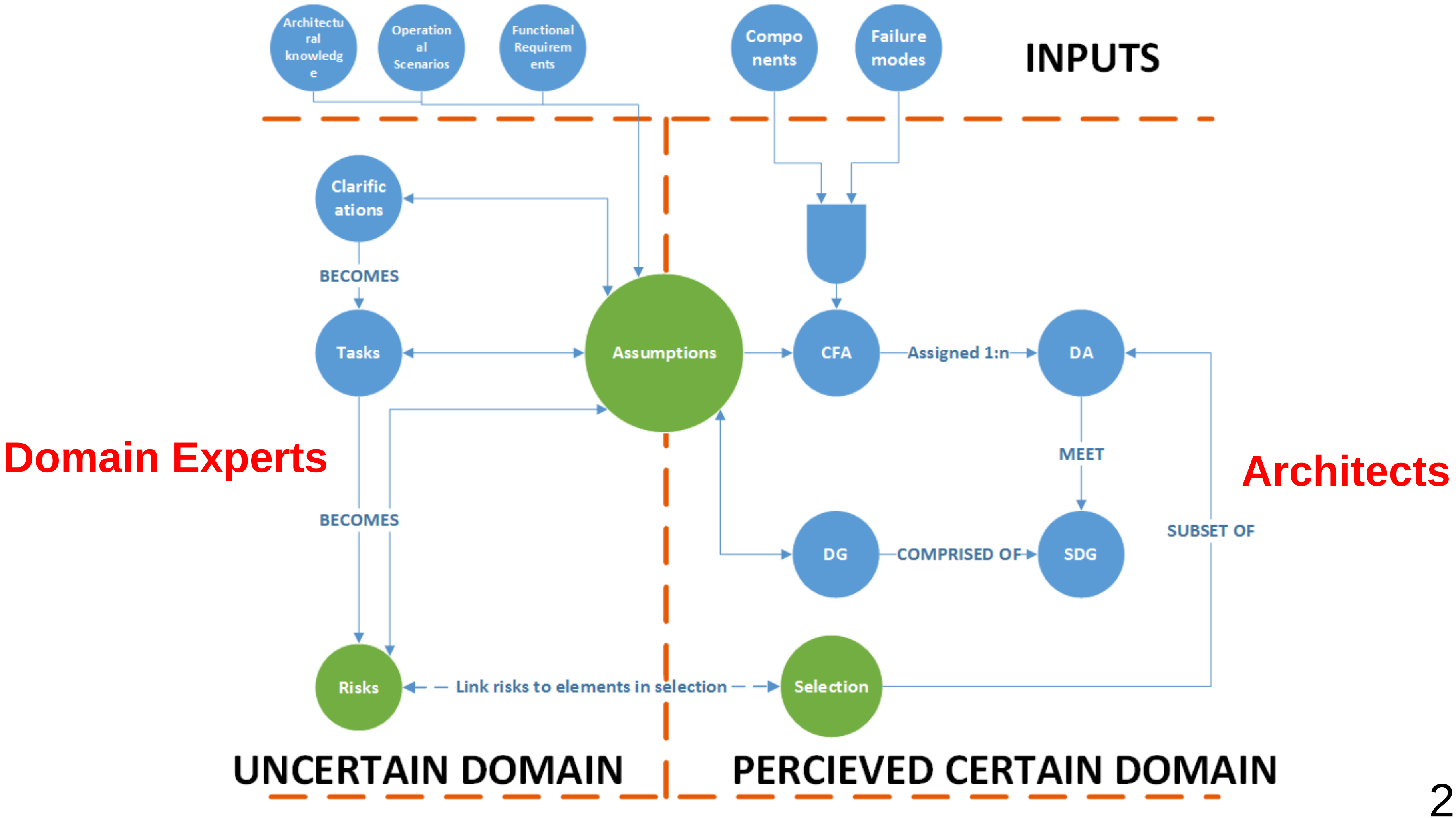
Subsystem 7

# Scope and delimitations

→ ATRIUM ***does not*** guarantee safety;

→ Safety depends highly on usecases and functional requirements.

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



INPUTS

Architectural knowledge

Operational Scenarios

Functional Requirements

Components

Failure modes

Clarifications

BECOMES

Tasks

BECOMES

Risks

Assumptions

CFA

Assigned 1:n

DA

MEET

SDG

SUBSET OF

DG

COMPRISED OF

Link risks to elements in selection

Selection

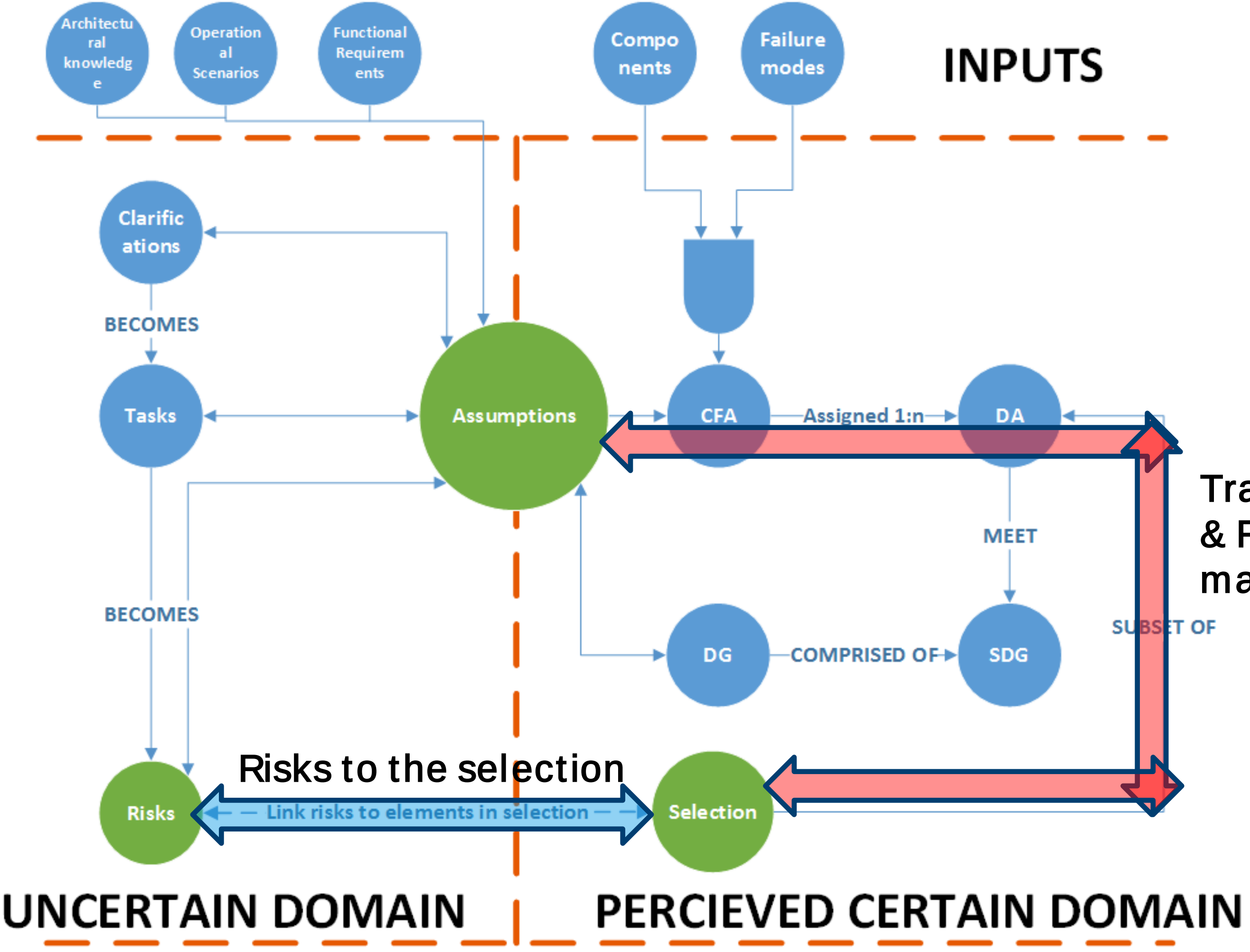
Domain Experts

Architects

UNCERTAIN DOMAIN

PERCIEVED CERTAIN DOMAIN

L3...
L4?



Risks to the selection

Traceability & Rationale management

_

# What are the assumptions we should make?

How smart should your sensors be for safe L5 vehicles?

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

Billion miles of driving?

View on ATRIUM? Practicalities in your domain?

Fuses? Mechanical handovers? Out of scope for safety?

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

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