1. Some excerpts from the EAST-ADL course

Jacques Ehrlich
D'Jet Conseil, Formation, Projet

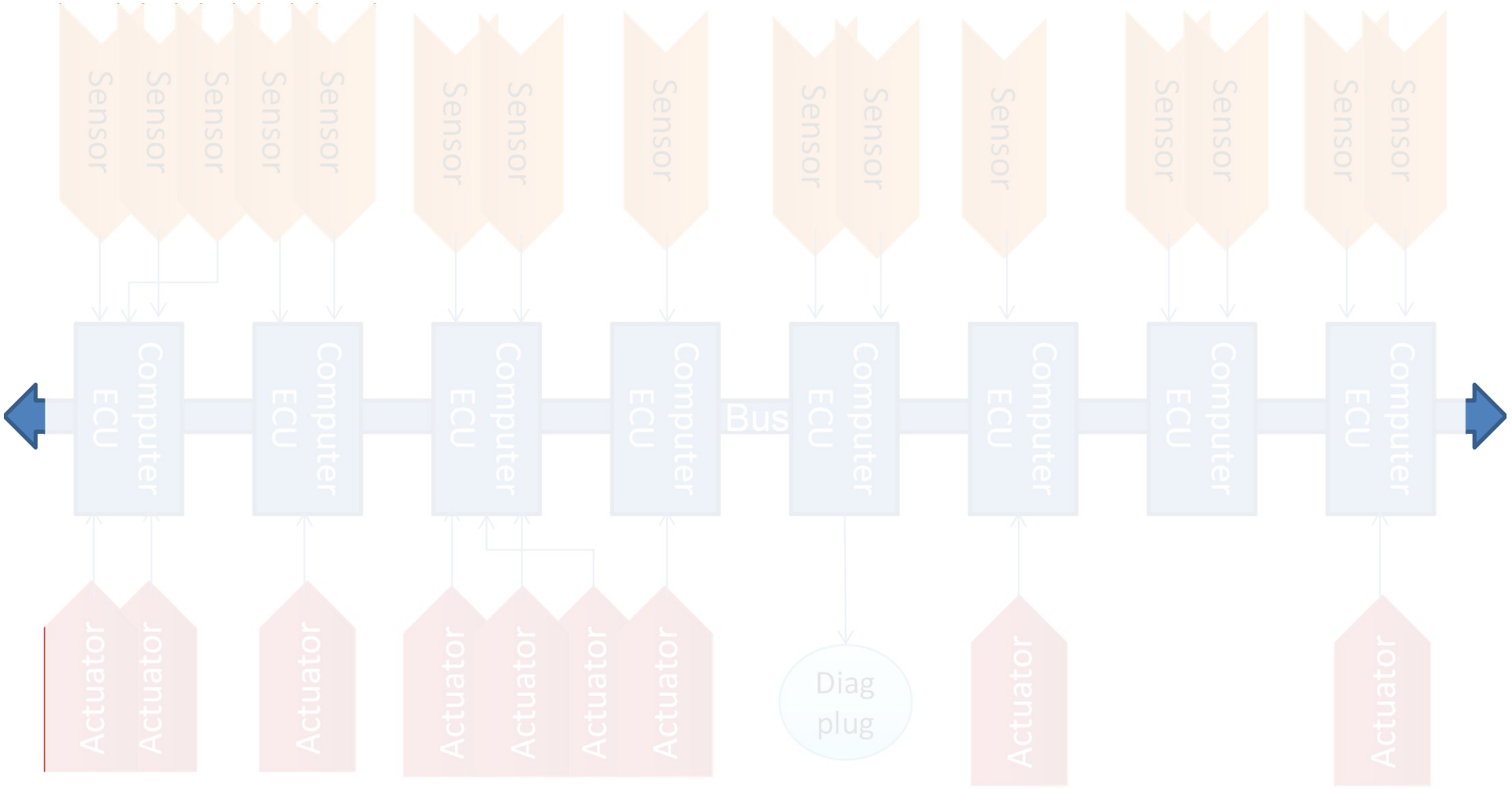
1. Introduction to distributed architecture

Jacques Ehrlich
D'Jet Conseil, Formation, Projet

Solution: multiplexing

- Multiplexing consists in combining several signals into a single connection.
- Multiplexing relies on « bus » (simplified communication networks) which convey digital information form one node (emitter) to several other nodes (receivers)
  - Most popular bus are CAN, LIN, MOST, FLEXRAY
  - Ethernet can also be used as a bus

The present: multiplexed architecture



Less wires, less connection → more reliable
More easy to diagnose, more easy to extend

History of technical developments

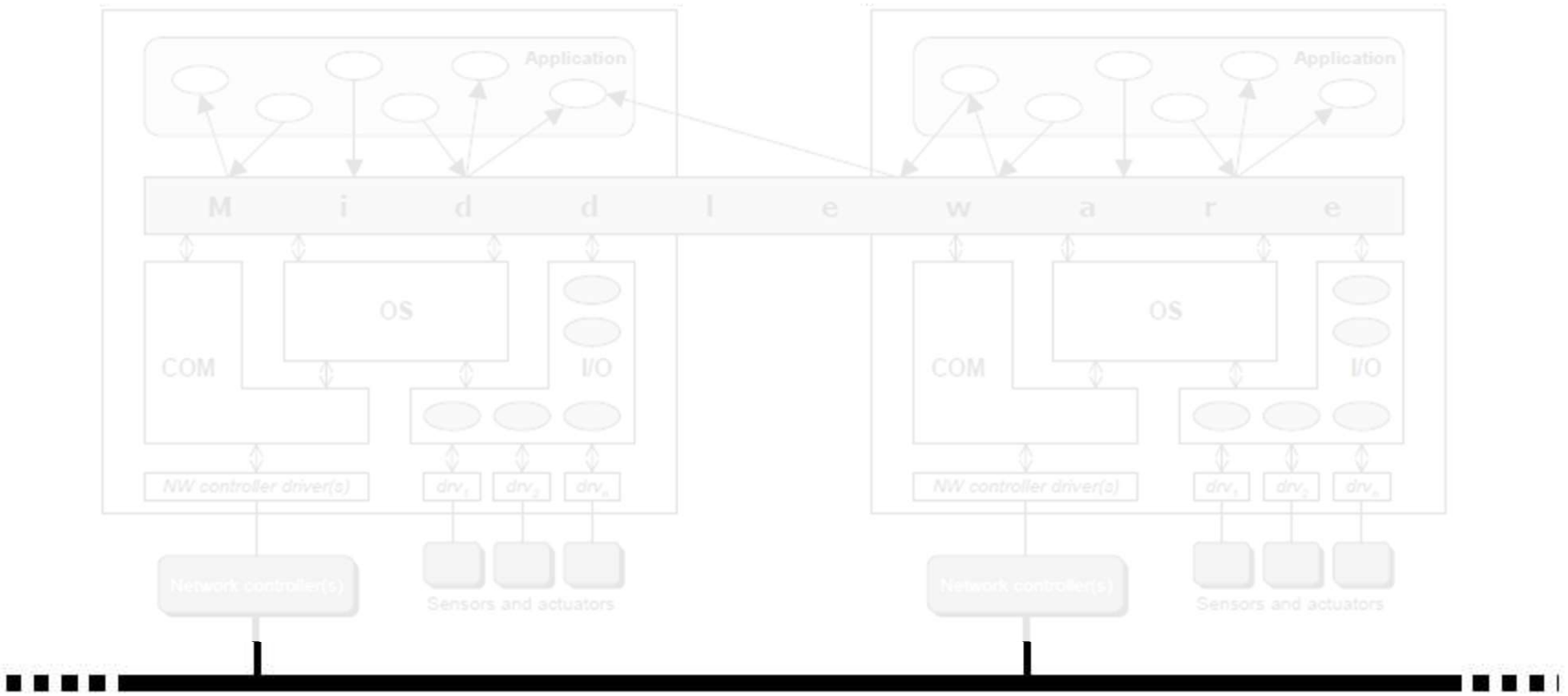
- Before 1960: No electronics
  - For each function a mechanical or electrical link between the command to its execution
- 1970: Independant electronics
  - Electronic sub-systems are independent one from each other. No communication[1] between sub-system
- 1980: First linked electronic system
  - Some sub-systems can communicate with others
- 1990: Widespread communication
  - All sub-system can communicate with each others, but real-time constraints are not always fulfilled
- 200: Real-time communication
  - Real-time constraints are satisfied by the introduction of "time triggered" buses

[1]Note : in this context « communication » refers to data exchange between internal subsystems of the embedded architecture, not with external system like other cars or roadside equipment.

Components of architecture

- Data producers
  - Control (switch, pedal etc) and sensors
    - ✓Examples: throttle pedal, rain sensor, radar
- Data consumer
  - Display devices and actuators
    - ✓Examples : instrument panel, brakes actuator, wiper motor
- Calculator
  - Electronic Control Unit
    - ✓Examples: Freescale, Raspberry Pi, Microautobox
- In-vehicle communication networks
  - Bus CAN, LIN, Flexray, MOST, Ethernet etc.

Middleware



The middleware is an abstraction software layer located between the platform (hardware, OS, protocols) and the applications, allowing first of all to ignore the distribution of tasks, sensors and actuators.
Thanks to the middleware a given task does not need to know where another task, sensor or actuator with which it has to exchange is located.

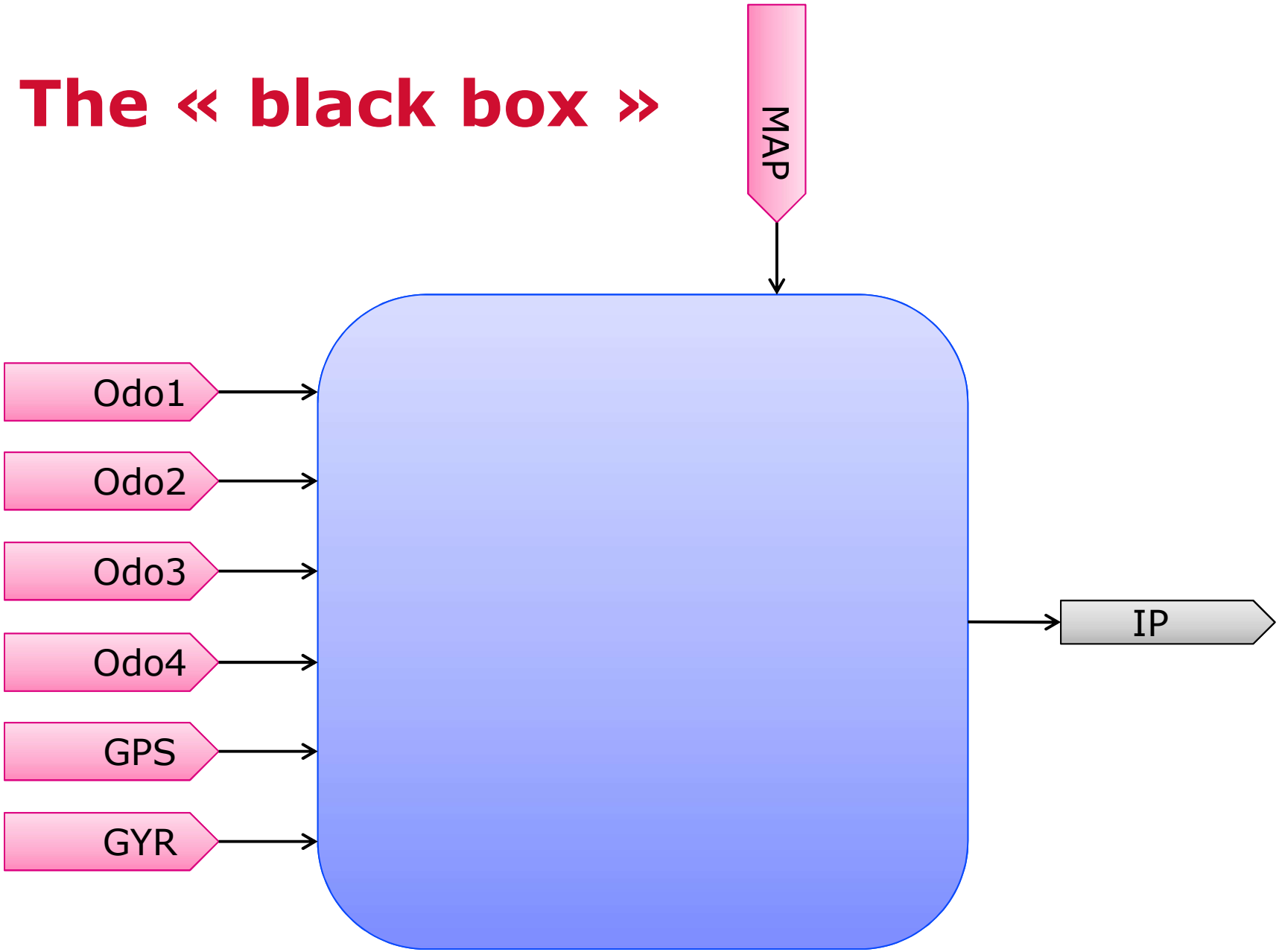
Reducing complexity: decomposition into sub-functions.

- FA1 process is too complex
  - We break it down into two sub-processes SF1, SF2
- SF1 is also too complex
  - We break it down into EF11, EF12, EF13
- As for SF2
  - We break it down into EF21, EF22
- … and so on …
  - Until the complexity is manageable

Exercice: vehicle positionning on the road

- Objective: provide vehicle position on a road
- Sensors (input):
  - four odometers on the four wheels (ODO1 … ODO4)
  - GPS receiver: delivers latitude and longitude (GPS)
  - Gyrometer: delivers yaw rate (GYR)
  - Digital map: provide a digital representation of the road network (MAP)
- Functions
  - F1: Averaging calculation
  - F2: Trajectory estimation (dead reckoning)
  - F3: Map matching
- Output
  - Vehicle position on the instrument panel (IP)
- Work to do
  - Draw a DFG which fulfil the objective

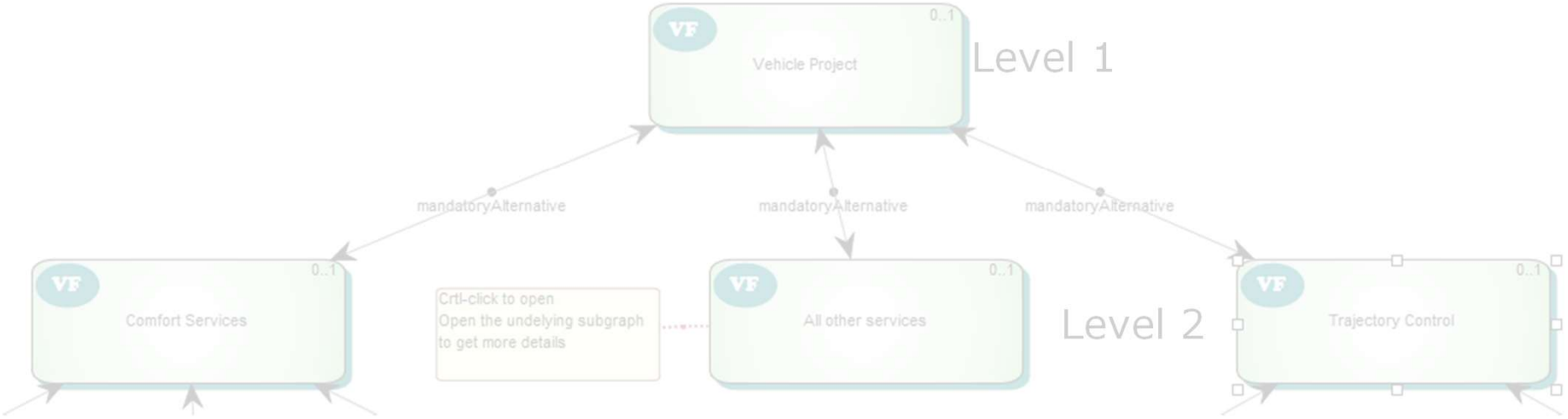
The « black box »



2. Introduction to EAST-ADL

Jacques Ehrlich
D'Jet Conseil, Formation, Projet

Exercice (cont): complete this graph (add level 3 and 4)



Note: It is a simplified view of the top level.
A real vehicle would probably be much more complex

Exercice 5 on FDA

- Complete this FDA so that it delivers a position on a map segment

3. Case study: ISA++

ISA = Intelligent Speed Adaptation

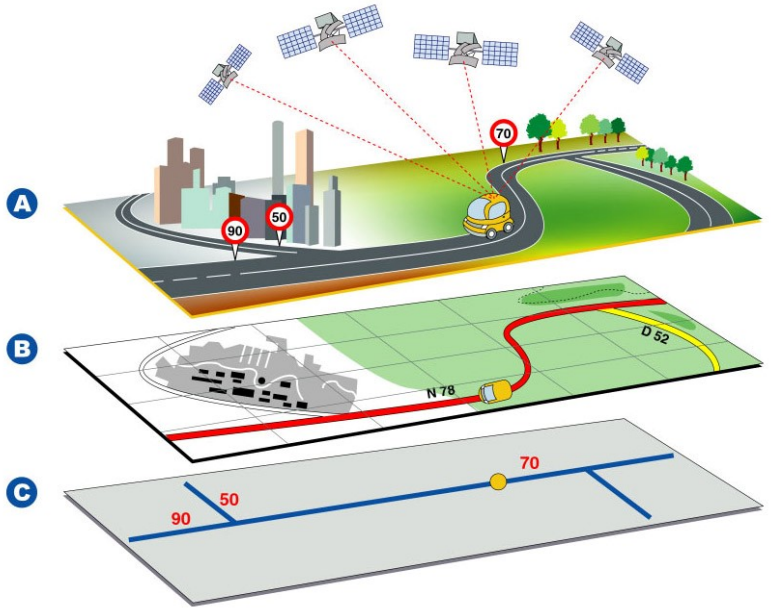
Jacques Ehrlich
D'Jet Conseil, Formation, Projet

Please, avoid falling into the 20/80 trap

- 20% of your energy will be invested to develop features that will be used by 80% of users (and maybe more than 80%...)
  - Marketing people and seller like simplicity
- Unfortunately, you will spend 80% of your energy to develop features that will only be used by 20% of users (and maybe less than 20% ...)
  - Engineers like complexity

Exploring ISA++ in depth

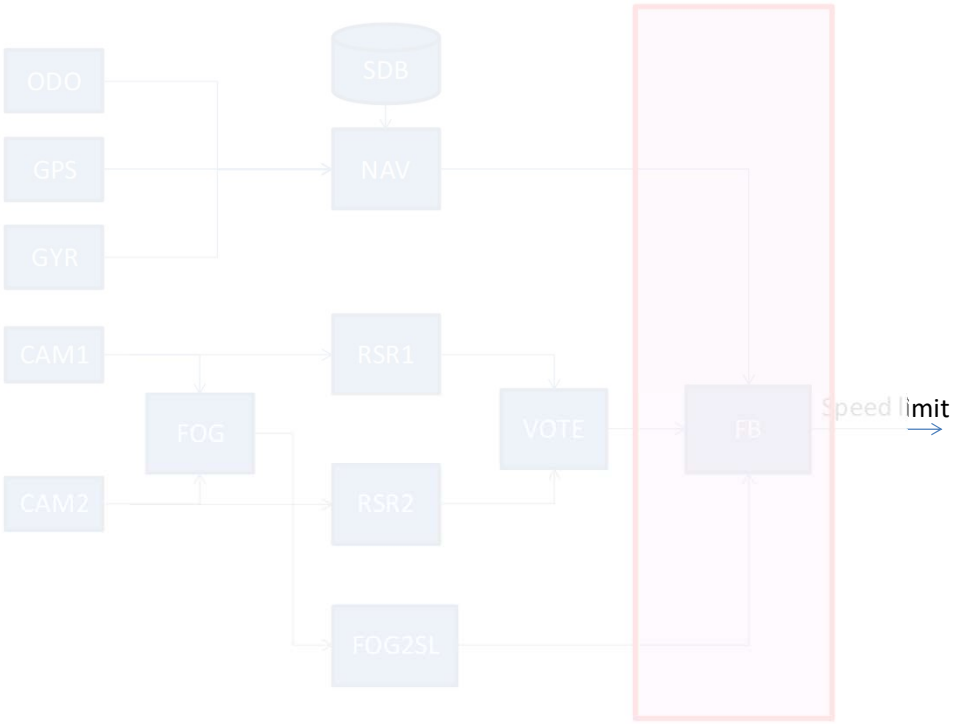
- Location of the vehicle on the road
  - Fusion of GPS, odometer and gyrometer yield absolute vehicle coordinates (fig. a)
  - These coordinates are then entered into a map matching algorithm that allows the vehicle to be positioned on a road segment of a digital map (fig b)
- Getting the speed limit from the speed data base
  - To each road segment is attached the speed limit in force at this location: this is the speed database (fig. c)
  - Thus, knowing the segment number on which you are driving, you can extract the speed limit in force.



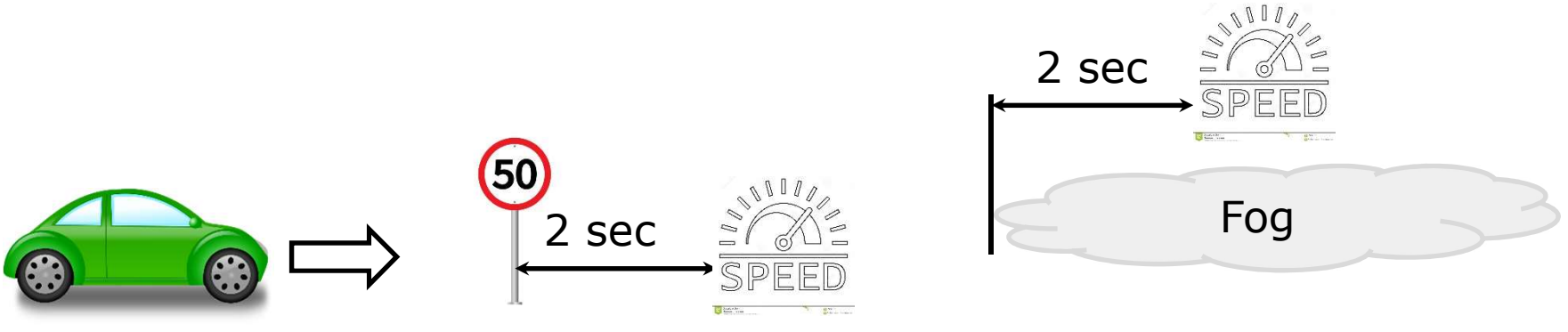
Need for more details ?

Overview of ISA++ functional architecture

- The fusion box
  - It receives three speed limit values coming respectively from the speed data base (digital map), the road sign recognition and the estimated visibility distance in fog.
  - It delivers a speed limit calculated as follows
    - ✓Speed limit from fog prevails if its value is lower than other speed limits
    - ✓Speed limit from road sign recognition prevail on speed limit from data base if confidence indicator is OK



Timing (cont)



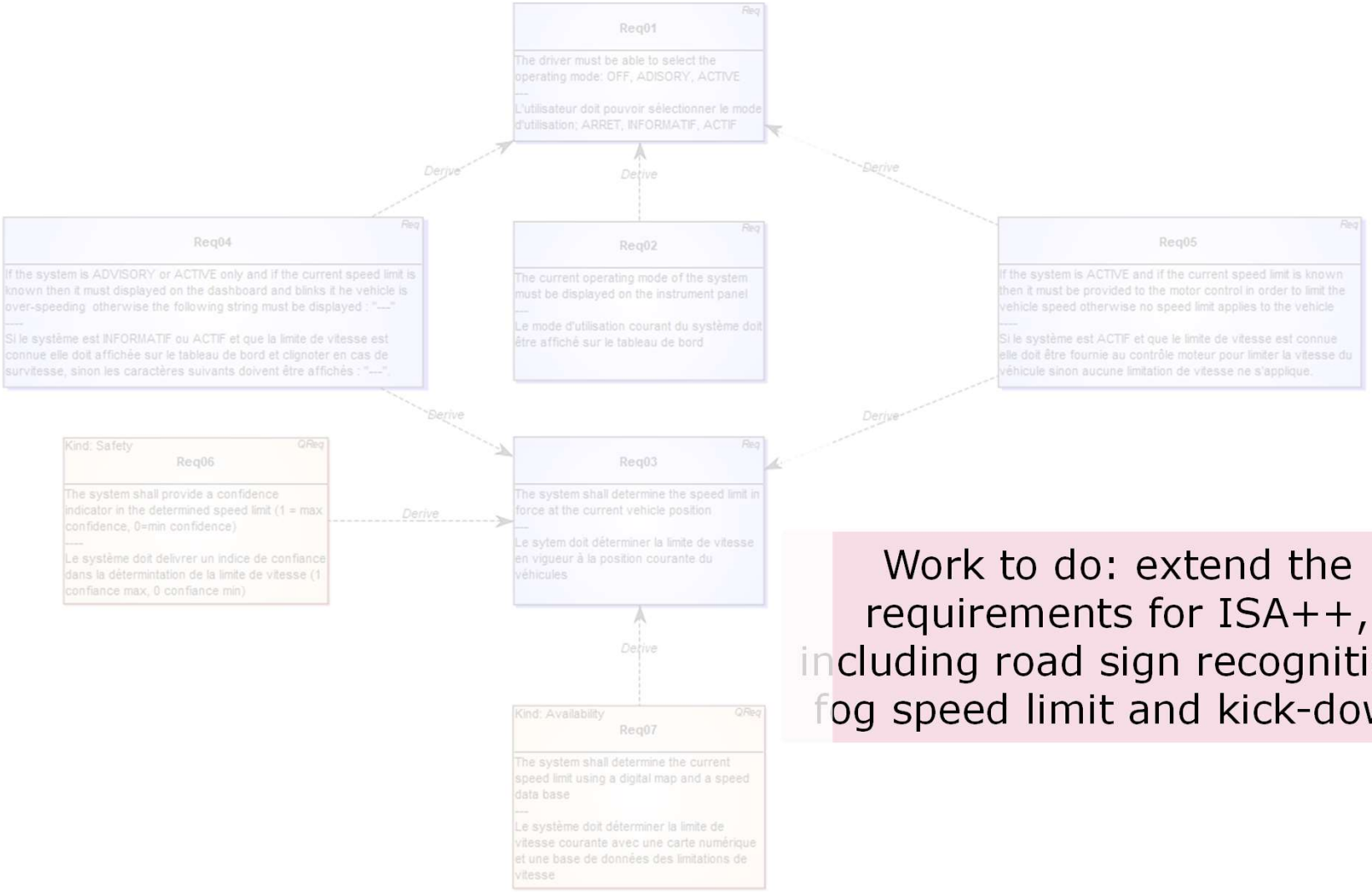
90

RS nr. n

50

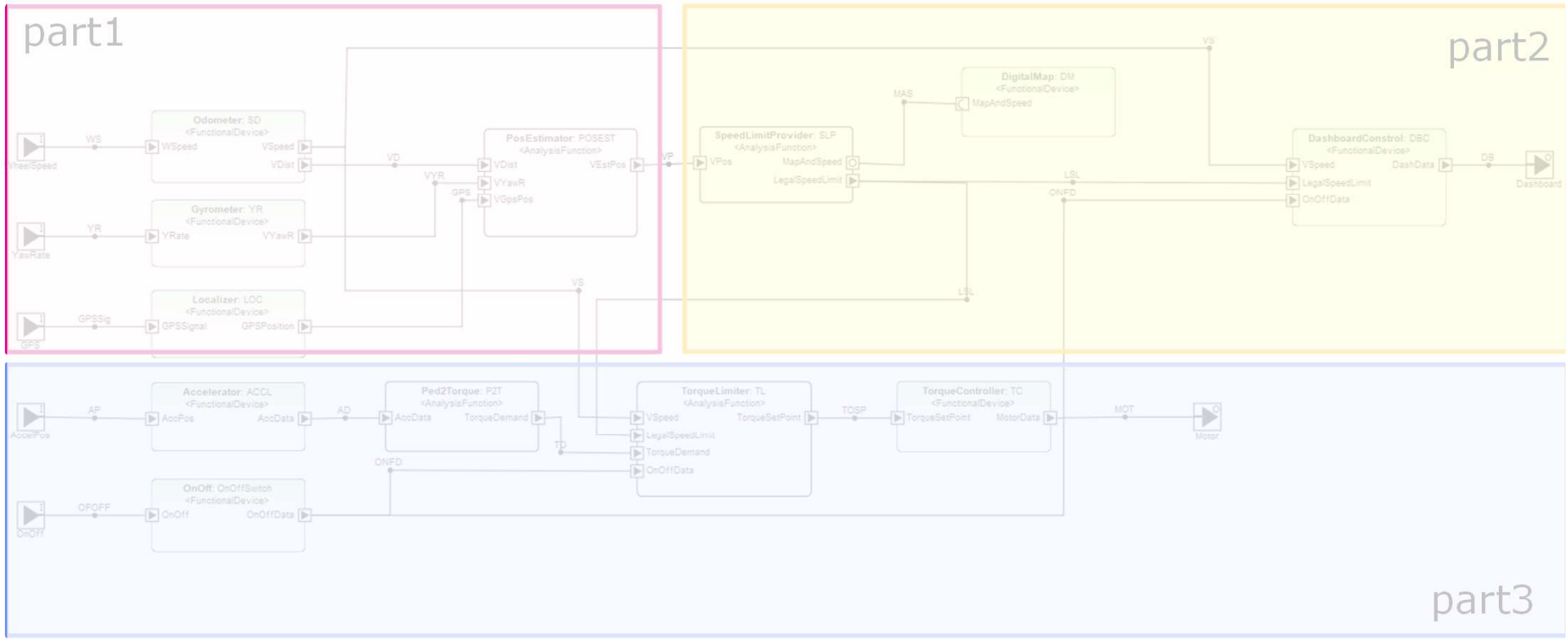
RS nr. N+1

ISA requirement with EAST-ADL



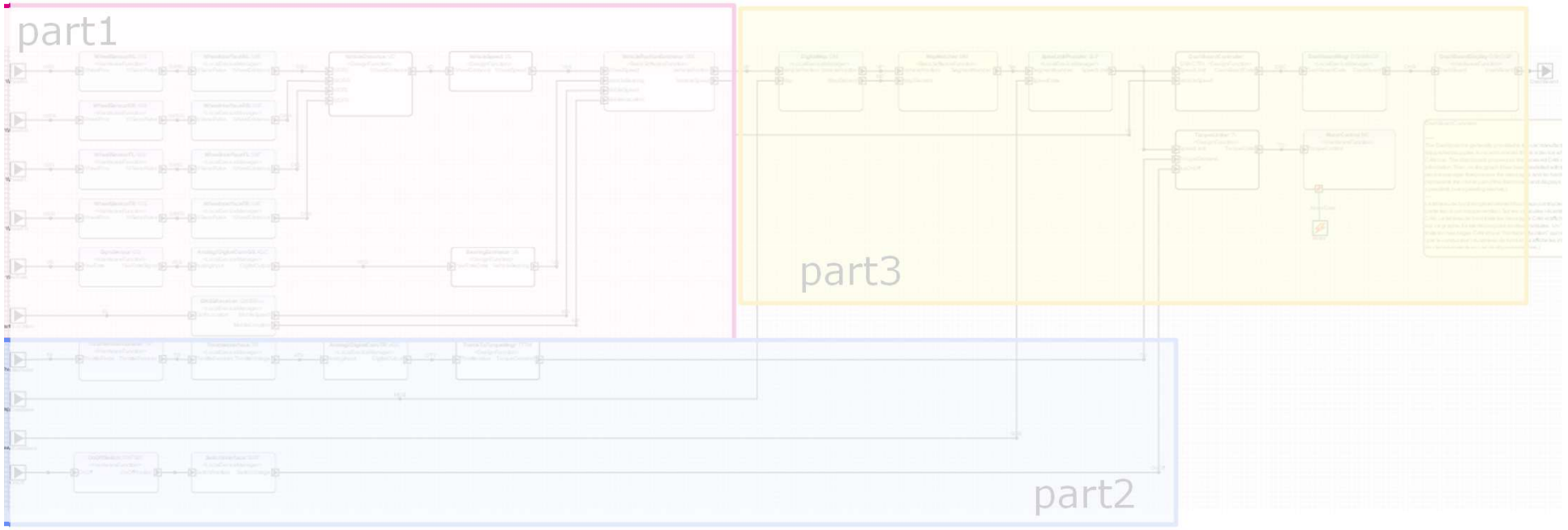
Work to do: extend the requirements for ISA++, including road sign recognition, fog speed limit and kick-down

Exercice on FAA for ISA++



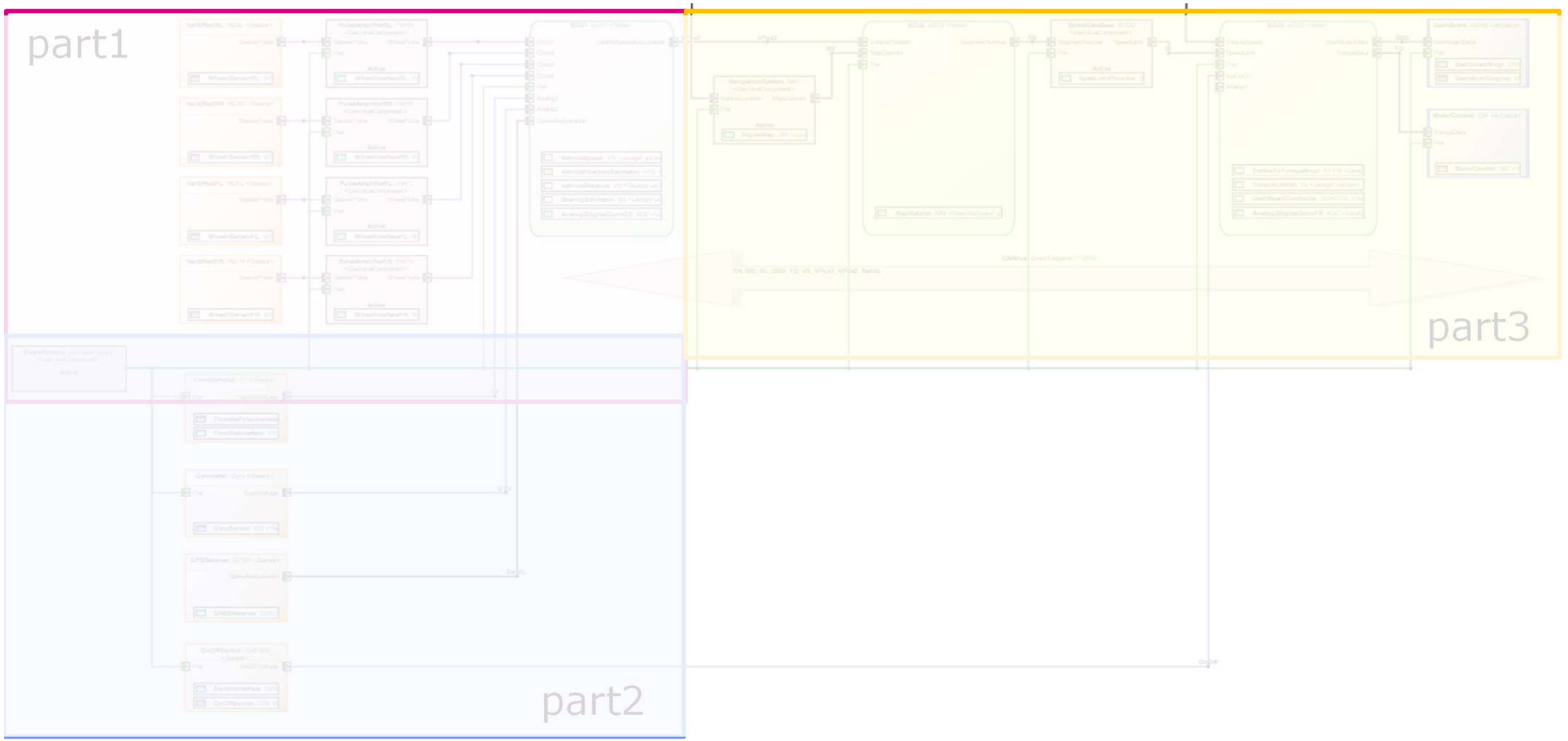
Work to do : extend the FAA for ISA++

Exercice on FDA for ISA++



Work to do : extend the FDA for ISA++

Exercice on HDA for ISA++



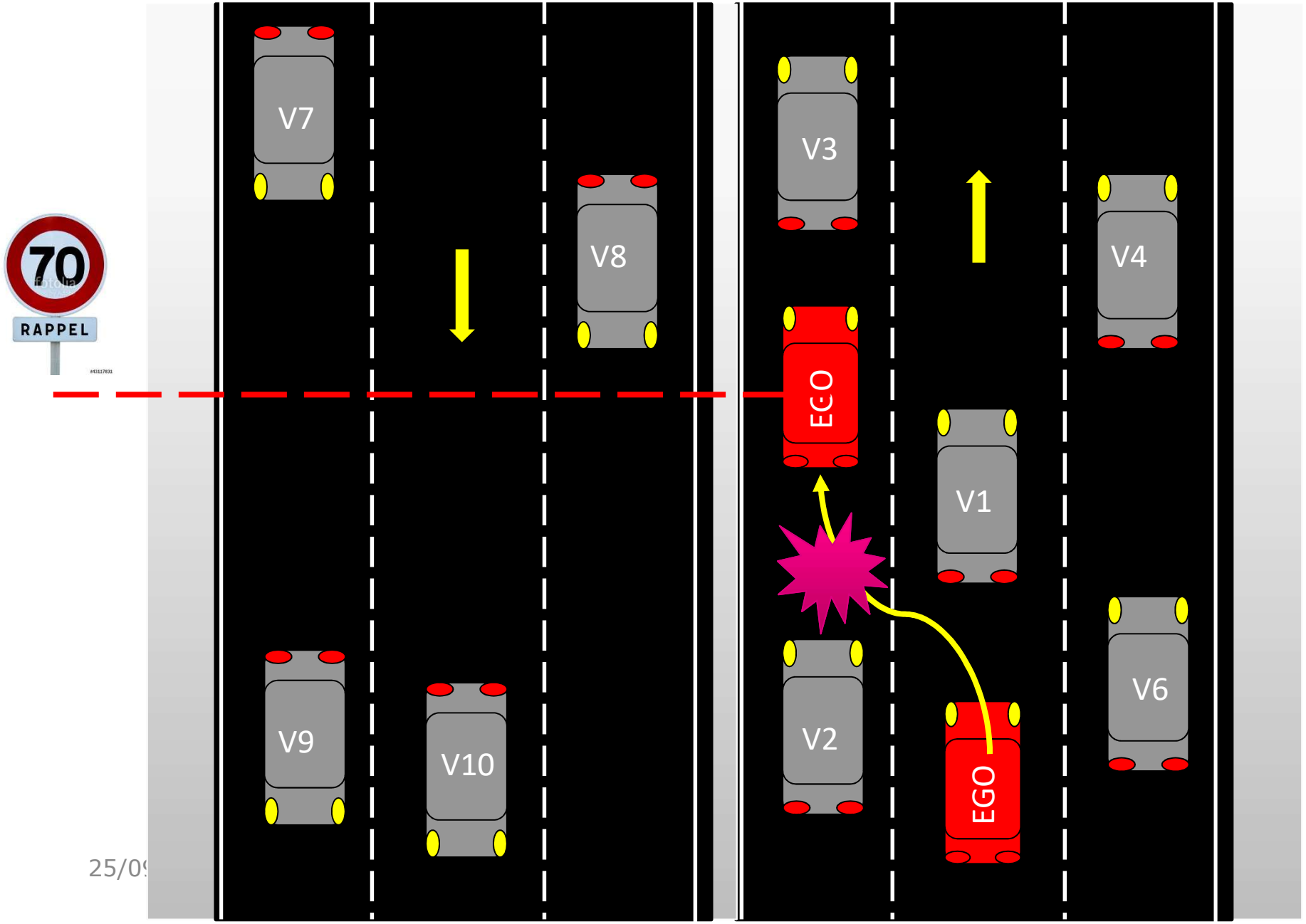
Work to do : extend the HDA for ISA++

4. ISA++ PHA(1), risk and timing consideration

Jacques Ehrlich
D'Jet Conseil, Formation, Projet

(1) Preliminary Hazard Analysis

R3: Dual carriage way while overtaking: rear collision risk



Risk level estimation (ASIL)

- The determination of ASIL is the result of hazard analysis and risk assessment in the context of ISO 26262
  - Each hazard is assessed in terms of severity (S) of possible injuries …
  - within the context how much of the time a vehicle is exposed (E) to the possibility of the hazard happening …
  - as well as the relative likelihood that a typical driver can act to prevent the injury namely the controllability (C).

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Dependency graph for R1

Exercice

- Build a risk analysis for R4: kick-down failure
- Design the dependability model with MetaEdit+

5. Howto …

Jacques Ehrlich
D’Jet Conseil, Formation, Projet

GPS …

- GPS is the simplest way to get the car position
  - It provides a position on the earth surface (not on a road)
- However …
  - GPS may be inaccurate (+/- 5-10 meters)
  - GPS may malfunction due to lost of satellites signals
    - ✓Tunnel
    - ✓Urban canyon
- Then, positioning must rely on many data sources (sensors)
  - Odometer (ODO): provides a measurement of the car displacement (a distance)
  - Gyrometer (GYRO): provides the vehicle yaw rate and the vehicle heading after integration
- Fusion allows to estimate the vehicle trajectory
  - This is called “dead-reckoning”

Map-matching

- Map matching consists in positioning a car on a digital map
  - The current vehicle position is “mapped” on the map internal representation
  - The simplest way to do that is to map the current vehicle position on the neartest road segment