Dependability and Driving Delegation

Gilles LE CALVEZ – ITE VEDECOM Vehicle Program Director

October 18th, 2017
VEDECOM, A unique French Research Hub

Partnering Foundation from Université de Versailles Saint-Quentin-en-Yvelines (UVSQ)

Granted Institut pour la Transition Énergétique in 2014 French National Research Agency (ANR)

Set up in the frame of the Programme d’Investissements d’Avenir

VEDECOM is a major contributor to « Plan Véhicule Autonome » of Nouvelle France Industrielle (NFI)
Number of employees: 175 (more than 110 researchers including 45 PhD students)
2017 Budget: k€ 31,150 (subsidies: k€ 15,800 ANR+CD78)
Capital assets: k€ 9,100 (end 2016/material and immaterial)
Large and diversified ecosystem
## MAIN ACHIEVEMENTS

### Current assets

**2014:** 1 M€  
**2015:** 7,2 M€  
**2016:** 5,1 M€

<table>
<thead>
<tr>
<th>Workshops</th>
<th>Infrastructure</th>
<th>Rolling platforms</th>
<th>IT Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Electric motor prototyping</td>
<td>• Road equipped with connectivity features (G5 – LTE 5G)</td>
<td>• Platforms devoted to perception and data collection</td>
<td>• Automated driving simulator</td>
</tr>
<tr>
<td>• Power electronics reliability testing</td>
<td>• Smart grid configuration (Mako, H2 station, 10 bikes)</td>
<td>• Self-driving and connected platforms</td>
<td>• Mobility simulator</td>
</tr>
<tr>
<td>• Power electronics (1st stage)</td>
<td>• Dynamic and inductive charging track (FABRIC)</td>
<td>• « Wizard of Oz » vehicle to analyze user interface and self-driving vehicle use</td>
<td></td>
</tr>
</tbody>
</table>

- Infrastructure
- Rolling platforms
- IT Platforms
VEHICLE ELECTRIFICATION

Improve urban air quality by a dramatic greenhouse gas emissions reduction

Breakthrough
- Total cost of ownership
  - Powertrain cost
  - Energy storage cost
- No limit range
  - Fast charging
  - Dynamic charging
  - Shared network connection

Innovative electric motor prototyping and reliability testing

Fast and/or dynamic charging

Smart grid
SELF-DRIVING AND CONNECTIVITY

Boost the emergence of the levels 4 and 5 applications to propose safer and more efficient mobility solutions (increase free time) :
Level 4 for passenger cars – Level 5 for “robot-taxis”

Breakthrough
- Technologies (sensors-IA-ECU, etc...)
  - Operational safety => SOTIF
  - Human factors compatibility
  - Connectivity : 5G and/or G5
  - Infrastructure
- Societal acceptance
  - Responsibility / Liability
  - Law and regulation
  - Insurance
  - Ethics
Optimize future mobility services systems based on carbon-free, connected and self-driving vehicles

Breakthrough
- Shared energy
- New sustainable use
- Shared mobility
- Multimodal trips
- “Car-sharing”
- “Carpooling”
- Cooperation with local authorities according to the “smart cities” project for mobility

Societal trends & Mobility local assessment
Let’s see what we are talking about ...

- JUNE 2017
- ITS Strasbourg

From Strasbourg (F) ...

To Kehl (G) ...

And Back!
DIFFERENT LEVELS OF DRIVING DELEGATION

Levels of Automated Driving

- **Level 0 (Driver Only)**: No intervening vehicle system active.
- **Level 1 (Assisted)**: The other driving task is performed by the system.
- **Level 2 (Partial Automation)**: System performs the longitudinal and lateral driving task in a defined use case.
- **Level 3 (Conditional Automation)**: System performs the lateral and longitudinal dynamic driving task in all situations in a defined use case. Recognizes its performance limits and requests driver to resume the dynamic driving task with sufficient time margin.
- **Level 4 (High Automation)**: System performs the lateral and longitudinal dynamic driving task in all situations encountered during the entire journey. No driver required.
- **Level 5 (Full Automation)**: System performs the longitudinal and lateral dynamic driving task and the driving environment at all times; must always be in a position to resume control.

Driver continuously performs the longitudinal and lateral dynamic driving task.

Driver continuously performs the longitudinal or lateral dynamic driving task.

Driver must monitor the dynamic driving task and the driving environment at all times.

Driver does not need to monitor the dynamic driving task nor the driving environment at all times; must always be in a position to resume control.

System performs the lateral and longitudinal dynamic driving task in all situations in a defined use case.
An Autonomous Vehicle is ...A VEHICLE !

Standards from Automotive apply to Autonomous Vehicle

- Hardware based requirements (Electronic and Mechanical Components)
  - FMEA / Reliability Testing ...

- Software based requirements (Functional / Safety)
  - ISO 26262 with ASIL definition (Automotive Safety Integrity Levels)

- Back-up modes (Limp Home / degraded modes ...)

Is this enough ? ...
An Autonomous Vehicle is ...AUTONOMOUS!

- METRO
- AERONAUTICS

Let’s not reinvent everything ...
## Safety principles

<table>
<thead>
<tr>
<th>Principles</th>
<th>Technical Domain</th>
<th>Positive Point for AV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ALARP</strong></td>
<td>Applied every safety measure that reduce risk, in a reasonable financial scope</td>
<td>Nuclear</td>
</tr>
<tr>
<td><strong>AFAP</strong></td>
<td>Reduce all risks whatever their importance</td>
<td>Medical</td>
</tr>
<tr>
<td><strong>MEM</strong></td>
<td>Calculation of the acceptable risk level based on an independent safety objective</td>
<td>(Transportation)</td>
</tr>
<tr>
<td><strong>GAME</strong></td>
<td>The new system must demonstrate a similar or lower risk than its predecessor</td>
<td>Railway Aeronautics</td>
</tr>
</tbody>
</table>
THE DRIVING DELEGATION relies on multiple factors:

- PERCEPTION / LOCALIZATION

NO SINGLE POINT OF FAILURE

→ REDUNDANCY IS MANDATORY
(CAMERA / LIDAR / RADAR ... GPS / INERTIAL UNIT ... CONNECTIVITY)
THE DRIVING DELEGATION relies on multiple factors:

- PERCEPTION / LOCALIZATION

- DECISION
DEPENDABILITY AND SAFE BEHAVIOUR

MOOVE
Véhicules équipés et
Big data

Risk situations

Statistics for the UE Safety

Safe Functional Architecture

Mobility

Simulation Tools

Data and representative scenarios for the uses-cases

Dimensioning Parameters of the infrastruture

Dimensioning Parameters of the climatic environment

Performances of the technologie and bricks of perception

Algo. For Perception and Fusion

Behaviour of mobile Objects around the ego-Véhicule

Algorithms for Planification

Risky situations

18/10/2017
SETTING UP FUNCTIONAL RULES : (under definition)

- Consider a set of critical situations from a safety point of view
  (library of scenarios and identified situations)
- « Refuge locations » must always be identified, in case driver does not take over

- **Standard Criteria** for assertion :
  - Manual control take-over time
  - Driver Monitoring
  - Alerts
  - Activation / De-Activation / Take-over

- **Continuous Analysis process** for Incidents and Failures in action
A QUANTITATIVE APPROACH

THE REFERENCE IS SET UP :

- **Database** of Accidentology

<table>
<thead>
<tr>
<th>Probabilities</th>
<th>France « LAB » « VCN » VE</th>
<th>France « Highway » VE</th>
<th>Germany « Pegasus » « Highway »</th>
<th>« Average »</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Fatalities</td>
<td>3,04. 10^{-8}/h</td>
<td>10^{-7}/h</td>
<td>1,5. 10^{-7}/h</td>
<td>1.10^{-7}/h</td>
</tr>
<tr>
<td>S2 Wounded</td>
<td>1,52. 10^{-7}/h</td>
<td>3. 10^{-7}/h</td>
<td>1,88. 10^{-6}/h</td>
<td>7,8. 10^{-7}/h</td>
</tr>
<tr>
<td>S1 Lightly Wounded</td>
<td>3,42. 10^{-7}/h</td>
<td>2,5. 10^{-6}/h</td>
<td>8. 10^{-6}/h</td>
<td>3,6.10^{-6}/h</td>
</tr>
</tbody>
</table>

- **Improvement Factor** is defined : 10 (btw : 90% of accidents are caused by Human Factor)

- **Allocate the SAFETY Goals** per Sub-system / Organ (Objectives of Failures)

Consider Both ISO 26262 (known) and SOTIF (Objective Proven In Use)
### PUTTING THIS IN ACTION ...

<table>
<thead>
<tr>
<th>Cut-In</th>
<th>scenography/animation</th>
<th>scene (initial)</th>
<th>event</th>
<th>action</th>
<th>scene (final)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut in in front of ego vehicle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lanes separated by median strip</td>
<td>Ego vehicle is on its lane</td>
<td>Vh1切入在ego车道前</td>
<td>Vh1 is the new target of the ego</td>
<td>For ego vehicle follows its target</td>
<td></td>
</tr>
</tbody>
</table>

### SCENARIO LIBRARY

**REAL-LIFE MEASURE**

**MODELING**

**SIMULATION**

**TESTING / HOMOLOGATION**
DEPENDABILITY OF THE AUTONOMOUS VEHICLE RELIES ON:

- **STANDARD PROCESS FROM AUTOMOTIVE + EXPERIMENTS**

- **BASICS FROM OTHER TECHNICAL DOMAINS**

- **LEADS TO ADDRESS ALSO SECURITY**
  
  (Connectivity → Cyber-security)

- **NEW FIELDS (TAKE-OVER / CHANGING ENVIRONMENT / MIXITY ...)**

A CONTINUOUS PROCESS THAT IS ONLY BEGINNING ...
Thank you for your attention

Together to accelerate the mobility of tomorrow!