French automotive industry Safety Argumentation for automated vehicle SAE level of automation 3 and 4

« Position paper » describes French automotive industry opinion (WG « Safety » from PFA)

- RSA, Valeo, PSA, SystemX, Vedecom
- Dedicated to « safety argumentation » for automated vehicle

The Safety Of The Intended Functionality (SOTIF)
ISO/PAS 21448

The automated driving system is safe

Other safety requirements (incl Cybersecurity, passive safety, etc)

Its failures are adequately avoided or mitigated

ISO26262 : Functional Safety
Hazard Analysis and Risk Assessment
Design, Verification and Validation (V&V) requirements
Safety management

Its behaviour is adequate for the intended operation domain

ISO/PAS 21448 : Safety of the Intended Functionality
Scenario identification incl. Reasonably foreseeable misuses
Functional improvements
V&V strategy

Scope of ISO/TC22/SC32/WG8

Its behaviour is adequate for the intended operation domain

The vehicle functionality is safe

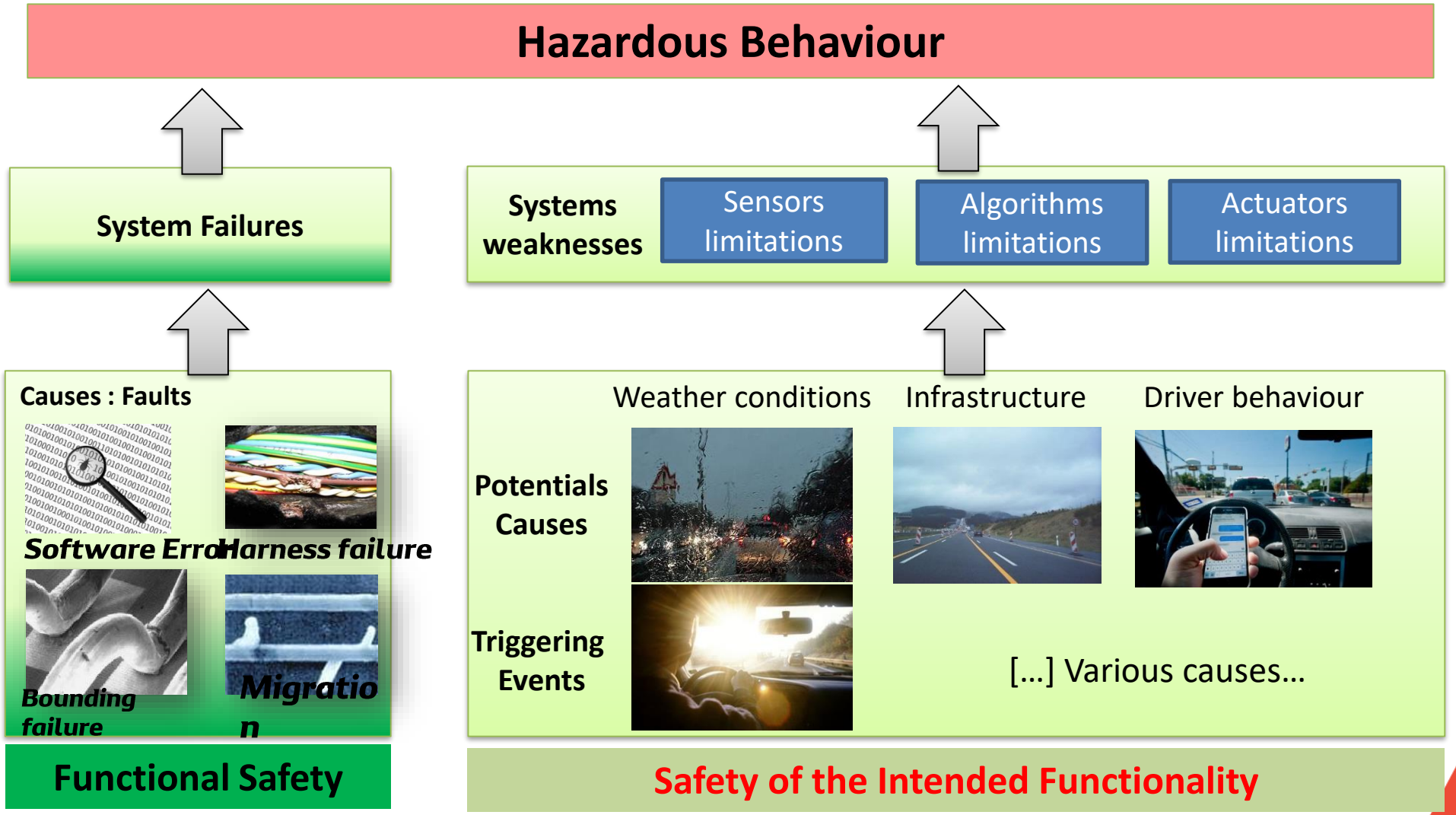
The function expected behaviour is complete and safe
Potential misuses are identified and mitigated

Its technical implementation is safe

The system performance limitation are identified and acceptable
-sensors and environment perception
-decision algorithms
-actuation

Scope of ISO 21448

Causes of hazardous behaviour



SAFETY ARGUMENTATION FOR AUTOMATED VEHICLE
SAE LEVEL OF AUTOMATION 3 AND 4 : SAFETY CONTEXT

- "Potentially hazardous behavior, in absence of failure": SOTIF

- French automotive industry opinion regarding "SOTIF issues" is that:

- Automated Vehicle development shall comply with ISO/PAS21448
- Some guidelines could be useful to apply ISO/PAS21448, concerning:
  - specification of the ISO/PAS21448 requested "acceptance criteria"
  - high level safety-related guidelines

The following elements describe these guidelines

Safety Argumentation for automated vehicle SAE level of automation 3 and 4

1. **"Automated Vehicle deployment shall improve the road safety"**
   - This overall intention helps to define the ISO/PAS21448 requested SOTIF acceptance criteria.
2. **"The automated vehicle is free from unreasonable risk"**
   - **Qualitative safety principles**
     - The vehicle shall comply with a set of **high-level safety rules** contributing to safety, whether or not their safety impact can be quantitatively assessed,
     - Design and verification/validation phases shall take into account relevant driving scenarios, including relevant misuses.
   - **Quantitative approach: SOTIF acceptance criteria**
     - ISO/PAS21448 request "acceptance criteria" to be defined.
     - Our "acceptance criteria" is a **validation stop quantitative criteria**,
   - **Field experience**
     - **Field experience** shall be taken into account to continuously improve vehicle safety.
     - Lessons learned from the field should be **shared** as far as possible.

EXAMPLES OF QUALITATIVE SAFETY PRINCIPLES

T-01	A single perception malfunction without failure should not induce a hazardous event. Consequently, the set of sensors used for the perception of a safety relevant environmental feature shall not be based on a single physical principle.
ODD-01	The vehicle shall not be in AD mode out of its ODD.
DRV-01	The vehicle shall manage risks according to the following rules: ○ Vehicle shall not create accident by its own ○ Vehicle shall be robust, as far as reasonably possible, to risks caused by others ○ Vehicle shall comply with applicable driving rules (including those applicable to human drivers) unless it is the only way to avoid an accident This rule shall be fulfilled: ○ wherever the vehicle is driving (e.g. country, road, …) ○ whenever the vehicle is driving (e.g. despite dynamic lane assignment; time dependent rule, introduction of a new type of traffic sign; rule change …)
TR-01	A deliberate driver action is required to activate AD mode.
SC-01	The OEMs shall set up a common process to create and maintain a common catalog (*) of scenario, including misuses, to be used for safety argumentation during design and verification/validation phases (**).

(*) the catalog will be enriched continuously
(**) in compliance with laws (e.g. competitive laws)

QUANTITATIVE APPROACH – SOTIF ACCEPTANCE CRITERIA

This “validation acceptance criteria”

- **ensure that the safety demonstration and its validation have a sufficient coverage.**
- **ensure that the introduction of a highly automated vehicle on highways will not increase the risk level,**
- **is not the admission of a permissible level of accidents in the field: any credible safety-related scenario must be mitigated, including those appearing after vehicle start of sale.**

FIELD EXPERIENCE - Market Feedback & After sales

The following rules concern after sale process to be setup **in order to continuously increase the safety level of the automated vehicle**

AS-01	The OEM shall set up internally, a process to collect, analyze and treat incidents/accidents faced by the customers, and if necessary, update the vehicles.
AS-02	The OEMs shall share the lessons learnt from field experience, including safety-related events occurring in real life vehicle use, in order to enrich a common scenario catalog.

Note: this common scenario catalog has to be set up and managed

PFA « Position Paper »
Safety argumentation for automated vehicle

"Potentially hazardous behavior, in absence of failure" is the main challenge: **SOTIF is the key point**

French automotive industry opinion is:

- Automated Vehicle development shall comply with ISO/PAS 21448.
- ISO/PAS21448 application shall include:
  - **A quantitative "acceptance criteria (e.g. validation target)"** for relevant ODD,
    - In a first step, French accidentology data on highways has been considered
  - **A common set of qualitative safety principles** (technical rules, ODD, AD mode, transitions to/from AD mode, MRM),
  - **A shared catalog of scenarios** to be used for Design & V&V phases, including reasonably foreseeable misuses and so **a common process to create and maintain** this catalog**,**
  - **An AV-oriented field monitoring process** (market feedback and after-sales) and a lessons learnt sharing process, in order to continuously increase the safety level of the automated vehicle.

Thank you
Merci

Emmanuel ARNOUX

ADS Validation Expert – Renault Testing Division
ADS Validation WG Pilot – PFA
France

Emmanuel Arnoux, PhD and engineer from Ecole Centrale de Lyon began his career at University of Lyon for Renault on mechatronic suspension systems. He then joined Renault Chassis and ADAS research team in 2003, and led this team from 2007 to 2013. Then he joined the AD and ADAS design department where he was assigned Chassis and ADS Simulation Expert in 2015. Since 2019, he integrated Renault Vehicle Testing Division as Chassis and ADS Validation and Testing Expert. Emmanuel Arnoux is also Pilot of a working group on ADS Validation for the PFA (French Automotive Platform).