

GIANCARLO SCAPPATURA

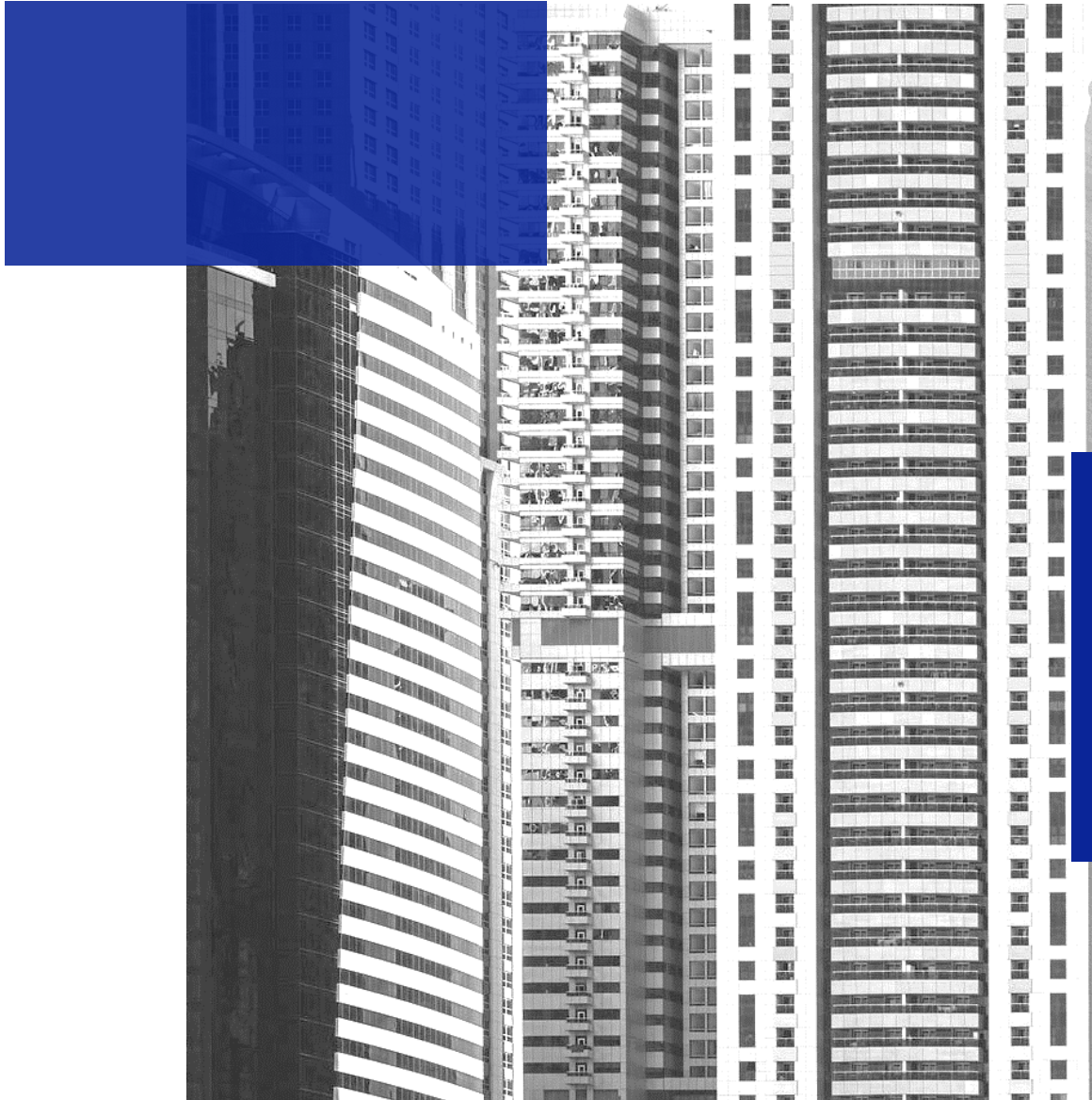
AUTOMOTIVE AI: CHALLENGES, RISKS AND STANDARDS

Bologna - 21st May 2026

OBJECTIVES

THIS PRESENTATION WILL PROVIDE AN OVERVIEW OF HOW THE AUTOMOTIVE SECTOR CURRENTLY ADDRESSES THE TOPIC OF ARTIFICIAL INTELLIGENCE.

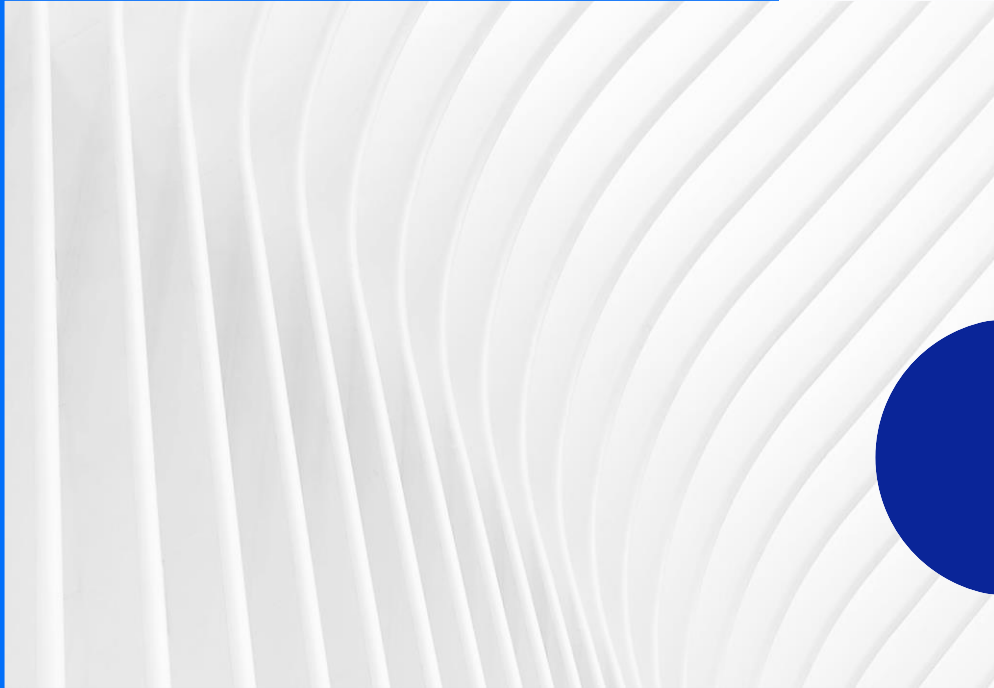




AGENDA

- INTRODUCTION
- AI IN AUTOMOTIVE
- AI STANDARDS
- CONCLUSIONS

INTRO



AI and **ML**: Why are they central to the automotive industry?

- Vehicles are increasingly: **autonomous**, **connected**, and **software-oriented** (software-defined vehicle).
- AI introduces new features but also brings with it **new complexity**.
- The challenge for manufacturers is to innovate while maintaining **reliability** and **safety**.



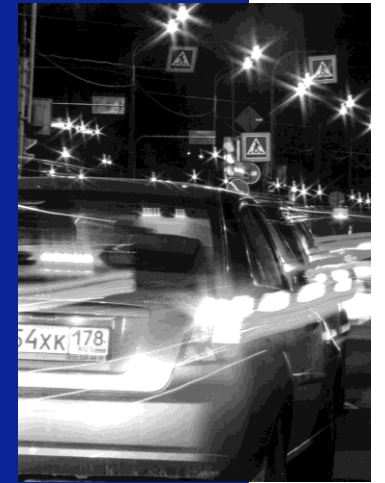
AI IN AUTOMOTIVE



AI IN AUTOMOTIVE

Systems that learn from data rather than being explicitly programmed.

Compared to traditional **deterministic SW**, **AI is not deterministic** and this is the main difference that is highlighted today.



EXAMPLES

Area	Examples AI usage	AI Techniques used
ADAS	<ul style="list-style-type: none">• Lane Keeping• AEB• adaptive cruise control• automatic parking	<ul style="list-style-type: none">• Computer vision• Object detection• Sensor fusion
Autonomous Driving	<ul style="list-style-type: none">• Environment perception• path planning• Robotaxi	<ul style="list-style-type: none">• Deep learning• Behavior prediction
Driver Monitoring System (DMS)	<ul style="list-style-type: none">• Drowsiness detection• Distraction monitoring	<ul style="list-style-type: none">• Face tracking• Eye tracking
Connected Vehicles	<ul style="list-style-type: none">• Intelligent routing• Personalized infotainment	<ul style="list-style-type: none">• Predictive analysis• Federated learning
Digital Twin	<ul style="list-style-type: none">• Virtual simulation of vehicle and components	<ul style="list-style-type: none">• Simulation and generative AI

AI RISKS

AI systems introduce significant **safety risks** when **trained** or validated with **low-quality, incomplete, or biased data**.

Key risks include **non-deterministic behavior**, difficulty handling rare or unexpected **edge cases, data bias** that may lead to unsafe decisions, and limited explainability of “black-box” models.

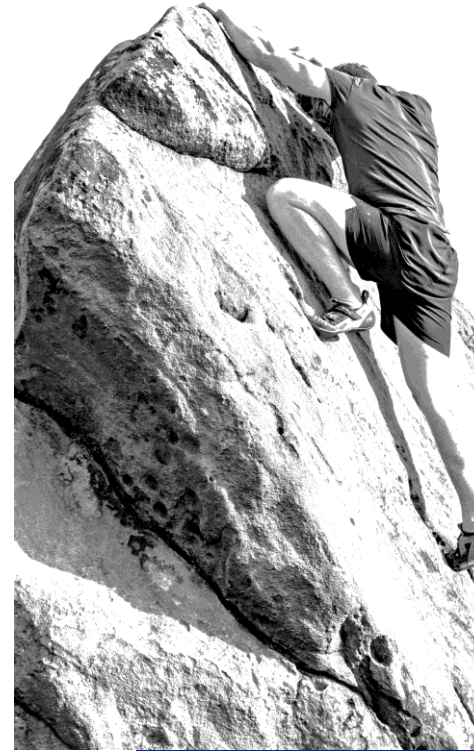
These factors make verification, validation, and compliance with safety standards more complex, especially in safety-critical automotive applications.



CHALLENGES

AI is already implemented, but it's not in its complete and optimized form; it still needs to be enhanced.

The **main challenge** of AI in automotive is ensuring **safety**, reliability, and **standards compliance** in complex real-world conditions.



AI STANDARDS



AI: 4-LEVEL STRUCTURE

In the Automotive, currently there is no single AI standard.

Instead, there is a four-tier structure:

- **Approval laws** (UNECE R155/R156...), they are **mandatory** laws
- **Technical standards** (ISO 26262, 21434...) with **voluntary** application
- **AI Act UE** establishing **high-risk AI governance** (The riskier AI, the safer it must be). It adds to other standards such as approval laws or technical standards to ensure that AI is safe.
- **Cyber laws** (CRA, Data Act...) for **cybersecurity** aspects



ISO 26262 AUTOMOTIVE

ISO 26262 is the international reference standard for **Functional Safety** in the **automotive** sector.

It defines processes, requirements and activities to ensure that electrical and electronic (E/E) systems in road vehicles are developed in a way that reduces the risk of hazardous malfunctions to an acceptable level.



ISO 26262 TIMELINE



2005

Work began on **creating** an international standard for functional safety in vehicles.

2011

First edition of ISO 26262

2018

Second edition of ISO 26262

2027

Third edition: The second phase of the **working draft** (WD) has currently begun.

DIFFERENCES OVERVIEW

Topic	ISO 26262: 2018 (Ed. 2)	ISO 26262 Ed. 3 (under development)
Architectures	ECU-centric	Software Defined Vehicles
Fail-operational concept	Marginal	Explicitly addressed
Cybersecurity	Marginal	Linked to ISO 21434
AI / ML	Not covered (SW deterministic)	Explicit requirements
Reused Software	Limited	Structured (PAS 8926 - Use of pre-existing software)
SOTIF	External	Integrated / linked



ISO 26262 AND ISO PAS 8800

The third edition of ISO 26262 will contain explicit **AI requirements**, aligning with the emerging ISO PAS 8800 standard.

The key concepts for the safety of AI in road vehicles, according to ISO PAS 8800, revolve around managing risks arising from AI errors and integrating with existing safety standards.

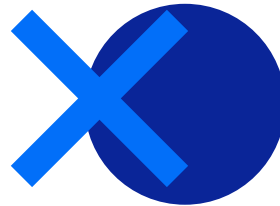


FUNDAMENTAL AI SAFETY DEFINITION



AI SAFETY

The absence of unreasonable risks due to hazards caused by potentially erroneous behavior of AI systems.



AI ERROR

A discrepancy between the actual value or condition of an AI element (such as a model or component) and the correct, specified, or theoretical value or condition.



AI TRIGGERING CONDITION

A specific condition that triggers a functional failure of the AI element, leading to an error.

AI SAFETY PROPERTIES

AI System Properties Related to Safety

The ISO PAS 8800 document identifies several crucial **properties** that must be guaranteed to ensure **safety**:

- **Robustness**: The ability of an AI model to maintain its performance despite small changes in inputs or sensor noise.
- **Generalization**: The ability of an AI model to provide correct predictions on data that was not used during training.
- **Resilience**: The goal of maintaining the system even in the presence of errors.
- **Controllability**: The ability to maintain the system in a safe state by controlling AI errors.
- **Predictability** and **Explainability**: Concepts related to the ability to understand and anticipate system behavior.

LIFECYCLE AND DATA MANAGEMENT

The ISO PAS 8800 document defines:

- **AI Safety Lifecycle:** A structured approach that includes design, development, testing, validation, and live measurements.
 - **Dataset Lifecycle:** Acquisition and Ingestion, Labeling, Splitting into Specific datasets for training, Validation and Testing
- **Data Quality:** Because AI (especially machine learning) is data-driven, the quality, completeness, and integrity of training, validation, and testing datasets are considered critical to safety.
- **Assurance Argument:** A central concept is the use of a safety assurance argument, which provides a logical structure and evidence to demonstrate that the AI's safety requirements have been met.



RELATIONSHIP WITH OTHER STANDARDS: ISO 26262

ISO PAS 8800 does not work in isolation but **integrates** with **other standards** such as ISO 26262. The goal is to create a comprehensive framework based on:

- Allocation of **responsibilities** as previously mentioned, "classic" FuSa (26262) and safety for AI systems (8800)
- Alignment with the **ASIL** levels of **26262**
- **Derivation of requirements:** AI requirements are derived or allocated starting from the **safety concept** of **ISO 26262**
- **Analysis of failures and insufficiencies:** if the error is a **hardware failure or a systematic error**, **26262** applies; if the error results from a specific functional **insufficiency of the AI model** (such as a lack of robustness), **8800** is used
- **Annex C of 8800** provides a **gap analysis** and **tailoring** compared to 26262. For example, the tailoring of ISO 26262-4 (System-Level Development) provides examples of how to tailor and interpret the requirements of the "technical security concept" at the system level. The tailoring of ISO 26262-6 (Software-Level Development) includes detailed tables (such as Table C.3-1) listing specific requirements and methods, proposing how they should be "tailored" for machine learning. For example, it explains how to handle:
 - The specification of software requirements in the absence of traditional source code
 - Verification and testing criteria that should be replaced or supplemented with statistical performance metrics typical of machine learning.

RELATIONSHIP WITH OTHER STANDARDS: ISO 21448

The relationship between ISO/PAS 8800 and SOTIF (ISO 21448) is close and complementary, as both address functional deficiencies and trigger conditions in the absence of hardware failures, but ISO 8800 delves into the specific details of AI-based systems.

ISO 8800 describes how AI activities interact with the clauses of ISO 21448 (Table 6-2).

Safety Decision Tree: When unsafe behavior is observed, the standard provides guidance (Figure 13-1) for determining the cause: if the error is not due to the AI model but to a conventional element or a general performance deficiency, the safety analysis must continue following ISO 21448.

In summary, while **SOTIF** defines the **safety** of the **overall function** (e.g. "automatic emergency braking"), **ISO 8800 provides the technical tools** to ensure that the part of the **AI** contributing to that function **does not introduce unreasonable risks**.



AI AND ASPICE 4.0

Although **ISO PAS 8800 does not mention ASPICE**, the standard includes "**AI Safety Management**" and assumes that **quality management** principles are applied throughout development. AI is introduced in Automotive SPICE 4.0 primarily through the new Machine Learning Engineering (**MLE**) process area, officially introduced in version 4.0, released at the end of 2023.

In essence, ASPICE 4.0 recognizes that modern vehicles (ADAS, autonomous driving, perception, driver monitoring, predictive maintenance, etc.) no longer rely solely on traditional deterministic software, but also on ML/AI models that must be developed, verified, and maintained with controlled processes. The main new features are:

- New process areas MLE.1 - MLE.4
- Greater emphasis on data management
- Traceability for datasets and models
- Integration with safety and cybersecurity
- More explicit support for iterative/agile workflows typical of the ML lifecycle
- New AI/ML process areas

ASPICE 4.0 adds four processes dedicated to machine learning:

- **MLE.1** Definition of ML requirements
- **MLE.2** Design of the ML architecture
- **MLE.3** Development of the ML model
- **MLE.4** Verification and validation of the ML model
- **SUP.11** Machine Learning Data Management

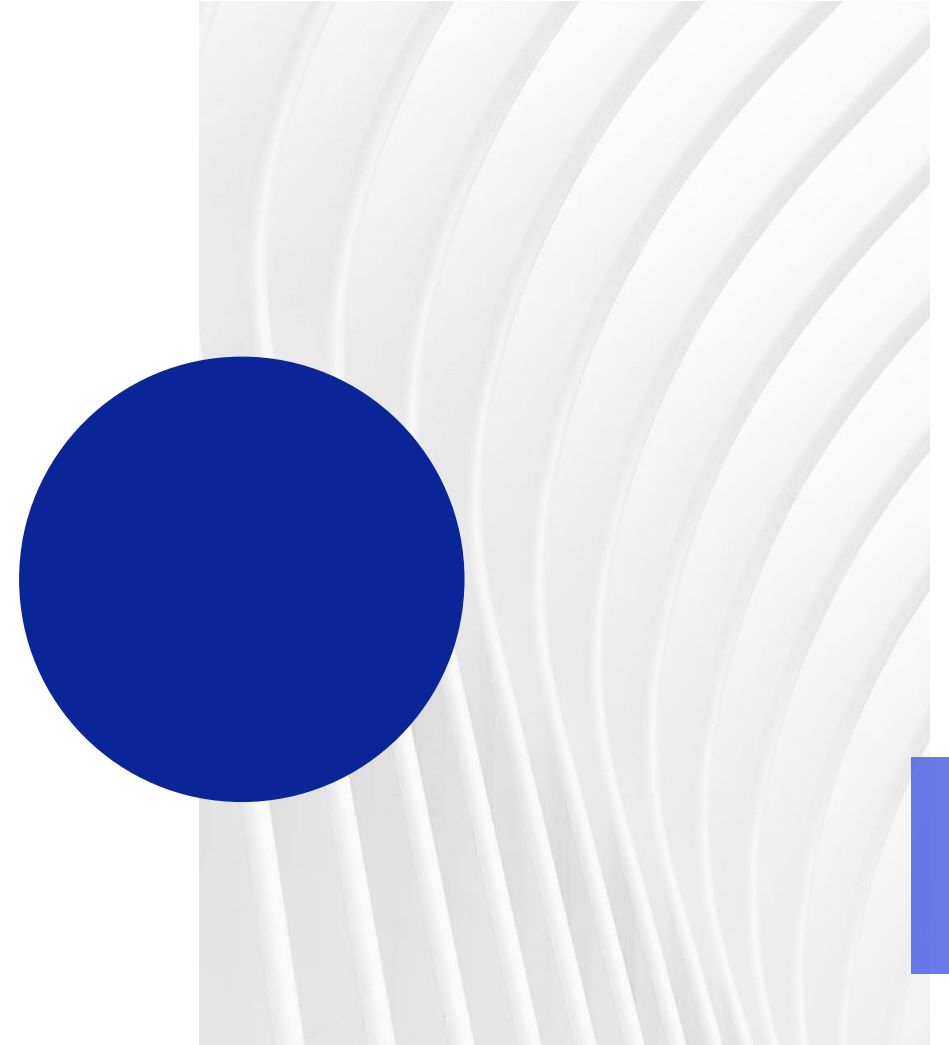
AI FUTURE TRENDS

ISO/PAS 8800 addresses the topic of **Explainable AI** (XAI), defining it as a fundamental property of safety-related artificial intelligence systems. The standard provides a specific definition for AI explainability in clause 3.1.4, describing it as a property of the AI system. Along with predictability, explainability is considered crucial for understanding and anticipating system behavior. It is considered useful for supporting the safety assurance argument by providing evidence about the model's decision-making logic. It helps identify and mitigate functional deficiencies, allowing developers to understand why the model made a particular unsafe decision. In summary, for ISO/PAS 8800, explainability is not just a theoretical requirement, but a practical safety engineering tool for analyzing errors, validating model behavior, and building a robust safety case for the vehicle.

ISO Pass 8800 does not mention trends currently in use such as **Federated Learning** (FL) or **Edge AI** but the regulatory environment in the AI sector is constantly evolving

CONCLUSIONS

- AI is a huge opportunity for the automotive industry.
- However, it introduces new risks. Companies must integrate safety and data science and adopt new standards; the regulatory framework is constantly evolving.
- Whoever knows how to manage AI and Safety will have a competitive advantage



GIANCARLO SCAPPATURA

GRAZIE!

giancarlo.scappatura@intecstechnologies.it

