
# Functional Safety, SOTIF and Cybersecurity – Validation and conformity demonstrator extended in Horizon SHASAI project

C. Donzella, G. Nicosia

V1.1 – 21/05/2026

# The context



In the last four years, EXIDA has been involved in three European R&D Horizon Projects:

1. **SAFEXPLAIN: SAFE AND EXPLAINABLE CRITICAL EMBEDDED SYSTEMS BASED ON AI;** (start 10/2022, end 09/2025); https://safexplain.eu/ -> *some results from this project have been already presented at ASPIN 2014*

2. **EdgeAI-Trust: Decentralized Edge Intelligence: Advancing Trust, Safety, and Sustainability in Europe;** (start 01/2024, end 04/2027); https://www.edgeai-trust.eu/

3. **SHASAI: Secure Hardware and Software for AI systems;** (start 11/2025, end 04/2029); https://shasai.eu/

The common denominator for all EXIDA participations has always been to further advance **tools and methodologies for Safety and Security compliance of Autonomous Vehicles**.

# R&D focus in the three projects



*EXIDA final results in **SAFEXPLAIN (concluded)***

- Verification and Validation **(V&V) methods and tests** for ML-based applications
- **SW Core Platform** with one fully simulated virtual car use case
- **Extension to** extracts of Taiwan's III's FORMOSA **real-driving dataset**

SAFEXPLAIN
Safe and Explainable Critical Embedded Systems based on AI

*EXIDA intermediate results in **EdgeAI-Trust (entered last year)***

- **Extension** of SW Core Platform and porting **to new HW platforms**
- **Extension to lab vehicle** for road surface detection
- **Extension to modified homologated car** for V&V of connected ADAS at intersections

EdgeAI-Trust

*EXIDA expected results in **SHASAI (just concluded 'concept phase' after 6m)***

- Verification and Validation **(V&V) methods and tests to include cybersecurity**
- **Extension** of SW Core Platform **to tackle cybersecurity solutions**
- **Extension to urban delivery vehicle** enabling unmanned last mile

SHASAI

# Multidisciplinary V&V Integration: FuSa, SOTIF, and Cybersecurity



The increasing complexity of the vehicle system (ADAS) nowadays is involving different disciplines such as:

- **Functional Safety (ISO 26262)**,
- **SOTIF (ISO 21448)** and
- **Cybersecurity (ISO/SAE 21434)**

360-degree safety & security is a technical and normative necessity for autonomous vehicles.

The proposed approach aims to demonstrate as the Verification & Validation (V&V) phases as the ideal touchpoint to merge these disciplines

Breaking down vertical silos to move toward a unified, integrated engineering environment.

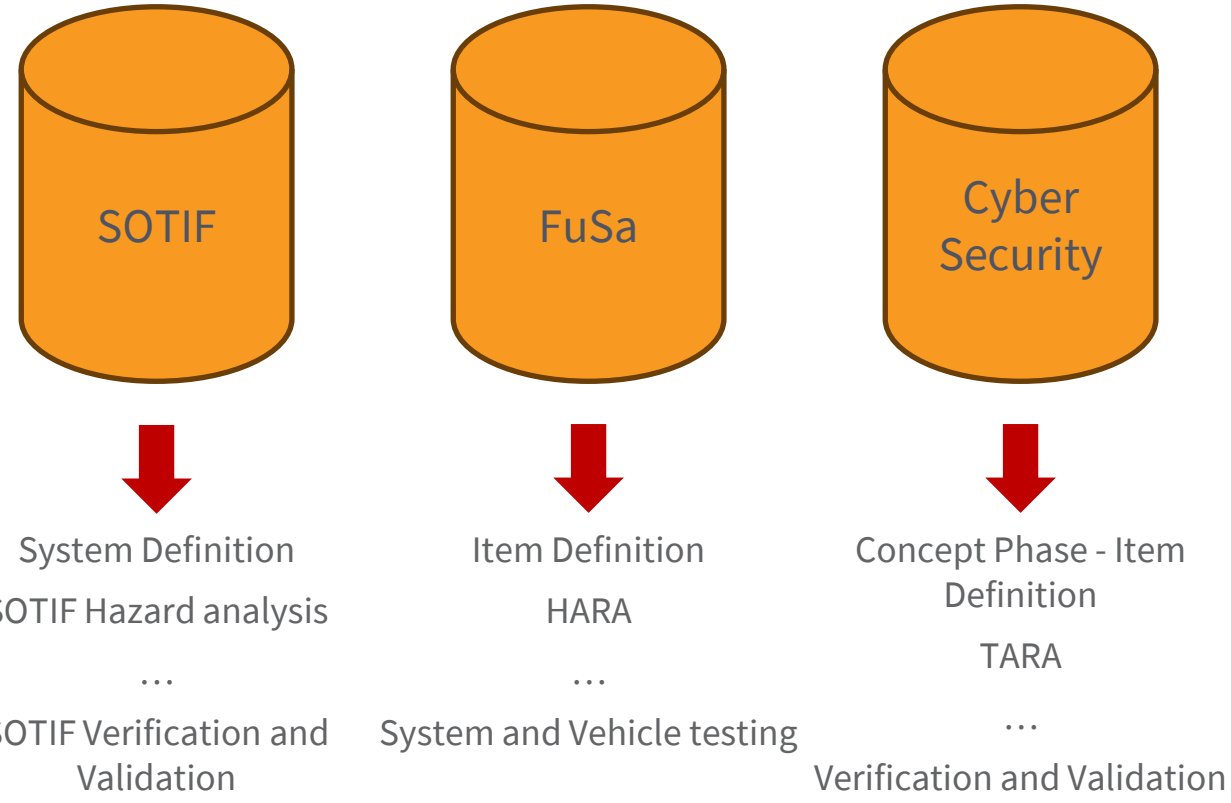

*Security today is no longer a choice, but a technical and regulatory requirement.*

# Isolated approach



In the great majority of the cases ISO 26262, ISO 21448 and ISO 21434 disciplines are managed as independent silos.

This approach leads to activities redundancy and high effort consumption.

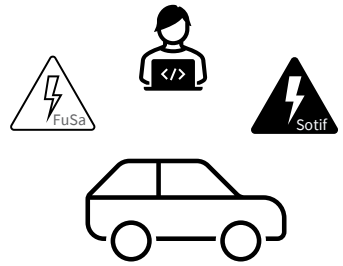


# V&V integrated approach



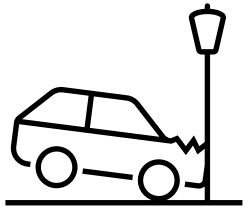
A cyber-attack (e.g., an adversarial exploit or sensor spoofing) does not violate only a Cybersecurity Goal but it can trigger also:

- **SOTIF violations**
- **Functional Safety violations**




The approach focuses on scenarios defined according to the ODD and on the FuSa, SOTIF and Cybersecurity related triggering conditions that can lead to functional insufficiencies.

V&V activities will not test cyber security related features only, but also the Fusa and SOTIF related ones.



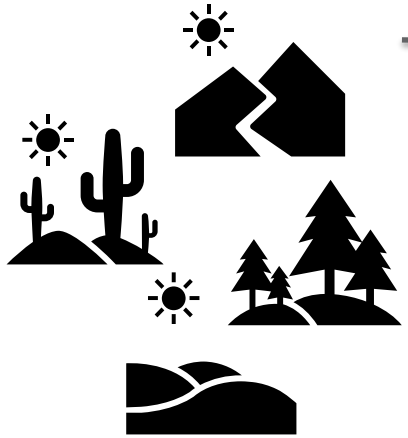
# SHASAI Automotive Use case – Case study



The integrated approach is built on the results of the SAFEXPLAIN project and it will be applied within the new European project SHASAI

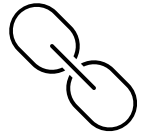
The V&V strategy considers a cross-functional approach, utilizing as main input the item definition, the TARA (Threat Analysis and Risk Assessment) and its derived mitigations.

The TARA shall be tailored as follow:



TARA Improvement introducing the driving scenarios

TARA



Cyber attack link with driving scenarios and architectural elements

Creation of scenario catalogue with relevant vehicle testing scenarios

STPA inputs

# TARA tailoring



The TARA extension allows:

- The execution of analysis and testing activities to confirm the system behaviour considering ISO 26262, ISO 21448 and ISO 21434 practices
- To use the Item Definition as the bridge to map cyber-attacks to vehicle-level safety hazards
- understanding which element is impacted by a cyber-attack

To realize this strategy, the first step is the formal mapping of the Attack Path to Vehicle Control and including the Operational situation. This allows to identify which specific cyber-attacks can trigger an Unsafe Control Action (UCA) and which scenario shall be considered during the testing activites.

# Vehicle validation



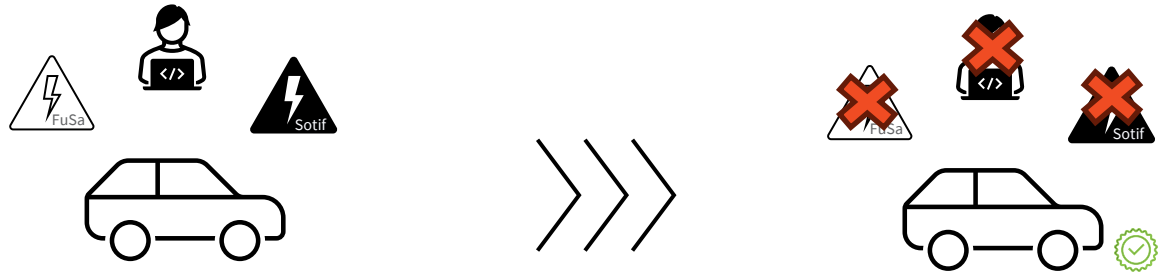
The V&V strategy goal at vehicle level is focused on:

- [Operational Situation] + [Cyber-Safety Trigger].

To address the quantitative aspects is necessary to consider aspect such as:

- FTTI (Fault Tolerant Time Interval)

The model allows the simultaneous or sequential injection of functional faults, SOTIF limitations, and cyber-attack vectors within the same critical scenarios, with the goal to ensure joint vehicle validation session



# Component validation



The V&V strategy goal at component level is focused on:

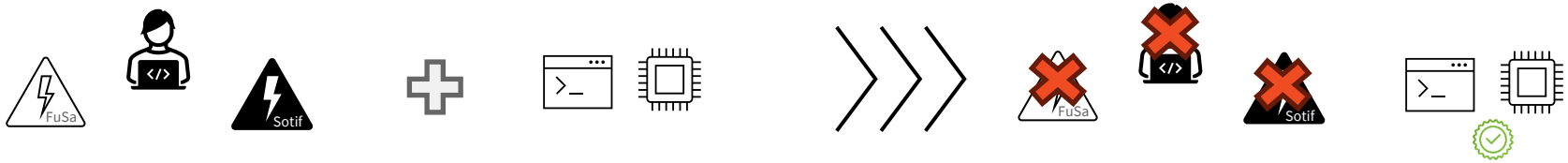
- [Security-Safety Mechanism] + [Threat Vector].

The strategy uses the Item Definition (Input-Logic-Output) as a bridge to map the Attack Path (into the TARA) directly with the STPA (System-Theoretic Process Analysis). Therefore, it would be possible to link 'Data Manipulation' or 'Denial of Service' into an Unsafe Control Action (UCA).

To address the quantitative aspects is necessary to consider aspect such as:

- FHTI (Fault Handling Time Interval)

The model allows Analysis of software vulnerabilities and hardware limitations as triggering conditions.

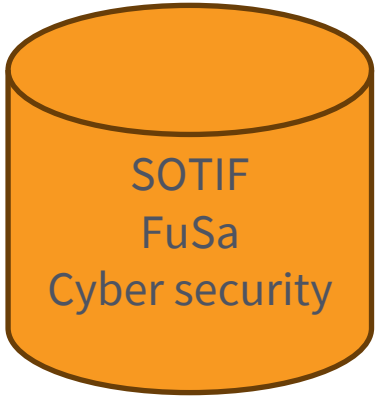


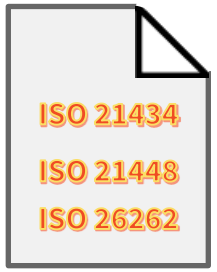
# Integrated V&V objectives




The **Integrated V&V** framework allows:

- to reduce the redundancies
- to reduce the effort consumption
- to create a unique and comprehensive test report
- Obtain compliance to ISO 26262, 21448 and 21434 standards



# Integrated V&V example vehicle level



**TARA (Cyber):**
An attacker poisons the dataset (Data Poisoning) to ensure that the model does not see a stationary vehicle if it has a certain shape.

Plausible Scenario:
- driving on urban roads at 30 km/h
- driving on country road

**Test:**
As the vehicle approaches a target, we inject the ‘compromised’ model (or simulate its error using software).
**Pass/Fail criteria:**
The system enters a **Safe State** (Limited Speed) upon detecting a mismatch between sensors.

# Conclusions



The key points of the extended V&V framework are:

- ***TARA and HARA integration****: Overcoming the limitations of traditional TARA by introducing driving scenarios (typical of HARA) to map cyberattacks into real operational situations. This enables the derivation of a catalogue of scenarios to be used to derive vehicle level test cases.*
- ***Joint Component validation****: Analysis of software vulnerabilities and hardware limitations as 'triggering conditions' by means of STPA method. In this approach, a cybersecurity issue, an HW random or systematic failure or a sensor performance limitation is treated as a trigger that could lead to the violation of the Safety/Cybersecurity Goals.*
- ***Joint Vehicle validation****: The model allows the simultaneous or sequential injection of functional faults, SOTIF limitations, and cyber-attack vectors within the same critical scenarios.*

With its own methods and tools (partly open, partly proprietary), **EXIDA** assists the development of virtual and physical demos of partners from **the Netherlands, Austria, Turkey and Taiwan**.

We would be delighted to support partners from **Italy**, too.

# Thank you for your attention!


Via Ribes 5, 10010 Colleretto Giacosa (TO) – Italy