D6.8 Final Exploitation Report

Version 1.5

Documentation Information

Contract Number	101069595
Project Website	www.safexplain.eu
Contractual Deadline	30.09.2025
Dissemination Level	PU
Nature	R
Authors	Carlo Donzella (EXI), Valeria Dallara (EXI)
Contributors	all partners
Reviewer	Jaume Abella (BSC), Frank Geujen (Navinfo)
Keywords	exploitation, IPs, IPRs, copyright, licences, safety, dependability, AI, ML, DL, CAIS, software, OS, railway, space, automotive, AV

This project has received funding from the European Union's Horizon Europe programme under grant agreement number 101069595.

Change Log

Version	Description Change
V1.0	First complete draft
V1.1	First Internal Review
V1.5	Final version

Table of Contents

1 Executive Summary

Task 6.2 “Exploitation activities”, which runs from M1 to M36 (the entire duration of the project), has a strong business approach, to the extent allowed by the nature of this R&D project and its TRL. One of its major aims is to analyse the exploitation context and business opportunities to understand the actual market situation, that is the field of AI-based solutions is moving at blazing speed. Based on this information, potential target markets/users (both in terms of early adopters and followers) are being identified and analysed, and the competitive environment surrounding the expected exploitation items is being assessed. While technologies and applications are evolving faster than ever, the adopted approach is well in line with well consolidated business planning and competition analysis methodologies.

Task 6.2 focuses on:

1) defining the exploitation plan for project results.
2) defining the plan for business and cost-benefit opportunities.
3) establishing management plans for IP rights and knowledge ownership.
4) indicating roadmaps for replication of results in other domains.

In the first twenty-four months of the project, exploitation activities have focused on defining, actuating and monitoring the exploitation plan. Three deliverables were prepared as part of this task: D6.2, D6.6, D6.7, D6.8.

The deliverable *D6.2 Exploitation Plan* defined the initial plan including and defining the methodology.

Deliverable *D6.6 Initial Exploitation Report* represented an extension on the initial plan and was updated to include further conversations with project partners and information gathered from the market.

This current Deliverable *D6.8 Final Exploitation Report* represents the state-of-the-art of the end of the project, reporting on all the already existing exploitation results and pointing out to all opportunities for take up after the completion of the contract provisions.

2 Exploitation Strategy at M36

Exploitation activities have been planned, since the start of the project and especially after the publication of the Exploitation Plan at M3 along two major groups:

1st GROUP OF ACTIVITIES, MOSTLY THROUGH INTERNAL STUDY:

- Identification of project exploitable assets (with business propositions)
- Identification of the main exploitation routes for the consortium (cluster of exploiters)
- The procedures to protect IPR (including legal aspects)

2nd GROUP OF ACTIVITIES, MOSTLY THROUGH EXTERNAL RELATIONSHIPS:

- Identification and analysis of the target users (early adopters and followers)
- Analysis of the exploitation context and business opportunities (market demand)
- Assessing the competitive environment surrounding the project (market offer and constraints)

In the *D6.2 Exploitation Plan*, issued at M3, the major methodological issues have been discussed, and key choices have been made, with arguments for them. In particular, section 1.4 of the *D6.2 Exploitation Plan* exposes why the relatively old methodology proposed by Geoffrey Moore in his seminal *Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers* (1991, revised 1999 and 2014) is still an outstanding resource for identifying, describing and taking to market high-tech products. What the project has adopted very specifically is its simple but extremely effective framework for establishing compelling and clearly differentiated Unique Selling Propositions (USPs) for what we call Exploitable Items.

In the period elapsed from the Initial Exploitation Report (M12) and the Interim Exploitation Report (M24), the initial strategy has been confirmed as extremely valid although – as all valid strategy – ready for adaptation in an extremely volatile environment such as the AI/ML/DL Solutions for Critical Systems.

In this last period from the Interim Exploitation Report (M24) to this Final Exploitation Report (M36), the strategy has not changed, rather further confirmed by the increasing number of results coming from both groups of activities (internal study and external relationships), that pave the way for a highly credible further uptake after the end of the contractual duration of the project.

3 Exploitation Results at M36

As per today (M36), the consortium's partners (specifically, Partner Exploitation Managers supported by the Project Exploitation Manager) have reviewed, revised and reclassified the Exploitable Items into **16** core exploitable results, classified into **6** (up from **5**) major categories:

1. Open-Source Software (**6**)
    1. **pWCET-AI by BSC**: a novel probabilistic timing analysis tool
    2. **DLETLib by BSC & EXIDA**: a dedicated DL Explainable and Traceable library, incorporating a strongly structured and layered software architectural design
    3. **SemDRlib by BSC**: a dedicated DL library to generate diverse redundant versions of image-based DL models
    4. **ROSGUARD by BSC & IKERLAN**: a run-time bandwidth monitoring mechanism
    5. **Safety YOLO by IKERLAN & EXIDA**: a basic software library with re-design/implementation of a subset of YOLO functions in compliance with Functional Safety (FuSa) standards requirements against SW systematic errors
    6. **EXPLib by RISE**: a software platform in the form of an opensource repository containing methodology and tools enabling the use of XAI techniques to support safety assurance of AI based systems
2. Proprietary Software (**2**)
    1. **Orin-PMULib by BSC**: a dedicated Performance Monitoring Unit Library
    2. **JANE by AIKO**: an autonomous navigation application - AI software implementing algorithms for navigation
3. Open Content (**2**)
    1. **AI-Functional Safety Management (AI-FSM 2.0) by IKERLAN & EXIDA, BSC**: a safety lifecycle suite of documents (procedures, guidelines, templates) that extends the traditional FuSa management (as defined in ISO/IEC 61508 and ISO 26262) to AI techniques and methods
    2. **V&V-SCENARIOS by EXIDA & NAVINFO, IKERLAN, AIKO**: a catalogue of ODD-compliant automotive, railway, space scenarios
4. Proprietary Content (**2**)
    1. **V&V-TESTSPECS by EXIDA:** a full set of tests specification, associated with V&V-SCENARIOS
    2. **Safety Pattern Library (SPL) by IKERLAN**: a set of documented exemplary safety-case(s) and exemplary safety-concept(s), with a technical focus on safety and XAI
5. Open Demo (**3**)
    1. **CoreDemo by BSC & EXIDA, IKERLAN, RISE:** an open SW platform demo, with all SW functions enabled and with significant examples for space, rail and car sectors
    2. **CarDemo by NAVINFO & EXIDA:** an automotive use case open demo
    3. **RailDemo by IKERLAN & EXIDA:** a railway use-case open demo
    4. 6. Proprietary Demo (**1**)
    5. **SpaceDemo by AIKO:** a critical Guidance, Navigation, and Control (GNC) space demo

The detailed list of the exploitable results, together with their complete descriptions in the form of the Moore's template, is presented in the following section.

Concerning results related to external relationship**,** the consortium has also actively sought to engage and transfer knowledge and project technology to project stakeholders, including external certification authorities, experts and other relevant communities.

An important relationship has been built with **iNTACS** and the Quality Management in the German Association of the Automotive Industry e.V. (**VDA-QMC**). This relationship has opened the door to future opportunities to share knowledge, in addition to the participation in the ASPICE MLE Working Group (WG). This WG was established and has already produced the complete set of course syllabus, now under revision for a new version, that will include several further examples from SAFEXPLAIN (see below).

SAFEXPLAIN is also actively participating in discussions and trends in AI and Safety in standards coming from **international standardization bodies ISO and IEC**. Exida group members, knowledgeable about SAFEXPLAIN, are delegates of some of the technical committee of the standards listed below, which opens the door to greater opportunities for exchange with these bodies:

1. ISO/CD PAS 8800 -Road Vehicles – Safety and artificial intelligence
2. ISO 26262-1:2018 – Road vehicles – Functional safety (new version will include AI section)
3. ISO 21448:2022 – Road vehicles – Safety of the intended functionality (new version will include specific AI section)
4. IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems (new version will include an AI section)

We are not able to report any direct mentions of SAFEXPLAIN results, as ISO committee members are bound to strict confidentiality about sessions, and we haven't established any NDAs/protocols with them.

Moreover, a SAFEXPLAIN partner (exida development) is also an active corporate member of **ASAM e.V. (Association for Standardization of Automation and Measuring Systems)** and participates in the consortium's activities, including the election of technical committees. This close contact with our target audiences of certification authorities and experts helps extend the message that SAFEXPLAIN technology provides a safe approach for DL certification and safety guidelines for future standards.

4 USPS at M36

In this third version of the Exploitation Report, the consortium is presenting 16 USPs, 2 of which are new ones. 2 USPs presented in previous version have been cancelled (as already noticed, not a negative sign, this represents the ability of project partners to dynamically align with both project evolution and market analyses).

All partners have agreed that each USP must be defined genuinely and honestly, with appropriate efforts, with a small disclaimer: USPs are not exploitation schedules with timing end-result attached.

USPs are statements of exploitation interest. All USPs described in this document, confirmed or new, are considered feasible and of business interests for the indicated owners; just that full exploitation needs resources beyond the scope and/or the duration of the project.

We remind that Geoffry Moore's original 6-step Unique Selling Proposition template is:

- For (*target customer*)
- Who (*statement of need or opportunity*)
- The (*product name*) is a (*product category*)
- That (*statement of key benefit* - that is, *compelling reason to buy/adopt*)
- Unlike (*primary competitive alternative*)
- Our product (*statement of primary differentiation*).

Full description of the methodology can be retrieved in D6.2.

4.1 EXI01

This USP has been cancelled. It was the only EXI USP present in the Exploitation Plan and in the Initial Exploitation Report, but EXI has decided (with the support of the Exploitation Manager) to get rid of it and create two new ones that are closer to the revised EXI work plan in the project and to the updated business interest of the company.

More specifically, the original USP was closely related to original implementation plan related to project requirement R2.4: "*New methods for safety analysis shall be provided to consider the quantification of DL-software failure rate in the assessment of the overall system residual risk during development and operation*". During the work in WP2, it became evident that the original implementation was no longer considered as the best one and a new implementation was proposed and carried out; this has led to the cancellation of this USP and the formulation of the new EXI02 and EXI03 (see below).

(Note: Original EXI01 description can be retrieved in D6.2)

4.2 EXI02

Item ID	EXI02
Primary Owner	EXI
Other Owner(s)	NAVINFO, IKERLAN, AIKO
IPR Type	Open
For	embedded software developers in automotive, railway and aerospace sectors,
Who	need to use advanced ML and DL techniques for highly dependable systems
The	**V&V-SCENARIOS** is a catalogue of ODD-described scenarios
That	extends the traditional FuSa Verification and Validation (V&V) model to AI techniques and methods.
Unlike	other scenarios languages and tools, like *Foretellix's open scenario* and *IVEX's scenario catalogue,*
Our	catalogue is ready to be used, based on public data, available as open-source content, integrated with test cases specification.

Exploitation review findings:

Meetings dedicated to the revision and improvement of these USPs have been held on the 26/07/24 and the 02/08/24, then finally confirmed on 30/06/25. This USP, jointly with the following EXI03, is replacing the old EXI01.

EXI02 is related to Scenarios, and although scenarios are directly described by EXI, they are reviewed and eventually adapted in collaboration with the three user-case owners and for this reason, it was agreed that they are co-owned with them. Some of those scenarios are included in the open demo USPs (see below).

EXI02 (differently from EXI03) is classified as open content.

4.3 EXI03

Item ID	EXI03
Primary Owner	EXI
Other Owner(s)	-
IPR Type	Proprietary
For	embedded software developers in automotive, railway and aerospace sectors,
Who	need to verify advanced ML and DL techniques for highly dependable systems
The	**V&V-TESTSPECS** is a full set of tests specification
That	extends the traditional FuSa Verification and Validation (V&V) model to AI techniques and methods.
Unlike	other available test suites, like *Foretellix's V-suites* and *IVEX's trajectory checker*,
Our	test specs are developed according to ISO/IEC 61506, ISO 26262 and SOTIF and ready to be run to test use cases defined within the AI-V&V-SCENARIOS.

Exploitation review findings:

Meetings dedicated to the revision and improvement of these USPs have been held on the 26/07/24 and the 02/08/24, then finally confirmed on 30/06/25.

This USP, jointly with the following EXI02, is replacing the old EXI01.

EXI03 is related to Test Specifications, and they are fully owned by EXI. Some of them are used in the open demo USPs (see below).

EXI03 (differently from EXI02) is classified as proprietary content.

4.4 BSC01

Item ID	BSC01
Primary Owner	BSC
Other Owner(s)	-
IPR Type	Proprietary
For	embedded software developers and V&V engineers in automotive, railway and aerospace sectors
Who	need to use configure and collect information on hardware events on the NVIDIA® Jetson Orin™
The	**Orin-PMULib** is a dedicated Performance Monitoring Unit Library
That	allows configuration on target performance monitoring counters and debug devices.
Unlike	the generic and high-level performance monitoring library solutions like *perf, oprofile, perfmon2, or PAPI*
Our	library is specifically adapted to the platform and provides a lightweight but accurate way to configure and retrieve precise information on traceable hardware events.

Exploitation review findings:

Meetings dedicated to revision and improvement of this USP were held on 29/03/23, 05/07/23, then finally confirmed on 30/06/25.

This USP version already incorporates adjustments based on early findings that were indicated in the Exploitation Plan, and it has been remarkably stable since its first definition.

Competition analysis is quite complete, and licencing model is available internally.

4.5 BSC02

Item ID	BSC02
Primary Owner	BSC
Other Owner(s)	-
IPR Type	Open
For	embedded software developers and V&V engineers in automotive, railway and aerospace sectors
Who	need to characterize the performance of advanced ML and DL solutions for highly dependable systems.
The	**pWCET-AI** is a novel probabilistic timing analysis tool
That	allows to characterize the timing behaviour and to derive probabilistic Worst-Case Execution Time (pWCET) estimates of AI-based solutions.
Unlike	existing tools based on traditional deterministic timing analysis approaches, such as static timing analysis (e.g. *AbsInt aIT*), dynamic analysis (e.g. *RapiTime, SymTA/S, AbsInt Timeweaver*) or exploiting existing probabilistic methods, such as those based on Extreme Value Theory (e.g. *MBPTA-CV, RocqStat*)
Our	library allows for trustworthy and tight execution time bounds capturing the specific non-deterministic traits of ML and DL software solutions running on complex SoCs such as, for example, the NVIDIA® Jetson Orin™.

Exploitation review findings:

Meetings dedicated to revision and improvement of this USP were held on 29/03/23, 05/07/23, then finally confirmed on 30/06/25.

This USP version already incorporates adjustments based on early findings indicated in the Exploitation Plan, and it has been remarkably stable since its first definition.

The competition analysis is quite complete (even with categories of competitors); licencing models are addressed in the dedicated section below.

4.6 BSC03

Item ID	BSC03
Primary Owner	BSC
Other Owner(s)	EXI
IPR Type	Open
For	embedded software developers and V&V engineers in automotive, railway and aerospace sectors
Who	need to build explainable and traceable DL components to be integrated in their systems
The	**DLETlib** is a dedicated DL Explainable and Traceable library, incorporating a strongly structured and layered software architectural design
That	allows for the development of DL components following the requirements from functional safety standards like ISO 26262, ISO 21448 (SOTIF), IEC 61508 and others.
Unlike	traditional DL frameworks (e.g. *TensorFlow, PyTorch or Caffe*) that only focus on creating a DL infrastructure without supporting explainability/traceability features
Our	library provides an extension to popular AI frameworks (similarly to TensorFlow-probability) to accelerate the adoption of safety standards when DL is used.

Exploitation review findings:

Meetings dedicated to revision and improvement of this USP were held on 29/03/23, 05/07/23, 30/08/23, then finally confirmed on 30/06/25.

This USP version incorporates adjustments based on early findings indicated in the Exploitation Plan.

In July 2023, EXI realized that some of its project results, which were not expected to contribute to its own EXI01 USP, could be integrated with the BSC's exploitable item described in this USP (the cancellation of EXI01 USP does not affect this joint ownership). EXI approached BSC with a proposal for transforming this *individual* USP into a bilateral, collaborative USP between BSC and EXI. Negotiations followed and a final version was agreed upon based on an intended Open-Source licensing model.

Compared with RISE01 (EXPLib), this USP is more oriented to show full integration with SAFEXPLAIN-developed SW middleware, while RISE01 (EXPLib) is more oriented towards XAI techniques with a complete Space toy model.

4.7 BSC04

Item ID	BSC04
Primary Owner	BSC
Other Owner(s)	-
IPR Type	Open
For	embedded software developers and verification engineers in automotive, railway and aerospace sectors
Who	need to build DL components with diverse redundancy to be integrated in their systems and match requirements for the highest safety integrity levels
The	**SemDRlib** is a dedicated DL library to generate diverse redundant versions of image-based object detection DL models
That	applies several user-selected transformations in input images to perform multiple diverse inferences intended to provide semantically identical, yet not bit-identical, results
Unlike	other traditional approaches such as *DMR (Dual Modular Redundancy), TMR (Triple Modular Redundancy), and DCLS (Dual-Core LockStep - a variant of DMR),* which need to produce bit-level identical outcomes and use additional means to introduce diversity,
Our	library instantiates the very same DL model multiple times applying semantic-neutral transformations in the input image so that inference for each of the images is diverse at the physical (e.g., electrical) level so that faults (e.g., particle strikes) affecting redundant instances will not produce identical errors.

Exploitation review findings:

This was a new USP for BSC, their fourth one, appearing for the first time in the previous report.

A meeting dedicated to revision and improvement of this USP was held on the 24/07/24, after which followed its definite confirmation on the 30/06/25.

BSC plans to exploit it through consultancy and bilateral projects. It is classified as open source.

4.8 BSC05

Item ID	BSC05
Primary Owner	BSC
Other Owner(s)	IKERLAN
IPR Type	Open
For	embedded software developers in automotive, railway and aerospace sectors,
Who	need to control memory bandwidth usage and prevent unregulated multicore timing interference to affect the execution of critical applications
The	**ROSGUARD** is a run-time bandwidth monitoring mechanism
That	controls bandwidth memory usage of non-critical applications and temporarily stops them whenever they exceed the allocated quota.
Unlike	other memory bandwidth regulation approaches such as *BAM (Bandwidth Allocation and Monitoring), and BandWatch (System-Wide Memory Bandwidth Regulation System for Heterogeneous Multicore),* that build on specific hardware or OS support,
Our	solution builds on ROS2 modular architecture and is easily portable across platforms and setups.

Exploitation review findings:

This is a new USP for BSC, their fifth one.

This Exploitable Result was co-developed with IKERLAN.

A meeting dedicated to presentation and improvement of this USP was held on the 30/06/25.

BSC plans to exploit it through consultancy and bilateral projects. It is classified as open source.

4.9 BSC06

Item ID	BSC06
Primary Owner	BSC
Other Owner(s)	EXI, IKERLAN, RISE
IPR Type	Open
For	Critical autonomous AI-Based Systems (CAIS) developers and decision-makers in transportation and mobility sectors,
Who	need evidence of what type of evaluation and support are available regarding the certifiability of their CAIS solution concepts and prototypes
The	**CoreDemo** is an open, complete SW platform
That	can demonstrate critical functionalities such as Temporal Consistency, Supervision to Decision, Diagnostic & Monitoring, Safety Control and others on selected 'toy' examples in Space, Railway and Automotive.
Unlike	the other SAFEXPLAIN Car, Rail, and Space Demos that are equipped with ODD-based scenarios and test-cases but only for their specific industrial sector
Our	demo is showing the SAFEXPLAIN capabilities to prospects and early users in all the transportation and mobility value chains.

Exploitation review findings:

This is a new USP for BSC, their sixth one, an open asset co-owned with EXI, IKR and RISE.

It has a unique story that is worth to be known. At M30, most of the results of WP2, WP3 and WP4 were already available while the full use-case demos were expected for M36, as per project plan.

Given the neck breaking speed of the reference market, the Exploitation Manager floated the idea of putting together a “core demo” with all the already existing results, even if equipped only with ‘toy’ examples from the use-cases developed in WP5.

The idea was discussed in detail during the F2F meeting of May 2025 in Barcelona, and it was accepted as a valid temporary solution to have something ‘running’ to show before the end of the project. The Core Demo ‘premiered’ at the ASPIN 2025 event on May 29th, held near Milan.

The success was so immediate that it was decided that it has a reason to stay also when the other three full demos are officially released in Sept 2025; in fact, it will have a focus more on the SW side and will incorporate simple(r) examples from all the three transportation sectors.

BSC confirmed its commitment to this USP on the 30/06/25.

4.10 NAV01

This USP has been cancelled. It was present in the previous Reports, but NAV has decided to cancel it to focus on its only remaining USP (see below NAV03).

The USP, named “NIA GuardAI platform for developing and assessing safe and explainable ADAS systems”, was “discontinued after extensive market validation”, as communicated on 30/06/25.

(Note: Original NAV01 description can be retrieved in D6.6)

4.11 NAV02

This USP has been cancelled. It was present in the Exploitation Plan and in the Initial Exploitation Report, but NAV has decided (with the support of the Exploitation Manager) to focus on its other USP.

The USP, named “NIA Safe AI Development and Deployment Guidelines”, was declared too generic to justify the significant extra efforts being allocated to its development.

(Note: Original NAV02 description can be retrieved in D6.6)

4.12 NAV03

Item ID	NAV03
Primary Owner	NAVINFO
Other Owner(s)	EXI
IPR Type	Open
For	ML, DL and computer vision engineers, researchers and programmers working on the automotive use-cases
Who	want to develop safe and explainable AI for autonomous driving
The	**CarDemo** is an automotive use case open demo
That	provides a flexible and high-fidelity environment with ODD-compliant safety scenarios aligned with functional safety standards, allowing rigorous testing of the agent's capabilities.
Unlike	other autonomous automotive demos such as *Self-Driving-Car-Demo, Scale Automotive Data Engine, SelfDrive_AI Gym,*
Our	autonomous driving environment, developed with a modular architecture, facilitates the integration of explainability features and a supervision module that enhance the safety and interpretability of the agent's decision-making process; the agent demonstrates competence in perception, planning, and vehicle control within the simulated environment.

Exploitation review findings:

A meeting dedicated to the implementation of this new USP was held on the 08/07/24, then confirmed at a new meeting on 12/06/25.

This USP is one of the three USPs that have been defined to exploit the three sectoral use-cases.

The primary owner is NAV as responsible of the use-case, EXI is co-owner due to its contribution to the ODD-based automotive scenarios.

The original Open status has been provisionally confirmed on 12/06/25, then definitely so on 30/06/25.

4.13 IKR01

Item ID	IKR01
Primary Owner	IKERLAN
Other Owner(s)	-
IPR Type	Proprietary
For	dependable and Critical autonomous AI-Based Systems (CAIS) developers in the automotive, railway, industrial and aerospace sectors
Who	need to develop and safety certify automated, heteronomous or autonomous systems integrating DL components
The	**Safety Pattern Library (SPL)** is a basic technical reference foundation that provides a set of documented exemplary safety-case(s) and exemplary safety-concept(s), with a technical focus on safety and XAI
That	describe common safety design approaches (solutions) to common design requirements (recurrent problems).
Unlike	the current need to define system-specific designs and argumentations (from scratch) due to a lack of formalized (public) 'reference foundations'
Our	**SPL** provides a basic set of documented 'FuSa patterns to use in DL-based solutions', with a subset of them assessed by internal/external experts (e.g., TÜVR) as part of the safety-case assessment(s) (e.g., railway). **SPL** is complementary to **AI-FSM**.

Exploitation review findings:

Meetings dedicated to revision and improvement of this USP were held on 29/03/23, 29/06/23, then on 19/07/24.

This USP version incorporates all adjustments based on early and later findings indicated in the Exploitation Plan, and it has been remarkably stable since its first definition.

The competition analysis is articulated but still only shows 'abstract' competition, rather than specific competitors; this is deem provisionally acceptable given the special nature of this asset.

This USP has been eventually confirmed during a dedicated meeting on 13/06/25.

4.14 IKR02

Item ID	IKR02
Primary Owner	IKERLAN
Other Owner(s)	BSC, EXI
IPR Type	Open
Partner	IKERLAN
For	dependable and CAIS developers in the automotive, railway, industrial and aerospace sectors
Who	need to develop and certify for safety: automated, heteronomous or autonomous systems integrating DL components
The	**AI-Functional Safety Management (AI-FSM 2.0)** development is a 'safety lifecycle' (procedures, guidelines, templates) defined in compliance with existing AI-safety standards (e.g., ISO 5469)
That	provides the required basic procedures, guidelines and templates to support the development of DL-components for CAIS systems, with a technical focus on safety and XAI.
Unlike	the lifecycles in Functional Safety Managements (FSM) for FuSa standards, that do not (yet) explicitly consider DL-software
Our	Safety lifecycle provides a starting point for developing DL-based dependable CAIS systems, which can be integrated as an extension to traditional Functional Safety Management (FSM) (e.g., IEC 61508, ISO 26262). **AI-FSM** is complementary to **SPL**.

Exploitation review findings:

Meetings dedicated to revision and improvement of this USP were held on 29/03/2023, 29/06/2023, then on 19/07/24.

This USP version incorporates all adjustments based on early and later findings indicated in the Exploitation Plan, and it has been remarkably stable since its first definition.

The competition analysis is articulated but still only shows 'abstract' competition, rather than specific competitors; this is deem provisionally acceptable given the special nature of this asset.

This asset is the one best poised to get an immediate promotion from the signed agreement with intacs and the ASPICE MLE assessment (see below), where comparison and advantages of joint compliance with AI-FSM and ASPICE MLE are investigated.

Very interestingly and significantly, this USP has evolved extending the co-ownership to BSC and EXI and changing its IPR type from Proprietary to Open. This asset has been officially registered in Spain.

This USP has been fully confirmed during a dedicated meeting on 13/06/25.

4.15 IKR03

Item ID	IKR03
Primary Owner	IKERLAN
Other Owner(s)	EXI
IPR Type	Open
For	dependable and CAIS developers in the automotive, railway, industrial and aerospace sectors
Who	need to develop and certify safety automated, heteronomous or autonomous systems integrating DL components
The	**Safety YOLO** library is a basic software re-design/implementation of a subset of YOLO functions in compliance with FuSa standards requirements against SW systematic errors
That	provides a safety software implementation of a subset of YOLO functions for the safe execution of DL-models.
Unlike	software implementations of DL-libraries such as the basic YOLO library itself
Our	safety YOLO library provides a safety software design and implementation, that integrates a structured and layered software architecture, for the deployment of DL-components.

Exploitation review findings:

Meetings dedicated to revision and improvement of this USP were held on 29/03/23, 29/06/23, 30/08/23, then on 19/07/24.

This USP version incorporates all adjustments based on early and later findings indicated in the Exploitation Plan, and it has been remarkably stable since its first definition.

In July 2023, EXI realized that some of its project results that were not expected to contribute to its own EXI01 USP could be integrated with IKR's exploitable item described in this USP (the cancellation of EXI01 USP does not affect this joint ownership). EXI approached IKR with a proposal to transform this *individual* USP into a bilateral, collaborative USP between EXI and IKR. Negotiations followed and a final version was agreed upon based on an intended Open-Source licensing model.

This USP has been fully confirmed during a dedicated meeting on 13/06/25.

4.16 IKR04

Item ID	IKR04
Primary Owner	IKERLAN
Other Owner(s)	EXI
IPR Type	Open
For	dependable and CAIS developers in the railway sector
Who	need to develop and certify safety automated, heteronomous or autonomous systems integrating DL components
The	**RailDemo** is a railway use case open demo
That	is based on the ROS2 architecture and consists of four main nodes: the video player (or the camera output simulator), the object and track detection node, the stereo depth estimation node and finally the safety function node.
Unlike	other railways demos such as *Open Rails' Demo-Model-1, OpenBVE's train simulator, Libre TrainSim*, which are not AI-based,
Our	decision function node can identify whether the detected obstacles are critical or not, whether they are on top of the segmented tracks or are off the rails, and act with appropriate alarms, within ODD-compliant safety scenarios that are verifiable with test suites.

Exploitation review findings:

A meeting dedicated to the implementation of this new USP were held on the 19/07/24.

This USP is one of the three USPs that have been defined to exploit the three sectoral use-cases.

The primary owner is IKR as responsible of the use-case, EXI is co-owner due to its contribution to the ODD-based railway scenarios.

The original Open status has been fully confirmed on 13/06/25.

The Railway Demo has been the subject of a formal ASPICE MLE Assessement on 16-17/09/25, and the CL1 target has been successfully achieved, augmenting the appeal of this USP as an appealing demonstrator also in industrial sectors.

4.17 AIKO01

This USP has been cancelled as too generic to justify the significant extra efforts being allocated to its development.

It was present in the Exploitation Plan, but AIKO has later decided (with the support of the Exploitation Manager) to focus on the following two USPs.

(Note: Original AIKO01 description can be retrieved in D6.2)

4.18 AIKO02

Item ID	AIKO02
Primary Owner	AIKO
Other Owner(s)	-
IPR Type	Proprietary
Partner	AIKO
For	space industry companies employing assets which require navigation and control (Earth Observation, Telecommunications, Space Debris Collection and Removal, In-Orbit Servicing, etc.)
Who	need algorithms for enabling autonomy in their missions
The	**JANE** autonomous navigation application is an AI software implementing algorithms for navigation
That	makes space assets more autonomous and reactive and reduces the effort of ground staff.
Unlike	AI-solutions for autonomous navigation, pose estimation and object detection developed by innovative companies like *SCOUT Space, Rogue Space Systems and LMO Space*
Our	AIKO autonomous navigation application enables space critical systems with safe and explainable AI for their navigation operations, complaint to ECSS standards for space software verification and validation (ECSS-E-ST-10-02C), dependability and safety (ECSS-Q-HB-80-03A).

Exploitation review findings:

Meetings dedicated to revision and improvement of this USP were held on 29/03/23, 28/06/23, then on 24/07/24.

This USP was deeply revised before M24 and now addresses all previously unaddressed findings from the first review.

This USP has been fully confirmed during a dedicated meeting on 04/06/25.

4.19 AIKO03

Item ID	AIKO03
Primary Owner	AIKO
Other Owner(s)	
IPR Type	Proprietary
For	the space industry entities, both commercial companies and public agencies
Who	need algorithms for enabling autonomy in their missions
The	**SpaceDemo** is a critical Guidance, Navigation, and Control (GNC) Space Demo
That	that can detect the target to provide accurate information on its position and distance from the agent and operates at a safe distance to avoid crashing or damaging the assets.
Unlike	other examples such as *Mathworks' Simulated UAV* and *Lunar Module Digital Autopilot* which are neither AI-based, nor considering safety integrity level,
Our	demo component can produce labelled data for the use case, with pictures comprising a target spacecraft and a background showing deep space and Earth, in different perspectives, in ODD-compliant safety scenarios that are verifiable with test suites.

Exploitation review findings:

A meeting dedicated to the implementation of this new USP were held on the 24/07/24.

This USP is one of the three new USPs that have been defined to exploit the three sectoral use-cases.

During a new meeting on 04/06/25, AIKO expressed reservations about the opportunity of classifying this demo as open on the ground that all the catalogue of examples would contain too much AIKO's owned industrial secrets. It was therefore decided that the best option is to reclassify this specific *SpaceDemo* as proprietary, but in exchange to provide the so-called *CoreDemo* (see above BSC06) with a generous subset of significant space examples.

The owner is AIKO as responsible of the space use-case.

4.20 RISE01

Item ID	RISE01
Primary Owner	RISE
Other Owner(s)	-
IPR Type	Open
For	Industry and research communities in safe and explainable AI
Who	need to use AI techniques for safety critical systems,
The	**EXPLib** is a research software platform in the form of an opensource repository containing methodology and tools enabling the use of XAI techniques
That	provides a knowledge base and approach for using XAI to support the application of AI-based components in safety critical systems, including a Satellite docking Toy Model.
Unlike	Existing best practices and opensource libraries about explainable AI (such as *Alibi, AIX360, Xplique*)
Our	**EXPLib** focuses on a systematic approach to applying Explainable AI techniques for supporting different stages of the DL safety lifecycle, including a proposal of evaluation metrics.

Exploitation review findings:

This USP is the final elaboration of the original RISE USP.

Meetings dedicated to the revision and improvement of this USP were held on 29/03/2023, 23/06/2023, then again on 10/07/24.

This USP has been revised and addresses all expected aspects: although maintaining its generic category of "research platform", it's further specified as an open-source repository.

This USP has been fully confirmed during a dedicated meeting on 10/06/25.

Compared with BSC03 (DLETLib), this USP is more oriented towards XAI techniques with a complete Space toy model, while BSC03 (DLETLib) is more oriented to show full integration with SAFEXPLAIN-developed SW middleware.

5 USPs Summary Table

This table summarizes the most critical attributes of the sixteen USPs identified and confirmed since the start of the project. In the column STATUS, 'confirmed' means compared to previous Interim Report, 'new' means introduced in this last year (but all are confirmed now).

USP	Name	STATUS	NATURE	IPR TYPE	OWNER	CO-1	CO-2	CO-3
BSC02	**pWCET-AI**	confirmed	code	open	BSC			
BSC03	**DLETlib**	confirmed	code	open	BSC	EXI		
BSC04	**SemDRlib**	confirmed	code	open	BSC			
BSC05	**ROSGUARD**	new	code	open	BSC	IKR		
IKR03	**Safety YOLO**	confirmed	code	open	IKR	EXI		
RISE01	**EXPLib**	confirmed	code	open	RISE			
AIKO02	**JANE**	confirmed	code	proprietary	AIKO			
BSC01	**Orin-PMULib**	confirmed	code	proprietary	BSC			
EXI02	**V&V-SCENARIOS**	confirmed	content	open	EXI	NAV	IKR	AIKO
IKR02	**AI-FSM 2.0**	confirmed	content	open	IKR	EXI	BSC	
EXI03	**V&V-TESTSPECS**	confirmed	content	proprietary	EXI			
IKR01	**SPL**	confirmed	content	proprietary	IKR			
BSC05	**CoreDemo**	new	demo	open	BSC	EXI	IKR	RISE
IKR04	**RailDemo**	confirmed	demo	open	IKR	EXI		
NAV03	**CarDemo**	confirmed	demo	open	NAV	EXI		
AIKO03	**SpaceDemo**	confirmed	demo	proprietary	AIKO			

6 IPRs and Licencing Issues

IPRs and Licences for *proprietary* exploitable assets have not been much investigated. It was agreed at an early stage that proprietary assets would not be co-owned and not given any recommendations/indications for licensing.

When organizations choose to stick to proprietary approach, typically confidentiality issues are overwhelming, and the space for common discussion at consortium level are scarce. Also, proprietary licences build on the foundational '*All Rights Reserved*' model, further restricting the scope for common discussion on these issues.

Completely different is the situation with *open* exploitable assets. Here the motivation for wider ownership is strong (9 out of 11 have been declared with joint ownership) and convergence to common open models is welcome and pursued.

All partners interested in open licences have been polled on their preferences/inclinations. Out of the dozens of available models (see e.g. https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses with more than 40 listed models), three of them have emerged as the favourite ones:

1. Apache 2.0 (https://www.apache.org/licenses/LICENSE-2.0)
2. CC BY-NC-SA 4.0 DEED (https://creativecommons.org/licenses/by-nc-sa/4.0/deed.en)
3. GPL v.3.0 (https://www.gnu.org/licenses/gpl-3.0.en.html) and its Affero variant (https://www.gnu.org/licenses/agpl-3.0.en.html)

There is not much surprise here, these are among the most known and adopted models worldwide, created and supported by three highly-reputed American no-profit organizations, respectively:

1. Apache Software Foundation (https://www.apache.org/)
2. Creative Commons (https://creativecommons.org/)
3. Free Software Foundation (https://www.fsf.org/)

There is also an emerging pattern in terms of criteria for choice, with *Apache 2.0* for SW Platforms and Demos, *CC BY-NC-SA* for Models and Datasets, and *GPL v.3.0* for SW Library and Tools; however, no definitive conclusions are drawn, and owners reserve the right of the final choice.

7 DevSecOps and Repositories

Associated with the choice of the licencing models (but well distinct from it), there is the choice of the DevSecOps (Development, Security, Operations) SW platforms and the general-purpose repositories where the assets will be made available. Here, too, partners have been polled.

A non-surprising convergence has emerged towards two well-known DevSecOps options:

1. GitLab (https://about.gitlab.com/)
2. GitHub (https://github.com/)

Both options are extremely popular worldwide, not only for Open Software. For the kind of services expected by SAFEXPLAIN assets' owners, they are basically equivalent. GitLab is available as a community edition and a commercial edition, while GitHub, although commonly used to host Open software, it's a proprietary platform.

The two companies operating these DevSecOps (Development, Security, Operations) SW platforms are both headquarted in San Francisco (CA), although with a quite different story. GitLab originated in Europe in 2011, it was originally incorporated in The Netherlands, then it migrated to US in 2015. GitHub started in 2008 in US and was acquired by Microsoft in 2018.

Concerning the general purpose repositories, in this case, happily, one of the most known and reputed options is European, that is to say, Zenodo (https://zenodo.org/), launched in 2013 and operated by CERN (https://home.cern/); all partners have quickly and uncontroversially converged on this choice.

So, to sum it up, *source code and directly related documentation* are being made available in GitLab or in GitHub, while extensive content work products such as *deliverables, guidelines, papers, presentations, models, datasets and so on* are being made available on Zenodo.

> *Note: after the extensive discussion with the partners, on August 11, 2025, Thomas Dohmke announced that he was to step down as CEO of GitHub at the end of 2025, to pursue entrepreneurial endeavors. Most of specialized press is not taking this lightly, fearing a 'Nokia' or 'Skype' final solution from Microsoft. It is too early to speculate and to change abruptly policy, however, after this breaking news, the preference, by default, for SAFEXPLAIN project results, is tilting toward GitLab.*

8 Applicability to other domains

At proposal time, SAFEXPLAIN consortium used the term *CAIS* (Critical AI-based Systems) extensively but informally. Within this intuitively well-defined, but not explicitly scoped field in term of industrial sectors, the consortium identified a significant subset of it: namely *automotive, railway,* and *space.*

These three sectors together do not fully overlap with the wider concept of *transportation*, even less of *mobility*, although they represent a significant high percentage of this quite huge worldwide market (there are several sources on the matter with slightly different estimates, however, there is a convergence that the current size is between 8 and 10 trillion USD – as a reference, about one third of US GDP, and slightly less than 10% of worldwide GDP).

Most of this huge market is safety-critical and – yes – most of it is bracing for applicability of AI-based solutions, for (semi-)autonomy and beyond. So, it is important to consider that the exploration of applicability to different sectors is interesting, but it is not spurred by the limited size of the current market.

The EU AI Act was published (and then adopted) after the start of the SAFEXPLAIN project. Interestingly, it defines the class of *High-Risk AI Systems*, and "*Transportation Systems*: Autonomous vehicles and AI-driven traffic management systems" are one of the three officially given examples, together with *Healthcare* and *Critical Infrastructure* (see e.g.: https://www.euaiact.com/blog/high-risk-ai-systems-under-the-eu-ai-act).

Internal discussion on which extra domains are promising (beyond the ones directly addressed in the project through the user cases developed in WP5) started early and intensified in the last year. A very relevant event that kicked off a more focused discussion was the participation of several consortium's partners to the HIPEAC workshop in January 2025.

The active participation of four SAFEXPLAIN partners (IKERLAN, BSC, EXIDA and RISE) to the HIPEAC workshop on 21/01/25, proved to be extremely successful not only in terms of research-oriented dissemination, but also for exploitation: participants and speakers were not only from academia but also from top industries, with some ideal candidates to become SAFEXPLAIN early users.

Particularly relevant was the one-day session organized by IKERLAN on "*MCS: Mixed Critical Systems – Safe Intelligent CPS and the development cycle*". Out of the many outstanding research results, at least two major exploitation takeaways appeared in all their relevance:

1. *Transportation is quite wider than Automotive, Railway and Space;*
2. *Automotive is today at the forefront in terms of Safety and AI technical standards.*

The first point is maybe more obvious, presentations were covering big sectors already well established (e.g.: *Maritime, including underwater vessels*) and forcefully emerging niches (e.g.: *Drones / UAVs*).

The second point is subtler, until ten years ago the automotive sector was not considered a very high-tech sector, at least compared with other SW-intensive sectors; then the Electric/Connected/Autonomous Vehicle Revolution is changing everything, and it boasts now the most complete set of technical standards for AI-based solutions, and the other transportation sectors are looking at it for guidance and inspiration.

The poker of integrated safety standards, extending functional safety to AI functions:

- ISO 26262 *Road vehicles — Functional safety*
- ISO 21448 *Road vehicles — Safety of the intended functionality (SOTIF)*
- ISO 34502 *Road vehicles — Test scenarios for automated driving systems*
- ISO/PAS 8800 *Road vehicles — Safety and artificial intelligence*

offers an unparalleled support to achieve the coveted "state-of-the-art" (critical in case of litigation) with certifiable qualifications. For those in the know, the current 'rage against the standards' in the automotive communities appears more as a form of 'civilization discontent' (because of the undeniable huge effort) rather than a form of grievance.

Equipped with all these considerations, the strategy to extend applicability to other domains (*beyond those already directly addressed* by the three-project use-cases) is twofold. Even without venturing outside transportation/mobility, there are plenty of 'adjacent' sub-sectors for which the project results can be applied with moderate effort. It is here presented an initial tentative classification:

- VEHICLES
  - Bus and Trucks
  - Agricultural machines
  - Earthmoving machines
  - Road infrastructures

- RAILWAY
  - MRT (Mass Rapid Transit)
  - Railway infrastructures

- AEROSPACE
  - Manned spacecrafts
  - Avionics
  - Drones / UAVs
  - Air traffic and ground control infrastructures
  - Spacecraft control infrastructures

- MARITIME
  - Passengers and Cargo Vessels
  - Underwater Watercrafts
  - Marine traffic monitoring infrastructures

As said, the plate is extremely rich even without venturing outside transportation/mobility; however, thanks to the intense dissemination activities, we have noted striking similarities in open issues and collected expressions of interest for the project results from at least these further domains:

- Robotics
- Medical devices
- Smart manufacturing

The strategy here is of a more 'passive' interest; if other parties are approaching result owners with financed experimentation, no doubt they will be pursued, although the 'business development' approach will be active mostly in transportation.

Last but not least, it is worth mentioning that there are strong indications that the same general SAFEXPLAIN approach to AI-safety for critical systems could be the basis also for AI-security. This is not present only as an objective in Regulations (the AI Act does mention Cybersecurity, and the Cyber Resilience Act mentions AI), but also in the technical literature the two themes are increasingly elaborated together, despite not having much already captured by technical standards.

A presentation at ASPIN 2025, where SAFEXPLAIN was invited to 'premiere' publicly its Core Demo, by Stefan Wild, cybersecurity head of Continental, was titled "*Leveraging SOTIF Activities for Enhanced Cybersecurity*", and his thesis was that significant part of SOTIF, with special reference to ODD-based scenarios, analyses and V&V models, are largely applicable to cybersecurity, too.

This is exactly what three partners of SAFEXPLAIN, namely IKERLAN, EXIDA, and BSC, are going to experiment within in the brand-new Horizon Project #101225866 SHASAI "*Secure Hardware and Software for AI systems"*, due to start on 01/11/25.

Interestingly, this project will have these three following use cases:

a. Agrifood industry: Cutting machines.
b. Health: Eye-tracking systems in augmentative and alternative communication.
c. Automotive: Tele-operated last mile delivery vehicle.

9 Key Performance Indicators (KPIs)

There were no specific quantitative targets identified in the DoA. They were introduced in the Exploitation Plan, quantified and initially measured in the Initial Exploitation Report at M12. There are now a set of results that can be presented after three rounds of monitoring (comparison presented in 'Measure' column here is against M24).

KPI Short name	KPI description	Measure
#01 Exploitable Results	identified and named exploitable results	16 (+1)
#02 Categories of products	impacted categories of products in the market	6 (+1)
#03 Competitive Products	primary competitive products	41 (+1)
#04 Competitive Orgs	primary competitive organisations	22 (=)
#05 Target User Groups	target groups of customers/users	6 (=)
#06 User-case Scenarios	opportunities in user-case scenarios	3 (=)
#07 Proprietary Products	proprietary products announcements	5 (=)
#08 Open-Source Products	open-source products announcements	11 (+1)

Four KPIs have remained the same, four have slightly further improved.

10 External Relationships: intacs® and VDA

The **intacs®** scheme (https://intacs.info/) is an independent and legally registered nonprofit organization with open and transparent operations in an honorary capacity and a global presence; it also works in strict collaboration with VDA-QMC, the Quality Management Centre (QMC) of the German Association of the Automotive Industry e.V. (VDA) (https://vda-qmc.de/en/) for the coordination and the advancement of the Automotive SPICE standard. SAFEXPLAIN signed an early NDA with intacs to collaborate freely and openly with the **ASPICE MLE Working Group.**

After the successful first pilot training for the intacs® certified machine learning (ML) automotive SPICE® training held on the 30-31 of July 2024 at a training facility near Stuttgart, the WG went into recess until the year end. (The pilot course was the official international debut of the ASPICE MLE Training for ASPICE Assessors worldwide and included significant examples and references to SAFEXPLAIN).

It restarted activities on February the 13th, with the SAFEXPLAIN member invited again; this time the major tasks were set as the revision of the syllabus made based off the collected feedback and the preparation of the revision of the model itself.

Associated with this participation (although no longer dependent on it), SAFEXPLAIN is self-assessing compliance of own results to ASPICE MLE, to give evidence that AI-FSM approach is compliant not only with ISO 61508 but with the most advanced and coveted mechatronics process quality standard (ASPICE PRM/PAM 4.0).

More specifically, a formal ASPICE MLE assessment was planned by the end the project, with two SPICE assessors affiliated to EXIDA, and the team responsible for the development of the Railway Demo at IKERLAN, are engaged in the assessment process that, given the novelty of the matter, has been split in two rounds, one pre-assessment held on 15/16 July, the formal assessment held on 16/17 Sept.

As per the SPICE regulations, a sponsor was nominated for the assessed org (Irune Agirre), and she is the owner of the results on behalf of IKR. She has authorised the lead assessor to disclose the feedback report in full, that is reported as **Annex I**.

The results are quite positive, in pre-assessment the CL1 (Capability Level 1) target has been achieved and confirmed in the official assessment in September, with even better practice and attribute ratings.Assessors and practitioners have also gathered important information for more detailed statements on mapping and compliance between ASPICE MLE and AI-FSM.

Major results already achieved by the assessment:

- The new training syllabus of ASPICE-MLE will make systematic use of examples coming from the assessment and the Railway Demo (two members of the intacs MLE WG participated to the assessment as Guest Assessors).

- An invitation has been received to present a paper on the assessment experience at: https://conf.researchr.org/home/profes-2025/quemales-2025 (Quality Evaluation of ML-based Software Systems 2025 – 1-3 December 2025, Salerno , Italy); paper has been submitted and already accepted.

11 External Relationships: Taiwan (MoU with III)

A fully-fledged **Memorandum of Understanding (MoU)** between **BSC** (on behalf of the whole SAFEXPLAIN consortium) and **III** (on behalf of the Taiwanese AI community), was signed by the respective legal representatives in Sept 2024. III, as stated, is not there only representing itself, but it acts as a Taiwanese partners hub for new project proposals and initiatives.

A delegation from III participated to the F2F SAFEXPLAIN meeting in Barcelona, held on May 2025. The delegation, thanks to the MoU that covers also NDA aspects, followed entirely the meeting, where a specific session was dedicated to exploration of reciprocal interests and opportunities.

The SAFEXPLAIN consortium much appreciated the articulated but focused dedicated presentation of key Taiwanese projects.

The Taiwanese *Automotive Edge AI* includes an impressive DL Database. AI Perception results are also extremely relevant and advanced based on fusion of sensing technologies.

AI-based technology solutions designed and manufactured by Taiwanese industries were already partially known, now a better in-depth overview is available to SAFEXPLAIN partners., with special reference to the role of *FAiTH Evaluation Center*.

The final objectives of *FAiTH* are largely complementary with the objectives of SAFEXPLAIN: to assist companies to validate the safety of AI-based critical systems and products.

By and large, also methodologies have similarities; however, even at an initial stage of comparison, two main differences already emerged clearly:

- FAiTH has access to (and maintains) a huge database of real data, while SAFEXPLAIN has limited virtual simulations
- FAiTH tests already manufactured products, while SAFEXPLAIN validation is focused on development phase, capturing failures before start of production

It is therefore believed that there is an ideal complementarity between FAiTH and SAFEXPLAIN.

SAFEXPLAIN would be able to provide an invaluable advantage to FAiTH customers to detect *and correct* design failures (i.e. failed tests) BEFORE the start of production, leading to massive cost reductions. It is not controversial in technical literature that there is at least one order of magnitude of cost impact for defects escalating to each later phase of product lifecycle.

SAFEXPLAIN, on the other hand, would be able to exploit the massive real data of FAiTH and might deploy its highly structured ODD-scenarios and test suites, compliant to the most advanced automotive safety standards (the basic Functional Safety of ISO 26262, the Safety of the Intended Functions of ISO 21448, the AI safety for Road Vehicles as per the brand new ISO 8800), using real world data and not just simulated environments as it is today the case. It would also be able to address the existing gap due to lack of real data in current demos.

It was therefore recommended to further increase the collaboration in the last months of life of the SAFEXPLAIN project, hosting a full Taiwanese delegation at the final event in Barcelona (see: https://safexplain.eu/final-event/), paving the way for new structured forms of collaboration after the completion of the European project. This plan materialised with a delegation of four people from Taiwan attending the Final Event and an extra day entirely dedicated to the exploration of future collaborations.

In this occasion, III presented another extremely interesting set of slides on ongoing Taiwanese projects built around the FORMOSA dataset, and proposed a specific scheme for collaboration, that SAFEXPLAIN's more directly interested partners are actively considering; a monthly consultation mechanism has been agreed.

A selection of slides from III presentations in Barcelona (in May and in September) are reported as **Annex II**.

Annex I: Feedback report of the ASPICE MLE Assessment

Assessment Information - Overview

Organization and Project	
Project:	**Railway Demo in SAFEXPLAIN Project** *T53*
Organizational Unit:	**Cybersecurity and Dependability Dept. - IKERLAN**
Sponsor:	**Irune Agirre**
Start / End Date:	**2025-09-16** to **2025-09-17**
Purpose and Context	
Purpose description:	**Process improvement**
Context:	

Assessment Information – Scope

Scope, Instances, and Highest Capability Level	
Assessed Processes, # of process instances in ()	**MLE.1(1), MLE.2(1), MLE.3(1), MLE.4(1), SUP.11(1), SWE.1(1)**
Highest Capability Level:	**1**
Process Assessment Model(s) and Guidelines	
• **Automotive SPICE 4.0**	

Assessment Team

Name	Role	License Number	Assessor Grade
Carlo Donzella	Lead Assessor	IT21-2471-20878-03	Principal
Giuseppe Nicosia	Co-Assessor	IT21-2427-30387-01	Provisional
Fabian Mueller	Guest Assessor	DE21-2471-24169-03	Principal
Chandrasekaran Babu	Guest Assessor	IN21-2419-23185-03	Principal

Rating, Instance: Main Project

ID	Name	BP1	BP2	BP3	BP4	BP5	BP6	BP7	PA1.1	CL
Automotive SPICE 4.0										
SWE.1	Software Requirements Analysis	F	F	F	L	L	L		F	1
MLE.1	Machine Learning Requirements Analysis	F	F	L	P	L	L		L	1
MLE.2	Machine Learning Architecture	L	F	L	L	F	P	L	L	1
MLE.3	Machine Learning Training	F	F	F	L	L			F	1
MLE.4	Machine Learning Model Testing	F	F	F	F	F	L	L	F	1
SUP.11	Machine Learning Data Management	F	F	F	F	L	L		F	1

PRE-ASSESSMENT SITUATION

ID	Name	BP1	BP2	BP3	BP4	BP5	BP6	BP7	GP1.1.1	PA1.1	CL
Automotive SPICE 4.0											
SWE.1	Software Requirements Analysis	L	L	P	P	L	L		L	L	1
MLE.1	Machine Learning Requirements Analysis	L	L	L	L	P	L		L	L	1
MLE.2	Machine Learning Architecture	P	F	L	L	F	P	L	L	L	1
MLE.3	Machine Learning Training	L	F	F	P	L			L	L	1
MLE.4	Machine Learning Model Testing	L	L	F	F	F	L	L	L	L	1
SUP.11	Machine Learning Data Management	L	L	F	F	L	L		L	L	1

Scope and Premises

- *This assessment has a significant list of unusual premises:*
  - the project is an R&D demo, not not an industrial product
  - it is a Railway, not an Automotive project
  - processes have been originally described according to another model, AI-FSM
- *The scope is purposedly limited to the 4 new MLE group processes and the new SUP.11 (plus SWE.1), and to CL1*
- *Beyond the main obvious objective of assessing ASPICE compliance, there are other aims:*
  - *examples and lesson learnt to ASPICE MLE intacs WG*
  - *open materials for a GATE4SPICE event*
  - *content for a paper models comparison at QUEMALES int. conference (Dec 2025)*

ASPICE MLE and AI-FSM (I)

- During the July pre-assessment, it was noted that the complexity of the mapping between ASPICE MLE and AI-FSM is muchhigher than previously thought and some general hints on how to cope with were given
- Following this full assessment, more precise indications have been collected and will be fed to both AI-FSM and ASPICE MLE responsible in order to facilitate convergence
- More specifically, two major 'process structural weaknesses' have been noticed for AI-FSM:

ASPICE MLE and AI-FSM (II)

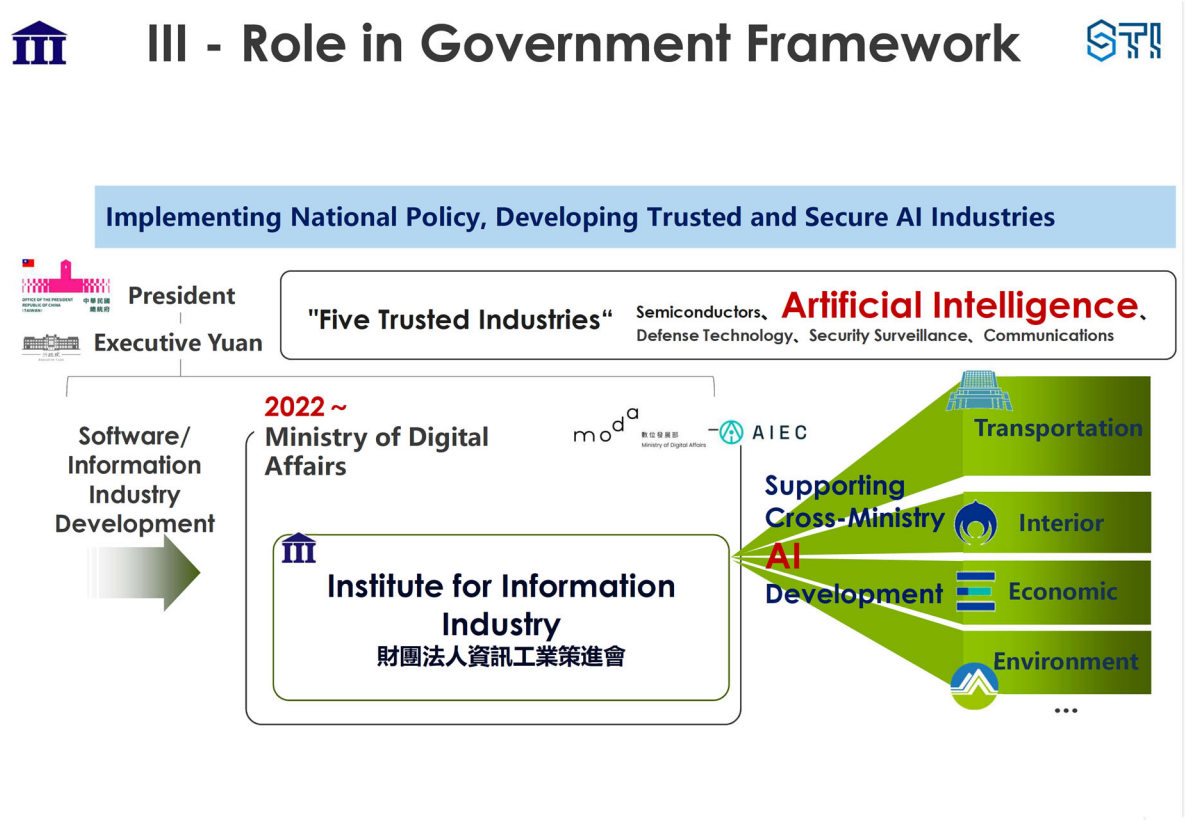
- The process Ph2 is called "Requirements Specification" but, in fact, it abuses/misuses (i.e.: it stretches excessively) the meaning of 'requirement'; whatever is expected to be specified is called requirement. This makes almost impossible to apply the strict rules of 'good requirements' to be systematically applied and verified to all type of (improperly defined) requirements. It should be better just call it "LM Specifications" and have chapters on properly said requirements, but also on design aspects, inspection criteria, verification measures, etc…
- This goes hand in hand with the previous point, ML Architectural Design, that in fact does not exist as such… all aspects of design are absorbed into 'requirements', making almost impossible to be compliant to all practices of MLE.2; content is mostly there but specific design analyses and traceability are hard to be identified. With a dedicated 'design' chapter within "ML Specifications", this could be amended with limited impact on the overall model.

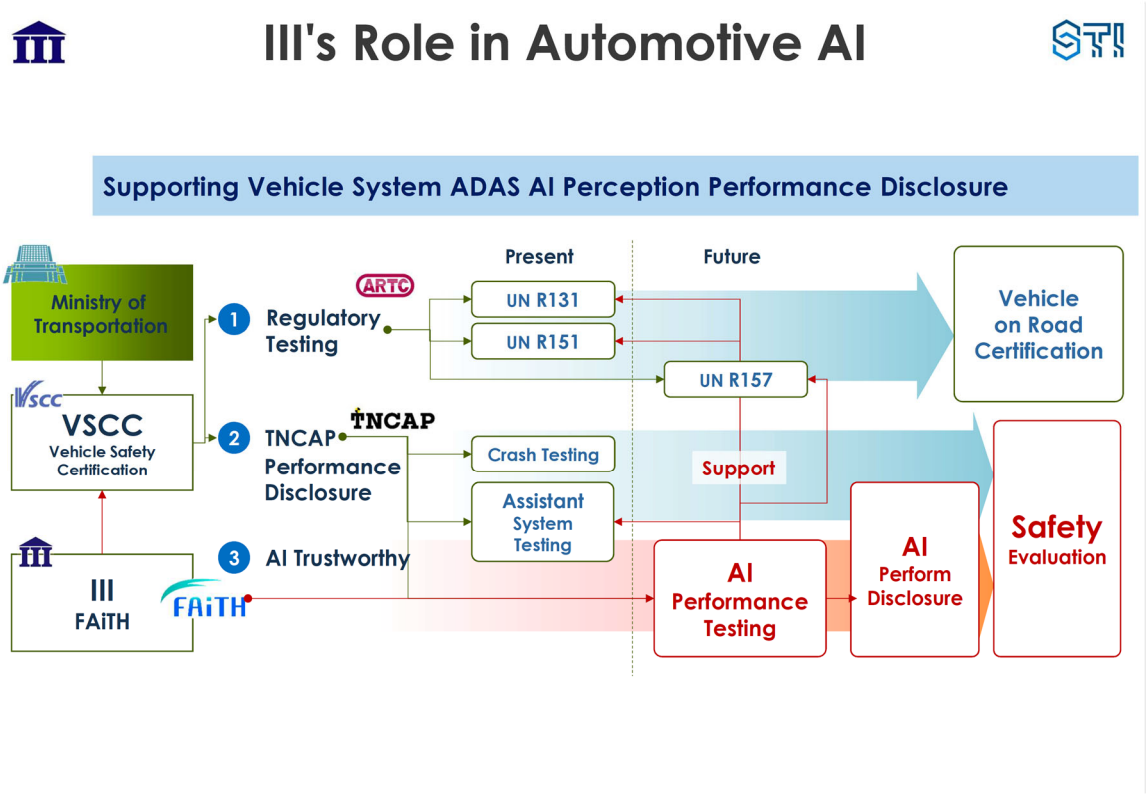
Conclusions

- Against all odds, all processes have achieved CL1, and four of them have further improved PA1.1 rating from "L", to "F".
- This major result has been achieved with dedicated effort to recommendations given at the pre-assessment
- The remaining weaknesses are related to 'unmitigated' mapping issues between AI-FSM and ASPICE MLE (see previous slides)
- The targeted objectives for the organisation of an ASPICE assessment with such unique characteristics have been therefore fully achieved
- The assessment team wishes to congratulate the assessed team for the dedicated effort and to warmly thank the guest assessors (also members of the ASPICE MLE intacs WG) for their kind availability to participate as observers

Annex II: excerpts from the III presentations in Barcelona

From the presentation in May:





FAiTH – Formosa AI Trustworthy Hub

On **July 22, 2024**, Taiwan's automotive electronics industry collectively voiced their expectation for the Institute for Information Industry (III) to **establish a software assessment center** that aligns with international **development of assessment processes** and verification, promoting the enhancement of Taiwan's domestic vehicle industry value chain

Consensus across Taiwan's automotive sector

- **5 Association** (TEEMA、TTIA、TADA、TEVIA、ITS Taiwan)
- **5 ADAS** (oToBrite、CHIMEI-Motor、Alpha Network、WHETRON、CubTEK)
- **5 Chipset** (Sunplsus、ELAN、iCatch、Kneron、eYs3D)
- **4 Accreditation** (SGS、DEKRA、TUV Nord、TUV Rheinland)
- **3 Intelligent Cockpit** (AUO、INNOLUX、FIC)

Assessment of AI recognition accuracy and reliability

Poor visibility at night, raindrop obstruction

Blurred image quality, high recognition difficulty

Complex object types, judgment errors

AI accuracy

Weather Image quality

Real-World Test

Comprehensive vehicle test outcomes

AI Perception Testing

Testing for AEB, BSIS AI Perception Modules (Image-based)

Products for vehicle
- OEMs/Tier1/Module
- Other interests groups

ADAS AI Model

Test Report

BSIS AI Testing
R151

FAiTH 未來移動安全信賴評測中心

Testing

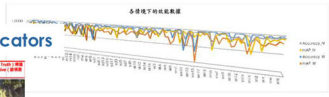
Result

Formosa Dataset (Taiwan Scenario Data)

Analysis → Test Scenarios → Testing Framework → Performance Evaluation

Testing Process/Tools

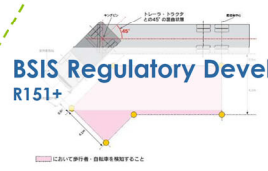
Testing Mechanism/Indicators



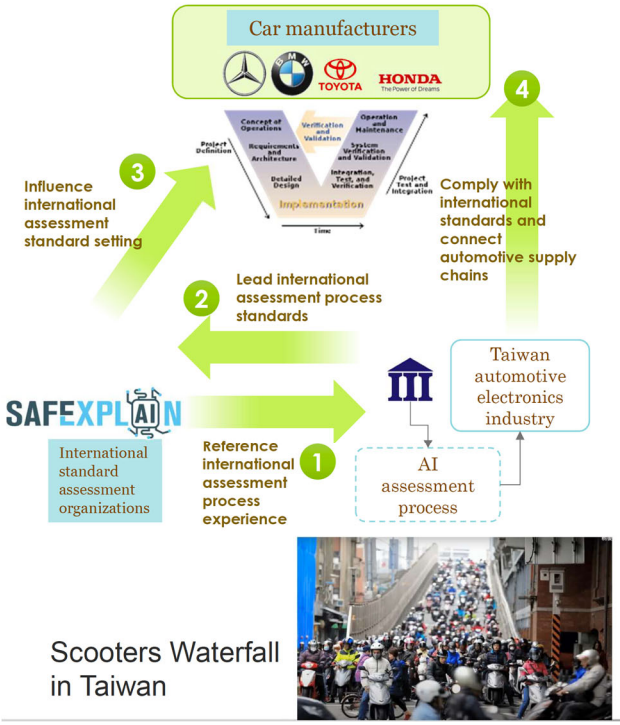
Scenario Selection

Data Analysis

BSIS Regulatory Development
R151+



Automotive Software Assessment



Scooters Waterfall in Taiwan

- **Develop AI assessment methods** and related standards needed for "domestic" automotive electronics industry
  - Combined with III's technical experience in AI development and testing, plus our rich road data, together we can develop AI assessment methods and standards needed by Taiwan's automotive industry.
- International standard assessment organizations can **incorporate III's assessment methods** into their standard guidance templates
  - This can help "domestic" automotive electronics industries quickly pass evaluations and increase opportunities to secure "international" orders.
- Empower "domestic" automotive electronics industry **capability and quality improvement**
  - Through feedback from International standard assessment organizations. III can modify and enhance assessment methods, further empowering "domestic" automotive electronics industry capabilities and quality.
- **Join international AI assessment standard** setting through International assessment organizations
  - By jointly designing AI assessment process methods and standards, and proving feasibility with assessment data from Taiwan's diverse real traffic environments, we can advocate for related regulations domestically and join international AI assessment standard setting through assessment organizations .

Assessment Process Overview

*Testing with **real street scenes** to understand **AI perception** safety limits*

1 Product Assessment Analysis
- Specification analysis
- Regulatory target mapping

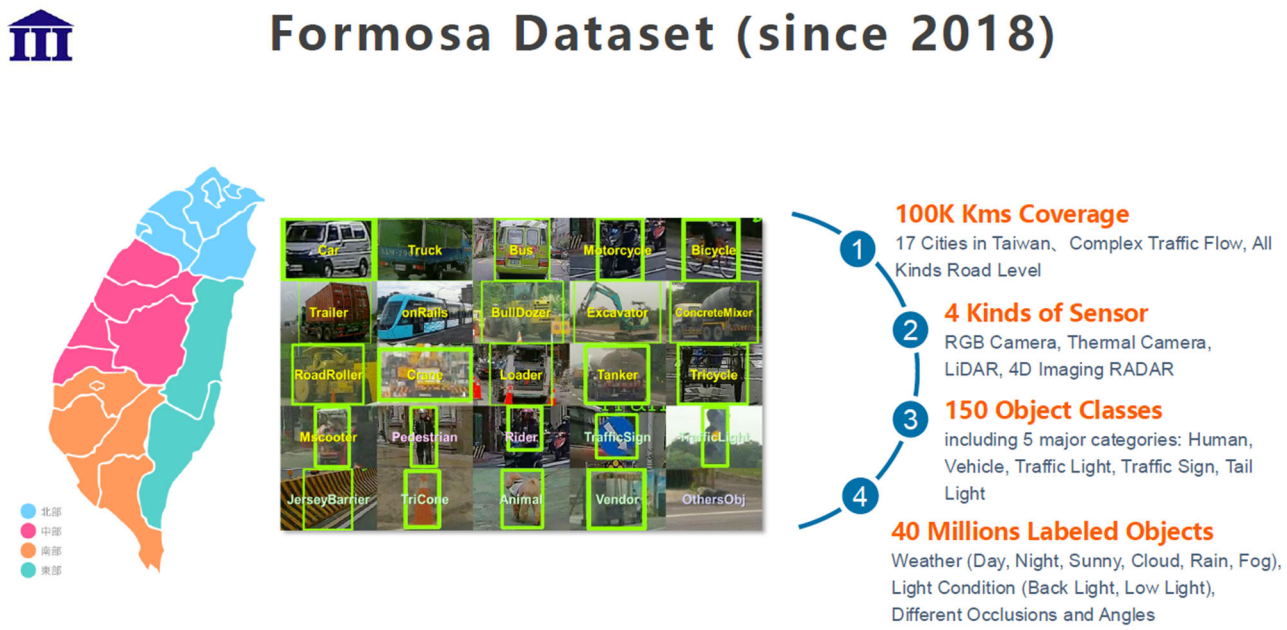
3 Assessment Content Definition
- Assessment scenario definition
- Standardized test data analysis

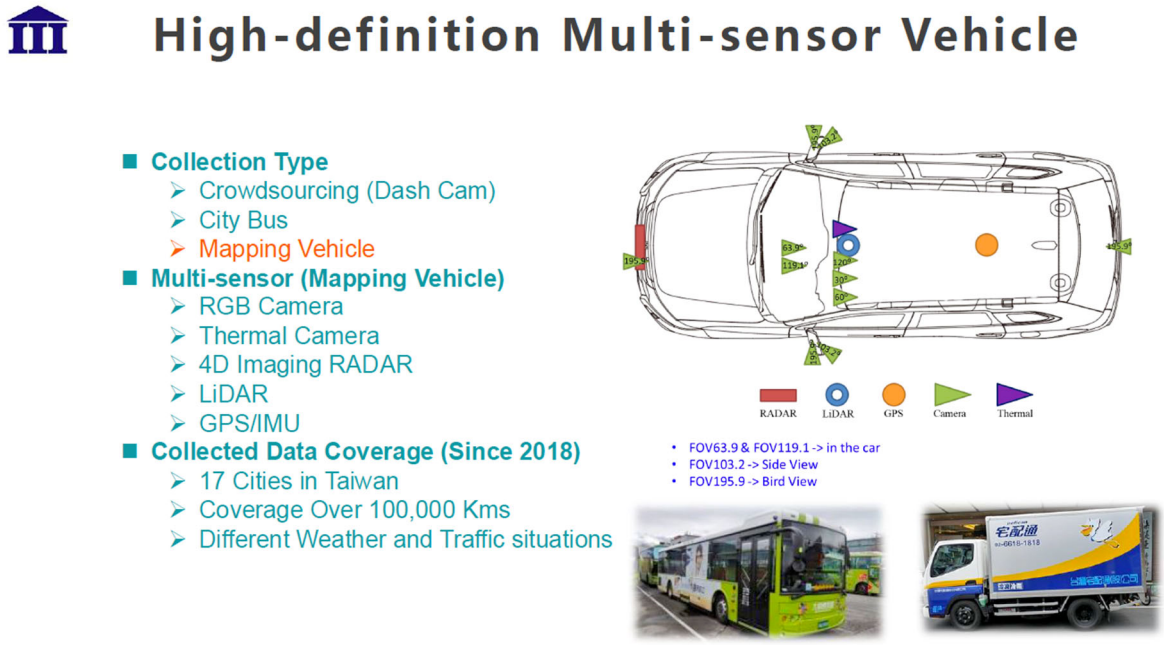
5 Assessment Result Analysis
- Assessment data compilation
- Quantitative chart analysis
- Qualitative semantic analysis
- Final assessment report"

2 Data Collection
- Perception data collection
- Perception scenario planning

4 Product Testing
- Test case output interface
- Test result input
- Initial data analysis check

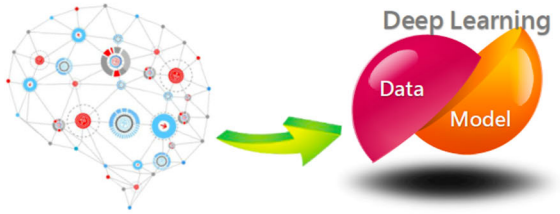
From the presentation in September:

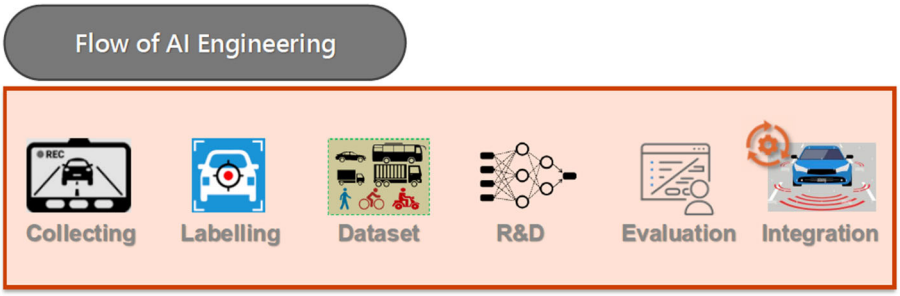




AIOps

Own Data Team, own multi-sensor labeling platform

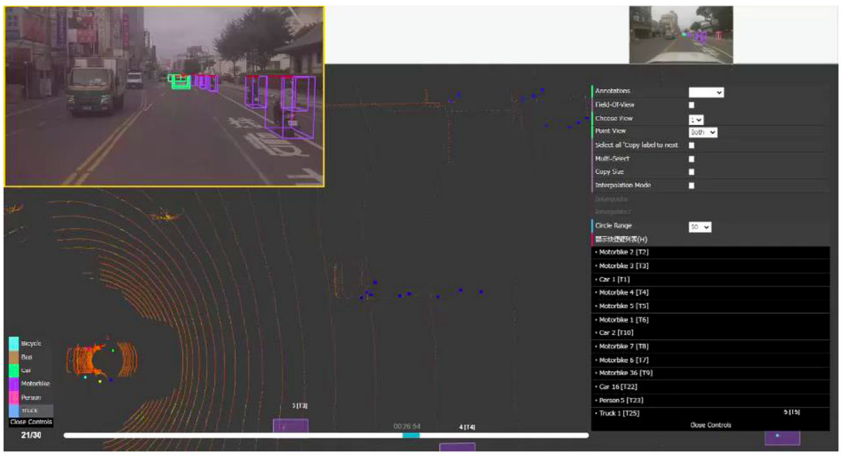




Formosa Dataset

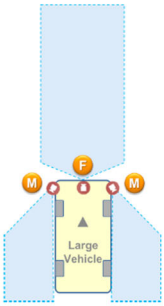
Multi-Sensor Data Annotation Platform

- **Specification**
  - 2D Bounding Box/Polygon (for Image)
  - 3D Point Cloud Cube (for RADAR & LiDAR)
  - Pre-labeling Function
  - Projection Matrix for Multi-sensor



Driving Risk Analysis for Highway Bus

Collaboration with NYCU for MOTC project (since 2021~now)



Low Resolution

High Noise

Rear Side

Rainy Day

III Dataset to Simulation

Collaboration Concept

Real-World
Street Scene Data

Source: Collected in Taiwan's urban environments with multiple sensors (camera, LiDAR, radar, thermal, etc.).

Role: Provides the real-world basis, including vehicles, pedestrians, signals, and road markings.

Follow
OpenLABEL

Purpose: Annotate data using the ASAM OpenLABEL standard.

Content: Objects, behaviors, and environmental conditions.

Value: Unified labeling format across modalities for flexible usage.

Conversion
OpenSCENARIO

Purpose: Transform annotated events into reproducible, parameterized scenarios.

Example: "A vehicle turns right at an intersection while a pedestrian crosses."

Value: Enables generation of large-scale test cases

Integration with
CARLA

CARLA: Open-source platform

Role: Load scenarios (**OpenSCENARIO**) and road networks (**OpenDRIVE/OSM**) into the simulator, enabling interactive closed-loop testing.

SAFEXPLAIN
Validation

SAFEXPLAIN : For large-scale scenario analysis and explainability assessment.

Provides certification expertise, structuring evidence into Safety Cases (ISO 26262 / SOTIF) for regulatory approval.

Annex III: Acronyms and Abbreviations

- ADAS – Advanced Driver Assistance System
- CA – Consortium Agreement
- CAIS - Critical AI-based Systems
- D – Deliverable
- DoA – Description of Action (Annex 1 of the Grant Agreement)
- EB – Executive Board
- EC – European Commission
- FuSa – Functional Safety
- GA – General Assembly / Grant Agreement
- HPC – High Performance Computing
- IPR – Intellectual Property Right
- KPI – Key Performance Indicator
- M – Month
- MS – Milestones
- OEM - Original Equipment Manufacturer
- PM – Person month / Project manager
- TRL – Technology Readiness Level
- WP – Work Package
- WPL – Work Package Leader
- XAI – Explainable Artificial Intelligence