D6.7 Intermediate Exploitation Report

Version 1.0

Documentation Information

Contract Number	101069595
Project Website	www.safexplain.eu
Contractual Deadline	30.09.2024
Dissemination Level	PU
Nature	R
Authors	Carlo Donzella (EXI), Valeria Dallara (EXI)
Contributors	all partners
Reviewer	Irune Yarza (IKERLAN)
Keywords	exploitation, IPs, IPRs, copyright, licences, safety, dependability, AI, CAIS, software, OS, railway, space, automotive

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

Change Log

Version	Description Change
V0.1	Initial draft
V0.2	Reviewed version
V1.0	Final version

Table of Contents

1 Executive Summary

Task 6.2 “Exploitation activities”, that runs from M1 to M36, has a strong business approach, to the extent allowed by the nature of this R&D project. One of its major aims is to analyse the exploitation context and business opportunities to understand the actual market situation. 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. All this is very much in line with traditional, 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, and 4) preparing a handbook that establishes 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.

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.

Both D6.2 and D6.6 set out to analyse the exploitation context and business opportunities to uncover the current and potential market situation. Based on this analysis a methodology and strategy for the appropriate management of knowledge generated by the project (IP) was defined.

This Interim version of the Exploitation Report (D6.7) is an evolution of the D6.6 Initial Exploitation Report, which was issued in September 2023. As described in its previous version, this document is dedicated to coordinating all partners' effort toward the collective and individual exploitation of the project's results. This second version of the Exploitation Report corresponds to the planned annual update of its previous version.

The current Exploitation Report analyses the progress of the partners’ previously introduced exploitation context and business opportunities, their successes and developments, and sets the frame for the next and final twelve-month period leading to project’s natural completion.

2 Exploitation Strategy at M24

Great advancements have been made in exploitation thanks to ongoing activities that maximize exploitation activities, particularly the identification of the core exploitable results and the pursuit of external relationships with early adopters and target users thanks to the task leader´s deep understanding of the context and business opportunities on the field. An overview of the activities pursued as part of these tasks is detailed below.

Exploitation activities have been planned, since the start of the project and especially after the publication of the Exploitation Plan at M6, 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, session 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 a 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 this 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.

3 Exploitation Results at M24

As per today (M24), the consortium's partners (specifically, Partner Exploitation Managers supported by the Project Exploitation Manager) have reviewed, revised and reclassified the Exploitable Items into **15** core exploitable results, classified into **5** (up from **3**) major categories:

1. Open Source Software (**5**)
    1. **pWCET-AI by BSC**: a novel probabilistic timing analysis tool
    2. **Orin-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. **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
    5. **XAI for Safety by RISE**: a research 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 (**3**)
    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. **NIE GuardAI by NAVINFO**, a platform comprised of specialized AI modules for developing and assessing safe and explainable ADAS systems that complies to the FuSa and explainability requirements
3. Proprietary Content (**2**)
    1. **AI-V&V-TESTSPECS by EXIDA:** a full set of tests specification
    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
4. 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. **AI-V&V-SCENARIOS by EXIDA & NAVINFO, IKERLAN, AIKO**: a catalogue of ODD-described automotive, railway, space scenarios
4. Open Demo (**3**)
    1. **AODemo by NAVINFO & EXIDA:** an automotive use case open demo
    2. **RODemo by IKERLAN & EXIDA:** a railway use case open demo
    3. **SODemo by AIKO & EXIDA:** a critical Guidance, Navigation, and Control (GNC) component of an open 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 (e.g. event participations planned for M24-M36), 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, that include the following highlights:

- A section on "*Other standards and regulations*", including a dedicated slide entirely developed by the member nominated by SAFEXPLAIN;
- A first pilot training held in July 2024, where trainers were the WG members;
- The course scheme material will become the only authorized model for qualifying ML ASPICE assessors worldwide;
- All of the major "challenges" for the use of the ML/DL techniques included in the training material come from NAVINFO and will be presented as results of the SAFEXPLAIN collaboration;
- A "grandfathering" scheme that will allow SAFEXPLAIN to self-assess compliance of own results to ASPICE MLE thanks to the participation of a principal assessor who is member of SAFEXPLAIN in the WG.

SAFEXPLAIN is also actively participating in discussions and trends in AI and Safety in standards coming from **international standardization bodies ISO and IEC**. An exida group member who is knowledgeable in the SAFEXPLAIN perspective is a delegate of a 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)

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 M24

In this second version of the Exploitation Report, the consortium is presenting 15 USPs, 7 of which are brand new USPs. 3 USPs presented in previous editions have been cancelled (far from being a negative sign, this represents the ability of project partners to dynamically align with both project evolution and market analyses).

3 new USPs are all based on a simplified – but fully operative and open license - demo version for the three project use cases. What the consortium wants as the main exploitation objective for the upcoming year is to each have an open demo to be made publicly available. The consortium wants to have USPs that are usable, runnable and publicly available.

All partners have agreed that each USP has to be defined genuinely and honestly, with appropriate efforts, with a small disclaimer: USPs are not exploitation schedules with timing end-result attached. This means that their actual implementation won't be necessarily foreseen within the lifecycle of the project, because the work that needs to be done has not been precisely estimated, which means that as of now, it is not possible to know if there is enough budget left by the end of the project for a full implementation of the USPs.

USPs are statements of exploitation interest. All new USPs described in this document, confirmed or new, are considered feasible and of business interests for the indicated owners; just their actual full implementation will be dependent on availability of resources, meaning that some of them might need 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 and D6.6.

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 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 D6.6)

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	**AI-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. 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 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	**AI-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.

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

EXI02 is related to Test Specifications, and they are fully owned by EXI. Some of them are used in the open demo USPs (see below).

EXI02 (differently from EXI03) 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.

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 initial thoughts on a licencing model have already been discussed internally.

This USP has been fully confirmed during a dedicated meeting on 24/07/24.

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.

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 was previously non-existent and is quite complete (even with categories of competitors) and initial thoughts on a licencing model already being discussed internally.

This USP has been fully confirmed during a dedicated meeting on 24/07/24.

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 (similar 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.

This USP version already 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.

This USP has been fully confirmed during a dedicated meeting on 24/07/24.

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 DL models
That	applies a number of 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 is a new USP for BSC, their fourth one.

A meeting dedicated to revision and improvement of this USP was held on the 24/07/24.

BSC plans on making the prototype for this USP, test the functionality to see which results they can get, and then apply the exploitation through consultancy and bilateral projects.

Classified as open source.

4.8 NAV01

Item ID	NAV01
Primary Owner	NAVINFO
Other Owner(s)	-
IPR Type	Proprietary
For	Critical autonomous AI-Based Systems (CAIS) solution providers (Engineers, AI researchers and developers) for the autonomous industry
Who	plan to design vision-based models with explainability and safety in mind and evaluate the reliability and safety of their AI system
The	**NIE GuardAI** is a platform comprised of specialized AI modules for developing and assessing safe and explainable ADAS systems that complies to the FuSa and explainability requirements.
That	provides the foundational AI components for developing explainable perception models (e.g., CNN layer, pretrained feature extractors, decoders), and evaluation protocols for extensively assessing them for adherence to functional safety.
Unlike	Other software tools (e.g. *PyTorch*), which utilizes DL components that do not adhere to the safety and evaluation frameworks (e.g *Neurocat, Bosch AI Shield*) that only assess the models for adversarial robustness under laboratory settings,
Our	Framework allows the solution providers to develop and evaluate customized production-ready AI based perception systems for their specific use cases and conduct exhaustive safety and explainability assessment on a wider range of vision task in real-world setting, allowing the overall AI system to be safety certified. Additionally, it provides easy integration in existing MLop workflows.

Exploitation review findings:

Meetings dedicated to the revision and improvement of this USP were held on 29/03/23, 02/06/23.

This USP has been deeply revised and addresses most of previously unaddressed findings from the first review.

The beneficiaries section now identifies significant categories more precisely.

A new tentative name has been given to the exploitable result that is better specified both as positioning and as characterization.

Three potential competitors in two categories have been identified (none had been identified previously).

The statement of primary differentiation has been made more elaborated.

This USP has been fully confirmed during a dedicated meeting on 08/07/24.

4.9 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 two USPs.

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)

4.10 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	**AODemo** 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.

This USP is one of the three new 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.

4.11 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.

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 now more articulated but still only shows 'abstract' competition, rather than specific competitors.

This USP has been fully confirmed during a dedicated meeting on 19/07/24.

4.12 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 explicitly consider DL-software
Our	SLDL 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). **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.

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.

Competition analysis is now more articulated but still only shows 'abstract' competition, rather than specific competitors.

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 USP has been fully confirmed during a dedicated meeting on 19/07/24.

4.13 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.

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

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 19/07/24.

4.14 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	**RODemo** is a railway use case open demo
That	is based on the ROS2 architecture and consist 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 is able to identify whether the detected obstacles are critical or not, whether they are on top of the segmented tracks or they 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 new 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.

4.15 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)

4.16 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:

This USP is a new one compared with the previous AIKO01 USP in the Exploitation Plan.

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

This USP has been deeply revised and now addresses all previously unaddressed findings from the first review.

The beneficiaries section now precisely identifies significant categories.

A tentative name that is better specified has been given to the exploitable result.

Three potential competitors have been identified (none were previously identified).

The statement of primary differentiation has been made more specific, including the mention of specific sectoral standards.

This USP has been fully confirmed during a dedicated meeting on 24/07/24.

4.17 AIKO03

Item ID	AIKO03
Primary Owner	AIKO
Other Owner(s)	EXI
IPR Type	Open
For	the space industry entities, both commercial companies and public agencies
Who	need algorithms for enabling autonomy in their missions
The	**SODemo** is a critical Guidance, Navigation, and Control (GNC) component of an Open Space Demo
That	that is able to 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 open examples such as *Mathworks' Simulated UAV and Lunar Module Digital Autopilot* which are neither AI-based, nor considering safety integrity level,
Our	demo component is capable of producing 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.

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

4.18 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 platform in the form of an opensource repository (GPL3 license or equivalent) 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 (SDSL), including a proposal of evaluation metrics.

Exploitation review findings:

This USP is a further 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 deeply revised and addresses all previously unaddressed findings from the first and the second review.

The exploitable result, although maintaining its generic category of "research platform", it's further specified as an open-source repository.

The statement of primary differentiation has been expanded and made more specific.

5 USPs Summary Table

This table summarizes the most critical attributes of the eighteen USPs identified since the start of the project.

	USP	STATUS	IPR TYPE	NATURE	OWNER	CoOwner-1	CoOwner-2	CoOwner-3
1	EXI01	cancelled	proprietary	content	EXI			
2	EXI02	new	open	content	EXI	NAV	IKR	AIKO
3	EXI03	new	proprietary	content	EXI			
4	BSC01	confirmed	proprietary	code	BSC			
5	BSC02	confirmed	open	code	BSC			
6	BSC03	confirmed	open	code	BSC	EXI		
7	BSC04	new	open	code	BSC			
8	NAV01	confirmed	proprietary	code	NAV			
9	NAV02	cancelled	proprietary	content	NAV			
10	NAV03	new	open	demo	NAV	EXI		
11	IKR01	confirmed	proprietary	content	IKR			
12	IKR02	confirmed	open	content	IKR	EXI	BSC	
13	IKR03	confirmed	open	code	IKR	EXI		
14	IKR04	new	open	demo	IKR	EXI		
15	AIKO01	cancelled	proprietary	content	AIKO			
16	AIKO02	confirmed	proprietary	code	AIKO			
17	AIKO03	new	open	demo	AIKO	EXI		
18	RISE01	confirmed	open	code	RISE			

6 Key Performance Indicators (KPIs)

As it was mentioned in the first Exploitation Report at M12, there are now a set of results that can be presented after a year of monitoring.

KPI Short name	KPI description	Measure
#01 Exploitable Results	identified and named exploitable results	15 (+5)
#02 Categories of products	impacted categories of products in the market	5 (+1)
#03 Competitive Products	primary competitive products	40 (+10)
#04 Competitive Orgs	primary competitive organisations	22 (+2)
#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	10 (+5)

Three KPIs have remained the same, five have improved.

7 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.

Sharing SAFEXPLAIN results and including project examples as part of intacs® certification offers an important opportunity for the project to disseminate its findings to a relevant audience who is committed to quality and safety.

The **ASPICE MLE Working Group** has been established and has already produced a complete draft of the course syllabus for internal review: one section on "Other standards and regulations" has been entirely developed by the member nominated by SAFEXPLAIN that has also a dedicated slide.

A first pilot training for the intacs® certified machine learning (ML) automotive SPICE® training was scheduled and held on the 30-31 of July 2024 at a training facility near Stuttgart, where trainers were the WG members.

SAFEXPLAIN partner, exida development, provided invaluable contributions to the two days of pilot training, after months of exchange as part of the intacs® working sub-group.

Exida development was especially proactive in providing evidence from the SAFEXPLAIN project that Machine Learning for Automotive SPICE® is actually able to help improve the ML development quality and for sharing a comprehensive overview of the currently relevant ML standards and regulations.

Major ”challenges” for the use of the ML/DL techniques were included in the training material. All of them came from NAVINFO and were presented as results of the SAFEXPLAIN collaboration, which turned out to be well-received, thanks to their value as the only “real world” examples included in the training syllabus.

Thanks to the participation to this group, the so-called “grandfathering” scheme would allow SAFEXPLAIN to self-assess compliance of own results to ASPICE MLE thanks to the participation of a principal assessor who is member of SAFEXPLAIN in the WG itself.

8 External Relationships: Taiwan (InnoVEX, MoU)

SAFEXPLAIN was invited to give a keynote speech at **InnoVEX** an international event held in Taipei from the 4th to the 7th of June. It is part of the major Computex fair with expected 1,600 exhibitors and 40,000 professional visitors.

The keynote speech had the title “Enabling the Future of EV with Trustworthy AI”, and was opening the “Toward the EV Era” session (LINK).

The invitation to this event came from TÜV Taiwan, which expressed interest in widening collaboration of the SAFEXPLAIN project with TÜV innovation areas, especially in EV.

During the mission, at least another structured meeting was organized with III, The Institute for Information Industry of Taiwan, a powerful private/public organization with thousands of researchers, covering all aspects of IT and very keen on furthering international collaboration in AI.

SAFEXPLAIN was for the first time presented to a fully non-European audience. To be precise, to an Asian-Pacific audience, with specific direct participation from Taiwan (and Greater China), Singapore, Japan, India and Korea.

The presentation was extremely well received, and particularly the “Architecting DL solutions enabling certification/qualification“ goal was considered of extreme interest by most of the participants.

Many organisations have stated expressions of interests, including TÜV NORD Taiwan (LINK) and the Software Technology Dept. of III (Institute for Information Industry – LINK).

The stated interest from III has already evolved into a fully-fledged **Memorandum of Understanding (MoU)** between BSC (on behalf of the whole SAFEXPLAIN project) and III (on behalf of the Taiwanese AI community), that has been already fully negotiated and is being ratified by the signatures of respective legal representatives.

Annex I: SAFEXPLAIN-based excerpts from the ASPICE MLE Syllabus

Real world example: Open-source driver assistance system - openpilot

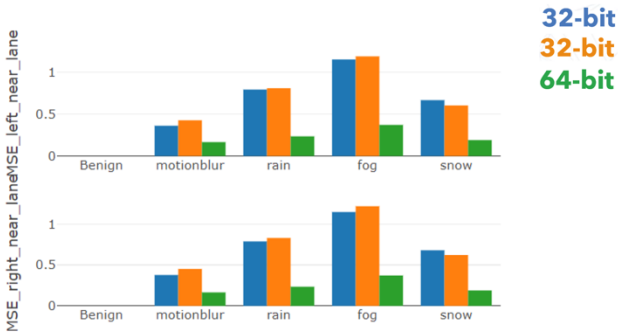
- openpilot is an ML-based system performing functions of:
  - Adaptive Cruise Control (ACC)
  - Automated Lane Centering (ALC)
  - Forward Collision Warning (FCW)
  - Lane Departure Warning (LDW)
- During development the project decided to switch from **64-bit floating point to 32-bit floating point,** to pursue advantages such as *less memory usage, less resources, smaller model* etc.
- All of the measured metrics (e.g., **accuracy**, **precision**) stayed the same or even improved and therefore the switch was made.

OSS Reference: https://github.com/commaai/openpilot

Example courtesy of Navinfo Europe BV, in charge of the SAFEXPLAIN automotive use case in the EU project:

Real world example: Open-source driver assistance system - openpilot

- When evaluating the new version NAVINFO realized that **it seemed to perform worse in suboptimal conditions**,
  - e.g. when motion blur degraded the camera image or rain or snow reduced image clarity.
- The graph on the right shows an error function of lane detection performance
  - a lower bar is “better”
- It shows a stable 64-bit version compared to two different (newer) 32-bit versions.
- You can see that the 64-bit version performs significantly better than both 32-bit versions in suboptimal conditions such as rain, fog, or snow.



Source: Navinfo Europe BV

Example courtesy of Navinfo Europe BV, in charge of the SAFEXPLAIN automotive use case in the EU project:

Example: Emergency Braking – pedestrian recognition (I - TESTPASS)

- Actual simulation developed in the automotive use-case of the Horizon SAFEXPLAIN project.
- The system is designed to recognize **vulnerable road users** and stop the vehicle to prevent collision.
- **Scenarios and test cases** have been developed to verify the behaviour in appropriate **ODDs** (Operational Design Domains).
- In this video, the system recognizes the adult and is able to **actuate the brake in order to avoid the collision**.

Example courtesy of Navinfo Europe BV, in charge of the SAFEXPLAIN automotive use case in the EU project:

15 intacs® certified Machine Learning for Automotive SPICE® | © 2024

Example: Emergency Braking – pedestrian recognition (II - TESTPASS)

- Another actual simulation developed in the SAFEXPLAIN project.
- Same operational situation, but with **suboptimal condition: rainy weather**.
- In this video, the system recognizes the adult and is able to **actuate the brake in order to avoid the collision, in spite of suboptimal weather condition**.
- The system shows similar robustness in other tested suboptimal conditions.

Example courtesy of Navinfo Europe BV, in charge of the SAFEXPLAIN automotive use case in the EU project:

16 intacs® certified Machine Learning for Automotive SPICE® | © 2024

Example: Emergency Braking – pedestrian recognition (III - TESTFAIL)

- Another video in a similar scenario
  - everything is the same but the **pedestrian** is **not** an **adult,** instead it is a **child**.
- The system recognizes the child, but
  - **detection happens too late** and
  - the system is **not** able to **actuate the brake fast enough to avoid the collision**.
- Initial analysis of the error is pointing to the following hypotheses:
  - not enough children in **ML training data**
  - children **physically too small** for the system to detect at a far distance

Example courtesy of Navinfo Europe BV, in charge of the SAFEXPLAIN automotive use case in the EU project:

17 intacs® certified Machine Learning for Automotive SPICE® | © 2024

European authorities have played a major role in AI Regulations

European Commission (EC) published the seminal ***Ethics guidelines for trustworthy AI*** in April 2019.

German Federal Ministry for Justice and Consumer Protection followed suit, with ***Opinion of the Data Ethics Commission*** in October 2019.

A draft of ***Regulation 2019/2144*** governing "*modern technologies used in vehicles, including specific requirements for automated and fully automated ('driverless') vehicles and the systems they employ, to ensure that they are safe to use*", was published on ***27 November 2019*** *(final regulation adopted on 06 July 2022).*

A proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on "*adapting non-contractual civil liability rules to artificial intelligence*" (AI Liability Directive) was published on ***28 September 2022*** *(in discussion).*

*….and especially now we have the world-famous **EU AI Act**:*

- Proposal by EC on 21/4/2021; Approved by EU Parliament on 09/12/2023; Final text on 13/03/2024
- Official name: ***REGULATION LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE***
- Final text: *459 pages, 180 Whereases, 68 Definitions, 113 Articles*

Some relevant aspects of the EU AI Act

The AI ACT *is the first attempt at regulating AI, worldwide*

The AI ACT *is of staggering complexity in terms of aspects to be considered/covered*

The AI ACT *calls for huge efforts in terms of new definitions, practices, rules (including ad hoc new 'harmonised technical standards')*

Whereas (12) attempts to define 'AI systems', distinguishes it from "*simpler traditional software systems or programming approaches*" and insists on the fact that it "*should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations*".

It continues by stating that "*The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved.*"

Full final text of AI Act available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

Complementary ML models, incorporating FuSa life-cycle: SAFEXPLAIN

- In Oct 2022, the **EU Horizon project SAFEXPLAIN** kicked-off, with the aim of providing methods to allow **FuSa certifications of Autonomous AI-based Systems (CAIS)** in cars, trains and satellites.
- It is proposing an **extension of the traditional FuSa life-cycle** that incorporates the new MLE processes, positioning such model somewhat in between the ASPICE MLE model and the EASA model.

More details at:
https://safexplain.eu/

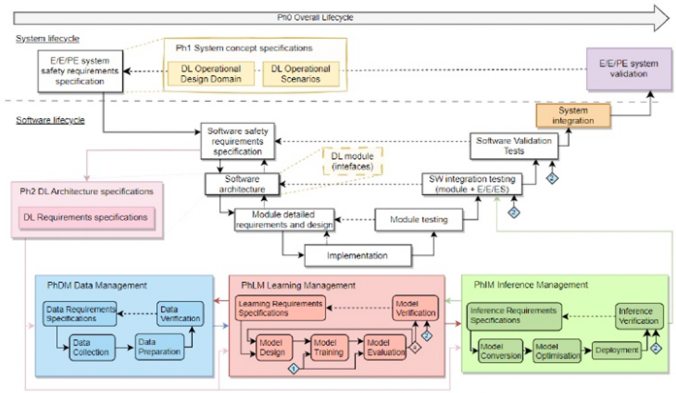


Figure 4. Mapping AI lifecycle with traditional functional safety lifecycle

SAFEXPLAIN
Safe and Explainable Critical Embedded Systems based on AI

Annex II: excerpts from the MoU between SAFEXPLAIN and III (Taiwan)

MEMORANDUM OF UNDERSTANDING

Regarding Collaboration and Cooperation
In the field of Trustworthy AI for Critical Systems
Between SAFEXPLAIN and III

INTRODUCTION

The SAFEXPLAIN Horizon Project (101069595), represented here by its coordinating partner Barcelona Supercomputing Center – Centro Nacional de Supercomputación (hereinafter referred to as “BSC-CNS”) […], Spain, of the one part, and the Institute for Information Industry (hereinafter referred to as “III”) […], Taiwan, of the other part, hereinafter referred to as the "Parties", having recognised the key role that Trustworthy AI for Critical Systems shall play in economic and social development and the benefits of a strategic partnership between EU and Taiwan, have reached the following understanding:

[…]

OBJECTIVE
2. The parties will

(a) Promote cooperation in Trustworthy AI for Critical Systems in areas of mutual interest, especially those relevant to economic and social development;
(b) Promote exchange of information in supporting Trustworthy AI for Critical Systems development; and
(c) Facilitate staff interactions amongst relevant R&D centers, innovation agencies, industry and business sectors; and
[…]

METHODS
3. In order to pursue the objectives listed in paragraph 2 above, the parties will:

(a) Encourage and support increased interaction between EU’s and Taiwan’s organizations with specific interests in Trustworthy AI for Critical Systems through facilitating visits, exchange of delegations, favour participations to relevant events in each other’s countries;

(b) Promote the identification of projects that can attract funding to support Trustworthy AI for Critical Systems collaboration between EU and Taiwan; and

(c) Instigate the joint examination of the interest in establishing networks for Trustworthy AI for Critical Systems to represent them on regional bases in the EU and in Asia-Pacific region.

[…]

Annex III: Acronyms and Abbreviations

- CA – Consortium Agreement
- D – Deliverable
- DoA – Description of Action (Annex 1 of the Grant Agreement)
- CAIS - Critical AI-based Systems
- 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
- PM – Person month / Project manager
- OEM - Original Equipment Manufacturer
- WP – Work Package
- WPL – Work Package Leader
- XAI – Explainable Artificial Intelligence
- ADAS – Advanced Driver Assistance System