Call: HORIZON-JU-Chips-2024-2-RIA
(HORIZON-JU-Chips-2024-2-RIA)

Topic: HORIZON-JU-Chips-2024-2-RIA-T1

Type of Action: HORIZON-JU-RIA
(HORIZON JU Research and Innovation Actions)

Proposal number: 101194342-1

Proposal acronym: AIDOSec

Type of Model Grant Agreement: HORIZON Action Grant Budget-Based

Table of contents

Proposal ID **101194342-1**

Acronym **AIDOSec**

1 - General information

Fields marked * are mandatory to fill.

Topic	HORIZON-JU-Chips-2024-2-RIA-T1	Type of Action	HORIZON-JU-RIA
Call	HORIZON-JU-Chips-2024-2-RIA	Type of Model Grant Agreement	HORIZON-AG

Acronym: AIDOSec

Proposal title: AI-augmented automation for efficient DevOps, a model-based framework for continuous and Secure development of complex systems

Note that for technical reasons, the following characters are not accepted in the Proposal Title and will be removed: < > " &

Duration in months: 36

Free keywords: *Enter any words you think give extra detail of the scope of your proposal (max 200 characters with spaces).*

Abstract *

DevOps is gaining more and more success in increasing development velocity while improving the quality. However, there remained a risk that the continuous integration/continuous delivery (CI/CD) pipeline introduces security vulnerabilities into the market; thus. SecDevOps seeks to address this risk by integrating security into the entire DevOps process. It expands the impact of DevOps by adding security tools and practices that help developers and operations teams to perform their own security analysis, discover security issues and improve the way they code and operate the software.
The AIDOSec proposal aims to define and develop a model-based framework supporting DevOps practices by considering security aspects in the early stage of the continuous system and software development. The project aims to use Model Driven Engineering (MDE) and Artificial Intelligence (AI) principles and techniques to automate decisions and processes and complete the system development tasks. MDE will contribute by (i) providing better abstraction principles and techniques, (ii) facilitating activities automation, and (iii) supporting technology integration among all the covered design and development activities. AI, notably Machine Learning (ML), will contribute by automating repetitive and time-consuming cybersecurity tasks; incorporating ML into the security workflow, tasks can be accomplished faster. Furthermore, the project aims at exploiting traceability to correlate different security controls and related results in different DevOps phases, with the aim to enable reuse, predict vulnerability and discover root causes.
We expect an industrial uptake of AIDOSec technologies on the development of complex systems that scales up to real systems demand with relevance for all security-critical applications, while enabling up or downscale easily. AI-augmented automation promises vast and long-term economic value added in ultra-large system development.

Remaining characters 39

Has this proposal (or a very similar one) been submitted in the past 2 years in response to a call for proposals under any EU programme, including the current call? (•) Yes ( ) No

Please give the proposal reference or contract number.
101140174

Administrative forms

Proposal ID **101194342-1**

Acronym **AIDOSec**

Declarations

Field(s) marked * are mandatory to fill.

1) We declare to have the explicit consent of all applicants on their participation and on the content of this proposal. *	☒
2) We confirm that the information contained in this proposal is correct and complete and that none of the project activities have started before the proposal was submitted (unless explicitly authorised in the call conditions). *	☒
3) We declare: - to be fully compliant with the eligibility criteria set out in the call - not to be subject to any exclusion grounds under the EU Financial Regulation 2018/1046 - to have the financial and operational capacity to carry out the proposed project. *	☒
4) We acknowledge that all communication will be made through the Funding & Tenders Portal electronic exchange system and that access and use of this system is subject to the Funding & Tenders Portal Terms and Conditions. *	☒
5) We have read, understood and accepted the Funding & Tenders Portal Terms & Conditions and Privacy Statement that set out the conditions of use of the Portal and the scope, purposes, retention periods, etc. for the processing of personal data of all data subjects whose data we communicate for the purpose of the application, evaluation, award and subsequent management of our grant, prizes and contracts (including financial transactions and audits). *	☒
6) We declare that the proposal complies with ethical principles (including the highest standards of research integrity as set out in the ALLEA European Code of Conduct for Research Integrity, as well as applicable international and national law, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Appropriate procedures, policies and structures are in place to foster responsible research practices, to prevent questionable research practices and research misconduct, and to handle allegations of breaches of the principles and standards in the Code of Conduct. *	☒
7) We declare that the proposal has an exclusive focus on civil applications (activities intended to be used in military application or aiming to serve military purposes cannot be funded). If the project involves dual-use items in the sense of Regulation 2021/821, or other items for which authorisation is required, we confirm that we will comply with the applicable regulatory framework (e.g. obtain export/import licences before these items are used). *	☒
8) We confirm that the activities proposed do not - aim at human cloning for reproductive purposes; - intend to modify the genetic heritage of human beings which could make such changes heritable (with the exception of research relating to cancer treatment of the gonads, which may be financed), or - intend to create human embryos solely for the purpose of research or for the purpose of stem cell procurement, including by means of somatic cell nuclear transfer. - lead to the destruction of human embryos (for example, for obtaining stem cells) These activities are excluded from funding. *	☒
9) We confirm that for activities carried out outside the Union, the same activities would have been allowed in at least one EU Member State. *	☒

The coordinator is only responsible for the information relating to their own organisation. Each applicant remains responsible for the information declared for their organisation. If the proposal is retained for EU funding, they will all be required to sign a declaration of honour.

False statements or incorrect information may lead to administrative sanctions under the EU Financial Regulation.

2 - Participants

List of participating organisations

#	Participating Organisation Legal Name	Country	Role	Action
1	MALARDALENS UNIVERSITET	Sweden	Coordinator	
2	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	AT	Partner	
3	DYNATRACE AUSTRIA GMBH	Austria	Partner	
4	GTS GROUND TRANSPORTATION SYSTEMS AUSTRIA GMBH	AT	Partner	
5	UNIVERSITAT LINZ	Austria	Partner	
6	KAPSCH TrafficCom AG	Austria	Partner	
7	LIEBERLIEBER SOFTWARE GMBH	AT	Partner	
8	msg Plaut Austria GmbH	AT	Partner	
9	VYSOKE UCENI TECHNICKE V BRNE	CZ	Partner	
10	CAMEA SPOL SRO	CZ	Partner	
11	COGNITECHNA SRO	CZ	Partner	
12	ACORDE TECHNOLOGIES SA	ES	Partner	
13	HI IBERIA INGENIERIA Y PROYECTOS SL	ES	Partner	
14	PRODEVELOP SL	ES	Partner	
15	UNIVERSIDAD DE CANTABRIA	ES	Partner	
16	FUNDACIO PER A LA UNIVERSITAT OBERTA DE CATALUNY	ES	Partner	
17	UST SPAIN INSIDE S.L.	Spain	Partner	
18	ABO AKADEMI	FI	Partner	
19	HALTIAN OY	Finland	Partner	
20	PROCESS GENIUS OY	FI	Partner	
21	SOLIDCOMP OY	FI	Partner	

Administrative forms

Proposal ID **101194342-1**

Acronym **AIDOSec**

#	Participating Organisation Legal Name	Country	Role	Action
22	THINGLINK OY	FI	Partner	
23	ITA-SUOMEN YLIOPISTO	FI	Partner	
24	INSTITUT MINES-TELECOM	FR	Partner	
25	SOFTEAM	FR	Partner	
26	THALES	FR	Partner	
27	ABINSULA SRL	IT	Partner	
28	INNOVATION RIVER S.R.L.	IT	Partner	
29	INTECS SOLUTIONS SPA	IT	Partner	
30	Swascan SRL	IT	Partner	
31	TEKNE SRL	IT	Partner	
32	UNIVERSITA DEGLI STUDI DI CAGLIARI	IT	Partner	
33	UNIVERSITA DEGLI STUDI DI SASSARI	IT	Partner	
34	UNIVERSITA DEGLI STUDI DI TERAMO	Italy	Partner	
35	UNIVERSITA DEGLI STUDI DELL'AQUILA	IT	Partner	
36	Alstom Rail SWEDEN AB	SE	Partner	
37	RISE RESEARCH INSTITUTES OF SWEDEN AB	SE	Partner	
38	WESTERMO NETWORK TECHNOLOGIES AB	SE	Partner	

Organisation data

PIC	Legal name
999881530	*MALARDALENS UNIVERSITET*

Short name: MDU

Address

Street	HOGSKOLEPLAN 1
Town	VASTERAAS
Postcode	721 23
Country	Sweden
Webpage	www.mdu.se

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	28/01/2022 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	IDT	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Box 883	
Town	Västerås	
Postcode	721 23	
Country	Sweden	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Gunnar**

Last name* **Widforss**

E-Mail* **gunnar.widforss@mdu.se**

Position in org. Project manager

Department Embedded systems

☐ Same as organisation name

☒ Same as proposing organisation's address

Street HOGSKOLEPLAN 1

Town VASTERAAS

Post code 721 23

Country Sweden

Website *Please enter website*

Phone +46 70 6922763

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Caroline	Ressault	caroline.ressault@mdu.se	+xxx xxxxxxxxx
Antonio	Cicchetti	antonio.cicchetti@mdu.se	+xxx xxxxxxxxx
Shahid	Raza	shahid.raza@mdu.se	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Prof	Marjan	Sirjani	Woman	Iceland	marjan.sirjani@mdu.se	Category A Top grade re		0000-0001-5478-0987	Orcid ID
Dr	Sara	Abbaspour	Woman	Sweden	sara.abbaspour@mdu.se	Category B Senior resea		0000-0002-5058-7351	Orcid ID
Dr	Antonio	Cicchetti	Man	Sweden	antonio.cicchetti@mdu.se	Category B Senior resea		0000-0003-0416-1787	Orcid ID
Prof	Wasif	Afzal	Man	Sweden	wasif.afzal@mdu.se	Category A Top grade re		0000-0003-0611-2655	Orcid ID
Prof	Shahid	Raza	Man	Sweden	shahid.raza@mdu.se	Category A Top grade re		0000-0001-8192-0893	Orcid ID

Administrative forms

Role of participating organisation in the project

Project management	☒
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☐
IPR management incl. technology transfer	☒
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*R. Jongeling, F. Ciccozzi, J. Carlson, A. Cicchetti: Consistency management in industrial continuous model-based development settings: a reality check. Softw. Syst. Model. 21(4): 1511-1530 (2022)*
Publication	*R. Eramo, V. Muttillo, L. Berardinelli, H. Bruneliere, A. Gómez, A. Bagnato, A. Sadovykh, A. Cicchetti: AIDOaRt: AI-augmented Automation for DevOps, a Model-based Framework for Continuous Development in Cyber-Physical Systems. DSD 2021: 303-310*
Publication	*Anum Khurshid, Sileshi D. Yalew, Mudassar Aslam, Shahid Raza. ShieLD: Shielding Cross-zone Communication within Limited-resourced IoT Devices running Vulnerable Software Stack. IEEE Transactions on Dependable and Secure Computing, vol. 20, no.2, March/April 2023*
Publication	*Fereidoun Moradi, Sara Abbaspour, Bahman Pourvatan , Zahra Moezkarimi, Marjan Sirjani: CRYSTAL framework: Cybersecurity assurance for cyber-physical systems. Journal of Logical and Algebraic Methods in Programming (JLAMP) (2024)*
Publication	*G. Jabeen, S. Rahim, W. Afzal, D. Khan, A.A. Khan, Z. Hussain, T. Bibi: Machine learning techniques for software vulnerability prediction: a comparative study.Appl. Intell. 52(15): 17614-17635 (2022)*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
Aidoart	*AI-augmented automation supporting modeling, coding, testing, monitoring, and continuous development in Cyber-Physical Systems*
Serendipity	*Secure and dependable platforms for autonomy*
SACSys	*Safe and Secure Adaptive Collaborative Systems*
RELIANT	*Industrial graduate school: Reliable, Safe and Secure Intelligent Autonomous Systems*
ARCADIAN-IoT	*H2020 ARCADIAN-IoT: Autonomous Trust, Security and Privacy Management Framework for IoT* *[2021-2024] (Technical Project Leader, Scored 15/15)*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999584128	*AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH*

Short name: AIT

Address

Street	GIEFINGGASSE 4
Town	WIEN
Postcode	1210
Country	Austria
Webpage	http://www.ait.ac.at/

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	no
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2022	- no
SME self-assessment	31/12/2022	- no
SME validation	14/01/2009	- no

Departments carrying out the proposed work

Department 1

Department name	Center for Digital Safety & Security	☐ not applicable
	☒ Same as proposing organisation's address	
Street	GIEFINGGASSE 4	
Town	WIEN	
Postcode	1210	
Country	Austria	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Benjamin**

Last name* **Rainer**

E-Mail* **benjamin.rainer@ait.ac.at**

Position in org. Research Engineer

Department Center for Digital Safety & Security

☐ Same as organisation name

☒ Same as proposing organisation's address

Street GIEFINGGASSE 4

Town WIEN

Post code 1210

Country Austria

Website *Please enter website*

Phone '+43 664 6207813

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Petra	Volkmann	petra.volkmann@ait.ac.at	+43 664 88390735

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier	
Dr	Benjamin	Rainer	Man	Austria	benjamin.rainer@ait.ac.at	Category C Recognised	Leading	https://scholar.google.at/citations?user=BKI-TQQAAAAJ&hl=de	Other ID	Google Scholar
Mrs	Christl	Korbinian	Man	Austria	christl.korbinian@ait.ac.at	Category C Recognised	Team member	https://publications.ait.ac.at/de/persons/korbinian.christl	Other ID	Research Profile
Mr	Christoph	Schmittner	Man	Germany	christoph.schmittner@ait.ac.at	Category C Recognised	Team member	https://scholar.google.at/citations?user=wgjCgBAAAAAJ&hl=de&oi=ao	Other ID	Google Scholar
Mr	Egger	Manuel	Man	Austria	egger.manuel@ait.ac.at	Category D First stage r	Team member	https://scholar.google.at/citations?user=wgjCgBAAAAAJ&hl=de&oi=ao	Other ID	Research Profile
Mrs	Hanna	Kumhera	Woman	Austria	hanna.kumhera@ait.ac.at	Category D First stage r	Team member	https://publications.ait.ac.at/en/persons/hanna.kumhera	Other ID	Research Profile
Dr	Stefan	Schauer	Man	Austria	stefan.schauer@ait.ac.at	Category B Senior resea	Team member	https://scholar.google.at/citations?user=s7apyuoAAAAJ&hl=de&oi=ao	Other ID	Google Scholar

Mrs	Petra	Volkmann	Woman	Austria	petra.volkmann@ait.ac.at	Category D First stage r	Team member	https://publications.ait.ac.at/de/persons/petra-volkmann	Other ID	Research Profile

Administrative forms

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☐
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*https://link.springer.com/chapter/10.1007/978-3-031-17108-6_10*
Publication	*https://arxiv.org/abs/2210.03207*
Software	*ThreatGet https://documentation.threatget.com/20.06/index.html*
Software	*CASSANDRA (Cascading Effects Simulation)*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AI-augmented automation supporting modelling, coding, testing, monitoring and continuous development in Cyber-Physical Systems*
LearnTwins	*LearnTwins establishes a method kit for automated learning of trustable digital twins of cyber-physical systems (CPS).*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
895401472	*DYNATRACE AUSTRIA GMBH*

Short name: DT

Address

Street	AM FUNFUNDZWANZIGER TURM 20
Town	LINZ
Postcode	4020
Country	Austria
Webpage	http://www.dynatrace.com/

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	02/03/2015 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	Research Lab	☐ not applicable
	☒ Same as proposing organisation's address	
Street	AM FUNFUNDZWANZIGER TURM 20	
Town	LINZ	
Postcode	4020	
Country	Austria	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Andreas**

Last name* **Hametner**

E-Mail* **andreas.hametner@dynatrace.com**

Position in org. Research Lab Lead

Department Research Lab

☐ Same as organisation name

☒ Same as proposing organisation's address

Street AM FUNFUNDZWANZIGER TURM 20

Town LINZ

Post code 4020

Country Austria

Website *Please enter website*

Phone *+xxx xxxxxxxxx*

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Stefan	Achleitner	stefan.achleitner@dynatrace.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Stefan	Achleitner	Man	Austria	stefan.achleitner@dynatrace.com	Category A Top grade re	Leading	0000-0002-5499-6101	Orcid ID

Administrative forms

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Adversarial Network Forensics in Software Defined Networking*
Publication	*Cyber Deception: Virtual Networks to Defend Insider Reconnaissance*
Publication	*MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*
Publication	*Towards Reconstructing Multi-Step Cyber Attacks in Modern Cloud Environments with Tripwires*
Publication	*Rapid Prototyping for Microarchitectural Attacks*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*The AIDOaRt Consortium focus on cyber-physical systems engineering process with AI-augmented methods (AIOps), integrating DevOps and Model Driven Engineering (MDE) principles, to observe and analyse collected data from both runtime and design time artefacts.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999750192	*GTS GROUND TRANSPORTATION SYSTEMS AUSTRIA GMBH*

Short name: GTS

Address

Street	HANDELSKAI 92
Town	WIEN
Postcode	1200
Country	Austria
Webpage	https://www.thalesgroup.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	05/05/2006 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	Technology and Innovation	☐ not applicable
	☒ Same as proposing organisation's address	
Street	HANDELSKAI 92	
Town	WIEN	
Postcode	1200	
Country	Austria	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Peter**

Last name* **Tummeltshammer**

E-Mail* **peter.tummeltshammer@thalesgroup.com**

Position in org. Research Coordinator

Department Technology and Innovation

☐ Same as organisation name

☒ Same as proposing organisation's address

Street HANDELSKAI 92

Town WIEN

Post code 1200

Country Austria

Website *Please enter website*

Phone +43 664 88974976

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Christoph	Ruggenthaler	christoph.ruggenthaler@urbanandmainlines.co	+xxx xxxxxxxxx
Klaus	Reichl	klaus.reichl@urbanandmainlines.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Christoph	Ruggenthaler	Man	Austria	christoph.ruggenthaler@urbanandmainlines.com	Category D First stage r	Team member		

Administrative forms

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☐
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Hollaus, Aymeric et al. "The efficient use of digitisation in conventional interlocking technology", Signal+Draht 04/2024*
Publication	*Hametner, Reinhard, et al. "Cloud architecture for SIL4 railway applications." Signal+Draht 03/2022*
Software	*TAS Platform: Vital fault tolerance computing platform for SIL 4 signaling applications*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
ENABLE-S3 (ECSEL, H2020)	*Industry-driven project that aspires to substitute today's cost-intensive verification & validation efforts by more advanced and efficient methods to pave the way for the commercialization of highly automated cyber physical systems (ACPS). Thales Austria acts as a domain expert and our focus lies in novel formal methods for V&V.*
Productive4.0 (ECSEL, H2020)	*Capability to efficiently design and integrate hardware and software of Internet of Things (IoT) devices in today's digital industry. Thales Austria's interest lies in creating safe and secure IoT devices for future railway applications*
certMILS(H2020)	*Compositional security certification for medium- to high assurance COTS-based systems in environments with emerging threats. Thales Austria work towards a modular security architecture under the umbrella of IEC 62443*
SECREDAS (ECSEL, H2020)	*Security, safety and privacy across multiple application domains: Road, Rail and Health. Thales Austria works towards virtualization solutions for enabling cloud readiness of railway control applications.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
Integration Lab	*Development, integration and maintenance support setup for our railway solutions are located in Vienna, Austria. Complete HW lab with real test bed for development and testing.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999892976	*UNIVERSITAT LINZ*

Short name: JKU

Address

Street	ALTENBERGER STRASSE 69
Town	LINZ
Postcode	4040
Country	Austria
Webpage	http://www.jku.at

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	27/01/2022	- no
SME self-assessment	27/01/2022	- no
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name	Department of Business Informatics - Software Engineering	☐ not applicable
	☒ Same as proposing organisation's address	
Street	ALTENBERGER STRASSE 69	
Town	LINZ	
Postcode	4040	
Country	Austria	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title: Prof.

Gender: ○ Woman ◉ Man ○ Non Binary

First name*: **Manuel**

Last name*: **Wimmer**

E-Mail*: **manuel.wimmer@jku.at**

Position in org.: Department Head

Department: Department of Business Informatics - Software Engineering

☐ Same as organisation name

☒ Same as proposing organisation's address

Street: ALTENBERGER STRASSE 69

Town: LINZ

Post code: 4040

Country: Austria

Website: *Please enter website*

Phone: +437 3224684241

Phone 2: *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Luca	Berardinelli	luca.berardinelli@jku.at	+43 678 1260771

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Prof	Manuel	Wimmer	Man	Austria	manuel.wimmer@jku.at	Category A Top grade re	Team member	0000-0002-1124-7098	Orcid ID
Prof	Johannes	Samentinger	Man	Austria	johannes.samentinger@jku.at	Category B Senior resea	Team member	0000-0002-0637-6602	Orcid ID
Dr	Luca	Berardinelli	Man	Italy	luca.berardinelli@jku.at	Category B Senior resea	Team member	0000-0003-2416-2867	Orcid ID

Administrative forms

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☐
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*https://ieeexplore.ieee.org/document/9640612* *Digital Twin Platforms: Requirements, Capabilities, and Future Prospects*
Publication	*https://ieeexplore.ieee.org/document/9190077* *Leveraging Iterative Plan Refinement for Reactive Smart Manufacturing Systems*
Publication	*https://ieeexplore.ieee.org/document/9613376* *AML4DT: A Model-Driven Framework for Developing and Maintaining Digital Twins with AutomationML*
Publication	*Michael Riegler, Johannes Sametinger, Michael Vierhauser, Manuel Wimmer,* *A model-based mode-switching framework based on security vulnerability scores,* *Journal of Systems and Software,* *Volume 200,* *2023,* *111633,* *ISSN 0164-1212,* *https://doi.org/10.1016/j.jss.2023.111633*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
CDL Mint	*https://cdl-mint.se.jku.at/* *Christian Doppler Laboratory for Model-Integrated Smart Production*
LeaxDSL	*https://se.jku.at/lea-language-engineering-for-analyzable-executable-dsmls/* *LEAxDSML: Language Engineering for Analyzable Executable DSMLs*
Lowcomote	*http://www.lowcomote.eu/*
AIDOaRt	*https://www.aidoart.eu/*
IT Security	*https://se.jku.at/it-security/* *IT security is about protecting information and information systems from unauthorized access and use.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
IoT Lab	*Smart Room*
Smart Manufactoring Lab Demonstrator	*Smart Manufactoring Lab Demonstrator*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
985098051	*KAPSCH TrafficCom AG*

Short name: KAPSCH

Address

Street	Am Europlatz 2
Town	Wien
Postcode	1120
Country	Austria
Webpage	www.kapsch.net

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	28/06/2002	- no
SME self-assessment	unknown	
SME validation	28/06/2002	- no

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title _____ Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Martin** Last name* **Linauer**

E-Mail* **martin.linauer@kapsch.net**

Position in org. Vice President Innovation, IPR Management & Research CooperationsCorporate Tec

Department KAPSCH TrafficCom AG ☒ Same as organisation name

☒ Same as proposing organisation's address

Street Am Europlatz 2

Town Wien Post code 1120

Country Austria

Website *Please enter website*

Phone *+xxx xxxxxxxxx* *Phone 2* *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Robert	Koelbl	robert.koelbl@kapsch.net	+xxx xxxxxxxxx
Juliane	Hoebarth	juliane.hoebarth@kapsch.net	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
	Juan Jesus	Jimenez Cubero	Man	Spain	juanjesus.jimenezcubero@kapsch.net				
	Christian	Poschinger	Man	Austria	christian.poschinger@kapsch.net				
	Khadidja	Djebairia	Woman	Algeria	khadidja.djebairia@kapsch.net				
	Juliane	Hoebarth	Woman	Austria	Juliane.Hoebarth@kapsch.net				

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☒
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
CONCORDA (CEF)	*The CONCORDA (Connected Corridor for Driving Automation) flagship project contributes to the preparation of European motorways for automated driving and high density truck platooningwith adequate connected services and technologies. The combination of 802.11p and LTE-V2X connectivity required the operation without affecting existing services in terms of interferences and interoperability and was tested to ensure backwards C-ITS service interoperability with the services harmonized.*
Digibus Austria	*The Austrian flagship project "Digibus Austria" investigated the reliable and safe operation of automated minibuses in local public transport where independence and driving safety of autonomous vehicles should be improved with measures for communication between the vehicle and other road users. An G5 infrastructure was built by Kapsch TrafficCom for testing of automated driving away from the highway or from cities in and around the municipality of Koppl in Austria.*
NordicWay 2	*Based on NordicWay1, NW2 focuses on pilot deployment of interoperable day 1 and 1.5 C-ITS and supporting infrastructure readiness for connected and automated driving. One objective is to contribute to harmonisation and interoperability of C-ITS in Europe. Hence, an architecture, systems and services have been put in place under the Action, which are interoperable and in line with European developments, including with the specifications and other interoperability requirements.*
C-ROADS Spain	*The C-Roads Platform is a joint initiative of European Member States and road operators for testing and implementing C-ITS services in light of cross-border harmonisation and interoperability. The objective of C-Roads is that authorities and road operators join forces to harmonise the deployment activities of cooperative intelligent transport systems across Europe.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
Deep Learning Versatile Platform	*The Kapsch Deep Learning Versatile Platform (DLVP) is a comprehensive ecosystem driven by A.I., enabling complex traffic monitoring and empowering traffic management applications. It uses DL-frameworks to detect and classify road users (vehicles of all kinds, pedestrians).*
RIS-9160	*RIS-9160 is the latest generation Kapsch 5.9GHz Roadside Unit (RSU). It provides IEEE 802.11pwireless communication for both the ETSI ITS-G5, IEEE WAVE, and 5G-V2X standards for applications within the Cooperative ITS (C-ITS) environment and ITS applications.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
950575751	*LIEBERLIEBER SOFTWARE GMBH*

Short name: LIE

Address

Street	HANDELSKAI 340 TOP 5
Town	WIEN
Postcode	1020
Country	Austria
Webpage	www.lieberlieber.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2022	- yes
SME self-assessment	31/12/2022	- yes
SME validation	unknown	

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title: Dr

Gender: ◯ Woman ◉ Man ◯ Non Binary

First name*: **Konrand**

Last name*: **Wieland**

E-Mail*: **konrad.wieland@lieberlieber.com**

Position in org.: CEO

Department: LIEBERLIEBER SOFTWARE GMBH

☒ Same as organisation name

☒ Same as proposing organisation's address

Street: HANDELSKAI 340 TOP 5

Town: WIEN

Post code: 1020

Country: Austria

Website: *Please enter website*

Phone: +43 662906002017

Phone 2: *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Robert	Sicher	robert.sicher@lieberlieber.com	+xxx xxxxxxxxx
Peter	Lieber	peter.lieber@lieberlieber.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
	Robert	Sicher	Man	Austria	robert.sicher@lieberlieber.com	Category B Senior resea	Team member		
	Richard	Deininger	Man	Austria	richard.deininger@lieberlieber.com		Team member		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Software	*Diff & Merge Tool for UML/SysML Models (LemonTree)*
Software	*Systems Engineering Tools Enterprise Architect*
Software	*Code Generator for Embedded Systems*
Software	*Universal Queryable Model Interface, an open framework for model-based languages*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
Valu3s	*Verification and Validation of Automated Systems' Safety and Security*
KisMOD	*AI-assisted sustainable development and management of systems engineering models.*
EMBEET	*Embedded Model-Based Environment for Engineering and Test*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? ○ Yes ◉ No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
893010519	*msg Plaut Austria GmbH*

Short name: MSG

Address

Street	Modecenterstraße 17
Town	Wien
Postcode	1110
Country	Austria
Webpage	https://www.msg-plaut.com/at/

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	unknown
Secondary or Higher education establishment	unknown
Research organisation	unknown

SME Data

Based on the below details from the Participant Registry the organisation is unknown (small- and medium-sized enterprise) for the call.

SME self-declared status	unknown
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	Business Competence Center Mobility Solutions	☐ not applicable
	☒ Same as proposing organisation's address	
Street	Modecenterstraße 17	
Town	Wien	
Postcode	1110	
Country	Austria	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Ayhan**

Last name* **Mehmed**

E-Mail* **ayhan.mehmed@msg-plaut.com**

Position in org. Lead Business Consultant

Department Business Competence Center Mobility Solutions,

☐ Same as organisation name

☒ Same as proposing organisation's address

Street Modecenterstraße 17

Town Wien

Post code 1110

Country Austria

Website *Please enter website*

Phone +43 664 80740 139

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Borislav	Nikolov	borislav.nikolov@msg-plaut.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier	
Dr	Ayhan	Mehmed	Man	Bulgaria	ayhan.mehmed@msg-plaut.com	Category B Senior resea	Leading	https://scholar.google.com/citations?user=dCFY1T0AAAAJ&hl=en&oi=ao	Other ID	Google scholar

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☒
Research performer	☐
Technology developer	☐
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Forecast horizon for automated safety actions in automated driving systems https://scholar.google.com/citations?view_op=view_citation&hl=en&user=dCFY1T0AAAAJ&sortby=pubdate&citation_for_view=dCFY1T0AAAAJ:Tyk-4Ss8FVUC*
Publication	*Method and fault tolerant computer architecture for reducing false negatives in fail-safe trajectory planning for a moving entity https://scholar.google.com/citations?view_op=view_citation&hl=en&user=dCFY1T0AAAAJ&sortby=pubdate&citation_for_view=dCFY1T0AAAAJ:UeHWp8X0CEIC*
Publication	*The monitor as key architecture element for safe self-driving cars https://scholar.google.com/citations?view_op=view_citation&hl=en&user=dCFY1T0AAAAJ&sortby=pubdate&citation_for_view=dCFY1T0AAAAJ:ufrVoPGSRksC*
Publication	*Next generation real-time networks based on IT technologies https://scholar.google.com/citations?view_op=view_citation&hl=en&user=dCFY1T0AAAAJ&sortby=pubdate&citation_for_view=dCFY1T0AAAAJ:IjCSPb-OGe4C*
Service	*Services in: Automotive IT/OT Security, Safety, Embedded Enigneering, Model Driven Engineering, Homologation and Type Approval https://www.msg-plaut.com/mobility*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
UN R156 SUMS Gap Analyses and stragegy (OEM)	*Cyber-security gap analyes and strategy planning for UN R 156 SUMS (Software Update Management System) by international car maker.*
UN R156 SUMS Gap Analyses and stragegy	*Cyber-security gap analyes and strategy planning for UN R 156 SUMS (Software Update Management System) by international truck trailer producer.*
UN R155 SUMS Gap Analyses and stragegy	*Cyber-security gap analyes and strategy planning for UN R 155 CSMS(Cybersecurity Management System) by international truck producer.*
Cyber Resilience Act Gap and Strategy	*Cyber Resilience Act gap analyses and strategy planning for Cyber Resilience Act for an international producer of Grassland (Mowers, Tedders, Raking Technology, etc.)*
Data Act Gap and Strategy	*Data act gap analyses and strategy planning for Cyber Resilience Act for an international producer of Grassland (Mowers, Tedders, Raking Technology, etc.)*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
Database	*Comrahensive database implementation of ISO 21434 Cybersecurity Standard*
Penetration testing lab	*Automotive Penetration Testing Lab with embedded HW equipment*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999873091	*VYSOKE UCENI TECHNICKE V BRNE*

Short name: BUT

Address

Street	ANTONINSKA 548/1
Town	BRNO STRED
Postcode	601 90
Country	Czechia
Webpage	www.vutbr.cz

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	22/03/2024	- no
SME self-assessment	25/06/2018	- no
SME validation	21/11/2008	- no

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Prof.

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Pavel**

Last name* **Smrz**

E-Mail* **smrz@fit.vut.cz**

Position in org. Associated Professor

Department Faculty of Information Technology

☐ Same as organisation name

☐ Same as proposing organisation's address

Street Bozetechova 2,

Town Brno

Post code 61266

Country Czechia

Website https://www.fit.vutbr.cz

Phone +420541141282

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Radka	Kavalova	projadm@fit.vutbr.cz	+420541141282
Pavel	Smrz	smrz@fit.vutbr.cz	+420541141282

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Prof	Pavel	Smrz	Man	Czechia	smrz@vut.cz	Category B Senior resea	Leading	0000-0002-5638-1362	Orcid ID
Prof	Pavel	Zemcik	Man	Czechia	zemcik@vut.cz	Category A Top grade re	Team member	0000-0001-7969-5877	Orcid ID
Dr	Ivan	Homoliak	Man	Czechia	ihomoliak@fit.vut.cz	Category B Senior resea	Team member	0000-0002-0790-0875	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☒
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*BREITENBACHER Dominik, HOMOLIAK Ivan, AUNG Yan Lin, ELOVICI Yuval and TIPPENHAUER Nils Ole. HADES-IoT: A practical host-based anomaly detection system for IoT devices (Extended Version). IEEE Internet of Things Journal, vol. 9, no. 12, 2022, pp. 9640-9658. ISSN 2327-4662.*
Publication	*BAMBUŠEK Daniel, MATERNA Zdeněk, KAPINUS Michal, BERAN Vítězslav and SMRŽ Pavel. How Do I Get There? Overcoming Reachability Limitations of Constrained Industrial Environments in Augmented Reality Applications. In: 2023 IEEE Conference on Virtual Reality and 3D User Interfaces (VR). Shanghai, 2023.*
Publication	*KLEPÁRNÍK Petr, ZEMČÍK Pavel, TREEBY Bradley E. and JAROŠ Jiří. On-the-Fly Calculation of Time-Averaged Acoustic Intensity in Time-Domain Ultrasound Simulations Using a k-Space Pseudospectral Method. IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, vol. 69, no. 10, 2022, pp. 2917-2929. ISSN 1525-8955.*
Publication	*ZANIN Massimiliano, MENASALVAS Ernestina, RODRIGUEZ González Alejandro and SMRŽ Pavel. An Analytics Toolbox for Cyber-Physical Systems Data Analysis: Requirements and Challenges. In: Proceedings of the 43rd International Convention on Information, Communication and Electronic Technology (MIPRO 2020). New York: Institute of Electrical and Electronics Engineers, 2020, pp. 271-276. ISBN 978-953-233-099-1.*
Publication	*CASINO Fran, LYKOUSAS Nikolaos, HOMOLIAK Ivan, PATSAKIS Constantinos and HERNANDEZ-CASTRO Julio. Intercepting Hail Hydra: Real-Time Detection of Algorithmically Generated Domains. Journal of Network and Computer Applications, vol. 2021, no. 190, pp. 1-17. ISSN 1084-8045.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
National project SecTech	*SecTech - Safe and Secure Traffic Systems of New Generation, the Ministry of Interior of the Czech Republic, VB01000048, 2022-2023.*
National project TACR EMIR	*EMIR - 5G-Enhanced Embedded Intelligence for Robotic Autonomy and Smart City Monitoring Application, the Technological Agency of the Czech Republic, FW07010052, 2023-2025, cooperation with Cognitechna on the 5G-enabled communication of autonomous robots.*
Horizon 2020 project 5G-ERA	*5G-enhanced robot autonomy, EC Horizon 2020, 101016681, 2021-2024.*
National Centre of Competence SecuSen II	*SECUSEN II: SECure SENsors - Industrial Intelligence, the Technological Agency of the Czech Republic, TN01000077/14, 2021-2022.*
National project EmIC	*"Embedded Intelligence for Smart Cameras with Computer Vision Applications for Transportation and Industry, FW02020040, the Technology Agency of the Czech Republic, 2020-2023*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
IT4Innovations	*BUT forms a part of the national high-performance computing centre IT4Innovations that enables efficient processing of extremely large streams of data and training of huge machine learning models.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
998129031	*CAMEA SPOL SRO*

Short name: CAMEA

Address

Street	KARASEK 2290/1m RECKOVICE
Town	BRNO
Postcode	621 00
Country	Czechia
Webpage	www.camea.cz

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2021	- yes
SME self-assessment	31/12/2021	- yes
SME validation	23/12/2008	- yes

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Lukáš**

Last name* **Maršík**

E-Mail* **l.marsik@camea.cz**

Position in org. R&D Engineer

Department CAMEA SPOL SRO

☒ Same as organisation name

☒ Same as proposing organisation's address

Street KARASEK 2290/1m RECKOVICE

Town BRNO

Post code 621 00

Country Czechia

Website *Please enter website*

Phone +420732853334

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Eliška	Vlčková	e.vlckova@camea.cz	+420605237214

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Mr	Lukas	Marsik	Man	Czechia	l.marsik@camea.cz	Category C Recognised		0000-0002-5264-5455	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Other achievement	*Industrial video-inspection system for electronic components MODICAM – AVX Lanskroun, Czech Republic – reliable application of video processing in industrial environment (>1000 pcs)*
Other achievement	*Section Speed enforcement and Red Light enforcement system suitable also for monitoring UNICAM – Czech police and municipalities (>400 places in Czech Republic and aborad)*
Other achievement	*Nonwowen textile quality inspection systems – Pegas Bucovice, Czech Republic – industrial quality inspection system being installed on most of the production lines nowadays (>50 pcs)*
Other achievement	*Traffic monitoring and bicycles counting system – Municipality of Prague, the system is intended for traffic monitoring and bicycle in particular, various updates being continuously performed.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
MegaMaRt2	*ECSEL project addressing MegaModelling at Runtime - scalable model-based framework for continuous development and runtime validation of complex systems, 2017-2020*
SECUSEN	*TACR project oriented towards Secure SENsors and data, 2019-2021*
AIDOaRT	*ECSEL project addressing AI-augmented automation for efficient DevOps, a model-based framework for continuous development At RunTime in cyber-physical systems, 2021-2024*
MuSiC	*AENEAS a project addresing Multi-level Security for Critical Services, 2018-2021*
SECUSEN II	*TACR project adressing SECure SENsors and data, Industrial Intelligence, 2021-2022*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
1	*Thousands of cameras in field for traffic monitoring and quality inspection that can be remotely acessed.*
2	*Hunderds of radars and other sensors deployed.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? ○ Yes ◉ No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
900117515	*COGNITECHNA SRO*

Short name: COG

Address

Street	KARASEK 2290/1M
Town	BRNO
Postcode	621 00
Country	Czechia
Webpage	www.cognitechna.cz

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2021	- yes
SME self-assessment	31/12/2021	- yes
SME validation	unknown	

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title: Dr

Gender: ○ Woman ◉ Man ○ Non Binary

First name*: **Martin**

Last name*: **Musil**

E-Mail*: **m.musil@cognitechna.cz**

Position in org.: CTO

Department: COGNITECHNA SRO

☒ Same as organisation name

☒ Same as proposing organisation's address

Street: KARASEK 2290/1M

Town: BRNO

Post code: 621 00

Country: Czechia

Website: https://www.cognitechna.cz

Phone: +420602773710

Phone 2: *+xxx xxxxxxxxx*

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Martin	Musil	Man	Czechia	m.musil@cognitechna.cz	Category B Senior resea	Leading		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☒
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Good	*Smart City Monitoring Platform - The Cognitechna Smart City Monitoring Platform (SCMP) is a modular, edge-computing platform intended for monitoring objects of interest, contributing to the smart city concept.*
Service	*Production Inspection in Industry - A service for our customers (manufacturing cyber-physical products, chip producers, etc.) combining visual intelligence with IoT sensors, the platform can process large streams of data with its embedded processors and embedded machine learning algorithms.*
Software	*Road Surveys - The software enables maintaining exact and up-to-date knowledge of roads and related equipment, and to precisely detect, localise and revise over 300 traffic signs, traffic signals and road markings.*
Other achievement	*CogniSensors – An embedded solution for monitoring, reading, and analysing various input signals using advanced machine learning algorithms at the edge level – commercially available and applied at international markets.*
Service	*CogniCamera – An embedded solution for reading licence plates, vehicle type identification, speed measurement, and industrial inspection. Industrial applications typically consist of artificial intelligence for camera inspection systems for 100% quality control of electronic parts, non-woven textiles, paper mills, metal mills, etc. Marketing applications include audience analysis: counting persons in an area, tracking their movement or analyzing their behaviour."*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
International R&D project LoLiPoP IoT	*Cognitechna coordinates a large group of European companies and academic partners focusing on Long Life Power Platforms for the Internet of Things, Chips JU, SEP-210885163, 2023-2026.*
National project TACR EMIR	*Cognitechna was awarded in the national program for 5G communication by EMIR: 5GEnhanced Embedded Intelligence for Robotic Autonomy and Smart City Monitoring Application, TACR, FW07010052, 2023-2025.*
Horizon 2020 project 5G-ERA	*Cognitechna was awarded in the national program for 5G communication by EMIR: 5GEnhanced Embedded Intelligence for Robotic Autonomy and Smart City Monitoring Application, TACR, FW07010052, 2023-2025.*
OP Enterprise and Innovations for Competitiveness	*Cognitechna participates in EU co-financed project Machine Learning and Artificial Intelligence in Warehouse Management, the Czech Ministry of Industry and Trade, CZ.01.1.02/0.0/0.0/20_321/0024763, 2021-2023.*
National project EmIC	*Embedded Intelligence for Smart Cameras with Computer Vision Applications for Transportation and Industry, FW02020040, the Technology Agency of the Czech Republic, 2020-2023.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
EdgeLab	*In addition to its offices, the company has an in-house hardware laboratory that is fully equipped for prototyping embedded solutions. It also has significant expertise and experience in connecting its services to cloud platforms provided by Amazon, Microsoft, and Google and on-premised cloud.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? ○ Yes ◉ No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999796267	*ACORDE TECHNOLOGIES SA*

Short name: ACORDE

Address

Street	CALLE EL CASTRO 22N
Town	SANTANDER
Postcode	39011
Country	Spain
Webpage	www.acorde.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2021	- yes
SME self-assessment	31/12/2021	- yes
SME validation	31/12/2014	- yes

Departments carrying out the proposed work

Department 1

Department name	Communication Systems	☐ not applicable
	☒ Same as proposing organisation's address	
Street	CALLE EL CASTRO 22N	
Town	SANTANDER	
Postcode	39011	
Country	Spain	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mrs

Gender ◉ Woman ○ Man ○ Non Binary

First name* **Esther**

Last name* **López**

E-Mail* **esther.lopez@acorde.com**

Position in org. Senior Expert Product Development

Department Communication Systems

☐ Same as organisation name

☒ Same as proposing organisation's address

Street CALLE EL CASTRO 22N

Town SANTANDER

Post code 39011

Country Spain

Website *Please enter website*

Phone *+xxx xxxxxxxxx*

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Fernando	Herrera	fernando.herrera@acorde.com	+xxx xxxxxxxxx
Jacobo	Domínguez	jacobo.dominguez@acorde.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Fernando	Herrera	Man	Spain	fernando.herrera@acorde.com		Leading	0000-0003-1488-7637	Orcid ID
Dr	Jacobo	Dominguez	Man	Spain	jacobo.dominguez@acorde.com		Team member	0009-0009-4121-8261	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOART	*AI-augmented automation supporting modeling, coding, testing, monitoring, and continuous development in Cyber-Physical Systems. ACORDE works on a novel monitoring edge infrastructure, which will enable better federation of services, with a specific focus on geo-positioning, but including edge data processing and anomalies analysis.*
NextPerception	*"Development of the next generation smart perception sensors and enhance the distributed intelligence paradigm to build versatile, secure, reliable, and proactive human monitoring solutions for the health, wellbeing, and automotive domains.* *ACORDE developed a novel, versatil edge-platform suited for the novel sensor data collection, and AI/ML supported fusion at the edge. It also provided implementation for anonymization algorithms."*
COMP4DRONES	*COMP4DRONES brings a holistically designed ecosystem from application to electronic components, realized as a tightly integrated multi-vendor and compositional UAV embedded architecture solution and a tool chain complementing the compositional architecture principles. In COMP4DRONES ACORDE brought novel indoor/outdoor positioning solutions, with some incipient integration of security to react low-level attacks (jamming&spoofing)*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
ESD lab	*ESD protected lab for validation of electronic equipment, including high performance oscilloscopes, logic analyzer, pulse generators, microwave, spectrum analysers, network analysers. This equipment could be use validate and test project hardware & software integrations.*
CPD	*Hybrid cloud combining an on-premises high-available architecture and multiple cloud providers, support high-available services based on application containerization and OS virtualization technologies, allowing ACORDE to provide cloud services for its own experiments and other partner needs.*
EDA and ESL SW	*Electronic Design Automation and Electronic-System-Level design automation SW incl. a PCB mounting and testing laboratory, staff with long experience in PCB design software supported by customized libraries, incl. 3D footprints. ACORDE engineers have also experience on real-time embedded SW developm*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
996346074	*HI IBERIA INGENIERIA Y PROYECTOS SL*

Short name: HIB

Address

Street	CALLE JUAN HURTADO DE MENDOZA 14 PISO BA
Town	MADRID
Postcode	28036
Country	Spain
Webpage	www.hi-iberia.es

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2022	- yes
SME self-assessment	31/12/2022	- yes
SME validation	13/03/2009	- yes

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Raúl**

Last name* **Santos**

E-Mail* **rsantos@hi-iberia.es**

Position in org. R&D Project Manager

Department HI IBERIA INGENIERIA Y PROYECTOS SL

☒ Same as organisation name

☒ Same as proposing organisation's address

Street CALLE JUAN HURTADO DE MENDOZA 14 PISO BAJ

Town MADRID

Post code 28036

Country Spain

Website www.hi-iberia.es

Phone +34914585119

Phone 2 +34699830005

Other contact persons

First Name	Last Name	E-mail	Phone
Inmaculada	Luengo	iluengo@hi-iberia.es	+34914585119

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Ms	Paloma	Jimeno Sánchez-Patón	Woman	Spain	pjimeno@hi-iberia.es	Category C Recognised	Team member	0000-0002-0323-7287	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*van Tooren, Merijn, Daniel Reti, Daniel Schneider, Cédric Bassem, Raúl Santos de la Cámara, and Hans Dieter Schotten. "Research Questions in the Acceptance of Cybersecurity by SMEs in the EU."*
Publication	*K. Zabaleta, A. B. Lago, D. López-De-Ipiña, G. Di Modica, R. Santos De La Cámara and M. Pistore, "Combining Human and Machine Intelligence to Foster Wider Adoption of e-Services," 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, 2019, pp. 1854-1859, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-*
Publication	*Naranjo, Manuel, Diego Fuentes, Elena Muelas, Enrique Díez, Luis Ciruelo, César Alonso, Eduardo Abenza, Roberto Gómez-Espinosa, and Inmaculada Luengo. "Object Detection-Based System for Traffic Signs on Drone-Captured Images." Drones 7, no. 2 (2023): 112.*
Publication	*Martín-Wanton, T.; Muelas, E.; de la Cámara, S.; Rodríguez-Molina, J.; Li, X.; Martínez, J.-F. Modelado devehículos autónomos y la incertidumbre de su entorno para la seguridad de operaciones marítimas.In Proceedings of the IV Congreso Nacional de I+D en Defensa y Seguridad, San Javier, Murcia, Spain,16–18 November 2016*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*Focusses on AI-augmented automation supporting the continuous development of Cyber-Physical Systems (CPSs) in its phases, such as requirements, monitoring, modelling, coding, and testing. The growing complexity of CPS poses several challenges throughout all software development and analysis phases, but also during their service and maintenance life.*
SCRATCh	*ITEA(2018-2022) proposes an integrative approach to IoT, security and DevOps practices through a set of interoperable tools (toolkit) based on a common conceptual architecture and consisting of the following elements: (1)Security foundation for strong device identity, (2)DevOps IoT tools integrating processes and technologies that accelerate development and continuous deployment of IoT solutions.(3) A SecDevOps-inspired process consisting of procedures that actively promote continuous deploym*
Next Perception	*ECSEL project (2020-2023) in which a range of unobtrusive diverse sensing technologies (wearables, FMCW and UWB radars, video cameras) were understood together in a common fashion with the end goal of improving situational awareness in health, automotive and pedestrian scenarios. HIB was Use Case leader and Work Package leader.*
COMP4DRONES	*ECSEL JU project (2018-2023) coordinated by Indra that brings together a consortium of 48 partners with the aim of providing a framework of key enabling technologies for safe and autonomous drones. It brings to bear a holistically designed ecosystem from application to electronic components, realized as a tightly integrated multi-vendor and compositional UAV embedded architecture solution and a tool chain complementing the compositional architecture principles.*
AFarCloud	*ECSEL (2018-2021) provided a distributed platform for autonomous agriculture and animal husbandry that allows for the real-time integration and cooperation of physical computer systems, in order to improve efficiency, productivity, animal health, and food quality, while reducing agricultural labour costs, supporting monitoring and decision-making solutions based on big data and real-time data mining techniques. AFarEdge will be built on learnings of AFarCloud.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
AI Model Training and Data Center	*Data Center with high performance GPUs for training deep convolutional neural networks. Hosted with the maximum security requirements in situ at the Madrid HIB headquarters.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
996571696	*PRODEVELOP SL*

Short name: PRO

Address

Street	PLAZA DON JUAN DE VILLARRASA 14-5
Town	VALENCIA
Postcode	46001
Country	Spain
Webpage	www.prodevelop.es

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2019	- yes
SME self-assessment	31/12/2019	- yes
SME validation	16/08/1993	- yes

Departments carrying out the proposed work

Department 1

Department name	R&D Department	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Carrer del Cronista Carreres, 13	
Town	Valencia	
Postcode	46003	
Country	Spain	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Ismael**

Last name* **Torres Boigues**

E-Mail* **itorres@prodevelop.es**

Position in org. R&D Project Manager

Department R&D Department

☐ Same as organisation name

☐ Same as proposing organisation's address

Street Carrer del Cronista Carreres, 13

Town Valencia

Post code 46003

Country Spain

Website *Please enter website*

Phone +34 963 510 612

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Eduardo	Garro Crevillen	egarro@prodevelop.es	+34 963 510 612
Eliseo	Villanueva Morte	evillanueva@prodevelop.es	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Mr	Ismael	Torres Boigues	Man	Spain	itorres@prodevelop.es	Category B Senior resea	Leading		
Mr	Eliseo	Villanueva Morte	Man	Spain	evillanueva@prodevelop.es	Category B Senior resea	Team member		
Dr	Eduardo	Garro Crevillen	Man	Spain	egarro@prodevelop.es	Category B Senior resea	Team member		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Marc Gil, Christophe Joubert, Ismael Torres: Model-driven Engineering IDE for Quality Assessment of Data-intensive Applications. ICPE Companion 2017: 173-174*
Publication	*Simona Bernardi, Juan L. Domínguez, Abel Gómez, Christophe Joubert, José Merseguer, Diego Perez-Palacin, José Ignacio Requeno, Alberto Romeu: A systematic approach for performance assessment using process mining - An industrial experience report. Empirical Software Engineering 23(6): 3394-3441 (2018)*
Software	*Posidonia Smart port solution that can be used as UC*
Publication	*Llorente M.A.; Montesinos M.; Palau C.E.; et al., "Modelling port operations towards environmental impact reduction: IoT infrastructure and scenarios", Proceedings of 8th Transport Research Arena TRA 2020, Helsinki, Finland*
Publication	*Valero, C.I.; Ivancos Pla, E.; Vaño, R.; Garro, E.; Boronat, F.; Palau, C.E. Design and Development of an AIoT Architecture for Introducing a Vessel ETA Cognitive Service in a Legacy Port Management Solution. Sensors 2021, 21, 8133*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRT	*Development a UC for applying IA solutions to improve the DevOps Cycle*
PIACERE	*Development an Integrated Development Enviroment (IDE) that provides support for the PIACERE framework, it includes several tool for improving DEVSecOps philosophy*
DICE	*Development of a Use case that evaluates different DevOps tools developed during the project*
ASSISt-IoT	*Aims at the design, implementation and validation of an open, decentralized reference architecture, with associated enablers to assist human-centric applications in multiple verticals.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
IoT devices	*IoT devices that gather data from Ports and terminals*
AWS License	*AWS License count be use to deploy the needed resources to develop de UC*
Internal CI/CD tool	*Internal CI/CD tool (gitlab)*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? ○ Yes ◉ No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999880075	*UNIVERSIDAD DE CANTABRIA*

Short name: UNICAN

Address

Street	AVENIDA DE LOS CASTROS S/N
Town	SANTANDER
Postcode	39005
Country	Spain
Webpage	www.unican.es

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	02/02/2009	- no
SME self-assessment	unknown	
SME validation	02/02/2009	- no

Departments carrying out the proposed work

Department 1

Department name	Dept. of Computer and Electronic Engineering	☐ not applicable
	☒ Same as proposing organisation's address	
Street	AVENIDA DE LOS CASTROS S/N	
Town	SANTANDER	
Postcode	39005	
Country	Spain	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Julio**

Last name* **Medina**

E-Mail* **julio.medina@unican.es**

Position in org. Senior Lecturer

Department Dept. of Computer and Electronic Engineering

☐ Same as organisation name

☒ Same as proposing organisation's address

Street AVENIDA DE LOS CASTROS S/N

Town SANTANDER

Post code 39005

Country Spain

Website https://web.unican.es/Departamentos/iie

Phone +34942 201477

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Eugenio	Villar	villar@teisa.unican.es	+34942201398
Ruth	Arroyo	ruth.arroyo@unican.es	+34942201071
Juan Jose	San Miguel	miguelj j@gestion.unican.es	+34942200968

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Julio	Medina	Man	Spain	julio.medina@unican.es	Category B Senior resea	Leading	0000-0002-1305-9429	Orcid ID
Prof	Eugenio	Villar	Man	Spain	villar@teisa.unican.es	Category A Top grade re	Team member	0000-0002-6541-6176	Orcid ID
Dr	Carlos	Blanco	Man	Spain	carlos.blanco@unican.es	Category B Senior resea	Team member	0000-0001-9001-0904	Orcid ID
Dr	Diego	Garcia	Man	Spain	diego.garcia@unican.es	Category C Recognised	Team member	0000-0002-7182-7879	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☒
Research performer	☒
Technology developer	☐
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*"Security policies by design in NoSQL document databases. C. Blanco, D. García-Saiz, D. G.Rosado, A. Santos-Olmo, J.Peral, A.Maté, J.Trujillo and E. Fernández-Medina. Journal of Information Security and Applications (JISA) 65: 103-120, March 2022."*
Publication	*"Improving security in NoSQL document databases through model-driven modernization. Alejandro Maté, Jesús Peral, Juan Trujillo, Carlos Blanco, Diego García-Saiz and Eduardo Fernández-Medina. Knowledge and Information Systems (KAIS), Volume 63(8), pp.2209-2230, August 2021."*
Publication	*"High-Level Design of Wireless Sensor Networks for Performance Optimization Under Security Hazards. Pablo Peñil, Alvaro Díaz, Hector Posadas, Julio Medina, and Pablo Sánchez. ACM Trans. Sen. Netw. 13, 3, Article 19, 37 pages, August 2017."*
Publication	*"Security in Information Systems: Advances and new Challenges. C. Blanco, D.G. Rosado, L.E. Sanchez and J. Jurjens Computer Standards and Interfaces (CSI) 36(4): 687-688 (2014)."*
Publication	*Basis for an integrated Security Ontology according to a systematic review of existing proposals. C. Blanco, J. Lasheras, E. Fernández-Medina, R. Valencia and A. Toval Computer Standards & Interfaces (CSI) 33(4): 372-388. (2011)."*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
Project: DAIS. Type: HORIZON (ECSEL)	*Project Title: DAIS: DISTRIBUTED ARTIFICIAL INTELLIGENT SYSTEM. Funding Entity(s): EUROPEAN COMMISSION AND AEI.*
Project: AIDOaRT. Type: HORIZON (ECSEL)	*Project Title: AIDOaRt: AI-AUGMENTED AUTOMATION FOR EFFICIENT DEV-OPS, A MODEL-BASED FRAMEWORK FOR CONTINUOUS DEVELOPMENT AT RUNTIME IN CYBER-PHYSICAL SYSTEMS; Funding Entity(s): EUROPEAN COMMISSION AND AEI*
Project: COMP4DRONES. Type: HORIZON (ECSEL)	*Project Title: COMP4DRONES: FRAMEWORK OF KEY ENABLING TECHNOLOGIES FOR SAFE AND AUTONOMOUS DRONES' APPLICATIONS; Funding Entity(s): EUROPEAN COMMISSION AND MCIyU*
Project: MegaMart2. Type: HORIZON (ECSEL)	*Project Title: A scalable model-based framework for continuous development and runtime validation of complex systems - Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737494.*
Project: PRESECREL. Type: National project.	*"Models and platforms for predictable, secure and reliable industrial information technology systems Ref. PID2021-124502OB-C42 (PRESECREL)"*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
995992024	*FUNDACIO PER A LA UNIVERSITAT OBERTA DE CATALUNYA*

Short name: UOC

Address

Street	RAMBLA POBLENOU 154
Town	BARCELONA
Postcode	08018
Country	Spain
Webpage	www.uoc.edu

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	17/07/2023	- no
SME self-assessment	31/12/2020	- no
SME validation	24/11/1994	- no

Departments carrying out the proposed work

Department 1

Department name	SOM Research Lab Internet Interdisciplinary Institute (IN3)	☐ not applicable
	☒ Same as proposing organisation's address	
Street	RAMBLA POBLENOU 154	
Town	BARCELONA	
Postcode	08018	
Country	Spain	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Robert**

Last name* **Clarisó**

E-Mail* **rclariso@uoc.edu**

Position in org. Senior researcher

Department SOM Research Lab Internet Interdisciplinary Institute (IN3)

☐ Same as organisation name

☒ Same as proposing organisation's address

Street RAMBLA POBLENOU 154

Town BARCELONA

Post code 08018

Country Spain

Website *Please enter website*

Phone *+xxx xxxxxxxxx*

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Abel	Gómez	agomezlla@uoc.edu	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Abel	Gómez	Man	Spain	agomezlla@uoc.edu	Category B Senior resea			
Dr	Robert	Clarisó	Man	Spain	rclariso@uoc.edu	Category B Senior resea			

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Hugo Bruneliere, Vittoriano Muttillo, Romina Eramo, Luca Berardinelli, Abel Gómez, Alessandra Bagnato, Andrey Sadovykh, Antonio Cicchetti (2022). AIDOaRt: AI-augmented Automation for DevOps, a model-based framework for continuous development in Cyber–Physical Systems, Microprocessors and Microsystems, Volume 94, 2022,104672, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2022.104672.*
Publication	*Andrey Sadovykh, Wasif Afzal, Dragos Truscan, Pierluigi Pierini, Hugo Bruneliere, Alessandra Bagnato, Abel Gómez, Jordi Cabot, Orlando Avila-García (2019). On a tool-supported model-based approach for building architectures and roadmaps: The MegaM@Rt2 project experience, Microprocessors and Microsystems, Volume 71, 2019, 102848, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2019.102848.*
Publication	*Loli Burgueño, Robert Clarisó, Sébastien Gérard, Shaui Li, Jordi Cabot (2021). An NLP-Based Architecture for the Autocompletion of Partial Domain Models. In: La Rosa, M., Sadiq, S., Teniente, E. (eds) Advanced Information Systems Engineering. CAiSE 2021. Lecture Notes in Computer Science(), vol 12751. Springer, Cham. https://doi.org/10.1007/978-3-030-79382-1_6*
Publication	*Anjali Sree-Kumar, Elena Planas, Robert Clarisó (2018). Extracting software product line feature models from natural language specifications. In Proceedings of the 22nd International Systems and Software Product Line Conference - Volume 1 (SPLC '18). Association for Computing Machinery, New York, NY, USA, 43–53. https://doi.org/10.1145/3233027.3233029.*
Publication	*Robert Clarisó, Jordi Cabot, (2020). Diverse Scenario Exploration in Model Finders Using Graph Kernels and Clustering. In: Raschke, A., Méry, D., Houdek, F. (eds) Rigorous State-Based Methods. ABZ 2020. Lecture Notes in Computer Science(), vol 12071. Springer, Cham. https://doi.org/10.1007/978-3-030-48077-6_3.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
MegaM@Rt2	*MegaM@Rt2: MegaModelling at Runtime - scalable model-based framework for continuous development and runtime validation of complex systems (2017-2020). H2020 ECSEL Joint Undertaking #737494*
AIDOaRt	*AIDOART: AI-augmented automation for efficient DevOps (2021-2024). H2020 ECSEL Joint Undertaking Project ID: 101007350.*
TRANSACT	*TRANSACT: Transform safety-critical cyber-physical systems into distributed solutions for end-users and partners (2021-2024). H2020 ECSEL Joint Undertaking Project 2021 ID: 101007260.*
LOCOSS	*LOCOSS: Low-code development of smart software (2021-2024). Spanish Ministry of Science and Innovation PID2020-114615RB-I00.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
887713155	*UST SPAIN INSIDE S.L.*

Short name: UST

Address

Street	CALLE SANTA LEONOR 65 EDIFICIO G
Town	MADRID
Postcode	28037
Country	Spain
Webpage	https://www.ust.com/es

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	03/02/2022 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	Technology consulting	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Santa Leonor 65, Edificio G	
Town	Madrid	
Postcode	28037	
Country	Spain	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title _____ Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Daniel** Last name* **Field**

E-Mail* **daniel.field@ust.com**

Position in org. Manager

Department Technology consulting ☐ Same as organisation name

☐ Same as proposing organisation's address

Street Santa Leonor 65, Edificio G

Town Madrid Post code 28037

Country Spain

Website *Please enter website*

Phone +34671 65 81 72 *Phone 2* *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Francisco	Cosin	francisco.cosin@ust.com	+xxx xxxxxxxxx
Imanol	Valiente	imanol.valiente@ust.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Mr	Francisco	Cosin	Man	Spain	francisco.cosin@ust.com	Category B Senior resea	Leading		
Mr	Imanol	Valiente	Man	Spain	imanol.valiente@ust.com	Category B Senior resea	Team member		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☐
IPR management incl. technology transfer	☒
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Cyberattacks in the EV industry: A Disruption Waiting to Happen https://www.ust.com/en/insights/cyberattacks-in-the-ev-industry-a-disruption-waiting-to-happen*
Publication	*DevOps Trends 2021 https://www.ust.com/es/insights/devops-trends-2021*
Publication	*Improved application delivery speed and productivity with agile business framework and DevSecOps (ust.com) https://www.ust.com/en/insights/improved-application-delivery-speed-and-productivity-with-agile-business-framework-and-devsecops*
Publication	*Yuval Wollman – Cybersecurity | UST https://www.ust.com/au/our-thinking/cybersecurity-new-threats-new-models*
Publication	*What is DevOps, and where are all the Ops going? (ust.com) https://www.ust.com/en/insights/what-is-devops-and-where-are-all-the-ops-going*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
DevOps & Cloud Center of Excellence	*Project at a leading Spanish bank stablishing frameworks for esalable and secure DevOps procedures. Infrastrcuture as code for valivable and repeteable deployments, including secured pipelines for deploying only validated apps*
Sandbox	*New environments for testing applications on synthetic data to validate results with rea world-like data amounts.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
999903355	*ABO AKADEMI*

Short name: ABO

Address

Street	DOMKYRKOTORGET 3
Town	ABO
Postcode	20500
Country	Finland
Webpage	www.abo.fi

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	01/02/1979 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	Information Technology	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Vesilinnantie 3	
Town	Turku	
Postcode	20500	
Country	Finland	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Prof.

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Ivan**

Last name* **Porres**

E-Mail* **ivan.porres@abo.fi**

Position in org. Professor

Department Information Technology

☐ Same as organisation name

☐ Same as proposing organisation's address

Street Vesilinnantie 3

Town Turku

Post code 20500

Country Finland

Website *Please enter website*

Phone +358504096303

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Adnan	Ashraf	adnan.ashraf@abo.fi	+358409370378
Research	Services	research@abo.fi	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Prof	Ivan	Porres	Man	Finland	ivan.porres@abo.fi	Category A Top grade re	Leading	0000-0002-6791-2018	Orcid ID
Prof	Dragos	Truscan	Man	Finland	dragos.truscan@abo.fi	Category A Top grade re	Team member	0000-0002-4367-6225	Orcid ID
Dr	Adnan	Ashraf	Man	Finland	adnan.ashraf@abo.fi	Category B Senior resea	Team member	0000-0001-8015-2335	Orcid ID
Dr	Tanwir	Ahmad	Man	Pakistan	tanwir.ahmad@abo.fi	Category C Recognised	Team member	0000-0003-3164-1559	Orcid ID
	Gaadha	Chariyarupadannayil Sudheerbabu	Woman	India	gaadha.sudheerbabu@abo.fi	Category D First stage r	Team member		

Role of participating organisation in the project

Project management	☒
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Tanwir Ahmad, Dragos Truscan, Jüri Vain, Ivan Porres: Early Detection of Network Attacks Using Deep Learning. ICST Workshops 2022: 30-39*
Publication	*Andrey Sadovykh, Gunnar Widforss, Dragos Truscan, Eduard Paul Enoiu, Wissam Mallouli, Rosa Iglesias, Alessandra Bagnato, Olga Hendel: VeriDevOps: Automated Protection and Prevention to Meet Security Requirements in DevOps. DATE 2021: 1330-1333*
Publication	*Gaadha Sudheerbabu, Tanwir Ahmad, Filip Sebek, Dragos Truscan, Jüri Vain, Ivan Porres: A Two-phase Metamorphic Approach for Testing Industrial Control Systems. ETFA 2022: 1-4*
Publication	*Jarkko Peltomäki, Frankie Spencer, Ivan Porres: Wasserstein Generative Adversarial Networks for Online Test Generation for Cyber Physical Systems. SBST@ICSE 2022: 1-5*
Publication	*Jarkko Peltomäki, Ivan Porres: Falsification of Multiple Requirements for Cyber-Physical Systems Using Online Generative Adversarial Networks and Multi-Armed Bandits. ICST Workshops 2022: 21-28*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AIDOaRt is a 3 years long H2020-ECSEL European project involving 32 organizations, grouped in clusters from 7 different countries, focusing on AI-augmented automation supporting modelling, coding, testing, monitoring and continuous development in Cyber-Physical Systems (CPS). The growing complexity of CPS poses several challenges throughout all software development and analysis phases, but also during their usage and maintenance. https://www.aidoart.eu/*
MegaM@Rt2 - MegaModelling at Runtime	*ECSEL-JU. Methods and tools for continuous development and validation leveraging the advantages in scalable model-based methods to provide benefits in significantly improved productivity, quality and predictability of large and complex industrial systems. https://megamart2-ecsel.eu/*
RECOMP	*Artemis JU - The aim of RECOMP was to define a European standard reference technology for mixed-criticality multi-core systems supported by the European tool vendors participating in RECOMP. It provided reference designs and platform architectures together with the required design methods and tools for achieving cost-effective certification and recertification of mixed-criticality, component based, multi-core systems. https://artemis-ia.eu/project/21-recomp.html*
VeriDevOps	*H2020 - VeriDevOps is about fast, flexible system engineering that efficiently integrates development, delivery, and operations, thus aiming at quality deliveries with short cycle time to address ever-evolving challenges. Current system development practices are increasingly based on using both off-the-shelf and legacy components which make such systems prone to security vulnerabilities. Since DevOps is promoting frequent software deliveries, verification methods artefacts should be updated in a*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
942708663	*HALTIAN OY*

Short name: HAL

Address

Street	YRTTIPELLONTIE 1D
Town	OULU
Postcode	90230
Country	Finland
Webpage	www.haltian.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2022	- yes
SME self-assessment	31/12/2022	- yes
SME validation	unknown	

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Matti**

Last name* **Vakkuri**

E-Mail* **matti.vakkuri@haltian.com**

Position in org. Head of Research Operations

Department HALTIAN OY

☒ Same as organisation name

☒ Same as proposing organisation's address

Street YRTTIPELLONTIE 1D

Town OULU

Post code 90230

Country Finland

Website www.haltian.com

Phone *+xxx xxxxxxxxx*

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Fahad	Sohrab	fahad.sohrab@haltian.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Mr	Matti	Vakkuri	Man	Finland	matti.vakkuri@haltian.com	Category B Senior resea	Leading	0000-0002-1318-545X	Orcid ID
Dr	Marko	Tuhkala	Man	Finland	marko.tuhkala@haltian.com	Category C Recognised	Team member	0000-0003-3741-8630	Orcid ID
Dr	Fahad	Sohrab	Man	Pakistan	fahad.sohrab@haltian.com	Category C Recognised	Team member	0000-0002-8080-4011	Orcid ID
Mrs	Polina	Feshchenko	Woman	Finland	polina.feshchenko@haltian.com	Category D First stage r	Team member	0000-0001-8130-3588	Orcid ID

Role of participating organisation in the project

Project management	☒
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
917658316	*PROCESS GENIUS OY*

Short name: PG

Address

Street	TORIKATU 19 B
Town	JOENSUU
Postcode	80100
Country	Finland
Webpage	www.processgenius.fi

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	28/02/2023	- yes
SME self-assessment	28/02/2023	- yes
SME validation	unknown	

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Janne**

Last name* **Pekkala**

E-Mail* **janne.pekkala@processgenius.fi**

Position in org. Director of Quality, Processes & Research

Department PROCESS GENIUS OY

☒ Same as organisation name

☒ Same as proposing organisation's address

Street TORIKATU 19 B

Town JOENSUU

Post code 80100

Country Finland

Website www.processgenius.eu

Phone +358 400 367 771

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Henri	Parkkonen	henri.parkkonen@processgenius.fi	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Software	*Genius CoreTM platform for industrial digitalization and adding factory to your pocket.*
Software	*PGplant MW, 3D based Digital Twin platform for SME Industries for 24/7 situational awareness and utilization monitoring.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIToC	*Development of an integrated tool-chain for manufacturing engineering that supports decision making in early phases*
MIDIH	*PGplant: Boosting the uptake of Industrial Internet by a revolutionary multi-layered 3D Digital Twin*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
882254286	*SOLIDCOMP OY*

Short name: SC

Address

Street	MINNA CANTHIN KATU 66 LH 1
Town	KUOPIO
Postcode	70100
Country	Finland
Webpage	https://solidcomp.fi/

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2022	- yes
SME self-assessment	31/12/2022	- yes
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name: R&D Department ☐ not applicable

☒ Same as proposing organisation's address

Street: MINNA CANTHIN KATU 66 LH 1

Town: KUOPIO

Postcode: 70100

Country: Finland

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Sandor**

Last name* **Nagy**

E-Mail* **sandor.nagy@solidcomp.fi**

Position in org. CEO

Department R&D Department

☐ Same as organisation name

☒ Same as proposing organisation's address

Street MINNA CANTHIN KATU 66 LH 1

Town KUOPIO

Post code 70100

Country Finland

Website *Please enter website*

Phone +358505145104

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Tuomas	Korhonen	tuomas.korhonen@solidcomp.fi	+358405264398

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Mr	Tuomas	Korhonen	Man	Finland	tuomas.korhonen@solidcomp.fi	Category C Recognised	Team member		
Mr	Sandor	Nagy	Man	Finland	sandor.nagy@solidcomp.fi	Category C Recognised	Team member		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☒
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Software	*Reality Twin Digital Twin platform for utilizing 3D data with intdustrial ERP-systems to help maintenance, engineering and safety operations in wide variety of industrial factories.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
KDT MATISSE	*MATISSE (Model-Based Engineering of Digital Twins for Early Verification and Validation of Industrial Systems): Project duration will be 09/2024-08/2027.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
1	*3D Laser Scanning Technology, Drones (aerial photography), and Photogrammetry*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
893452063	*THINGLINK OY*

Short name: TL

Address

Street	OIKOPOLKU 12
Town	Kontiolahti
Postcode	80770
Country	Finland
Webpage	www.thinglink.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2023	- yes
SME self-assessment	31/12/2023	- yes
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name	R&D Department	☐ not applicable
	☒ Same as proposing organisation's address	
Street	OIKOPOLKU 12	
Town	Kontiolahti	
Postcode	80770	
Country	Finland	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title: Dr

Gender: ○ Woman ◉ Man ○ Non Binary

First name*: **Keijo**

Last name*: **Haataja**

E-Mail*: **keijo@thinglink.com**

Position in org.: Senior Manager Funded Projects

Department: R&D Department

☐ Same as organisation name

☒ Same as proposing organisation's address

Street: OIKOPOLKU 12

Town: Kontiolahti

Post code: 80770

Country: Finland

Website: https://www.thinglink.com/

Phone: +358451871687

Phone 2: *+xxx xxxxxxxxx*

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Keijo	Haataja	Man	Finland	keijo@thinglink.com	Category B Senior resea	Team member		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☒
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Service	*ThingLink Platform for fast and easy creation of interactive VR/AR learning environments, VR tours, and simulations for recruitment as well as employee on-boarding and training.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
KDT MATISSE	*MATISSE (Model-Based Engineering of Digital Twins for Early Verification and Validation of Industrial Systems): Project duration will be 09/2024-08/2027.*
KDT H2TRAIN	*H2TRAIN (Enabling Digital Technologies for Holistic Health-Lifestyle Motivational and Assisted Supervision Supported by Artificial Intelligence Networks): Project duration will be 05/2024-04/2027.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
991207984	*ITA-SUOMEN YLIOPISTO*

Short name: UEF

Address

Street	YLIOPISTONRANTA 8
Town	KUOPIO
Postcode	70211
Country	Finland
Webpage	www.uef.fi

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	09/09/2009	- no
SME self-assessment	09/09/2009	- no
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name	School of Computing, Kuopio Campus	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Microkatu 1	
Town	Kuopio	
Postcode	70211	
Country	Finland	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Keijo**

Last name* **Haataja**

E-Mail* **keijo.haataja@uef.fi**

Position in org. Project Manager

Department School of Computing, Kuopio Campus

☐ Same as organisation name

☐ Same as proposing organisation's address

Street Microkatu 1

Town Kuopio

Post code 70211

Country Finland

Website https://www.uef.fi/en

Phone +358451871687

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Pekka	Toivanen	pekka.toivanen@uef.fi	+358405439021

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Keijo	Haataja	Man	Finland	keijo.haataja@uef.fi	Category B Senior resea	Team member		
Prof	Pekka	Toivanen	Man	Finland	pekka.toivanen@uef.fi	Category A Top grade re	Leading		
Dr	Mazhar	Mohsin	Man	Finland	mazhar.mohsin@uef.fi	Category C Recognised	Team member		

Role of participating organisation in the project

Project management	☒
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☒
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Other achievement	*AI-related patents.*
Publication	*K. Haataja and P. Toivanen: Two Practical Man-In-The-Middle Attacks on Bluetooth Secure Simple Pairing and Countermeasures. IEEE Transactions on Wireless Communications, Vol. 9, No. 1, pp. 384–392, January 2010.*
Publication	*M. Mohsin, O. S. Balogun, K. Haataja and P. Toivanen: Defect Detection Using Deep Neural Networks and Algorithms: A Survey. Solid State Technology, Vol 66, pp. 23–39, 2023.*
Publication	*M. Mohsin, O. S. Balogun, K. Haataja and P. Toivanen: Convolutional Neural Networks For Real-Time Wood Plank Detection And Defect Segmentation. F1000Research. Vol. 12, No. 319, 2023.*
Publication	*M. Mohsin, K. Haataja and P. Toivanen: Deep Learning-Based Defect Detection and Segmentation for Wood Plank Surfaces with Real-Time Tracking. Electronic Imaging '23, 2023.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
KDT MATISSE	*MATISSE (Model-Based Engineering of Digital Twins for Early Verification and Validation of Industrial Systems): Project duration will be 09/2024-08/2027.*
KDT H2TRAIN	*H2TRAIN (Enabling Digital Technologies for Holistic Health-Lifestyle Motivational and Assisted Supervision Supported by Artificial Intelligence Networks): Project duration will be 05/2024-04/2027.*
Artemis ALMARVI	*ALMARVI (Algorithms, Design Methods, and Many-Core Execution Platform for Low-Power Massive Data-Rate Video and Image Processing): Project duration was 04/2014-06/2017.*
Artemis ACCUS	*ACCUS (Adaptive Cooperative Control in Urban SubSystems): Project duration was 06/2013-01/2016.*
Artemis DEMANES	*DEMANES (Design, Monitoring and Operation of Adaptive Networked Embedded Systems): Project duration was 05/2012-06/2012.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
SuperComputer	*UEF's CI (Computational Intelligence) research group has its own SuperComputer, which can be utilized for our AI-based research work.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
999849326	*INSTITUT MINES-TELECOM*

Short name: IMT

Address

Street	19 PLACE MARGUERITE PEREY
Town	PALAISEAU
Postcode	91120
Country	France
Webpage	www.imt.fr

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	05/04/2024 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	Department of Automation, Production and Computer Sciences	☐ not applicable
	☐ Same as proposing organisation's address	
Street	4 rue Alfred Kastler	
Town	Nantes Cedex	
Postcode	44307	
Country	France	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Hugo**

Last name* **Bruneliere**

E-Mail* **hugo.bruneliere@imt-atlantique.fr**

Position in org. Researcher

Department Department of Automation, Production and Computer Sciences

☐ Same as organisation name

☐ Same as proposing organisation's address

Street 4 rue Alfred Kastler

Town Nantes Cedex

Post code 44307

Country France

Website https://www.imt-atlantique.fr/en

Phone 00 33 (0)2 51 85 82

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Julien	Prud'homme	julien.prudhomme@imt-atlantique.fr	+xxx xxxxxxxxx
Jacky	Haurogné	dri-contrats@imt-atlantique.fr	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Hugo	BRUNELIERE	Man	France	hugo.bruneliere@imt-atlantique.fr	Category B Senior resea	Leading	0000-0002-5987-2175	Orcid ID
Dr	Massimo	TISI	Man	Italy	massimo.tisi@imt-atlantique.fr	Category B Senior resea	Team member	0000-0001-7891-9138	Orcid ID
Dr	Théo	LE CALVAR	Man	France	theo.le-calvar@imt-atlantique.fr	Category B Senior resea	Team member	0000-0003-2273-2053	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☐
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*James Pontes Miranda, Hugo Bruneliere, Massimo Tisi, Gerson Sunyé. Integrating the Support for Machine Learning of Inter-Model Relations in Model Views. The Journal of Object Technology, 2024, The 20th European Conference on Modelling Foundations and Applications (ECMFA 2024), pp.1-14. <To appear>*
Publication	*Andrey Sadovykh, Bilal Said, Dragos Truscan, Hugo Bruneliere. An Iterative Approach for Model-based Requirements Engineering in Large Collaborative Projects: A Detailed Experience Report. Science of Computer Programming, 2024, 232, pp.103047. ?10.1016/ j.scico.2023.103047?.*
Publication	*Hugo Bruneliere, Vittoriano Muttillo, Romina Eramo, Luca Berardinelli, Abel Gomez, et al.. AIDOaRt: AI-augmented Automation for DevOps, a Model-based Framework for Continuous Development in Cyber-Physical Systems. Microprocessors and Microsystems: Embedded Hardware Design, 2022, 94, pp.104672. ?10.1016/j.micpro.2022.104672?.*
Publication	*Théo Le Calvar, Fabien Chhel, Frédéric Jouault, Frédéric Saubion. Coupling solvers with model transformations to generate explorable model sets. Software and Systems Modeling, 2021, 20 (5), pp.1633-1652. ?10.1007/s10270-021-00867-0?.*
Publication	*Hugo Bruneliere, Florent Marchand de Kerchove, Gwendal Daniel, Sina Madani, Dimitris Kolovos, et al.. Scalable Model Views over Heterogeneous Modeling Technologies and Resources. Software and Systems Modeling, 2020, 19 (4), pp.827-851. ?10.1007/ s10270-020-00794-6?.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AI-augmented automation supporting modeling, coding, testing, monitoring, and continuous development in Cyber-Physical Systems (CPS). (ECSEL)*
MegaM@Rt2	*A scalable model-based framework for continuous development and runtime validation of complex systems (ECSEL)*
Lowcomote	*MSCA ITN 2018. Training the leaders of tomorrow engineering of low-code development platforms.*
MATISSE	*Model-based engineering of Digital Twins for early verification and validation of Industrial Systems (KDT JU)*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
906436677	*SOFTEAM*

Short name: SOFT

Address

Street	45-47 BOULEVARD PAUL VAILLANT-COUTURIER
Town	IVRY-SUR-SEINE
Postcode	94200
Country	France
Webpage	www.softeamgroup.fr

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is unknown (small- and medium-sized enterprise) for the call.

SME self-declared status	unknown
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name: BU Software ☐ not applicable

☒ Same as proposing organisation's address

Street: 45-47 BOULEVARD PAUL VAILLANT-COUTURIER

Town: IVRY-SUR-SEINE

Postcode: 94200

Country: France

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Andrey**

Last name* **Sadovyk**

E-Mail* **andrey.sadovykh@softeam.fr**

Position in org. Project manager

Department SOFTEAM Software

☐ Same as organisation name

☒ Same as proposing organisation's address

Street 45-47 BOULEVARD PAUL VAILLANT-COUTURIER

Town IVRY-SUR-SEINE

Post code 94200

Country France

Website *Please enter website*

Phone +33630101144

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Alessandra	Bagnato	alessandra.bagnato@softeam.fr	+33130121858

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Andrey	Sadovykh	Man	France	andrey.sadovykh@softeam.fr	Category B Senior resea		0000-0003-2384-5447	Orcid ID
Dr	Alessandra	Bagnato	Woman	France	alessandra.bagnato@softeam.fr	Category A Top grade re		0000-0003-2675-0953	Orcid ID
Dr	Bilal	Said	Man	France	bilal.said@softeam.fr	Category B Senior resea		0000-0003-2259-6063	Orcid ID

Role of participating organisation in the project

Project management	☒
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Software	*Modelio model-driven engineering workbench.*
Software	*ARQAN - NLP tool for requirements analysis.*
Software	*RQCODE - lightweight requirements formalization tool.*
Software	*Modelio INTO-CPS modules for orchestration of co-simulations.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
VeriDevOps	*Automated security requirements analysis, verification, validation and monitoring.*
AIDOaRt	*Model-based requirements engineerning*
MegaM@Rt	*Holistic system model for integrating software and hardware aspects on the system level*
REVAMP	*Product Lines Engineering modelling with SysML*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
1	*Modelio SAAS servers*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999751938	*THALES*

Short name: THA

Address

Street	4 RUE DE LA VERRERIE
Town	MEUDON
Postcode	92190
Country	France
Webpage	www.thalesgroup.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	22/11/2023 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name: TRT/STI ☐ not applicable

☐ Same as proposing organisation's address

Street: Av Augustin Fresnel

Town: PALAISEAU Cedex

Postcode: 91767

Country: France

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title _____ Gender ○ Woman ◉ Man ○ Non Binary

First name* **Rafik** Last name* **Henia**

E-Mail* **rafik.henia@thalesgroup.com**

Position in org. Research Engineer

Department TRT/STI ☐ Same as organisation name

☐ Same as proposing organisation's address

Street Av Augustin Fresnel

Town PALAISEAU Cedex Post code 91767

Country France

Website *Please enter website*

Phone 3169415571+3 *Phone 2* *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Philippe	Poyet	philippe.poyet@thalesgroup.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Laurent	Rioux	Man	France	laurent.rioux@thalesgroup.com	Category D First stage r			
Mr	Eric	DUJARDIN	Man	France	eric.dujardin@thalesgroup.com	Category D First stage r			

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Software	*Network latencies analysis & simulation tool*
Software	*Probes for network communications monitoring*
Dataset	*Network Traffic data*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
CPS4EU	*CPS4EU objectives:* *- Develop 4 key enabling technologies (computing, connectivity, sensing, cooperative systems)* *- Incorporate these CPS modules through pre-integrated architectures and design tools* *- Instantiate these architectures in dedicated use cases from strategic application: automotive, smart grid and industry automation* *- Improve CPS awareness and usage for all industrial sectors*
ResTSN	*The objective of this project is to define mechanisms allowing safe (timing and security constraints) dynamic reconfiguration of a TSN network after unpredictable failures.*
FED4SAE	*FED4SAE overall objective is to boost and sustain the digitization of the European industry in strengthening the European competitiveness in the CPS & Embedded system market by lowering both the technical and business barriers for innovative companies.* *The program aimed to:* *To bring innovative CPS technologies to business from any sector* *To link companies to suppliers across value-chains and regions in order to create innovative CPS solutions* *To link companies to investors across value-chain*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
TSN Network Infrastructure	*The TSN network is composed of switches, end-systems and drone applications*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
951632372	*ABINSULA SRL*

Short name: ABI

Address

Street	VIALE UMBERTO 42
Town	SASSARI SS
Postcode	07100
Country	Italy
Webpage	www.abinsula.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	31/12/2021	- yes
SME self-assessment	31/12/2021	- yes
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name: R&D&I ☐ not applicable

☒ Same as proposing organisation's address

Street: VIALE UMBERTO 42

Town: SASSARI SS

Postcode: 07100

Country: Italy

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ◉ Woman ○ Man ○ Non Binary

First name* **Maria Katiuscia**

Last name* **Zedda**

E-Mail* **katiuscia.zedda@abinsula.com**

Position in org. Senior Programme and Project Manager

Department R&D&I

☐ Same as organisation name

☒ Same as proposing organisation's address

Street VIALE UMBERTO 42

Town SASSARI SS

Post code 07100

Country Italy

Website https://abinsula.com/

Phone (+39) 3485466565

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Tiziana	Fanni	tiziana.fanni@abinsula.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Maria Katiuscia	Zedda	Woman	Italy	katiuscia.zedda@abinsula.com	Category A Top grade re	Leading	0009-0003-1059-8261	Orcid ID
Dr	Tiziana	Fanni	Woman	Italy	tiziana.fanni@abinsula.com	Category B Senior resea	Team member	0000-0002-4301-6497	Orcid ID
Mr	Giuseppe	Meloni	Man	Italy	giuseppe.meloni@abinsula.com	Category B Senior resea	Team member		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*T. FANNI, G. MELONI, M. MELIS, A. SOLINAS, M.K. ZEDDA, "The Multi-Sensor Gateway, a Unified Communication Scheme and Orchestration Actor for Heterogeneous Systems". In: Proceedings of the CPS Summer School PhD Workshop 2022, co-located with 4th Edition of the CPS Summer School (CPS 2022), Pula, Sardinia (Italy), September 19-23, 2022. Published in: CEUR Workshop Proceedings Vol-3252. ISSN 1613-0073. http://ceur-ws.org/Vol-3252/paper3.pdf*
Publication	*F Palumbo, T FANNI, C Sau, L Pulina, L Raffo, M Masin, E Shindin, P Sanchez de Rojas, K Desnos, M Pelcat, A Rodríguez, E Juárez, F Regazzoni, G MELONI, K ZEDDA, H Myrhaug, L Kaliciak, J. Andriaanse, J Olivieria de Filho, P Muñoz and Toffetti. "CERBERO: Cross-layer modEl-based fRamework for multi-oBjective dEsign of Reconfigurable Systems in unceRtain hybRid envirOnments: invited Paper: CERBERO Teams*
Publication	*Sau C., Rinaldi C., Pomante L., Palumbo F., Valente G., FANNI T., Martinez M., van der Linden F., Basten T., GeilenM., Peeren G., Kadlec J., Jääskeläinen P., Bulej L., Barranco F., Saarinen J., Säntti T., ZEDDA M. K., et all (2021) "Design and management of image processing pipelines within CPS: Acquired experience towards the end of the FitOptiVis ECSEL Project", Microprocessors and Microsystems, Volume 87, 2021*
Publication	*Masin Michael, Palumbo Francesca, Adriaanse J, Myrhaug Hans, Regazzoni Francesco, Sanchez, and ZEDDA Katiuscia, "Elicitation of Technical Requirements in Large Research Projects: the CERBERO approach" 34th ACM/SIGAPP Symposium On Applied Computing*
Publication	*R. Eramo, T. FANNI, D. Guidotti, L. Pandolfo, L. Pulina. M.K. ZEDDA, ""Verification of Neural Networks: Challenges and Perspectives in the AIDOaRt Project"", IPS-RiCeRcA-SPIRIT 2022: 10th Italian Workshop on Planning and Scheduling, RiCeRcA Italian Workshop, and SPIRIT Workshop on Strategies, Prediction, Interaction, and Reasoning in Italy. Published in: CEUR Workshop Proceedings Vol-3345. https://ceur-ws.org/Vol-3345/paper9_RiCeRCa2.pdf*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AIDOaRt is an ECSEL JU project with a consortium of 32 partners that aims at using AIOps to automate decision and process and complete system development tasks. Abinsula provides a Use Case in safety critical systems in the automotive domain that aims to enhance the human interaction and driving experience, proposing an electronic rear-view mirror that gets data from a set of video sensors and provides the rear image on a screen.*
COMP4DRONES	*COMP4DRONES is an ECSEL JU project with the aim of providing a framework of key enabling technologies for safe and autonomous drones. It brings to bear a holistically designed ecosystem from application to electronic components, realized as a tightly integrated multivendor and compositional UAV embedded architecture solution and a tool chain complementing the compositional architecture principles. Abinsula is involved in the Agricultural Use Case*
FitOptiVis	*FitOptiVis is an Ecsel JU project with the objective of to developing a cross-domain approach covering a reference architecture, supported by low-power, high-performance smart devices, and by methods and tools for combined design-time and run-time multi-objective optimisation within system and environment constraints. Abinsula has developed a multisensory gateway based on an Abinsula linux distribution*
CERBERO	*CERBERO is an H2020 European with a consortium of 12 partners that has developed a continuous design environment for adaptive CPS, reactive to different types of triggers. Abinsula contribution to CERBERO is related to tool integration. In this context, Abinsula actively collaborated in the development of the CERBERO Interoperability Framework (CIF).*

MYRTUS	*MYRTUS is an Horizon Europe Project coordinated by Abinsula. MYRTUS primary goal is to provide efficient computing continuum management, leveraging advanced technologies such as federated learning and swarm intelligence techniques.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	**Short description (Max 300 characters)**
Abinsula Incubator	*In May 2020, Abinsula became a certified incubator, the fifth in the whole of Southern Italy and one of the 38 certified incubators in Italy. The headquarters extends for 700 square meters and includes 50 workstations*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? ○ Yes ◉ No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
893283380	*INNOVATION RIVER S.R.L.*

Short name: INNORIV

Address

Street	P.ZZA ARDUINO ANGELUCCI 14
Town	Rieti
Postcode	02100
Country	Italy
Webpage	www.innovationriver.it

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	07/07/2021 - yes
SME self-assessment	07/07/2021 - yes
SME validation	unknown

Departments carrying out the proposed work

No department involved

Department name *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street *Please enter street name and number.*

Town *Please enter the name of the town.*

Postcode *Area code.*

Country *Please select a country*

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Diego**

Last name* **Grimani**

E-Mail* **diego.grimani@innovationriver.it**

Position in org. Chief Operating Officer

Department INNOVATION RIVER S.R.L.

☒ Same as organisation name

☒ Same as proposing organisation's address

Street P.ZZA ARDUINO ANGELUCCI 14

Town Rieti

Post code 02100

Country Italy

Website *Please enter website*

Phone *+xxx xxxxxxxxx*

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Marialuisa	Scalise	marialuisa.scalise@innovationriver.it	+xxx xxxxxxxxx
Nadia Caterina	Zullo Lasala	nadiacaterina.zullolasala@innovationriver.it	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Mrs	Nadia Caterina	Zullo Lasala	Woman	Italy	nadiacaterina.zullolasala@innovationriver.it	Category C Recognised	Team member		
Mr	Diego	Grimani	Man	Italy	diego.grimani@innovationriver.it	Category C Recognised	Leading		
Mrs	Marialuisa	Scalise	Woman	Italy	Marialuisa.scalise@innovationriver.it	Category C Recognised	Team member		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Development of a Performing Secure Platform for IEEE 802.15.4 WSN Applications*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
WAY2AGE	*Voice Assistants to detect early cognitive decline - HORIZON, proposal submission*
AGRITECH	*Smart agricolture - KDT2022, proposal preparation (early stage)*
aFarEdge	*Smart agricolture - KDT2022, proposal preparation (early stage)*
Sentient	*Key Technology capabilities for European Safety and security*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
1	*Dell Server Rack, Cloud storage equipment, Cisco Networking equipment, OVH Cloud services*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? ○ Yes ◉ No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
918599119	*INTECS SOLUTIONS SPA*

Short name: INT

Address

Street	VIA GIACOMO PERONI 130
Town	ROMA
Postcode	00131
Country	Italy
Webpage	www.intecs.it

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	18/10/2022	- no
SME self-assessment	31/12/2021	- no
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name	Automotive & Smart Systems	☐ not applicable
	☒ Same as proposing organisation's address	
Street	VIA GIACOMO PERONI 130	
Town	ROMA	
Postcode	00131	
Country	Italy	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ◉ Woman ○ Man ○ Non Binary

First name* **Katia**

Last name* **Di Blasio**

E-Mail* **katia.diblasio@intecs.it**

Position in org. Automotive & Smart Systems – Funded Research Projects T. U. Manager

Department Automotive & Smart Systems

☐ Same as organisation name

☒ Same as proposing organisation's address

Street VIA GIACOMO PERONI 130

Town ROMA

Post code 00131

Country Italy

Website *Please enter website*

Phone *+xxx xxxxxxxxx*

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Simone	Gianfranceschi	simone.gianfranceschi@intecs.it	+xxx xxxxxxxxx
Francesco	Teti	francesco.teti@intecs.it	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier

Role of participating organisation in the project

Project management	☒
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AI-augmented automation supporting modeling, coding, testing, monitoring, and continuous development in Cyber-Physical Systems - ECSEL Joint Undertaking (JU) under grant agreement No 101007350.*
VALU3S	*Design, implement and evaluate state-of-the-art V&V methods and tools in order to reduce the time and cost needed to verify and validate automated systems with respect to safety, cybersecurity and privacy (SCP) requirements - ECSEL Joint Undertaking (JU) under grant agreement No 876852*
AQUAS	*Efficient solutions for the entire product life-cycle within three essential capibilities: Design Technologies (DT), Cyber-Physical Systems (CPS), and European Asset5 Protection (EAP) considering inter-dependence of safety, security and performance of systems - Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737475*
MegaMart2	*A scalable model-based framework for continuous development and runtime validation of complex systems - Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737494.*
SAFECOP	*ML-based approaches for SW testing and cooperative function verification*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? ○ Yes ◉ No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
899412810	*Swascan SRL*

Short name: SWA

Address

Street	piazzale bande nere 9
Town	Milano
Postcode	20146
Country	Italy
Webpage	www.swascan.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	unknown
Secondary or Higher education establishment	unknown
Research organisation	unknown

SME Data

Based on the below details from the Participant Registry the organisation is unknown (small- and medium-sized enterprise) for the call.

SME self-declared status	unknown
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name: Cybersecurity Team ☐ not applicable

☐ Same as proposing organisation's address

Street: via Fabio Filzi 2B

Town: Cernusco sul Naviglio

Postcode: 20063

Country: Italy

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Giuseppe**

Last name* **Dongu**

E-Mail* **g.dongu@swascan.com**

Position in org. Cybersecurity Team

Department Cybersecurity Team

☐ Same as organisation name

☐ Same as proposing organisation's address

Street via Fabio Filzi 2B

Town Cernusco sul Naviglio

Post code 20063

Country Italy

Website *Please enter website*

Phone +393471461398

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Davide	Maniscalco	d.maniscalco@swascan.com	+xxx xxxxxxxxx
Cristina	Spagnoli	c.spagnoli@swascan.com	+xxx xxxxxxxxx
Stefania	Casella	s.casella@swascan.com	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Software	*Threat intelligence and Vulnerability Assessment SaaS Platform*
Software	*Vulnerability Management System (VMS)*
Publication	*Cyber Risk Indicators: Italian Critical Infrastructures*
Publication	*Beep malware: static and dynamic analysis*
Publication	⊠⊠*Vulnerability Report – Instant Developer RD3 (CVE-2022-39983)*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
Mobile POS	*Security requirements for the new Italian Mobile Digital Payment Circuit*
Banking Red Team	*Red teaming activity on one of the major italian banking group infrastructure*
SOCaaS	*Deployment of the Swascan Security Operation Center as a Service*
Incident Response	*Response and Recovery to Ramnsomware attacks*
CESA	*Automatic Security Assessment for Cloud Environments*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? ○ Yes ◉ No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
917522322	*TEKNE SRL*

Short name: TEK

Address

Street	CONTRADA SAN MATTEO 42
Town	POGGIOFIORITO
Postcode	66030
Country	Italy
Webpage	www.tekne.it

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	14/01/2022 - yes
SME self-assessment	14/01/2022 - yes
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	Research & Development	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Contrada Alboreto snc Ortona	
Town	Ortona	
Postcode	66026	
Country	Italy	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Francesco**

Last name* **Barcio**

E-Mail* **f.barcio@tekne.it**

Position in org. Technical Director

Department Research & Development

☐ Same as organisation name

☐ Same as proposing organisation's address

Street Contrada Alboreto snc Ortona

Town Ortona

Post code 66026

Country Italy

Website *Please enter website*

Phone +393483108969

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Carlo	Tieri	c.tieri@tekne.it	+393483108969

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AI-augmented automation supporting modeling, coding, testing, monitoring, and continuous development in Cyber-Physical Systems - ECSEL Joint Undertaking (JU) under grant agreement No 101007350.*
MegaMart2	*A scalable model-based framework for continuous development and runtime validation of complex systems - Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737494.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
1	*Automotive testing area*
2	*Automotive testing area*
3	*Integration Area*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999841663	*UNIVERSITA DEGLI STUDI DI CAGLIARI*

Short name: UNICA

Address

Street	VIA UNIVERSITA 40
Town	CAGLIARI
Postcode	09124
Country	Italy
Webpage	WWW.UNICA.IT

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	26/01/2022	- no
SME self-assessment	14/03/2014	- no
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name	Department of Electrical and Electronic Engineering	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Via Marengo, 3	
Town	Cagliari	
Postcode	09123	
Country	Italy	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title: Prof.

Gender: (•) Woman ( ) Man ( ) Non Binary

First name*: **Francesca**

Last name*: **Palumbo**

E-Mail*: **francesca.palumbo@unica.it**

Position in org.: Associate Professor

Department: Department of Electrical and Electronic Engineering

☐ Same as organisation name

☐ Same as proposing organisation's address

Street: Via Marengo, 3

Town: Cagliari

Post code: 09134

Country: Italy

Website: https://web.unica.it/unica/en/dip_ingelettrica.page

Phone: +393463953315

Phone 2: *+xxx xxxxxxxxx*

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Prof	Francesca	Palumbo	Woman	Italy	francesca.palumbo@unica.it	Category B Senior resea	Leading	0000-0002-6155-1979	Orcid ID
Prof	Luigi	Raffo	Man	Italy	raffo@unica.it	Category A Top grade re	Team member	0000-0001-9683-009X	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Francesco Ratto, Ángela Porras Máinez, Carlo Sau, Paolo Meloni, Gianfranco Deriu, Stefano Delucchi, Massimo Massa, Luigi Raffo, Francesca Palumbo: An Automated Design Flow for Adaptive Neural Network Hardware Accelerators. J. Signal Process. Syst. 95(9): 1091-1113 (2023)*
Publication	*Francesco Ratto, Stefano Esposito, Carlo Sau, Luigi Raffo, Francesca Palumbo: Multithread Accelerators on FPGAs: A Dataflow-Based Approach. PARMA-DITAM@HiPEAC 2022: 6:1-6:14*
Publication	*Claudio Rubattu, Francesca Palumbo, Shuvra S. Bhattacharyya, Maxime Pelcat: PathTracer: Understanding Response Time of Signal Processing Applications on Heterogeneous MPSoCs. ACM Trans. Model. Perform. Evaluation Comput. Syst. 6(4): 15:1-15:30 (2021)*
Publication	*Yehya Nasser, Carlo Sau, Jean-Christophe Prévotet, Tiziana Fanni, Francesca Palumbo, Maryline Hélard, Luigi Raffo: NeuPow: A CAD Methodology for High-level Power Estimation Based on Machine Learning. ACM Trans. Design Autom. Electr. Syst. 25(5): 41:1-41:29 (2020)*
Software	*Multi-Dataflow Composer tool (https://mdc-suite.github.io/) cite as Carlo Sau, Tiziana Fanni, Claudio Rubattu, Luigi Raffo, Francesca Palumbo: The Multi-Dataflow Composer tool: An open-source tool suite for optimized coarse-grain reconfigurable hardware accelerators and platform design. Microprocess. Microsystems 80: 103326 (2021)*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
MYRTUS	*The MYRTUS project aims at unlocking the new living dimension of CPS, embracing the principles of the EU CloudEdgeIOT Initiative, integrating edge, fog and cloud computing platforms. This integration requires the reinvention of programming languages and tools to orchestrate collaborative distributed and decentralised components. Additionally, components must be augmented with interface contracts covering both functional and non-functional properties.*
FitOptiVis	*In the realm of Cyber-Physical Systems (CPS), the need for swift and accurate image and video processing is paramount. In this context, the EU-funded FitOptiVis project aims to revolutionise this vital aspect of CPS integration. By leveraging a comprehensive approach supported by cutting-edge, low-power, high-performance smart devices, FitOptiVis will create a reference architecture for seamless integration of image- and video-processing pipelines.*
CERBERO	*CERBERO provides a model-based methodology and toolset for design, incremental prototyping, verification and continuous developments of adaptive CPS. Run-time CPS management is enabled leveraging on strategies for system-in-the loop co-simulation, continuous monitoring, optimization and system reconfiguration to provide high (optimal) performance, while being reactive to users' needs and changed environmental conditions.*
ALOHA	*DL algorithms are an extremely promising instrument in artificial intelligence. To foster their adoption in new applications and markets, a step forward is needed towards the implementation of DL inference on low-power embedded systems, enabling a shift to the edge computing paradigm. The main goal of ALOHA is to facilitate implementation of DL algorithms on heterogeneous low-energy computing platforms providing automation for optimal algorithm selection, resource allocation and porting.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
Microelectronics and Bioengineering Lab	*FPGA and CAD for embedded and cyber-physical system design*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
999465594	*UNIVERSITA DEGLI STUDI DI SASSARI*

Short name: UNISS

Address

Street	PIAZZA UNIVERSITA 21
Town	SASSARI
Postcode	07100
Country	Italy
Webpage	www.uniss.it

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	07/03/2014	- no
SME self-assessment	07/03/2014	- no
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name	Dipartimento di Scienze Umanistiche e Sociali,	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Via Roma 151	
Town	Sassari	
Postcode	07100	
Country	Italy	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title _____ Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Luca** Last name* **Pulina**

E-Mail* **lpulina@uniss.it**

Position in org. Professor

Department Dipartimento di Scienze Umanistiche e Sociali ☐ Same as organisation name

☐ Same as proposing organisation's address

Street Via Roma 151

Town Sassari Post code 07100

Country Italy

Website *Please enter website*

Phone *+xxx xxxxxxxxx* *Phone 2* *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Laura	Pandolfo	lpandolfo@uniss.it	+xxx xxxxxxxxx

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Prof	Luca	Pulina	Man	Italy	lpulina@uniss.it			0000-0003-0258-3222	Orcid ID
Dr	Laura	Pandolfo	Woman	Italy	lpandolfo@uniss.it			0000-0003-0258-3222	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☒
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*Guidotti, Dario, Luca Pulina, and Armando Tacchella. "pynever: A framework for learning and verification of neural networks." Automated Technology for Verification and Analysis: 19th International Symposium, ATVA 2021, Gold Coast, QLD, Australia, October 18–22, 2021, Proceedings 19. Springer International Publishing, 2021.*
Publication	*Guidotti, D., Leofante, F., Pulina, L., & Tacchella, A. (2020). Verification of Neural Networks: Enhancing Scalability Through Pruning. In ECAI 2020 (pp. 2505-2512). IOS Press.*
Publication	*Guidotti, D., Pandolfo, L., & Pulina, L. (2023, October). Verifying Neural Networks with SMT: An Experimental Evaluation. In 2023 IEEE 19th International Conference on e-Science (e-Science) (pp. 1-2). IEEE.*
Publication	*Guidotti, D., Pandolfo, L., & Pulina, L. (2023, November). Verifying Neural Networks with Non-Linear SMT Solvers: a Short Status Report. In 2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI) (pp. 423-428). IEEE.*
Publication	*Eramo, R., Fanni, T., Guidotti, D., Pandolfo, L., Pulina, L., & Zedda, K. (2022). Verification of neural networks: Challenges and perspectives in the aidoart project. Proceedings of RiCeRcA 2022, 3345.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AI-augmented automation supporting modeling, coding, testing, monitoring, and continuous development in Cyber-Physical Systems - ECSEL Joint Undertaking (JU) under grant agreement No 101007350.*
SECURED	*Scaling Up secure Processing, Anonymization and generation of Health Data for EU cross border collaborative research and Innovation - HORIZON-HLTH-2022-IND-13. Project ID: 101095717*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
998475709	*UNIVERSITA DEGLI STUDI DI TERAMO*

Short name: UNITE

Address

Street	VIA RENATO BALZARINI 1 3 5 7
Town	TERAMO
Postcode	64100
Country	Italy
Webpage	www.unite.it

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	01/11/1993	- no
SME self-assessment	01/11/1993	- no
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name	Department of Communication Science	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Campus "Aurelio Saliceti"via R. Balzar	
Town	Teramo	
Postcode	64100	
Country	Sweden	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title: Mrs

Gender: (•) Woman ( ) Man ( ) Non Binary

First name*: **Romina**

Last name*: **Eramo**

E-Mail*: **reramo@unite.it**

Position in org.: Assistant professor

Department: Department of Communication Science

☐ Same as organisation name

☐ Same as proposing organisation's address

Street: Campus "Aurelio Saliceti" via R. Balzarini 1

Town: Teramo

Post code: 64100

Country: Italy

Website: *Please enter website*

Phone: *+xxx xxxxxxxxx*

Phone 2: *+xxx xxxxxxxxx*

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Romina	Eramo	Woman	Italy	reramo@unite.it			0000-0002-3572-5875	Orcid ID
Prof	Luca	Tallini	Man	Italy	ltallini@unite.it			0000-0003-4238-173X	Orcid ID
Prof	Danilo	Pelusi	Man	Italy	dpelusi@unite.it			0000-0003-0889-278X	Orcid ID
Prof	Raffaele	Mascella	Man	Italy	rmascella@unite.it			0000-0002-1305-7853	Orcid ID
Dr	Davide	Fazio	Man	Italy	dfazio2@unite.it			0000-0002-1305-7853	Orcid ID
Dr	Vittoriano	Muttillo	Man	Italy	vmuttillo@unite.it			0000-0002-2220-8326	Orcid ID

Role of participating organisation in the project

Project management	☒
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☐
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*AIDOaRt: AI-augmented Automation for DevOps, a model-based framework for continuous development in Cyber-Physical Systems* *Bruneliere, H., Muttillo, V., Eramo, R., ...Sadovykh, A., Cicchetti, A., Microprocessors and Microsystems this link is disabled, 2022, 94, 104672*
Publication	*Romina Eramo, Vittoriano Muttillo, Luca Berardinelli, Hugo Bruneliere, Abel Gómez, Alessandra Bagnato, Andrey Sadovykh, Antonio Cicchetti:* *AIDOaRt: AI-augmented Automation for DevOps, a Model-based Framework for Continuous Development in Cyber-Physical Systems. DSD 2021: 303-310*
Publication	*Vittorio Cortellessa, Daniele Di Pompeo, Romina Eramo, Michele Tucci: A model-driven approach for continuous performance engineering in microservice-based systems. J. Syst. Softw. 183: 111084 (2022)*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AI-augmented automation supporting modeling, coding, testing, monitoring, and continuous development in Cyber-Physical Systems - ECSEL Joint Undertaking (JU) under grant agreement No 101007350.*
MegaMart2	*A scalable model-based framework for continuous development and runtime validation of complex systems - Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737494.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
999859511	*UNIVERSITA DEGLI STUDI DELL'AQUILA*

Short name: UNIVAQ

Address

Street	PIAZZA SANTA MARGHERITA 2
Town	L AQUILA
Postcode	67100
Country	Italy
Webpage	

Specific Legal Statuses

Legal person	yes
Public body	yes
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	yes
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	07/03/2014	- no
SME self-assessment	07/03/2014	- no
SME validation	unknown	

Departments carrying out the proposed work

Department 1

Department name	Center of Excellence DEWS	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Via Vetoio snc, Loc. Coppito	
Town	L'Aquila	
Postcode	67100	
Country	Italy	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Luigi**

Last name* **Pomante**

E-Mail* **luigi.pomante@univaq.it**

Position in org. Assistant Professor (tenured)

Department DISIM

☐ Same as organisation name

☐ Same as proposing organisation's address

Street Via Vetoio snc, Loc. Coppito

Town L'Aquila

Post code 67100

Country Italy

Website *Please enter website*

Phone *+xxx xxxxxxxxx*

Phone 2 *+xxx xxxxxxxxx*

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Luigi	Pomante	Man	Italy	luigi.pomante@univaq.it	Category B Senior resea	Leading		
Dr	Marco	Santic	Man	Italy	marco.santic@guest.univaq.it	Category C Recognised	Team member		
Dr	Vittoriano	Muttillo	Man	Italy	vittoriano.muttillo@guest.univaq.it	Category C Recognised	Team member		

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☒
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*C. Brandolese, W. Fornaciari, L. Pomante, F. Salice, D. Sciuto. "Affinity-Driven System Design Exploration for Heterogeneous Multiprocessor SoC", IEEE Transactions on Computers, vol. 55, no. 5, 2006.*
Publication	*L. Pomante, "System-Level Design Space Exploration for Dedicated Heterogeneous Multi-Processor Systems". IEEE Int. Conf. on Application-specific Systems, Architectures and Processors (ASAP), 2011.*
Software	*HEPSYCODE (www.hepsycode.com)*
Publication	*Luigi Pomante, Vittoriano Muttillo, Marco Santic, Paolo Serri, SystemC-based electronic system-level design space exploration environment for dedicated heterogeneous multi-processor systems, Microprocessors and Microsystems, Volume 72, 2020.*
Publication	*Muttillo, V., Pomante, L., Santic, M. & Valente, G. "SystemC-based co-simulation/analysis for system-level hardware/software co-design", Computers and Electrical Engineering, vol. 110, 2023.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
MEGAMART2	*In this project, the HEPSYCODE methodology has been extended to manage mixed-critical requirements at system-level. In AIDOSEC we will introduce also system-level security requirements.*
FITOPTIVIS	*In this project, the HEPSYCODE methodology has been extended to manage energy and power requirements at system-level. In AIDOSEC we will introduce also system-level security requirements.*
AQUAS	*In this project, the HEPSYCODE methodology has been extended to manage real-time requirements at system-level. In AIDOSEC we will introduce also system-level security requirements.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
974564433	*Alstom Rail SWEDEN AB*

Short name: AR

Address

Street	OSTRA RINGVAGEN 2
Town	VASTERAS
Postcode	721 73
Country	Sweden
Webpage	https://www.alstom.com/

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	08/07/2016 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	TCMS TWST Validation & Safety	☐ not applicable
	☒ Same as proposing organisation's address	
Street	OSTRA RINGVAGEN 2	
Town	VASTERAS	
Postcode	721 73	
Country	Sweden	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Mr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Singh**

Last name* **Inderjeet**

E-Mail* **singh.inderjeet@alstomgroup.com**

Position in org. Software Domain Leader

Department TCMS TWST Validation & Safety

☐ Same as organisation name

☒ Same as proposing organisation's address

Street OSTRA RINGVAGEN 2

Town VASTERAS

Post code 721 73

Country Sweden

Website *Please enter website*

Phone +46 765172367

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Daran	Smallay	daran.smalley@alstomgroup.com	+46769410637

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Mr	Inderjeet	Singh	Man	Sweden	Singh.inderjeet@alstomgroup.com	Category D First stage r	Leading		
Mr	Zulqarnain	Haider	Man	Pakistan	zulqarnain.haider@alstomgroup.com	Category D First stage r	Team member		
Mr	Daran	Smalley	Man	Australia	daran.smalley@alstomgroup.com	Category C Recognised	Team member		

Role of participating organisation in the project

Project management	☒
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☐
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Publication	*A Model-Based Test Script Generation Framework for Embedded Software (Feb 2021) Muhammad Nouman Zafar, Wasif Afzal, Eduard Paul Enoiu, Athanasios Stratis , Ola Sellin The 17th Workshop on Advances in Model Based Testing (A-MOST 2021)*
Software	*Soft TCMS is a software test environment, so that the integrated train software components can be tested and debugged in a simulated environment. Soft TCMS compiles the CCU C code for Windows, enabling it to run on a desktop computer. When multiple instances of the CCU code are running, the bus communication is simulated by Soft TCMS.*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
RELIANCE	*EUREKA/CELTICnext project on 5G communications use case for railway IoT*
IVVES	*EUREKA/ITEA3 project on Health and Performance monitoring of onboard railway equipment*
MegaM@rt2	*ECSEL project (grant agreement No 737494). MegaM@Rt created a framework incorporating methods and tools for continuous development and validation*
XIVT	*EUREKA/ITEA3 project on variant testing and product line engineering.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
Powerlab. Lab	*Alstom Västerås Powerlab. Lab for test and verification of rail and road electromobility powertrains. Will act as a source of data and as the base infrastructure of the implementation test bed for solutions developed in the project.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

Administrative forms

PIC	Legal name
999613422	*RISE RESEARCH INSTITUTES OF SWEDEN AB*

Short name: RISE

Address

Street	BRINELLGATAN 4
Town	BORAS
Postcode	501 15
Country	Sweden
Webpage	www.ri.se

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	yes
International organisation	no
Secondary or Higher education establishment	no
Research organisation	yes

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	23/12/2021 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	R&D RISE Västerås	☐ not applicable
	☐ Same as proposing organisation's address	
Street	Storagatan 36	
Town	Västerås	
Postcode	722 12	
Country	Sweden	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ◯ Woman ◉ Man ◯ Non Binary

First name* **Mehrdad**

Last name* **Saadatmand**

E-Mail* **mehrdad.saadatmand@ri.se**

Position in org. Senior Researcher; Program area manager of software engineering and testing

Department RISE Västerås ☐ Same as organisation name

☐ Same as proposing organisation's address

Street Storagatan 36

Town Västerås

Post code 722 12

Country Sweden

Website *Please enter website*

Phone +46 72 569 59 56

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Muhammad	Abbas	muhammad.abbas@ri.se	+46102284436

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Mehrdad	Saadatmand	Man	Sweden	mehrdad.saadatmand@ri.se	Category B Senior resea	Leading	0000-0002-1512-0844	Orcid ID
Mr	Muhammad	Abbas	Man	Pakistan	muhammad.abbas@ri.se	Category C Recognised	Team member	0000-0001-6418-9971	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☒
Provision of research and technology infrastructure	☒
Co-definition of research and market needs	☒
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☒
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☐
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Software	*VARA: Variability aware reuse recommendation and analysis*
Software	*SaFReL: A machine learning-assisted stress testing framework for smart generation of stress test cases leading to performance breaking points, without access to model or source code. It is able to learn how to find performance breaking points through observing performance behavior of software programs and re-playing the learnt policy in further situations.*
Publication	*"Requirements-driven Reuse Recommendation"; Muhammad Abbas, Mehrdad Saadatmand , Eduard Paul Enoiu; 25th ACM International Systems and Software Product Line Conference (SPLC 2021)*
Publication	*"Automated Performance Testing Based on Active Deep Learning"; Ali Sedaghatbaf, Mahshid Helali Moghadam, Mehrdad Saadatmand; ACM/IEEE International Conference on Automation of Software Test; May 2021*
Software	*"An Autonomous Performance Testing Framework using Self-Adaptive Fuzzy Reinforcement Learning"; Mahshid Helali Moghadam, Mehrdad Saadatmand , Markus Borg , Markus Bohlin, Björn Lisper; Software Quality Journal; March 2021*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
SmartDelta	*ITEA project on Automated Quality Assurance and Optimization in Incremental Industrial Software Systems Development*
IVVES	*Industrial-grade Verification and Validation of Evolving Systems (Oct 2019 – Dec 2022) ; 3-year international project consisting of 26 industrial and research partners from Sweden, Canada, Spain, Finland, and Netherlands, doing industrial research on application of AI and Machine Learning in verification and validation of systems, and also verification and validation techniques for systems with AI and ML components (http://ivves.eu/)*
AIDOaRt	*AIDOaRt is a 3-year European project involving 32 organizations, grouped in clusters from 7 different countries, focusing on AI-enhanced automation that supports modeling, coding, testing, monitoring and continuous development in Cyber-Physical Systems (CPS) or embedded system.*
XIVT	*XIVT - Excellence In Variant Testing (Nov 2018 – Mar 2022); 3-year international project consisting of 22 industrial and research partners from Sweden, Germany, Canada, Portugal, and Turkey, doing industrial research on testing of highly configurable variant-intensive systems (https://www.xivt.org/)*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

PIC	Legal name
906739123	*WESTERMO NETWORK TECHNOLOGIES AB*

Short name: WMO

Address

Street	METALLVERKSGATAN 6
Town	VASTERAS
Postcode	721 30
Country	Sweden
Webpage	www.westermo.com

Specific Legal Statuses

Legal person	yes
Public body	no
Non-profit	no
International organisation	no
Secondary or Higher education establishment	no
Research organisation	no

SME Data

Based on the below details from the Participant Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

SME self-declared status	24/04/2018 - no
SME self-assessment	unknown
SME validation	unknown

Departments carrying out the proposed work

Department 1

Department name	Westemo Network Technologies AB, Research and Development	☐ not applicable
	☒ Same as proposing organisation's address	
Street	METALLVERKSGATAN 6	
Town	VASTERAS	
Postcode	721 30	
Country	Sweden	

Links with other participants

Type of link	Participant

Main contact person

This will be the person the EU services will contact concerning this proposal (e.g. for additional information, invitation to hearings, sending of evaluation results, convocation to start grant preparation). The data in blue is read-only. Details (name, first name and e-mail) of Main Contact persons should be edited in the step "Participants" of the submission wizard.

Title Dr

Gender ○ Woman ◉ Man ○ Non Binary

First name* **Per Erik**

Last name* **Strandberg**

E-Mail* **per.strandberg@westermo.com**

Position in org. Project Manager

Department Westemo Network Technologies AB, Research and Development

☐ Same as organisation name

☒ Same as proposing organisation's address

Street METALLVERKSGATAN 6

Town VASTERAS

Post code 721 30

Country Sweden

Website *Please enter website*

Phone *+xxx xxxxxxxxx*

Phone 2 *+xxx xxxxxxxxx*

Other contact persons

First Name	Last Name	E-mail	Phone
Mikaela	Näslund	mikaela.naslund@westermo.com	+46705931226

Researchers involved in the proposal

Title	First Name	Last Name	Gender	Nationality	E-mail	Career Stage	Role of researcher (in the project)	Reference Identifier	Type of identifier
Dr	Per	Strandberg	Man	Sweden	per.strandberg@westermo.com	Category C Recognised	Leading	0000-0003-1688-6937	Orcid ID

Role of participating organisation in the project

Project management	☐
Communication, dissemination and engagement	☐
Provision of research and technology infrastructure	☐
Co-definition of research and market needs	☐
Civil society representative	☐
Policy maker or regulator, incl. standardisation body	☐
Research performer	☐
Technology developer	☒
Testing/validation of approaches and ideas	☒
Prototyping and demonstration	☒
IPR management incl. technology transfer	☐
Public procurer of results	☐
Private buyer of results	☐
Finance provider (public or private)	☐
Education and training	☐
Contributions from the social sciences or/and the humanities	☐
Other If yes, please specify: (Maximum number of characters allowed: 50)	☐

List of up to 5 publications, widely-used datasets, software, goods, services, or any other achievements relevant to the call content.

Type of achievement	Short description (Max 500 characters)
Software	*WeOS (the Westermo Operating System) is the GNU/Linux-based operating system used in many of Westermo products. It's an edge industrial network operating system. https://www.westermo.com/solutions/weos*
Publication	*J Cederbladh, R Eramo, V Muttillo, PE Strandberg. (2024). Experiences and challenges from developing cyber-physical systems in industry-academia collaboration. Wiley's Software: Practice and Experience*
Dataset	*PE Strandberg & Y Marklund. (2023). The Westermo test system performance data set. Technical report. https://arxiv.org/abs/2311.14510*
Publication	*M Abbas, A Hamayouni, M Helali Moghadam, M Saadatmand, and PE Strandberg. (2023). Making Sense of Failure Logs in an Industrial DevOps Environment. ITNG'23.*
Publication	*Strandberg, PE (2021). Automated system-level software testing of industrial networked embedded systems. Doctoral thesis. Mälardalen University (Sweden).*

List of up to 5 most relevant previous projects or activities, connected to the subject of this proposal.

Name of Project or Activity	Short description (Max 500 characters)
AIDOaRt	*AI-augmented automation supporting modeling, coding, testing, monitoring, and continuous development in Cyber-Physical Systems. AIDOaRt has a total turnover of € 24.4 million and employs 80 full-time equivalents with academic and industrial researchers, project managers and other staff in our 32 organizations.*
InSecTT	*Intelligent Secure Trustable Things: a pan-European effort with 52 key partners from 12 countries (EU and Turkey).*
Safe4Rail3	*Safe4RAIL-3 will deliver next-generation network devices with higher TRL that integrate the Drive-by-Data concept based on Time Sensitive Network technology*
FIN	*Future Industrial Networks explroes an efficient employment of new technologies and innovations in the process industry by reducing obstacles to the efficient exchange of information between IT and OT in a common infrastructure.*
TESTMINE	*Mining Test Evolution for Improved Software Regression Test Selection (TESTMINE) aimed at proposing and validating novel techniques for regression test selection that do not rely on code-coverage information. Instead, these techniques harness test evolution data to improve efficiency and effectiveness in system-level testing, particularly for real-time/embedded software.*

Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work.

Name of infrastructure of equipment	Short description (Max 300 characters)
Software Testing Laboratory.	*Software Testing Laboratory. Westermo has an internally developed test framework used for manual exploratory testing as well as automated testing of WeOS. In the test lab, more than a tonne of equipment is in place for this purpose. Part of the test lab is also third party testing tools such as Achi*
Hardware Laboratory	*Hardware Laboratory. Westermo has technical equipment for investigating prototypes, running temperature tests, debugging hardware, etc.*

Gender Equality Plan

Does the organization have a Gender Equality Plan (GEP) covering the elements listed below? (•) Yes ( ) No

Minimum process-related requirements (building blocks) for a GEP

- **Publication:** formal document published on the institution's website and signed by the top management
- **Dedicated resources:** commitment of human resources and gender expertise to implement it.
- **Data collection and monitoring:** sex/gender disaggregated data on personnel (and students for establishments concerned) and annual reporting based on indicators.
- **Training:** Awareness raising/trainings on gender equality and unconscious gender biases for staff and decision-makers.
- **Content-wise, recommended areas** to be **covered** and addressed via concrete measures and targets are:
    - work-life balance and organisational culture;
    - gender balance in leadership and decision-making;
    - gender equality in recruitment and career progression;
    - integration of the gender dimension into research and teaching content;
    - measures against gender-based violence including sexual harassment.

3 - Budget

No.	Name of beneficiary	Country	Role	Personnel costs/€	Subcontracting costs/€	Purchase costs - Travel and substistence/€	Purchase costs - Equipment/€	Purchase costs - Other goods, works and services/€	Internally invoiced goods and services/€ (Unit costs-usual accounting practices)	Indirect costs/€	Total eligible costs	Funding rate	Maximum EU contribution to eligible costs	Requested EU contribution to eligible costs/€	Max grant amount	Income generated by the action	Financial contributions	Own resources	Total estimated income
1	Malardalens Universitet	SE	Coordinator	671 808	40 000	25 000	4 389	10 000	0	177 799.25	928 996.25	35	325 148.69	325 148.69	325 148.69	0.00	0.00	0.00	325 148.69
2	Ait Austrian Institute Of Technology	AT	Partner	366 648	0	25 000	0	6 359	0	99 501.75	497 508.75	35	174 128.06	174 128.06	174 128.06	0.00	0.00	0.00	174 128.06
3	Dynatrace Austria Gmbh	AT	Partner	704 000	0	25 000	0	0	0	182 250.00	911 250.00	35	318 937.50	318 937.50	318 937.50	0.00	0.00	0.00	318 937.50
4	Gts Ground Transportation Systems	AT	Partner	601 000	0	28 000	0	0	0	157 250.00	786 250.00	35	275 187.50	275 187.50	275 187.50	0.00	0.00	0.00	275 187.50
5	Universitat Linz	AT	Partner	287 670	0	25 000	0	0	0	78 167.50	390 837.50	35	136 793.13	136 793.13	136 793.13	0.00	0.00	0.00	136 793.13
6	Kapsch Trafficcom Ag	AT	Partner	720 000	0	37 500	0	0	0	189 375.00	946 875.00	35	331 406.25	331 406.25	331 406.25	0.00	0.00	0.00	331 406.25
7	Lieberlieber Software Gmbh	AT	Partner	257 400	0	25 000	0	70 600	0	88 250.00	441 250.00	35	154 437.50	154 437.50	154 437.50	0.00	0.00	0.00	154 437.50
8	Msg Plaut Austria Gmbh	AT	Partner	573 187	0	26 000	4 000	0	0	150 796.75	753 983.75	35	263 894.31	263 894.31	263 894.31	0.00	0.00	0.00	263 894.31
9	Vysoke Uceni Technicke V Brne	CZ	Partner	438 300	0	30 000	0	117 075	0	146 343.75	731 718.75	35	256 101.56	256 101.56	256 101.56	0.00	0.00	0.00	256 101.56
10	Camea Spol Sro	CZ	Partner	336 000	0	20 000	15 000	51 250	0	105 562.50	527 812.50	35	184 734.38	184 734.38	184 734.38	0.00	0.00	0.00	184 734.38

11	Cognitechna Sro	CZ	Partner	180 000	0	25 000	0	0	0	51 250.00	256 250.00	35	89 687.50	89 687.50	89 687.50	0.00	0.00	0.00	89 687.50
12	Acorde Technologies Sa	ES	Partner	331 200	0	20 000	24 000	0	0	93 800.00	469 000.00	35	164 150.00	164 150.00	164 150.00	0.00	0.00	0.00	164 150.00
13	Hi Iberia Ingenieria Y Proyectos Sl	ES	Partner	451 200	0	20 000	0	0	0	117 800.00	589 000.00	35	206 150.00	206 150.00	206 150.00	0.00	0.00	0.00	206 150.00
14	Prodevelop Sl	ES	Partner	295 200	0	24 000	0	5 000	0	81 050.00	405 250.00	35	141 837.50	141 837.50	141 837.50	0.00	0.00	0.00	141 837.50
15	Universidad De Cantabria	ES	Partner	304 542	0	21 600	0	800	0	81 735.50	408 677.50	35	143 037.13	143 037.13	143 037.13	0.00	245 206.25	20 434.12	408 677.50
16	Fundacio Per A La Universitat	ES	Partner	274 881	0	24 000	2 475	11 290	0	78 161.50	390 807.50	35	136 782.63	136 782.63	136 782.63	0.00	0.00	0.00	136 782.63
17	Ust Spain Inside S.l.	ES	Partner	315 864	0	30 000	0	12 200	0	89 516.00	447 580.00	35	156 653.00	156 653.00	156 653.00	0.00	0.00	0.00	156 653.00
18	Abo Akademi	FI	Partner	614 160	0	35 000	10 000	10 000	0	167 290.00	836 450.00	35	292 757.50	292 757.50	292 757.50	0.00	0.00	0.00	292 757.50
19	Haltian Oy	FI	Partner	930 000	0	30 000	0	0	0	240 000.00	1 200 000.00	35	420 000.00	420 000.00	420 000.00	0.00	0.00	0.00	420 000.00
20	Process Genius Oy	FI	Partner	335 000	0	30 000	15 000	15 000	0	98 750.00	493 750.00	35	172 812.50	172 812.50	172 812.50	0.00	0.00	0.00	172 812.50
21	Solidcomp Oy	FI	Partner	335 000	0	5 000	30 000	30 000	0	100 000.00	500 000.00	35	175 000.00	175 000.00	175 000.00	0.00	0.00	0.00	175 000.00
22	Thinglink Oy	FI	Partner	725 000	0	30 000	15 000	10 000	0	195 000.00	975 000.00	35	341 250.00	341 250.00	341 250.00	0.00	0.00	0.00	341 250.00
23	Ita-suomen Yliopisto	FI	Partner	1 125 000	0	50 000	15 000	10 000	0	300 000.00	1 500 000.00	35	525 000.00	525 000.00	525 000.00	0.00	0.00	0.00	525 000.00
24	Institut Mines-telecom	FR	Partner	420 160	0	25 000	0	2 500	0	111 915.00	559 575.00	35	195 851.25	195 851.25	195 851.25	0.00	0.00	0.00	195 851.25
25	Softeam	FR	Partner	1 130 500	0	30 000	0	0	0	290 125.00	1 450 625.00	35	507 718.75	507 718.75	507 718.75	0.00	0.00	0.00	507 718.75
26	Thales	FR	Partner	1 488 000	0	50 000	10 000	9 000	0	389 250.00	1 946 250.00	35	681 187.50	681 187.50	681 187.50	0.00	0.00	0.00	681 187.50
27	Abinsula Srl	IT	Partner	220 500	0	19 500	0	0	0	60 000.00	300 000.00	35	105 000.00	105 000.00	105 000.00	0.00	0.00	0.00	105 000.00

28	Innovation River S.r.l.	IT	Partner	96 000	0	20 000	0	0	0	29 000.00	145 000.00	35	50 750.00	50 750.00	50 750.00	0.00	0.00	0.00	50 750.00
29	Intecs Solutions Spa	IT	Partner	280 000	0	20 000	0	0	0	75 000.00	375 000.00	35	131 250.00	131 250.00	131 250.00	0.00	0.00	0.00	131 250.00
30	Swascan Srl	IT	Partner	360 000	0	20 000	0	0	0	95 000.00	475 000.00	35	166 250.00	166 250.00	166 250.00	0.00	0.00	0.00	166 250.00
31	Tekne Srl	IT	Partner	283 200	0	20 000	0	0	0	75 800.00	379 000.00	35	132 650.00	132 650.00	132 650.00	0.00	0.00	0.00	132 650.00
32	Universita Degli Studi Di Cagliari	IT	Partner	67 500	0	23 125	0	0	0	22 656.25	113 281.25	35	39 648.44	39 648.44	39 648.44	0.00	0.00	0.00	39 648.44
33	Universita Degli Studi Di Sassari	IT	Partner	67 500	0	5 000	0	0	0	18 125.00	90 625.00	35	31 718.75	31 718.75	31 718.75	0.00	0.00	0.00	31 718.75
34	Universita Degli Studi Di Teramo	IT	Partner	143 500	0	20 000	0	0	0	40 875.00	204 375.00	35	71 531.25	71 531.25	71 531.25	0.00	0.00	0.00	71 531.25
35	Universita Degli Studi Dell'aquila	IT	Partner	108 000	0	20 000	0	0	0	32 000.00	160 000.00	35	56 000.00	56 000.00	56 000.00	0.00	0.00	0.00	56 000.00
36	Alstom Rail Sweden Ab	SE	Partner	1 264 000	0	20 000	0	14 597	0	324 649.25	1 623 246.25	35	568 136.19	568 136.19	568 136.19	0.00	0.00	0.00	568 136.19
37	Rise Research Institutes Of Sweden Ab	SE	Partner	440 000	0	25 000	0	4 000	0	117 250.00	586 250.00	35	205 187.50	205 187.50	205 187.50	0.00	0.00	0.00	205 187.50
38	Westermo Network Technologies	SE	Partner	601 998	0	20 000	1 091	8 000	0	157 772.25	788 861.25	35	276 101.44	276 101.44	276 101.44	0.00	0.00	0.00	276 101.44
			TOTAL	18 143 918	40 000	948 725	145 955	397 671	0	4 909 067.25	24 585 336.25		8 604 867.71	8 604 867.71	8 604 867.71	0.00	245 206.25	20 434.12	8 870 508.08

4 - Ethics & security

Ethics Issues Table

1. Human Embryonic Stem Cells and Human Embryos			Page
Does this activity involve Human Embryonic Stem Cells (hESCs)?	○ Yes	◉ No	
Does this activity involve the use of human embryos?	○ Yes	◉ No	
2. Humans			**Page**
Does this activity involve human participants?	◉ Yes	○ No	54
Are they volunteers for non medical studies (e.g. social or human sciences research)?	◉ Yes	○ No	54
Are they healthy volunteers for medical studies?	○ Yes	◉ No	
Are they patients for medical studies?	○ Yes	◉ No	
Are they potentially vulnerable individuals or groups?	○ Yes	◉ No	
Are they children/minors?	○ Yes	◉ No	
Are they other persons unable to give informed consent?	○ Yes	◉ No	
Does this activity involve interventions (physical also including imaging technology, behavioural treatments, etc.) on the study participants?	○ Yes	◉ No	
Does this activity involve conducting a clinical study as defined by the Clinical Trial Regulation (EU 536/2014)? (using pharmaceuticals, biologicals, radiopharmaceuticals, or advanced therapy medicinal products)	○ Yes	◉ No	
3. Human Cells / Tissues (not covered by section 1)			**Page**
Does this activity involve the use of human cells or tissues?	○ Yes	◉ No	
4. Personal Data			**Page**
Does this activity involve processing of personal data?	○ Yes	◉ No	
Does this activity involve further processing of previously collected personal data (including use of preexisting data sets or sources, merging existing data sets)?	○ Yes	◉ No	
Is it planned to export personal data from the EU to non-EU countries?	○ Yes	◉ No	
Is it planned to import personal data from non-EU countries into the EU or from a non-EU country to another non-EU country?	○ Yes	◉ No	
Does this activity involve the processing of personal data related to criminal convictions or offences?	○ Yes	◉ No	
5. Animals			**Page**
Does this activity involve animals?	○ Yes	◉ No	
6. Non-EU Countries			**Page**
Will some of the activities be carried out in non-EU countries?	○ Yes	◉ No	
In case non-EU countries are involved, do the activities undertaken in these countries raise potential ethics issues?	○ Yes	◉ No	
It is planned to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)?	○ Yes	◉ No	

Is it planned to import any material (other than data) from non-EU countries into the EU or from a non-EU country to another non-EU country? For data imports, see section 4.	○ Yes	◉ No	
Is it planned to export any material (other than data) from the EU to non-EU countries? For data exports, see section 4.	○ Yes	◉ No	
Does this activity involve low and/or lower middle income countries, (if yes, detail the benefit-sharing actions planned in the self-assessment)	○ Yes	◉ No	
Could the situation in the country put the individuals taking part in the activity at risk?	○ Yes	◉ No	

7. Environment, Health and Safety			Page
Does this activity involve the use of substances or processes that may cause harm to the environment, to animals or plants.(during the implementation of the activity or further to the use of the results, as a possible impact) ?	○ Yes	◉ No	
Does this activity deal with endangered fauna and/or flora / protected areas?	○ Yes	◉ No	
Does this activity involve the use of substances or processes that may cause harm to humans, including those performing the activity.(during the implementation of the activity or further to the use of the results, as a possible impact) ?	○ Yes	◉ No	

8. Artificial Intelligence			Page
Does this activity involve the development, deployment and/or use of Artificial Intelligence-based systems?	◉ Yes	○ No	54

9. Other Ethics Issues			Page
Are there any other ethics issues that should be taken into consideration?	○ Yes	◉ No	

I confirm that I have taken into account all ethics issues above and that, if any ethics issues apply, I will complete the ethics self-assessment as described in the guidelines How to Complete your Ethics Self-Assessment ☒

Administrative forms

Proposal ID **101194342-1**

Acronym **AIDOSec**

Ethics Self-Assessment

Ethical dimension of the objectives, methodology and likely impact

Human participants will be involved in the project. The research activities will not include vulnerable populations, or children. There are no medical trials or biological studies implied. However professionals as program developers will test and use systems that are the result of the project, to evaluate them. For this reason, the main issue of the project is related to the protection of personal data. To deal with this issue,
a large space will be given to data management (i.e., how to manage personal data (anonymisation), which will be collected during the testing phase of the project). Data will be anonymised and used just in aggregate form. The raw data will be stored in a key file that only the researchers involved in the research can access. The participants will be informed that data will be used exclusively for scientific and statistical purposes and with the maintenance of anonymity.
All the experimental procedures will be designed in accordance with the Declaration of Helsinki and will ensure the total absence of risk for harm to the participants. The experimental procedures will be submitted for the approval of the local institutional ethics committees. The activities and the impacts of the overall project will not cause any environmental damage, any political or financial adverse consequence, or the stigmatization of social groups. Resources will be used in an ethical manner, to avoid any wasteful or unnecessary use of resources. The results of the activities of the project do not lend themselves to any misuse

Remaining characters 3440

Compliance with ethical principles and relevant legislations

A Ethics and Privacy board will be established, to oversee all relevant processes and aspects. In the Project handbook one section will be dedicated to ethical issues and the strategies and guidelines to address them to guarantee that all the project's activities are conducted in compliance with fundamental ethical principles. Ethics guidelines will focus on the following issues:
Participants' privacy: Specific actions to preserve the privacy of the participants of the project's activities with respect to personal and sensitive data. A privacy format to be signed by each participant who will be part of any activity in the project, in accordance with the (EU) 2016/679 GDPR and national laws of the participating countries. Each participant in the activities will be informed about the data collected in specific actions such as in analysis and piloting activities. All data collected will be treated safely, respecting absolute transparency. All the evaluation information from participants will be treated in an aggregated manner and used only for project purposes, will not be transferred to third parties, and will be preserved within the partner organisations. In addition, project's partners will collect and share images and videos of the participants for dissemination purposes only when they give their consent in written form. No partner will have full access to all these collected data except the coordinator and the partner responsible for quality assurance and impact assessments and evaluations.
Participants' rights: the project involves different target groups of different profession, but all are older than 18, and they all will be clearly informed about their rights and responsibilities as well as the collection of data and the take of pictures and their management. AIDOSec follows a strict policy regarding data protection and management: MDU as the coordinator will guarantee specific formats to be filled by the participants ensure that they have received all needed information, and have read and understood it before their participation. Informed consent documents will be signed by the participants, stating, among others, the background and purpose of the activities, responsibilities, potential risks, procedures related to data storage, and that participants can withdraw from the study at any point during the pilot activities without any obligations whatsoever.
Participants' inclusion: to ensure the full and meaningful inclusion of participants in respect of diversity, the partners are committed to ensuring that participation of different targets in all project activities is managed in an inclusive manner, promoting symbiotic participation of people without any distinction related to any kind of characteristics or demographics.
Gender mainstreaming: A specific section will be dedicated to gender mainstreaming, defining commitment in ensuring the involvement of participants following a gender balance perspective and ensuring that participants of the project's activities will be not discriminated against in relation to their identity and gender. Therefore, a gender perspective will be adopted and strictly applied throughout the project.
Environmental impact: Our project includes several travels and the use of a lot of electronic devices, and both do have an impact on the environment. Therefore, the ethics guidelines will also include a further section dedicated to the environment. This section will set the green policies and measures that will be strictly implemented throughout the project.
Social safety and insurance: the health of everyone remains the top priority in any activity and at all times. We will always prepare and provide safety briefings and guidelines for concerned activities such as travel and the use of electronic devices or used technologies. In this regard, in the pilotings with professionals, we will make sure that they are also in the possession of health insurance prior to the activities. Participants will also be asked and encouraged to share with us any issues that they might have in advance.
Social liability insurance: all partners will have to provide a proof of their social liability insurance at the beginning of the project. We will make sure that the insurance covers damages caused by third parties and also to ensure that it supports possible damage that

can be incurred by the partners. This insurance will be further enhanced by legal protection insurance.
AI: All proposed AI-powered components will explicitly exhibit the following qualities and behaviour with respect to the EU Ethical AI requirements: (i) Human agency and oversight, (ii) Privacy and data governance, (iii) Transparency, (iv) Diversity, non-discrimination, and fairness, (v) Environmental and societal wellbeing, and (vi) Accountability. The proposal specifies dedicated tasks and deliverables for data and ethics management, and any relevant issue that may be raised will be resolved properly

Remaining characters 2

Administrative forms

Proposal ID **101194342-1**

Acronym **AIDOSec**

Security issues table

1. EU Classified Information (EUCI)[2]			Page
Does this activity involve information and/or materials requiring protection against unauthorised disclosure (EUCI)?	○ Yes	◉ No	
Does this activity involve non-EU countries which need to have access to EUCI?	○ Yes	◉ No	
2. Misuse			**Page**
Does this activity have the potential for misuse of results?	○ Yes	◉ No	
3. Other Security Issues			**Page**
Does this activity involve information and/or materials subject to national security restrictions? If yes, please specify: (Maximum number of characters allowed: 1000)	○ Yes	◉ No	
Are there any other security issues that should be taken into consideration? If yes, please specify: (Maximum number of characters allowed: 1000)	○ Yes	◉ No	

Security self-assessment

Please specify: (Maximum number of characters allowed: 5000)

Remaining characters 5000

[2]According to the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, "European Union classified information (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States".

[3]Classified background information is information that is already classified by a country and/or international organisation and/or the EU and is going to be used by the project. In this case, the project must have in advance the authorisation from the originator of the classified information, which is the entity (EU institution, EU Member State, third state or international organisation) under whose authority the classified information has been generated.

[4]EU classified foreground information is information (documents/deliverables/materials) planned to be generated by the project and that needs to be protected from unauthorised disclosure. The originator of the EUCI generated by the project is the European Commission.

Horizon Europe
Chips Joint Undertaking

Innovations Actions (IA) & Research and Innovations Actions (RIA)

Application Form
(HORIZON-JU-Chips-IA and RIA)
1st Stage – Project Outline (PO)

Project proposal – Technical description (Part B)
Proposal AIDOSec

Proposal Part B: technical description

AI-augmented automation for efficient DevOps, a model-based framework for continuous and Secure development of complex systems

Project acronym	AIDOSec
Major Challenges or Focus Topic addressed by the proposal*	Software engineering, operating systems, computer languages. Scientific computing, simulation, and modelling tools. Cyber-physical systems, Cybersecurity. Artificial intelligence, intelligent systems and multi-agent systems.
Anticipated start date of project	March 2025
Duration of project in months	36
Coordinator contact person	Gunnar Widforss

List of participants

Participant No	Participant organisation name	Participant short name	Country	National eligibility checked (Y/N)
1	Mälardalen University	MDU	SE	Y
2	AIT Austrian Institute of Technology GmbH	AIT	AT	Y
3	Dynatrace Austria GmbH	DT	AT	Y
4	GTS Ground Transportation Systems Austria	GTS	AT	Y
5	UNIVERSITAT LINZ	JKU	AT	Y
6	Kapsch TrafficCom AG	KAPSCH	AT	Y
7	LieberLieber Software GmbH	LIE	AT	Y
8	MSG Plaut	MSG	AT	Y
9	Vysoke uceni technicke v Brne	BUT	CZ	Y
10	CAMEA, spol. s r.o.	CAMEA	CZ	Y
11	COGNITECHNA s.r.o.	COG	CZ	Y
12	ACORDE Technologies SA	ACORDE	ES	Y
13	HI-IBERIA INGENIERIA Y PROYECTOS SL	HIB	ES	Y
14	Prodevelop SL	PRO	ES	Y
15	Universidad de Cantabria	UNICAN	ES	Y
16	Fundació per a la Universitat Oberta de Catalunya	UOC	ES	Y
17	Keen Software SL	UST	ES	Y
18	Åbo Akademi University	ABO	FI	Y
19	Haltian	HAL	FI	Y
20	Process Genius Ltd	PG	FI	Y

21	SolidComp Ltd	SC	FI	Y
22	ThingLink	TL	FI	Y
23	University of Eastern Finland	UEF	FI	Y
24	IMT Atlantique	IMT	FR	Y
25	SOFTEAM	SOFT	FR	Y
26	THALES S.A	THA	FR	Y
27	Abinsula Srl	ABI	IT	Y
28	Innovation River	INNORIV	IT	Y
29	Intecs Solutions Spa	INT	IT	Y
30	Swascan Srl	SWA	IT	Y
31	Tekne Srl	TEK	IT	Y
32	Università degli Studi di Cagliari	UNICA	IT	Y
33	Università degli Studi di Sassari	UNISS	IT	Y
34	Università degli Studi di Teramo	UNITE	IT	Y
35	Università degli Studi dell'Aquila	UNIVAQ	IT	Y
36	Alstom Rail Sweden AB	AR	SE	Y
37	RISE Research Institutes of Sweden AB	RISE	SE	Y
38	Westermo Network Technologies AB	WMO	SE	Y

List of abbreviations and acronyms

AI	Artificial Intelligence
AIoT	Artificial Intelligence of Things
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officers
CPS	Cyber-Physical Systems
CST	Cross-Sectional Technology
ECS	Electronic Components and Systems
ECS SRIA	ECS Strategic Research and Innovation Agenda
FTL	Foundational Technology Layer
GDPR	General Data Protection Regulation
IoC	Indicators of Compromise
IoT	Internet of Things

KAA	Key Application Areas
KPI	Key Performance Indicator
MCH	Major Challenge
MCARD	Model Project Consortium Agreement for Research, Development and Innovation - the consortium agreement template provided for KDT projects.
MDE	Model-Driven Engineering
ML	Machine Learning
NIS	Network Information SecuriTi
PoC	Proof of concept
PC	Project Coordinator
PEB	Project Executive Board - decision body reporting to the General Assembly
PMT	Project Management Team - support team around the Project Coordinator
R&D	Research and Development
RAN	Radio Access Networks
SoD	Segregation of Duties
SOTA	State-of-the-Art
TRL	Technology Readiness Level
TSN	Time Sensitive Networking
TTP	Techniques, Tactics and Procedures

Table of Content

1. Excellence

#@REL-EVA-RE@#

1.1 Objectives and ambition

#@PRJ-OBJ-PO@#

1.1.1 Challenges and Vision

DevOps is gaining more and more success in increasing development velocity while improving the quality of modern industrial software-intensive systems. However, there remains a risk that such fast and continuous integration/continuous delivery (CI/CD) processes introduce additional security vulnerabilities into systems in production. As a consequence, an unfortunate exponential growth of **cybersecurity** attacks is currently already observed. In fact, Gartner predicts that, by 2025, 45% of organisations worldwide will have experienced attacks on their software supply chains, a three-time increase from 2021[1].

DevSecOps and SecDevOps[2] have arisen in response to this major security problem. They promise to bridge the gap between continuous release cycles and security needs by addressing security at every stage of the development lifecycle. They notably aim to expand the impact of DevOps by also considering security tools and practices. The overall objective is to help developers and operation teams to perform their own security analysis, discover security issues and improve how they both code and operate the software.

Generally, DevSecOps and SecDevOps seek to achieve the same benefits as DevOps, i.e. the close integration of development and operation teams. Today, companies adopting DevOps also require the adoption of cybersecurity solutions to maintain control over the entire development lifecycle. In particular, cybersecurity automation allows for reducing the risk of security attacks without damaging the DevOps loop (i.e., performing security controls without affecting existing data or procedures).

While siblings, DevSecOps and SecDevOps are different complementary concepts. DevSecOps is primarily concerned with integrating security processes into every phase of the DevOps cycle while maintaining efficiency. Instead, SecDevOps prioritises security as much as the actual steps of integrating security into the DevOps process itself. The AIDOSec proposal aims at supporting **SecDevOps**, by considering security as a core dimension and concern of the entire DevOps process.

The need to better integrate security into development and operational processes is widely recognised, and some related tools, frameworks, and best practices are commonly adopted. The tasks related to security usually involve different teams and mainly are:

[1] Gartner, Top Trends in Cybersecurity for 2022, https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022
[2] Haber, M.J. (2020). *Secured DevOps (SecDevOps)*. Privileged Attack Vectors. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5914-6_19

- Gathering contextualised security information via threat intelligence[3];
- Modelling threats and their related countermeasures at design time;
- Analysing the code to find weaknesses and applying possible corrections, implementing the countermeasures at development time;
- Testing for vulnerabilities (vulnerability assessment, penetration tests and red teaming exercises) at the testing time;
- Monitoring the systems to find possible anomalies to detect attacks and respond in time at production time.

Practitioners secure their components by ensuring that they are safe in themselves, regardless of their location, context and interactions with other components. This behaviour, which can be considered atomistic, goes parallel to the constant research of correlations between the various elements and their interactions that determine the whole state of the system. However, such correlations can be complex, and the landscape of vulnerabilities, specific groups of attackers, and their techniques are broad. Moreover, each element is often treated disjointedly. As a consequence, adopting a holistic approach is challenging.

MISSION: to create a holistic framework that can support (i) the entire cybersecurity process and its practices, taking into account the relationship between causes, consequences and mitigation/recovery; (ii) the efficient and continuous engineering of industrial systems by leveraging security processes as a core element of DevOps pipelines that rely on both model-based methods and intelligent techniques.

The challenge of providing a holistic and comprehensive means to support cybersecurity concerns involves:

- Providing (intelligent) security controls that exchange feedback with each other, thus furnishing a broader view of security aspects within the DevOps pipeline;
- Validating mitigation results and correlating different analyses to help organisations improve their security posture[4] and minimise their attack surface[5];
- Providing security controls and analysis as a service, as well as enabling the correlation and reuse among the different development phases;
- Providing a traceability model and related support (*fil rouge*) allowing to have a precise picture of the system at any time during the SecDevOps cycle;
- Allowing security architects, developers and security analysts to identify and handle root causes, but also to make predictions in the early design phases that can guide subsequent analyses, and improve their security culture and awareness.

Finally, as advocated also by Gartner[6], such a holistic framework should enable:

- Distributed decisions. The CISOs (Chief Information Security Officers) need to execute centralised cybersecurity functions to support digital business priorities, while cybersecurity leaders are placed in different parts of the organisation to decentralise security decisions.
- Security culture. Currently, human errors are still the origin of most data breaches, showing that traditional approaches to security awareness training are ineffective. Thus, companies need to invest in holistic behaviour and culture change programs designed to establish more secure ways of working.

1.1.2 Project's Objectives

[3] Threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf).
[4] The security posture is a qualitative measure of how much a system is exposed to risk and is fed by different dimensions (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf)
[5] The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf).
[6] Top Trends in Cybersecurity, Gartner, https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

The **overall goal of AIDOSec** is to create a framework incorporating methods and tools for considering security as a key concern of continuous software and system engineering and validation, by combining model-based methods and intelligent techniques, in order to provide benefits in significantly improved productivity, quality and notably security of Cyber-Physical Systems (CPS) and, more generally, of all large and complex digital systems.

The importance of and focus on security aspects can affect the whole development process of systems. Thus, AIDOSec aims at providing a holistic approach for continuous systems engineering that:

- Provides a core model-based architecture and framework to secure the continuous systems engineering and validation process by focusing on cybersecurity aspects;
- Enhances the corresponding SecDevOps toolchain by integrating the use of AI techniques (notably Machine Learning) in order to improve both system engineering analysis & automation and related cybersecurity solutions;
- Supports key system security-related activities such as threat modelling and intelligence, security controls, or the detection and response of security problems.

The above statements can be best summarised in the following specific objectives with progress measured against the following key performance indicators (KPIs), which are further explored in the evaluation of the project impact (see Section 2). Please, note that these indicators will be refined and updated in the course of the project in order to reflect the detailed requirements from the project's use case providers as well the actual project technical realisations.
Note: To assess productivity and quality improvements in the different domains covered by AIDOSec, the target KPIs provide general guidelines for success criteria, which are based on the consortium's large industrial knowledge and expertise.

Table 1.1.2.a provides an insight into the AIDOSec project from the perspective of its main global objectives. In the remainder of the proposal, we will refer to the individual technical results in order to better clarify the outcomes of the main actions to be undertaken in the context of the different Work Packages and their corresponding Tasks.

Table 1.1.2.a - *AIDOSec specific objectives and KPIs*

Obj	Description	Target Key Performance Indicators
O1	**AIDOSec global model-based framework for scalable and efficient SecDevOps.** ● To improve the scalability and efficiency of SecDevOps thanks a model-based framework for supporting the entire cybersecurity process and its practices, within the continuous engineering of digital systems. It is suitable for large distributed cross-functional working teams and allows the integration of feedback on security aspects to improve the whole system's security posture.	**KPI 1.1**: Reduction of 30% in time/effort required for managing and handling all the involved cybersecurity practices **KPI 1.2**: Reduction of 20% in time/effort required for integrating new cybersecurity practices and services into a SecDevOps pipeline.
Emanate from ECS SRIA 2024 Challenges: FTL1.3 (MCH1, MCH2, MCH6), FTL 1.4 (MCH3), CST 2.3 (MCH1, MCH2, MCH3) Realised in tasks: T1.1, T1.3, T2.1, T2.2, T2.3, T5.1 With results in: D1.1, D1.3, D1.1, D2.2, D2.3, D5.1, D5.2		
O2	**AIDOSec cybersecurity toolkit for multiple security-related aspects** ● To improve the support for multiple security-related aspects of the system development process (e.g., threat modelling and intelligence, security controls, or the detection and response of security problems) via a combination of AIOps (based on AI/ML techniques) and MDE and by relying on the	**KPI 2.1**: Improvement of 20% in the early detection of security threats or vulnerabilities. **KPI 2.2**: Improvement of 20% of the time required for identification/resolution of security threats or vulnerabilities according to the multiple AIDOSec solutions implemented. **KPI 2.3**: Increase of 20% of the codebase and system components tested for security vulnerabilities.

	AIDOSec core model-based framework for SecDevOps.	**KPI 2.4**: Decrease 20% of the number of false alarms raised by the security system.
Emanate from ECS SRIA 2024 Challenges: FTL1.3 (MCH6), FTL 1.4 (MCH3), CST 2.3 (MCH1, MCH2, MCH3), CST2.4 (MCH3) Realised in tasks: T3.1, T3.2, T3.3, T3.4 With results in: D3.*, D5.4		
O3	**AIDOSec continuous validation and security improvement.** ● To verify that the system is working as expected, i.e., the security solutions do not affect the system operation while improving the whole security posture, via the use of AI/ML techniques ● To support the continuous feedback loop to make improvements to the whole security process. To employ AI/ML to improve the developers' security culture.	**KPI 3.1**: Automate 20% of the validation processes which are currently manual or not AI-based. **KPI 3.2**: Increase of 20% the coverage and quality of actionable feedback exchanged between the different phases of the SecDevOps cycle. **KPI 3.3**: The list of "security culture" contents will be populated after each security test iteration and submitted to developers.
Emanate from ECS SRIA 2024 Challenge: FTL1.3 (MCH2, MCH6), FTL 1.4 (MCH3), CST2.3 (MCH1, MCH2, MCH3), CST2.4 (MCH3, MCH5) Realised in tasks: T4.1, T4.2, T4.3 With results in: D4.*, D5.4		
O4	**AIDOSec demonstrators validation**. ● To develop specific demonstrators that apply the AIDOSec model-based framework and cybersecurity toolkit; ● To validate these AIDOSec technologies, through 10 complementary industrial case studies.	Generalising the previous KPIs we target: **KPI 4.1**: Productivity improvement in 20% of the SecDevOps process covered in the UCs. **KPI 4.2**: 20% of reduction of system vulnerabilities.
Emanate from Challenge: CST2.4 (MCH3, MCH5) and from the needs of KAA 3.1, KAA 3.3, KAA 3.4 and KAA 3.6. Realised in tasks: T1.1, T1.2, T5.1, T5.2, T5.3 With results in: D1.1, D1.2, D5.*		
O5	**Strengthening European excellence in Continuous System Engineering and notably SecDevOps.** The AIDOSec project incorporates an innovative research agenda and work plan by: ● contributing to maintain and further advance the Cybersecurity and DevOps world-class research that already exists in Europe (see Section 2.1.2.1); ● supporting European strategic autonomy in terms of sustainability and resilience (see Section 2.1.1.2); ● Fostering growth and innovation in different domains (see Section 2.1.2.3).	**KPI 5.1** Num. of communities in which AIDOSec partners promote their results > 15 **KPI 5.2** Num. of new research collaborations > 20 **KPI 5.3** Num. of new projects that inherit AIDOSec results or that are based on the new knowledge brought by AIDOSec > 3 Further KPIs will be defined in the FPP according to the complete Impact section. Please, notice that these KPIs will be refined, at the beginning of the project, in the Communication, Dissemination, and Exploitation plan (D6.2).
Emanate from the ECS SRIA 2024 Main Common Objectives 1, 2, 3 and 4. Realised in tasks: T6.1, T6.2, T6.3, T6.4 With final results in: D6.3, D6.5		
O6	**AIDOSec market uptake**. Promote the exploitation of the AIDOSec technology: ● by promoting awareness and security culture, supported by the *AIDOSec Awareness, training and security culture* component (see Section 1.2.2.7)	**KPI 6.1** Num. of business meetings in which AIDOSec-related results are discussed > 100 **KPI 6.2** Num. of results adopted by project partners > 15 **KPI 6.3** Num. of AIDOSec open source results > 15

	• by reaching the main relevant scientific and technology communities, public bodies and standardisation groups ; • through a relevant combination of open source solutions and commercial tools; • through the preparation of proper documentation, tutorials and seminars .	**KPI 6.4** Num. of proposals to standardisation bodies > 3 Further KPIs will be defined in the FPP according to the complete Impact section. Please, notice that these KPIs will be refined, at the beginning of the project, in the Communication, Dissemination, and Exploitation plan (D6.2).
Emanate from all the challenges and needs mentioned in O1, O2, O3, O4 and O5. Realised in tasks: T6.1, T6.2, T6.3, T6.4 With final results in: D6.3, D6.5		

The expected Technical Results of the project are summarised in Table 1.1.2.b. These results, supported by individual partners' results (see Section 1.1.5), are directly linked to the global project's Objectives as well as their respective KPIs. All the different steps that will enable to deliver the project's objectives and results will be described in detail in the Section 1.2 and Section 2.

Table 1.1.2.b - *AIDOSec expected technical results. For each result is provided an identifier (ID), a description, and each one is mapped to AIDOSec objectives (O).*

ID	Technical Results	O
R1. AIDOSec global model-based framework for SecDevOps (Details in Section 1.2.2.1)		
R1.1	**Model-based architecture and framework for SecDevOps.** Global architecture for the AIDOSec framework defining the whole process, components and capabilities in terms of cybersecurity activities, the expected artefacts, roles played by the involved stakeholders.	O1
R1.2	**Traceability methodology and language for SecDevOps.** Traceability methodology and related metamodel language, to link cybersecurity aspects and DevOps phases and implement the feedback-loop to improve the whole system's security posture.	
R2. AIDOSec cybersecurity toolkit		
R2.1	**AIDOSec solutions for threat modelling.** Methods and tools supporting threat modelling according to the AIDOSec framework architecture and approach. (Details in Section 1.2.2.2)	O2
R2.2	**AIDOSec solutions for security testing.** Methods and tools supporting security testing according to the AIDOSec framework architecture and approach. (Details in Section 1.2.2.3)	
R2.3	**AIDOSec solutions for detection and response.** Methods and tools supporting detection and response according to the AIDOSec framework architecture and approach. (Details in Section 1.2.2.4)	
R2.4	**AIDOSec solutions for threat intelligence.** Methods and tools supporting threat intelligence according to the AIDOSec framework architecture and approach. (Details in Section 1.2.2.5)	
R3. AIDOSec continuous validation and improvement support (Details in Section 1.2.2.6)		
R3.1	**AI-based solutions supporting analysis and automation.** AI-based solutions (including ML) to support the various analysis and automation activities that will be provided within the project.	O3
R3.2	**AIDOSec solutions for validation.** Methods and tools supporting the validation of the system, i.e., verifying that the system is working as expected while improving the whole security posture.	
R3.3	**AIDOSec solutions for improvement and security culture.** Methods and tools supporting the improvement of the security process and cybersecurity posture.	O3, O6
R4. AIDOSec case studies (Details in Section 1.2.4)		
R4.1	Abinsula - Resilient New Concept Cars	O4, O5, O6
R4.2	Alstom - Dependable AI for railway traction operation and e-mobility testing	

R4.3	Camea - Secure Smart Sensors for Traffic Monitoring	
R4.4	Ericsson - AI/ML for optimization the CloudRAN products	
R4.5	Hi Iberia - SecDevOps in Medical IoT applications	
R4.6	Prodevelop - Secure Smart Port Solutions by Design	
R4.7	Tekne - Wireless Communication Security	
R4.8	Thales - Tooled-Up Distributed Real-Time Drone Application	
R4.9	Thinglink - Collaborative Research and Development of Security-Critical AI-Based Solutions for ThingLink XR Trainings Platform	
R4.10	Westermo - AI and Model-Based Approaches for Industrial Communication Products	
R4.11	Harmonized EU-CyberBridge: Aligning EU Cybersecurity Standards and Regulations for Enhanced Cybersecurity Protection	

1.1.3 Relation to the KDT JU Work Programme 2023 and the ECS SRIA 2024

AIDOSec is a research and innovation action (RIA) project proposal that responds to the global callHORIZON-JU-Chips-2024-2-RIA, according to the ECS SRIA 2024 .

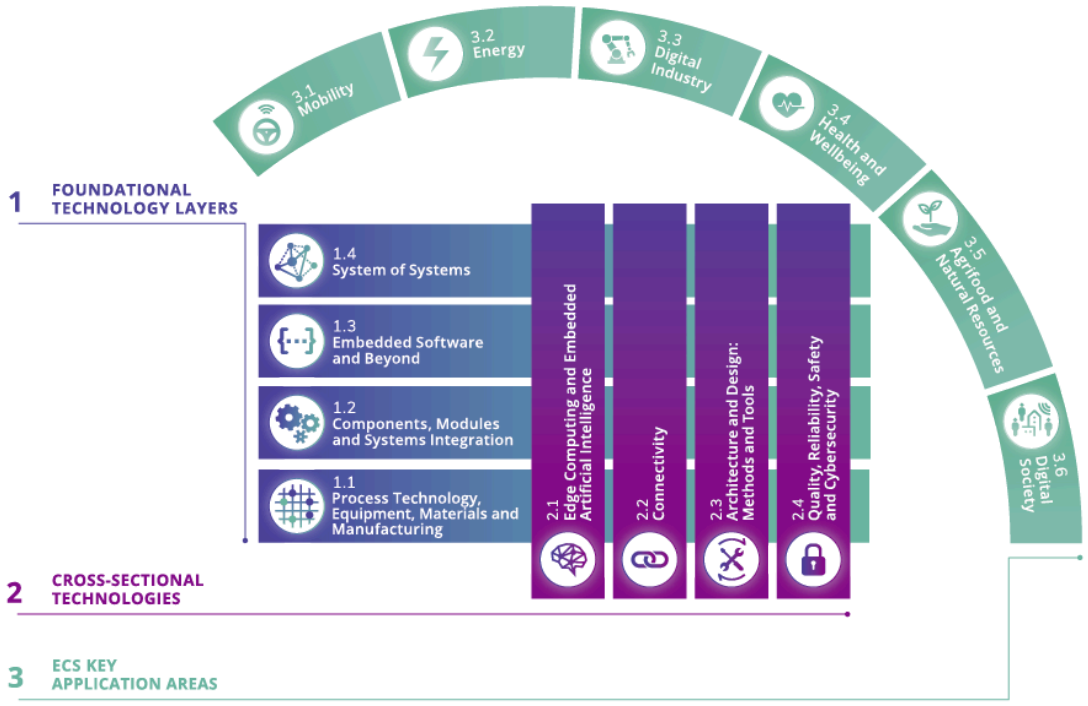


Figure 1.1.3 - *Focus areas from the ECS SRIA 2024*

In particular, AIDOSec technologies address the following Major Challenges, grouped per dimension as in the Electronic Components and Systems (ECS) Strategic Research and Innovation Agenda (ECS SRIA) 2023 structure depicted in Figure 1.1.3.

1. Foundational Technology Layers (FTL):

- **FTL 1.3 - Embedded Software and Beyond:**
  - Major Challenge 1: Efficient engineering of embedded software;

- Major Challenge 2: Continuous integration and deployment;
- Major Challenge 6: Software reliability and trust;

- **FTL 1.4 - System of Systems:**
  - Major Challenge 3: Evolvability of SoS composed of embedded and cyber-physical systems.

2. Cross-Sectional Technologies (CST):

- **CST 2.3 - Architecture and design: methods and tools:**
  - Major Challenge 1 Extending development processes and frameworks (to handle connected, intelligent, autonomous, evolvable systems);
  - Major Challenge 2: Managing new functionality in safe, secure and trustworthy systems;
  - Major Challenge 3: Managing complexity. This challenge deals with methods to handle the ever-increasing complexity of ECS-based systems;
- **CST 2.4 - Quality, reliability, safety and cybersecurity:**
  - Major Challenge 3: Ensuring cyber-security and privacy;
  - Major Challenge 5: Human systems integration.

3. ECS Key Application Areas (KAA)

- **KAA 3.1 - Mobility** (*Automotive, Railway, Traffic Monitoring, Maritime, Aerospace*)
  - Major Challenge 1: Enable CO2 neutral mobility and required energy transformation.
  - Major Challenge 2: Enable affordable, automated and connected mobility for passengers and freight on or off-road, rail, air and water.
  - Major Challenge 4: Provide tools and methods for validation and certification of safety, security and comfort of embedded intelligence in mobility.
  - Major Challenge 5: Achieve real-time data handling for multimodal mobility and related services.
- **KAA 3.3 - Digital Industry** (*Manufacturing, Industry Networks*)
  - Major Challenge 1: Responsive and smart production.
  - Major Challenge 4: Industrial service business, lifecycles, remote operations and teleoperation.
  - Major Challenge 5: Digital twins, mixed or augmented reality, telepresence.
- **KAA 3.4 - Health & Wellbeing** (*Health Monitoring*)
  - Major Challenge 2: Enable the shift to value-based healthcare, enhancing access to 4P's game-changing technologies.
  - Major Challenge 3: Support the development of the home as the central location of the patient, building a more integrated care delivery system.
  - Major Challenge 5: Ensure more healthy life years for an ageing population.
- **KAA 3.6 - Digital Society** (*Connectivity*)
  - Major Challenge 4: Facilitate supportive infrastructures and sustainable environments.

Table 1.1.3 explains how AIDOSec technical contributions and objectives address the major challenges, as stated in the call. AIDOSec contributions, presented in relation to the ECS SRIA key focus areas, are mapped to the project's objectives and technical KPIs presented in Table 1.1.2.a.

Table 1.1.3 - *AIDOSec pertinence to the ECS SRIA 2024*

Key focus area	AIDOSec technical contribution
FTL 1.3 - Major Challenge 1: Efficient engineering of embedded software	
• Model-based software engineering enabling systems to become part of SoS • Model-based testing that takes the re-use of uncontrolled systems into account • Embedded software architectures to enable SoS • Integrating embedded AI in software architecture and design	AIDOSec aims to develop a model-based framework to support the entire cybersecurity process and its practices, taking into account the relationship between causes, consequences and mitigation/recovery. It will support the efficient and continuous engineering of industrial systems by leveraging security processes as a core element of DevOps pipelines that rely on model-based and model-driven methods and techniques. AIDOSec will rely on the definition of its model-based architecture that will specify components, capabilities and relations between them. Also, the framework will rely on the definition of a metamodel language of the AIDOSec framework, to define concepts and relations, and a metamodel

	language for the AIDOSec traceability, to capture, collect, and use links between security phases and correspondent activities. The high level of abstraction allows the efficiency of the proposed solutions, better integration within the framework, and short feedback loops due to such improved tool-supported software development. **Related objectives: O1** **Related KPIs: KPI 1.1-2** **Technical results: R1.1-2**
Key focus area	**AIDOSec technical contribution**
FTL 1.3 - Major Challenge 2: Continuous integration and deployment	
• Model-based design to support system integration (HW/SW) and HW/SW co-development • Applying automation of engineering, taking architecture, platforms and models into account • Application of integration and orchestration practices • Enabling secure updates and extending useful life (DevOps) • Continuous integration, verification and validation (with and without AI), using model-based design technologies	The AIDOSec framework will support the SecDevOps pipeline by: • Exploiting model-based principles and techniques • Developing (AI-based) automated solutions for the identification or resolution of security threats or vulnerabilities, taking into account also design-time artefacts (including architectures and models) • Developing V&V solutions to verify that the system is working as expected, i.e., the security solutions do not affect the system operation while improving the whole security posture • Supporting the continuous integration in the SecDevOps lifecycle • Supporting the continuous feedback loop to make improvements to the whole security process. **Related objectives: O1, O3** **Related KPIs: KPI 1.1-2, 3.1-3** **Technical results: R1.1-2, R3.1-3**
Key focus area	**AIDOSec technical contribution**
FTL 1.3 - Major Challenge 6: Software reliability and trust	
• Security and privacy as a service, to become part of the software architecture	The AIDOSec framework will contribute to the software reliability and trust by developing security solutions to be integrated into the continuous software and system development. Related contribution: CST 2.4 - MC3 **Related objectives: O1, O2, O3** **Related KPIs: KPI 1.1-2, 2.1-4, 3.1-2** **Technical results: R1.1-2, R2.1-4, R3.1-2**
Key focus area	**AIDOSec technical contribution**
FTL 1.4 - Major Challenge 3: Evolvability of SoS composed of embedded and CPSs	
• Evolvable solutions for trust, availability, scalability, and interoperability	Although AIDOSec does not offer specific support for SoS, some scenarios described in the SRIA are included in our objectives. AIDOSec proposes a framework implicitly capable of supporting the constituent systems of the SoS in terms of security, both in the pre-deployment phase and in the evolved/composed/integrated SoS phase. In particular, the AIDOSec feedback loop and the AIDOSec traceability approach promote the dynamic adaptation of security requirements and risk mitigation during continuous development. New methods and tools will be developed for risk and vulnerability assessment and threat modelling. **Related objectives: O1, O2, O3** **Related KPIs: KPI 1.1-2, 2.1-4, 3.1-2** **Technical results: R1.1-2, R2.1-4, R3.1-2**
Key focus area	**AIDOSec technical contribution**

CST 2.3 - Major Challenge 1: Extending development processes and frameworks (to handle connected, intelligent, autonomous, evolvable systems)	
• Design processes to switch completely to model-based processes • Collecting relevant data in the operation phase, analysing it (using AI-based or other methods) and feeding it back into the development phase • Integration of new V&V methods	The AIDOSec model-based framework will extend the SecDevOps pipeline with new methods for cybersecurity to be integrated in the system development lifecycle to improve the whole security posture. **Related objectives: O1, O2, O3** **Related KPIs: KPI 1.1-2, 2.1-4, 3.1-2** **Technical results: R1.1-2, R2.1-4, R3.1-2**
Key focus area	**AIDOSec technical contribution**
CST 2.3 - Major Challenge 2: Managing new functionality in safe, secure and trustworthy systems	
• Modelling is essential for describing the system architecture, functionality, and behaviour; It is suitable for different purposes (analysis techniques, simulation, etc.) • Design and V&V methods for ECS evolving during lifetime (including AI-enabled systems)	Among the AIDOSec cybersecurity solutions, an extensive effort will be devoted to threat modelling activities, including analysis and verification of software models for threat identification and countermeasures. In the model-based framework of AIDOSec, this activity will be based on the use of model-based and model-driven principles and techniques for the effective and realistic creation of models to be used to ensure security in the different phases of DevOps. **Related objectives: O1, O2, O3** **Related KPIs: KPI 1.1-2, 2.1-4, 3.1-2** **Technical results: R1.1-2, R2.1-4, R3.1-2**
Key focus area	**AIDOSec technical contribution**
CST 2.3 - Major Challenge 3: Managing complexity. This challenge deals with methods to handle the ever-increasing complexity of ECS-based systems	
• Managing complexity by the reduction of effort during the engineering process (e.g., in test and V&V, ensuring compatibility and proper behaviour)	AIDOSec will implicitly support complexity management. In fact, the AIDOSec framework and toolkit will support the system development lifecycle by ensuring security. This involves also (for instance) secure deployment and update, which is an integral part of the DevOps cycle. **Related objectives: O1, O2, O3** **Related KPIs: KPI 1.1-2, 2.1-4, 3.1-2** **Technical results: R1.1-2, R2.1-4, R3.1-2**
Key focus area	**AIDOSec technical contribution**
CST 2.4 - Major Challenge 3: Ensuring cyber-security and privacy	
• Solutions to ensuring the protection of personal data in the embedded AI and data-driven digital economy against potential cyber-attacks • Ensuring cybersecurity and privacy of systems in the Edge to cloud continuum, via efficient automated verification and audits • Establishing a cybersecurity by-design European data strategy	AIDOSec will provide an end-to-end DevOps security framework for cybersecurity by-design concerns, ensuring data protection and privacy, and augmenting the SecDevOps practises with AI. Within the project, specific demonstrators will show the application of the AIDOSec framework and toolkit, and validate these technologies, through 11 complementary industrial case studies requiring privacy and security aspects. AIDOSec will cope with human factors as explained in *CST 2.4 - Major Challenge 5.* **Related objectives: O2, O3, O4** **Related KPIs: KPI 2.1-4, 3.1-3, 4.1-2** **Technical results: R2.1-2, R3.1-3, R4.***
Key focus area	**AIDOSec technical contribution**
CST 2.4 - Major Challenge 5: Human systems integration	

• Develop (modelling) methods for the early integration of Humans and Technologies. The virtual methods link early assessments, holistic design activities, and lifelong product updates and bring facilitate convergence among researchers, developers, and stakeholders	The AIDOSec process will address human system integration by employing AI/ML to generate contents to be submitted to developers (e.g., guidelines, best practices, assessment questionnaires, etc.) with the aim to improve their security culture. **Related objectives: O3, O4** **Related KPIs: KPI 3.3, 4.1-2** **Technical results: R3.3, R4.***
ECS KAAs	
The AIDOSec use cases developed in the project focus on Mobility (railway, maritime, and automotive), Digital Industry (manufacturing, industry networks), Health and Wellbeing (health monitoring) and Digital Society (connectivity) domains; however, the AIDOSec results can be extended to Energy and Agrifood domains as due to the particular subsystem (i.e., the propulsion system) and related concerns (i.e., reducing the environmental impact by improving both process and product related qualities) as brought by considered use cases. A description of the AIDOSec use cases, their motivations and their goal is provided in Section 1.2.4, while their contributions to the ECS SRIA 2024 expected outcomes and impacts is discussed in Section 2.1.1.2. **Related objectives: O4, O5, O6** **Related KPIs: KPI 4.1-2, Further KPIs will be defined in the FPP according to the complete Impact section.** **Technical results: R4.***	

1.1.4 AIDOSec ambition

In the following, we describe the scientific areas targeted by AIDOSec, the current state-of-the-art (SOTA), and the planned progress beyond the SOTA. It is worth mentioning here that the research areas taken into account aim to provide the necessary scientific and technical basis on which the project UCs will be specified, demonstrated, and validated. In turn, the UCs are tightly related to specific KAAs, FTLs and CSTs contained in the ECS SRIA 2024 and KDT workplan (as discussed in Section 1.1.3 and further detailed in Section 2).

1.1.4.1 MDE for the engineering of (cyber) secure software and systems

AIDOSec aims to provide a holistic framework for the continuous development of industrial systems supporting security management processes and practices. In this respect, we argue that the adoption of MDE mechanisms becomes necessary due to the complexity of the targeted industrial systems. To confirm this, the International Council on Systems Engineering (INCOSE) 2035 vision states: "***The future of Systems Engineering is predominantly Model-Based***"[7]. The increasing complexity is due to the overwhelming combination of several factors: the span of provided features; the multi-faceted set of quality attributes; the opportunity to profit from the immense amount of data accumulated throughout the whole system's life cycle. MDE can help tame such complexity by supporting communication and exchange across heterogeneous domains, enabling the analysis and ingestion of data coming from disparate sources, and by providing automated means to manage consistency, both intra- and inter- development stages.

The existing research literature already includes a significant number of investigations on the adoption of MDE for the development of secure software systems[8]. Moreover, recently there has been a growing interest in the co-design of safe and secure systems[9,10]. These interests are justified by the potential impact of security threats on safety-related properties of a system. In turn, safe and secure systems co-design discloses new intricacies, since

[7] https://www.incose.org/about-systems-engineering/se-vision-2035

[8] P.H. Nguyen, S. Ali, T. Yue, *Model-based security engineering for cyber-physical systems: A systematic mapping study, Information and Software Technology*, Vol. 83, 2017, Pages 116-135, doi: 10.1016/j.infsof.2016.11.004

[9] A. Mashkoor, A. Egyed, R. Wille, S. Stock, *Model-driven engineering of safety and security software systems: A systematic mapping study and future research directions*. J Softw Evol Proc. 2022;e2457. doi:10.1002/smr.2457

[10] E. Lisova, I. Šljivo and A. Čaušević, *Safety and Security Co-Analyses: A Systematic Literature Review*, in IEEE Systems Journal, vol. 13, no. 3, pp. 2189-2200, Sept. 2019, doi: 10.1109/JSYST.2018.2881017

safety and security adopt partly diverging handling approaches (prevent and mitigate vs monitor and react/adapt, respectively)[11,12].

A large majority of the existing works on secure software systems' development focus on the requirements analysis phases or on architecture/design phases, followed by testing[2,3]. This is not surprising, since understanding early the features and boundaries of the developed system is critical to reduce the risks of discovering issues in advanced stages, where changes are usually very expensive or even ruinous. However, without considering the process as a whole, there is a significant probability of introducing inconsistencies due to discontinuities, i.e. missing information to close the gaps between development stages that is necessarily completed by hand and is untracked in the related documents[13,14]. Moreover, such discontinuities often make the adoption of continuous development approaches impracticable due to consistency management[15]. Indeed, this is one of the foundations underlying the predecessor of AIDOSec, namely the AIDOaRt project[16]: AIDOaRt targets the creation of an AI/ML-augmented MDE framework and corresponding toolkit for enabling DevOps in industrial systems development. In this respect, AIDOSec leverages the MDE framework of its predecessor for supporting security concerns. The potential and relevance of traceability links, between different artefacts and development stages, are already highlighted in MetaSEnD, a meta-model for secure software development life-cycle[17]. AIDOSec aims at concretising such links in order to enhance automation in the development of industrial systems; the framework inherited from AIDOaRt will provide important components and know-how, especially related to data management and more generally to AIOps.

Progress beyond SOTA: AIDOSec provides a holistic framework based on AI-augmented MDE techniques to support security-aware DevOps of industrial systems. The framework is intended to cover the entire cybersecurity process and to enhance its degree of automation. Moreover, it is intended to support the co-design of multiple quality attributes, notably security and safety. Eventually, AIDOSec pursues the definition of a generic process that can be instantiated towards specific domains, enabling the integration of heterogeneous systems and the corresponding security processes and practices[8,18].

1.1.4.2 CyberSecurity and DevOps

DevOps has gained a lot of attention from the industry as a possible way of matching the increasing demand for quality with shorter development life-cycles. However, many industrial domains tend to be largely regulated, notably in terms of security requirements. As a consequence, the demanded agility of DevOps processes could negatively impact those quality attributes or the other way round, the regulations could make it difficult to implement DevOps while keeping an adequate level of quality assurance[19]. These challenges triggered the introduction of DevSecOps and SecDevOps, two extensions of DevOps (which in this context could also be referred to as DevOpsSec) aiming at integrating security concerns in the development process[20]. DevSecOps prescribes to include security as part of the development process and considers it as any other (non-)functional

[11] C. Ponsard, J. Grandclaudon, P. Massonet, *A goal-driven approach for the joint deployment of safety and security standards for operators of essential services*. J Softw Evol Proc. 2021; 33:e2338. https://doi.org/10.1002/smr.2338

[12] S. Ramachandra, J. Vankeirsbilck and J. Boydens, *Challenges in the Co-assurance of Functional Safety and Cybersecurity in Industry 4.0,* Conf on System Reliability and Safety (ICSRS), 2022, pp. 418-423, doi: 10.1109/ICSRS56243.2022.10067488

[13] B. Selic, *The pragmatics of model-driven development*, IEEE Software, Vol. 20, N.5, IEEE, 2003

[14] C. Ponsard, and P. Massonet, *Survey and Guidelines about Learning Cyber Security Risk Assessment*. Conf on Information Systems Security and Privacy (ICISSP 2022), pages 536-543, SCITEPRESS, DOI: 10.5220/0010900800003120

[15] R. Jongeling, J. Carlson and A. Cicchetti, *Impediments to Introducing Continuous Integration for Model-Based Development in Industry*, Conf. on Software Engineering and Advanced Applications (SEAA), 2019, pp. 434-441.

[16] H. Bruneliere, V. Muttillo, R. Eramo, et al. *AIDOaRt: AI-augmented Automation for DevOps, a model-based framework for continuous development in Cyber–Physical Systems*, Microprocessors and Microsystems, Vol. 94, 2022, 104672, doi: 10.1016/j.micpro.2022.104672

[17] D. Granata, M. Rak, and G. Salzillo, *MetaSEnD: A Security Enabled Development Life Cycle Meta-Model*. Conf on Availability, Reliability and Security (ARES 2022), August 23–26, 2022. https://doi.org/10.1145/3538969.3544463

[18] M. Mylrea, S. N. G. Gourisetti and A. Nicholls, *An introduction to buildings cybersecurity framework*, IEEE Symposium Series on Computational Intelligence (SSCI),, 2017, pp. 1-7, doi: 10.1109/SSCI.2017.8285228

[19] P. Abrahamsson, et al., *Towards a Secure DevOps Approach for Cyber-Physical Systems: An Industrial Perspective*. Journal of Systems and Software Security and Protection (IJSSSP), 11(2), 38-57. http://doi.org/10.4018/IJSSSP.2020070103

[20] V. Mohan and L. B. Othmane, *SecDevOps: Is It a Marketing Buzzword? - Mapping Research on Security in DevOps*, Conf. on Availability, Reliability and Security (ARES), 2016, pp. 542-547, doi: 10.1109/ARES.2016.92

attribute of the integrated system[21]. On the contrary, SecDevOps shifts the focus on security, and as such security concerns are integrated into all the development phases and prioritised[14,22].
Despite the clear need for security-aware processes and the existence of works both towards DevSecOps and SecDevOps directions[15,23], many literature surveys report several issues about their adoption in practice. In particular, automation and traceability are lacking, existing solutions only partially cover the system life-cycle, and tools availability is scarce[2,13,24]. In a broader perspective, these challenges make it difficult to take into account, adopt, and propagate the latest recommendations and security standards guidelines[25] in already existing processes.
Progress beyond SOTA: In AIDOSec, we aim to develop and transfer the needed technology to enable SecDevOps processes in industrial use case scenarios. As clarified in the SOTA, these efforts entail enhancements in the state-of-practice related to traceability, automation, and availability of tools, just to mention a few. In this respect, MDE provides the techniques to realise traceability mechanisms which, in turn, enable the automation of both intra- and inter-development stages. We also plan to conduct our investigations starting from the AIDOaRt results, especially considering the AI-augmented MDE framework to support DevOps in general and the support related to tool adoption in the industry.

1.1.4.3 Automation support for Cybersecurity

Cybersecurity is an important concern for modern societies, and its relevance is expected to grow in the future. We can notably mention that the European Union Agency for CyberSecurity (ENISA) publishes a yearly report on the threats landscape since 2012[26] and, through the years, it is possible to identify a number of safety-related incidents caused by security issues (e.g. health services malfunctions and outages). Moreover, these reports show rapidly moving targets, which require effective approaches to identify, contain, eradicate, and recover from security threats, while the difficulty in finding high-quality data can undermine current AI tools and their decision-making, thereby introducing new security, privacy, and safety risks. Unfortunately, currently, these tasks are largely manual and require the support of security experts in order to be completed[15,27]. Thus, there is a growing interest in technologies to assist security experts, and especially in AI/ML solutions[28]. Notably, there exist approaches to discover and update cyber threats based on publicly available documentation, like discussion forums, reports, etc.[29]. Complementary to these works, other AI/ML based solutions have been developed for threat hunting[30] and for security orchestration, automation, and response[21]. All these works could provide the basic technology for a broader, process-oriented, continuous handling of security in the system life-cycle.
Apart from threat-centric approaches, there are lines of research devoted to risk-centric and software-centric techniques[18]: the former ones focus on the (business) assets potentially affected by security concerns together with mitigation of risks/losses[31]; the latter ones target the design of the software itself, e.g., how it could be more

[21] T. Okubo, H. Kaiya, *Efficient secure DevOps using process mining and Attack Defense Trees, Procedia Computer Science*, Vol. 207, 2022, Pages 446-455, https://doi.org/10.1016/j.procs.2022.09.079
[22] X. Larrucea, A. Berreteaga, I. Santamaria, *Dealing with Security in a Real DevOps Environment*. In Systems, Software and Services Process Improvement. EuroSPI 2019. Communications in Computer and Information Science, Vol 1060. Springer, Cham. https://doi.org/10.1007/978-3-030-28005-5_35
[23] V. Casola et al., *A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach*, Journal of Systems and Software, Vol. 163, 2020, 110537, https://doi.org/10.1016/j.jss.2020.110537
[24] K. Tuma, G. Calikli, R. Scandariato, *Threat analysis of software systems: A systematic literature review, Journal of Systems and Software*, Vol. 144, 2018, Pages 275-294, https://doi.org/10.1016/j.jss.2018.06.073
[25] The Cyber Security Body of Knowledge (CyBOK), Knowledgebase, https://www.cybok.org/knowledgebase1_1/
[26] ENISA Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[27] J. Kinyua and L. Awuah, *AI/ML in security orchestration, automation and response: future research directions*, Intelligent Automation & Soft Computing, vol. 28, no.2, pp. 527–545, 2021
[28] W. Xiong, R. Lagerström, *Threat modeling – A systematic literature review*, Computers & Security, Vol 84, 2019, Pages 53-69, https://doi.org/10.1016/j.cose.2019.03.010
[29] MdR. Rahman, R.M. Hezaveh, and L. Williams, *What Are the Attackers Doing Now? Automating Cyberthreat Intelligence Extraction from Text on Pace with the Changing Threat Landscape: A Survey*. ACM Comput. Surv. 55, 12, Article 241 (December 2023), 36 pages. https://doi.org/10.1145/3571726
[30] Y. S. AlMahmeed and A. Y. Al-Omay, *Zero-day Attack Solutions Using Threat Hunting Intelligence: Extensive Survey*, Conf on Data Analytics for Business and Industry (ICDABI), 2022, pp. 309-314, doi: 10.1109/ICDABI56818.2022.10041568
[31] S.S. Zmiewski, J. Laufer, and Z.Á. Mann, *Automatic online quantification and prioritization of data protection risks*. In Conf on Availability, Reliability and Security (ARES 2022), August 23–26, 2022. https://doi.org/10.1145/3538969.3539005

exposed to certain kinds of security issues[32]. The main lessons learnt from these works is that automation mechanisms for cybersecurity handling are more effective when customised for the domain of usage and that the customisation shall include knowledge about threats, risks, mitigation, and recovery[21]. In this respect, processes like DevOps disclose the opportunity to continuously monitor and improve a system, possibly counteracting in a quicker way against emerging threats. However, an important precondition for this is the availability of traceability and automation mechanisms enabling the effective propagation of the enhancements[15,16].

Progress beyond SOTA: In AIDOSec, we aim to leverage MDE by i) using models and data handling techniques to support the work of security experts; ii) exploiting traceability and automation mechanisms to enable the continuous refinement of the systems. By going into more details, in i) we plan to use and extend the results coming from AIDOaRt with respect to data handling in order to include security concerns in the AI-augmented process. These concerns might include knowledge bases, standards, and AI/ML-based security management. Moreover, the learning process related to DevOps iterations and system monitoring will include security-related information. The mentioned re-use and extension enable, thanks to traceability and automation mechanisms (see point ii), to move from DevOps processes (as supported delivered in AIDOaRt) towards SecDevOps processes, which are the goal of AIDOSec.

1.1.5 Research and Innovation Maturity

The project will deliver the AIDOSec Model-Based Framework for SecDevOps (result R1 in Table 1.1.2.b), supported by an AI-enhanced cyber-security software toolkit for incorporating methods, tools and processes for enhancing the DevOps toolchain with modelling, security testing, detection and response, threat intelligence (result R2 in Table 1.1.2.b), and AI-based solutions for continuous validation and improvement (result R3 in Table 1.1.2.b). This technology is assessed in ten use cases (result R4 in Table 1.1.2.b). These elements will build on previous research (see Table 1.2.5) and the multidisciplinary capabilities of the consortium; as summarised by Figure 1.1.5 [left], the AIDOSec technological results (R1, R2 and R3) are supported respectively by 18, 28 and 26 individual technologies from AIDOSec partners (please, notice that certain technology can support more than one result) that are then assessed on the AIDOSec case studies (R4). The baseline technologies and their planned innovation are described in this section, along with their mapping to AIDOSec results and the expected final Technological Readiness Level (TRL).

Figure 1.1.5 [right] also illustrates an overview of the maturity of AIDOSec technology at the beginning of the project (@M1) up to the end of the project (@M36). From an analysis of AIDOSec partners' technologies and their current and target TRL, we can see as the initial TRL has its gravity centre around TRL2 (i.e., technology concept) and TRL3 (i.e., experimental proof of concept). During AIDOSec, the consortium will coordinate efforts to advance the development and maturity of the elements in the AIDOSec Framework to achieve overall a TRL 5 (i.e. Technology validated in a relevant environment). This TRL is estimated on the base of the target TRL declared by the partners, that spans in the range of TRL 3 -7, with a major density in the range TRL4-5. Some elements have a promising target maturity level, in fact, these will be developed and integrated within an existing complete and qualified system, or proven in an operational environment.

[32] K. Tuma, L. Sion, R. Scandariato, K. Yskout, *Automating the Early Detection of Security Design Flaws*. Conf on Model Driven Engineering Languages and Systems (MODELS '20), October 18-23, 2020. https://doi.org/10.1145/3365438.3410954

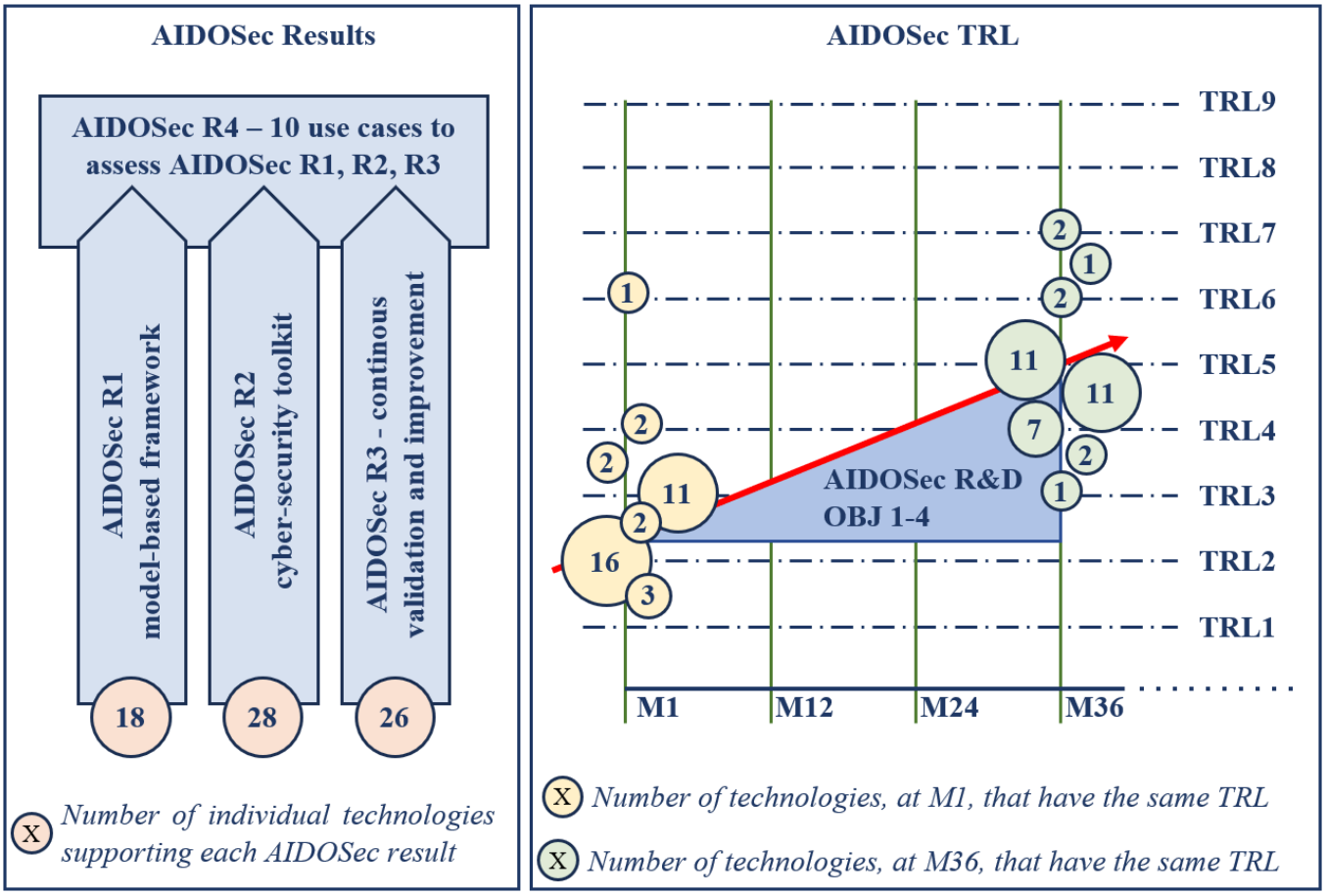


Figure. 1.1.5 - ***[left] AIDOSec Results - N. of technologies (pink circles) that support AIDOSec technical results; [right] AIDOSec TRL - N. of technologies, grouped by TRL, at M1 (yellow circles) and at M36 (green circles).***

The AIDOSec technologies will be, as first, developed and validated in laboratory environment (during the WP3-4 activities, see Section 3.1.2); then, use case providers will demonstrate the performance and industrial applicability of technical solutions, given that some have evaluated individual technologies in previous work and different contexts. In contrast, the global AIDOSec principles will be combined and validated in proper case studies, e.g., through controlled experiments at the premises of the use case providers (WP5, see Section 3.1.2).

Here we present the project's baseline technologies and their planned improvements, grouped by partners.

ABI provides innovative ICT solutions and integration services for Automotive, Precision Farming, e-Health and Web & Mobile. In AIDOSec, Abinsula is *Use Case Provider* and brings the *Resilient New Concept Cars Case Study* and its expertise in the Automotive domain, to support technology providers in the development of innovative technologies and methodologies.

- In particular, Abinsula is interested in studying the new frontiers of the cyber attacks in the automotive domain, and investigating new methods that could loosen the current technological limitations. The Resilient New Concept Cars Case Study is linked to **AIDOSec result R4.1** in Table 1.1.2.b, and it is detailed in the *Industrial use cases Section*.

ABO will contribute with the following technology and the planned improvement:

- **STGEM (System Testing using Generative Models)** (@M1 TRL 3, @M36 TRL 4-5): it is an academic tool for automatic test generation and prioritisation for software-intensive CPS. It uses AI/ML techniques to automate and improve the performance of several activities in the testing process. In the AIDOSec project, the tool will be improved and extended to provide support for vulnerability detection and to generate tests for security testing. This tool is mainly linked to **AIDOSec results R2.2, R2.3, R3.1.**

ACORDE will contribute with the following technology and the planned improvement:

- **Edge-Secure monitoring solutions** (@M1 TRL 2, @M36 TRL 4-5): AI/ML for security monitoring and for security threads detection, e.g. on monitored traces based on virtual models, Secure positioning. Attack

resilient monitoring solutions. Novel monitoring infrastructure for secure supply chain. These solutions contribute mainly to deliver **AIDOSec results R1.1, R2.1, R2.2, R2.3, R3.1, R3.2, R4.6.**

AIT will contribute to advancing the knowledge and methods on threat and risk modelling and simulation, considering cascade effects. AIT will contribute with the following technology and the planned improvement:

- **THREATGET** (@M1 TRL 3-4, @M36 TRL 4-5) and **Cassandra** (@M1 TRL 3, @M36 TRL 4-5): AIT will work on threat and modelling for SecDevOps, establishing a gate-based process for security related quality criteria. AIT will further work on the cascading effect simulation of threats and risks including repairability supporting DevOps. The AIT tools THREATGET and Cassandra (Cascading Effects Simulation) will be developed further. These solutions contribute mainly to deliver **AIDOSec results R2.1, R2.2, R2.4 and R3.1**

AR is a *Use Case Provider* and brings the *Dependable AI for Railway Traction Operation and E-Mobility Testing Case Study.* The use case is linked to **AIDOSec result R4.2** in Table 1.1.2.b, and it is detailed in the *Industrial use cases Section*. In the context of the UC, AR will contribute to:
Dependable AI: secure, safe and reliable implementation of AI in safety critical railway traction control systems and shared test system infrastructure applications.

BUT will contribute to advancing the knowledge on secure edge-cloud, studying secure communication patterns in the edge-cloud continuum and providing homomorphic encryption of cloud-based analysis. BUT will mainly work in the context of CAMEA UC (**AIDOSec result R4.3**) and provide:

- **large pre-trained SecDevOps Models** (@M1 TRL 2, @M36 TRL 4-5) for ML-driven tools able to provide automatic security testing and robustness evaluation.

BUT technology mainly contributes to deliver **AIDOSec technical results R1.1, R2.2** and **R2.4.**

CAMEA is a Use *Case Provider* and brings the *Secure Smart Sensors for Traffic Monitoring Case Study.* The use case is linked to **AIDOSec result R4.3** in Table 1.1.2.b, and it is detailed in the *Industrial use cases Section*. It's work is focused on:

- Smart sensors: Smart traffic cameras and radars for traffic monitoring domain. These sensors have a certain level of intelligence allowing data preprocessing. It could be licence plate detection in case of intelligent camera or speed measurements of individual tracked vehicles in case of smart radar including reporting information to the server or superior computer nearby.
- Addition of secure features and non-repudiability mechanisms embedded within the sensor (SW or HW).

COG will provide **technological modules** (@M1 TRL 2-3, @M36 TRL 4-5) for optimising and securing communication from IoT and edge devices, among others, cameras and other smart sensors in Camea's use case.

- Currently, existing systems for IoT secure data exchange do not employ efficient mechanisms for on-site undeniability and, in the case of today's tools based on deep learning, it is not possible to securely update the underlying recognition and data processing models. This will be enabled using the technology developed inside AIDOSec by Cognitechna.

COG technology mainly contributes to deliver **AIDOSec results R1.1, R2.4** and **R3.1.**

DT will contribute to advancing the knowledge on detection and analysis of vulnerabilities in software systems, with the goal of better understanding the requirements of SecDevOps regarding vulnerability analysis, context and detection.

- Specifically DT will work on **technological modules** (@M1 TRL 2-3, @M36 TRL 4-5) for vulnerability analytics, involving source code analysis for the use of machine learning techniques as well as analysing vulnerability metadata, to understand and categorise vulnerabilities in the context of larger systems. This contributes to threat intelligence information relevant for **R2.4** as well as development of methods and tools relevant for **R2.1** and **R2.2**.
- Further Dynatrace is interested to create prototypes from the gained knowledge in AIDOSec to eventually transfer such research innovation into product features.

GTS is part of the Thales group, and being a railway transportation use case provider in AIDOSec, offers a range of innovative solutions to ensure a safe, reliable and economical freight and passenger traffic on the rail network.
GTS will use the technologies developed in AIDOSec for pushing the cloud readiness of their railway solutions towards better runtime monitoring and thereby diagnosability and maintainability.

HAL is focusing on developing **Smart IoT Monitoring Solutions** (@M1 TRL 2, @M36 TRL 5) in which technology concepts and applications have been formulated. These solutions are intended to enhance the security and operational efficiency of IoT devices in various environments. **Planned Improvement:** The goal for Haltian is to advance these monitoring solutions to TRL 4-5 by the end of the project, demonstrating the technology in a

controlled environment with some integration into real-world applications. The integration of AI algorithms will allow for predictive maintenance and threat detection capabilities, improving the responsiveness and adaptability of IoT systems. **Contribution to AIDOSec Objectives:** Haltian's AI-enhanced monitoring systems will play a crucial role in fulfilling AIDOSec results **R2.3** and **R3.3**. These advancements will aid in the early detection of security threats and enable proactive maintenance strategies, thereby supporting the security framework developed in the AIDOSec project for connected devices and systems.

HIB is a *Use Case Provider* and brings the *SecDevOps in Medical IoT Applications Case Study.* The use case is linked to **AIDOSec result R4.5** in Table 1.1.2.b, and it is detailed in the *Industrial use cases Section*. HIB is also a AI software solution provider integrating DevOps in their portfolio.

- The use case would consist in the process of transition from an informal DevOps model to an integrated SecDevOps with emphasis on better testing of the hardware/software assets.
- Innovation will come from introducing the AI algorithms in the design phase with integrated security and other AI user aspects (acceptability, trust, data transparency) built into the e-health development pipeline.

IMT will contribute with the following technology and the planned improvement:

- **EMF Views** (@M1 TRL3-4, @M36 TRL 5): A solution that allows creating views that focus on only part of a model, and/or views that combine several models that conform to different metamodels. Views can be navigated and queried as regular models are, and they can be used as inputs to model transformations, code generation, etc. More advanced features are planned to be added to the tool according to the needs in terms of security in the context of CPS engineering. For example, an extended support, possibly AI/ML-based, for model view update and maintenance (i.e., to ensure models-view synchronisation) or for view access control is planned to be further researched and prototyped. Such features will be deployed and tested in the context of realistic industrial scenarios. The EMF Views solution is linked to **AIDOSec results R2.1 and R3.1**.
- **ATL** (@M1 TRL6, @M36 TRL 6-7): A model transformation language and toolkit. ATL provides ways to automatically produce a set of target models from a set of source models (that may conform to several different metamodels). New experiments are planned to be performed around the tool according to the needs in terms of security in the context of CPS engineering. For example, in order to allow for more secure model transformations during various CPS engineering activities. To this end, different verification techniques potentially applicable with model transformation will be studied, including constraint solvers or more formal proof systems. Such features will be deployed and tested in the context of realistic industrial scenarios. The ATL solution is linked to **AIDOSec result R3.1**.

INNORIV will contribute with the following technology and the planned improvement:

- **Encrypted communication protocols in embedded systems** (@M1 TRL3, @M36 TRL 5). Provide a global and long lasting system for reports on recent design upgrades denoted as the "Secure Platform" developing an Intrusion Detection System and also will contribute to design develop test and validate secure platform cloud system storage architecture. This technology is mainly linked to **AIDOSec results R1.1. R1.2, R3.2** and **R3.3.**

INT will contribute with the following technologies and the planned improvements:

- **Common Vulnerability Scanner** (@M1 TRL2, @M36 TRL 4-5): a tool that can scan various websites and databases to collect information on common vulnerabilities in Computer Systems and Hardware components. The tool automatically processes the collected data (coming from different sources) and converts it in a standardised format that can be easily stored locally for "intelligent" searches. This tool is mainly linked to **AIDOSec results R3.1.**
- **Cybersecurity Monitoring Tool** (@M1 TRL2, @M36 TRL 4-5): a software application that allows users to store and manage the list of components/elements/assets (we will refer to this list as a BOM) for a system that is currently in operation. The tool periodically performs vulnerability scans using the Common Vulnerability Scanner and alerts the user when a new vulnerability affecting an element in the BOM is detected. This tool is mainly linked to **AIDOSec results R2.3.**
- **Cyber Security Design Analysis Tool** (@M1 TRL3, @M36 TRL 4-5): a tool that enables users to perform a comprehensive analysis of potential security risks during the design phase of a project. The tool utilises the Common Vulnerability Scanner tool to identify potential vulnerabilities in the design by allowing it to perform queries in natural language. This tool is mainly linked to **AIDOSec results R2.1.**

JKU will work on the MDE techniques applied to SecDevOps. In particular, it will contribute with the following technology and the planned improvement:

- **DevOpsML** (@M1 TRL2, @M36 TRL 4): it is a conceptual framework for modelling and combining DevOps processes and platforms. The DevOps platform configurations can be mapped to software engineering processes of arbitrary complexity. This technology mainly contributes to delivering **AIDOSec results R1.1. R1.2**
- **AutomationML Modelling** (@M1 TRL3, @M36 TRL 5): it is a suite of model-driven research tools [33] based on the AutomationML standard. Conceived as a neutral data format based on XML for the storage and exchange of plant engineering information, it can be used as a general-purpose, template-based modelling language. It applies Eclipse Modeling Framework (EMF)-based technologies to CAEX (and then AutomationML). The suite currently includes 1) CAEX MDE Workbench; 2) UML profile for AutomationML; 3) UML/SysML to AutomationML Model Transformations. This technology mainly contributes to delivering **AIDOSec results R1.1. R1.2 R2.1**
- **Security Modes** (@M1 TRL2, @M36 TRL 4): this tool leverages MDE techniques to describe system configurations, modes, and mode switches and to react actively to newly reported vulnerabilities. This technology mainly contributes to delivering **AIDOSec results R1.1, R2.1 and R3.1**.

KAPSCH focus on leveraging technology of Intelligent Transportation Systems (ITS) like traffic management including orchestrated corridor and tolling solutions ranging from well-established to cutting-edge such as DSRC, RFID, GNSS, video and V2X (ITS-G5 and LTE-V2X) to establish services that include centralized systems housed in secure environments as well as remote systems positioned on the roadside, which use public networks. The planned improvements within AIDOSec is to raise the security bar even further for our products based on these technologies.

LIE will contribute with the following technology and the planned improvement.

- **LemonTree.Automation** (@M1 TRL2, @M36 TRL 7: in order to optimise this automation of the tool chain (pipeline, Continuous Integration, DevOps), we offer, with LemonTree.Automation, the possibility to integrate the MBSE world around Enterprise Architect even more completely into the tool chains of our automotive, defence and medtech customers. For example, documentation, architecture and specifications are included and the models can be built into different scenarios (build pipelines). This technology is mainly linked to **AIDOSec results R1.2, R2.1,** and **R3.1.**

MDU will work on the development of a traceability (meta-)model that will link the various phases of the SecDevOps process and hence propagate cybersecurity concerns across the development. This research contributes to **AIDOSec results R1.1 and R1.2.** MDU will also contribute with the following technology and the corresponding planned improvement.

- **Timed Rebeca and Afra** (@M1 TRL3, @M36 TRL 5): Rebeca is an actor-based language for the modelling and formal verification of concurrent and distributed systems. Actors, called rebecs, are instances of reactive classes and communicate via asynchronous message passing. Timed Rebeca, as an extension of Rebeca, has a notion of logical time that is a global time synchronised between all actors. Timed Rebeca is supported by a model checker tool Afra. Afra generates the state space of the Timed Rebeca model. These extensions mainly contribute to deliver **AIDOSec results R2.1 and R3.2**.
- **Lingua Franca (LF) and Epoch IDE** (@M1 TRL3, @M36 TRL 4): Lingua Franca is a metalanguage based on the Reactor model for programming Cyber-Physical Systems. A Reactor model is a collection of reactors. A reactor has one or more routines that are called reactions. Epoch IDE is a standalone application based on Eclipse that provides a syntax-directed editor, compiler, and diagram synthesis tool for Lingua Franca programs. These extensions mainly contribute to deliver **AIDOSec results R2.1 and R3.2**.
- **Microsoft Threat Modeling Tool** (@M1 TRL2, @M36 TRL 5): The Threat Modeling Tool is a core element of the Microsoft Security Development Lifecycle (SDL). It allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve. As a result, it greatly reduces the total cost of development. This extension mainly contributes to delivering **AIDOSec result R2.1**.

MSG specialises in providing expert services in Cybersecurity, Safety, Engineering, and Homologation, focusing primarily on the automotive sector through projects such as Automotive Cybersecurity Management Systems. Additionally, msg Plaut addresses cross-domain security concerns, such as those outlined in the Cyber Resilience Act, which is part of the EU's Digital Decade Strategy.

[33] https://github.com/amlModeling

In the AIDOSec project, msg Plaut acts as a Use Case Provider and introduces the Harmonised EU-CyberBridge Case Study. This study aims to conduct systematic analyses of Cybersecurity Standards and Regulations to explore the potential for harmonisation of these frameworks to achieve enhanced compliance and cybersecurity across the industry. This endeavor will assist technology providers in understanding and integrating broader regulatory insights, fostering a more resilient cybersecurity environment. The Harmonised EU-CyberBridge Case Study links directly to AIDOSec result R4.11 in Table 1.1.2.b and is detailed further in the Industrial Use Cases Section.

PG will mainly contribute with the work on the **Genius Core™ platform** (@M1 TRL4, @M36 TRL 6). Genius Core is a Digital Twin platform developed by Process Genius. With this platform 3D based visualisations of industrial processes and workflows can be created and populated with production data streams from various sources. PG main contributions will be:

- A collaborative research environment fostering innovation and knowledge exchange among AIDOSec participants.
- Enhanced security for the Genius Core™ platform through the incorporation of AI-driven security automation solutions and MDE techniques.
- Improved traceability solutions developed in collaboration with other AIDOSec participants, enabling better vulnerability prediction and root cause analysis.

This tool mainly contributes to deliver **AIDOSec results R1.1, R2.2, R2.4, R3.1**.

PRO is a *Use Case Provider* and brings the *Secure Smart Port Solutions by Design Case Study* The use case is linked to **AIDOSec result R4.6** in Table 1.1.2.b, and it is detailed in the *Industrial use cases Section*. It's work will focus on Static application security testing (SAST).

- SAST is lately used in order to include in the software development stage a proper review of the source code so that it helps in identifying sources of vulnerabilities. The problem with traditional SAST products is that they do not work for developers – they are too slow with scans that can take several hours, and they historically have had poor accuracy and returned too many false positives.
- Therefore, an **embedded, accurate SAST in real-time and actionable** will be implemented on AIDOSec aiming at helping on building software securely during the coding stage.

RISE, in general, will contribute to the project by providing AI- and ML-based solutions to enable automated analysis of security vulnerabilities by extracting threat patterns. In particular, RISE offers solutions for automated clustering and labelling of security issues from log files such as test reports. Moreover, RISE will also develop solutions for automated analysis of security-related textual requirements, identifying ambiguities and tackling security at the requirement level using natural language processing. RISE will also contribute in the area of security testing and test optimization to target security issues.

- **Security LogFlagger** (@M1 TRL2, @M36 TRL 4-5): In AIDOSec, novel solutions using machine learning techniques for automated analysis of security related issues at the requirement level and also based on system log files from system execution will be developed. As one example, use of large language models for security analysis and engineering will be a novel aspect that we will tackle in AIDOSec. LogFlagger uses SOTA language models and machine learning for automatically detecting (flagging) security-related failure and execution logs. In addition, LogFlagger will also use classifiers to further classify the malicious log into the common weakness enumeration classes, and can be easily integrated as part of a continuous engineering process. This technology mainly contributes to deliver **AIDOSec results R2.4** and **R3.1**.

SC is beginning the AIDOSec project with a focus on enhancing their **Model-Based Testing Tools** (@M1 TRL 3, @M36 TRL 5). These tools are currently at TRL 3, demonstrating initial proof-of-concept in controlled environments. The tools are designed to automate and streamline the testing processes in manufacturing, especially for complex electronic components. **Planned Improvement:** Throughout the AIDOSec project, SolidComp Oy aims to develop these testing tools further to reach TRL 5, validating the technology in a relevant industrial environment. The focus will be on integrating more comprehensive simulation features that can predict system behavior under various scenarios, thereby reducing the time and cost associated with physical testing. **Contribution to AIDOSec Objectives:** SolidComp's enhanced testing tools will contribute primarily to AIDOSec results **R2.2** and **R3.1**. By improving the accuracy and efficiency of testing processes, these tools will support the broader goal of advancing CyberSecurity measures within the SecDevOps framework for industrial applications.

SOFT will contribute with the **extension of Modelio** with the following **modules** (@M1 TRL 3, @M36 TRL 7) and the planned improvement:

- **ARQAN**: Security requirements analysis tool based on NLP technologies for extraction of requirements and recommendations of security practices. Tests recommendation engine. Application to software security practices applications. This module mainly contributes to deliver **AIDOSec results R2.4, R3.1.**
- **RQCODE** - repository for (security) requirements as code - provides the ability to verify the security requirements. The current technology is based on Security Technology Implementation Guides. The tests will be extended to new platforms such as Ubuntu 18+ and Windows 11. In addition, the tests for OWASP guidelines will be created. This module mainly contributes to deliver **AIDOSec results R2.2, R3.2.**
- **Security threat modelling**: Requirements models. Security requirements modelling in Modelio, integration with security threat modelling and testing methods. This module mainly contributes to deliver **AIDOSec results R1.1, R1.2, R2.1.**

SWA will contribute with the following technology and the planned improvement.

- **Swascan Cyber threat intelligence (SwCTI)** (@M1 TRL2, @M36 TRL 5): SwCTI Threat Intel Platform primarily focuses on analysing "raw" data which is collected during - recent and past - events in order to monitor, detect and prevent an organisation from threats, shifting the focus from reactive defence to preventive and "smart" security measures. We are interested in improving our platform by integrating it:
  with the machine learning components to improve correlations and data analysis;
  with the threat model, to make it more actual and context-aware, by using real data about possible threats;
  with the response components, to augment the investigation and response capabilities.

This tool mainly contributes to deliver **AIDOSec result R2.4.**

- **Vulnerability Management System (VMS)** (@M1 TRL2, @M36 TRL 5): The vulnerability management system is a platform that performs vulnerability scans on the platforms exposed by customers, analyses the results, filters out false positives, prioritises vulnerabilities so that they can be fixed, and opens intervention tickets to the teams in charge of the portions of the architecture where the fixes are expected, enabling them to monitor the forecasted SLAs. We are interested in improving false positives filtering through integration with ML for the analysis of the findings. Also we'd like to achieve a greater integration with the SecDevOps process. This tool mainly contributes to deliver **AIDOSec results R2.2, R3.2 and R3.3.**
- **Cloud Environment Security Assessment (CESA)** (@M1 TRL2, @M36 TRL 5): CESA performs an analysis of a Cloud environment such as, for example, an AWS account, an Azure subscription or a GCP project. Since the cloud environments will become even more pervasive in DevOps processes, we want to achieve a greater and effective integration of the solution, through ML. This tool mainly contributes to deliver **AIDOSec results R2.1 and R2.2.**

TEK is a *Use Case Provider* and brings the *Wireless Communication Security Case Study*. For its case study, TEK proposes an AI-based detector/classifier of attacks to physical and MAC layers of wireless communications. In AIDOSec, TEK aims to improve two technological aspects:

- the system adaptability to operational scenarios, which are highly dynamic with regard to wireless links as well as to sources of possible attacks;
- the AI models effectiveness, through their preventive analysis in new system configurations, their monitor during the operations, and their re-tuning with freshly collected but limited datasets.
- Moreover, on the process side, TEK aims to establish an effective DevOps development of AI systems, which it will experiment in the case study with the contribution of data scientists, software developers, operation people, and end-users.

The use case is linked to **AIDOSec result R4.7** in Table 1.1.2.b, and it is detailed in the *Industrial use cases Section*.

THA is a *Use Case Provider* and brings the *Tooled-Up Distributed Real-Time Drone Application Case Study.* The use case is linked to **AIDOSec result R4.8** in Table 1.1.2.b, and it is *d*etailed in the *Industrial use cases Section*. Thales will contribute to the project by improving the security attacks detection in the mixed critical real-time communication networks TSN (Time Sensitive Networking). For this purpose, Thales will develop:

- a first software module that will take at its input communication traces and generate an analytic model of the real-time behaviour of the traces.
- a second software module that includes an innovative security analysis that will be able to detect any security anomalies by analysing the real-time behaviour of the traces.

TL is a *Use Case Provider* and brings the *Collaborative Research and Development of Security-Critical AI-Based Solutions for ThingLink XR Trainings Platform Case Study*. The use case is linked to **AIDOSec result R4.9** in Table 1.1.2.b, and it is detailed in the *Industrial use cases Section*. It's technical work is focused on ThingLink:

- ThingLink is an innovative platform enabling critical sector customers to create immersive XR (Extended Reality) training for safety and onboarding purposes. We recognize the value of collaboration in achieving global success and securing a strong competitive position in the market.
- To this end, we actively participate and contribute to the AIDOSec project's AI-driven framework supporting DevOps practices with a strong emphasis on security, tailored to the specific needs of the manufacturing industry worldwide.

UEF will use security-critical AI-based Digital Solutions (@M1 TRL 2, @M36 TRL 5) to monitor and optimise production processes, test various conditions, and mitigate unexpected security events in manufacturing industries. UEF will also utilise security-critical AI-based MDE practices and techniques to automate activities and improve productivity, software quality, and security. UEF will contribute to:

- providing a security-critical AI-based holistic Finland Use Case for the continuous systems engineering;
- providing an AI-based core model framework for the efficient, secure, and continuous engineering; defining a security-critical AI-based continuous V&V strategy for the validation of functional and non-functional requirements at different levels of fidelity;
- providing security-critical services supporting AI-based prediction, testing, and monitoring; increasing productivity, reducing development costs, improving security, and reducing time-to-market, thanks to security-critical AI-based Finland Use Case;
- achieving project aims and thus improving the competitiveness of European industry in the security-critical manufacturing industry domain;
- and simplifying the development of security-critical AI-based systems in multiple domains (Finland Use Case can easily be extended into other domains) by utilising EDGE-Intelligence, AI-based CyberSecurity, and guaranteeing their quality while reducing the skill level required from the developer.

UEF research and solutions are linked to **AIDOSec results R1.1, R.2*, R.3*.**

UNICA will be involved mainly in the Resilient New Concept Cars Case Study and will provide support in porting and accelerating the selected algorithms on FPGA-based architectures. To do that we will bring into AIDOsec a toolchain to specify and port adaptive CNN at the edge (@M1 TRL3, @M36 TRL 4-5) on FPGA-based SoCs. As the toolchain leverages high-level synthesis, security-related features can be implemented and updated on the accelerator specification, thus contributing to AIDOSec result R1.1. The resulting hw-component is exploited within the UC and will contribute to **AIDOSec result R4.1.**

UNICAN proposes research efforts in these lines:

- On the one hand the **design and implementation of security metamodels and ontologies** (@M1 TRL 1-2, @M36 TRL 3-4) capable of capturing the security needs of CPS systems through the definition of security requirements, which are to be identified in accordance with the security recommendations of the ENISA and OWASP guides.
- On the other hand, in the context of DevOps processes, the more traditional model-based techniques for the simulation and design of secure software over trustable platforms will be our basis for proposing its improvement by the run-time evaluation of the final products at work and the feed-back refinement of design-time models accordingly. This approach applied to the **updating of schedulability analysis models** (@M1 TRL 1-2, @M36 TRL 3-4) and the techniques developed by our group will allow us to perform sharper timing analysis of software deployed on IMA secure platforms.
- From the perspective of the adoption of these innovations at industrial level, the idea here is to take advantage of the well-recognized need for security to show the ease and value of the insertion of these methodological and practical DevOps advances also for other model-based V&V processes. We plan here to demonstrate it for timing analysis but the project as a whole contributes also to experience improvements in many phases of the development processes, all the way from requirements to testing and deployment.
- Finally, we plan to populate all the enhancements that AIDOSec finds necessary into the modelling languages in these domains at industrial level by contributing to improve the corresponding standards in the technical task forces of the OMG.

UNICAN research is primarily mapped to **AIDOSec results R1.1, R3.2, and R4.8**.

UNISS will contribute to advance the knowledge on Representation and Reasoning techniques for threat modelling. An exhaustive **Threat Model** (@M1 TRL 1-2, @M36 TRL 3) will be carried out, to ensure a secure design of the framework.

- To such extent, standards and widely used threat modelling methodologies will be used in conjunction with formal representations of cyberthreats (ontologies), in order to enable the usage of automated reasoning

techniques for verification. In this regard, UNISS aims at improving the performance and the scalability of formal verification technologies for this task.

This research is mainly linked to **AIDOSec results R2.1, and R4.1**.

UNITE will contribute to extend the knowledge on model-based and model-driven engineering, AI/ML, and DevOps. In particular, UNITE aims at:

- Enhancing methodologies and technologies with the scope to support the design and development of a model-based framework for Security in DevOps;
- Applying model-based methods and techniques for the definition of the general AIDOSec architecture and framework and for the AIDOSec traceability approach;
- Acquiring new methodologies and techniques for cybersecurity pattern detection and correlation, supporting the designer in the continuous improvement of software security.
- Enhancing AI/ML techniques to mitigate vulnerabilities while preserving the integrity and confidentiality of models and data.

UNITE will also contribute with the following technologies:

- SLIDE-x (@M1 TRL 2, @M36 TRL 4): is an open-source framework and related toolchain that facilitates System-Level HW/SW Co-Design of Embedded Systems and Cyber-Physical Systems (CPSs) by creating datasets useful for analysis, comparison, and simulations/predictions. SLIDE-x will be extended in AIDOSec to address AI/ML vulnerabilities and data breaches, preventing incorrect HW/SW performance predictions, platform selection, and trade-off analysis. SLIDE-x will ensure model and data integrity and confidentiality through profiling and feature extractions that excludes information about source code applications, while also providing the opportunity to validate cryptographic algorithms across various application domains using specific benchmarks.This tool mainly contribute to deliver **AIDOSec results R1.1, R3.1 and R3.2**.

UNITE research is mainly linked to **AIDOSec results R1.1, R1.2, R2.1, R2.4, R3.***

UNIVAQ will contribute with the following technology and the planned improvement:

- **HEPSYCODE** (@M1 TRL2, @M36 TRL 4): it is a System-Level Methodology for HW/SW Co-Design of Heterogeneous Parallel Dedicated Systems; it will be extended (together with the related prototypal toolchain) to consider security-related requirements (e.g., cryptography, intrusion detection) directly at the system-level of abstraction. This tool mainly contributes to deliver **AIDOSec results R1.1** and **R3.2.**

UOC will contribute with the following technology and the planned improvement:

- **DescribeML** (@M1 TRL3, @36 TRL 4): DescribeML is a VSCode language plugin to describe machine-learning datasets. DescribeML aims at improving dataset documentation for machine learning. In AIDOSec, DescribeML may be used in different scenarios, such as: (i) a solution to describe the different datasets that are used during the development of the AI-based components of the AIDOSec Toolset; (ii) a solution to describe and to publish important information of the AIDOSec datasets, making easier to reproduce the project results to others, when the actual data cannot be shared because of privacy or confidentiality reasons; (iii) as a tool taking part of the AIDOSec Toolset to be used by users wanting to apply the project results and technologies to their own scenarios and problems. DescribeML mainly contributes to deliver **AIDOSec results R1.1** and **R3.1**.
- **MVM** (Model Validator Mixer) (@M1 TRL3, @36 TRL 4): MVM is an extension of the USE UML Specification Environment and its Model Validator plug-in to detect inconsistencies in UML/OCL specifications. In AIDOSec, the MVM validator may be used to verify security properties and constraints during the design stages. In this sense, the AIDOSec Toolset may rely on different models (design models, architectural models, security models) that can be verified using the MVM solver. MVM mainly contributes to deliver **AIDOSec results R1.1**, **R2.1** and **R2.2**.

UST will contribute to advancing knowledge and methods for Security Testing Automation in SecDevOps. UST has developed a complete **SecDevOps transformation framework** (@M1 TRL 4, @M36 TRL 6), our goal in this project is to guarantee the implementation of security tests in all the DevOps lifecycle phases by developing a strategic roadmap that defines the type of tests to be included in each phase and the suggested tools to be used adapted to our client's needs and restrictions. Testing in the AIDOSec project, we are going to focus on the following type of automated tests:

- Software composition analysis.
- Static application security testing.
- Dynamic application security testing.

- Interactive application security testing.
- Penetration automated security testing.
- Infrastructure as code security testing.
- Configuration management security testing.

UST technologies are linked to **AIDOSec results R1.1, R2.1, R2.2, R2.3** and **R2.4**.

WMO is a *Use Case Provider* and brings theCase Study on AI and Model-Based Approaches for Industrial Communication Products. The use case is linked to **AIDOSec result R4.10** in Table 1.1.2.b, and it is detailed in the *Industrial use cases Section*. WMO has sophisticated tools for product design, DevOps and test automation. Some of these are developed in-house, some are open source, and some are commercial third-party tools. During AIDOSec, WMO aims at extending these while also experimenting with the introduction of new tools to support the use case. These solutions will be developed by, or in cooperation with, academic partners in AIDOSec. Exploring already existing open-source tools could also be a possibility. These technologies will contribute to **AIDOSec results R2.1, R2.2, R2.3, R3.1, R3.2** and **R3.3**.

#§PRJ-OBJ-PO§#

1.2 Methodology

#@CON-MET-CM@# #@COM-PLE-CP@#

According to the ECS SRIA 2024, ensuring the security of modern systems is a major challenge due to the demand for greater functionality and the heterogeneity of multiple components and services. This demand causes interactions at multiple levels. The increase in computing power and communication of components and systems, along with hybrid and distributed architectures, requires a rethinking of traditional approaches to security. Artificial Intelligence (AI) and Machine Learning (ML) can be leveraged to improve security *(CST 2.4 "Quality Reliability, Safety and Cyber-Security")*.

Ensuring security is part of the continuous development process (in particular , DevOps process) and needs to be supported by tools for analysis and testing. These processes enable data collected during operation to be used for iterative development and updates of existing products. The techniques described in *CST 2.3 "Architecture and Design: Method and Tools"* complement the technologies involved in cyber-security processes.

According to this, the goal of AIDOSec is to provide a framework to support the entire cybersecurity process. It considers the relationship between causes, consequences, and mitigation/recovery. AIDOSec supports the engineering of industrial software-intensive systems by integrating security processes into DevOps pipelines using model-based and artificial intelligence techniques.

In the rest of the section, we introduce the concepts behind our methodology and we present the AIDOSec approach and main components.

1.2.1 Basic concepts

AIDOSec intends to promote DevOps from a security-centric point of view. Figure 1.2.1 below illustrates the security cycle (coloured purple) that surrounds the entire pipeline and consists of six steps considered the basis of a SecDevOps process.

Threat modelling[34,35,36] - Threat modelling is the process used to identify and prioritise potential threats and vulnerabilities in a system or application, in order to mitigate them before they can be exploited. It involves first identifying assets, potential attackers, and potential attack vectors, and then analysing the potential impact and likelihood of each threat. The goal of threat modelling is to provide a structured approach for improving the security of a system or application by anticipating and preventing potential attacks. There are several threat modelling methodologies, the choice depends on the specific needs and characteristics of the system or application being evaluated.

[34] Xiong, Wenjun, and Robert Lagerström. "Threat modeling–A systematic literature review." Computers & security 84 (2019): 53-69
[35] Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014
[36] https://www.threatmodelingmanifesto.org/

Security testing[37,38,39] **-** A security test is a type of software test that aims to identify vulnerabilities, weaknesses, and potential threats in a system or application. Security testing involves simulating attacks, attempting to exploit vulnerabilities, and identifying weaknesses in the system's defences. The goal of security testing is to uncover vulnerabilities before they can be used by attackers and to help ensure that the system is secure and compliant with relevant security standards.

Security testing can include a wide range of activities, such as penetration testing, vulnerability scanning, code reviews, and security audits. It may be performed manually or using automated tools, or a combination of both. The results of security testing are typically documented and used to prioritise security issues and develop strategies for mitigating identified risks.

Security Monitoring - Security Monitoring is an essential part of any DevOps cycle because it helps to ensure that the systems and applications being developed and deployed are secure and resilient against attacks. In a DevOps cycle, security monitoring typically involves continuously monitoring systems and applications for potential security threats or vulnerabilities. This can be done through a variety of methods, including log analysis and network monitoring.

Detection - Detection refers to the process of identifying potential security incidents or threats that may be occurring in a system or network. The primary goal of detection is to identify potential security breaches or attacks as early as possible so that appropriate action can be taken to mitigate the impact of the incident.

Detection can be performed using a variety of methods and tools, that use different techniques such as signature-based detection, anomaly detection, and behavioural analysis to identify potential threats or indicators of compromise.

Response - The detection phase is often followed by an investigation and response phase, where the security incident is analysed to determine its scope, severity, and impact. The response phase involves taking appropriate actions to contain the incident, minimise the damage caused by the incident, and prevent it from happening again in the future.

Overall, detection is a critical activity in cybersecurity, as it enables organisations to quickly identify and respond to potential security incidents, and helps to minimise the impact of these incidents on the organisation.

Validation - Together with monitoring (i.e., continuous observation of the system activity to identify potential security incidents or anomalies), validation provides ongoing visibility into the security posture of the system.

Validation, in particular, involves verifying that security controls are working as expected and that the system is compliant with relevant security policies and standards.

Feedback - The feedback loop, thus generated, enables continuous monitoring, analysis and improvement of safety activities based on observed results. This feedback loop, therefore, enables learning from past security incidents and using this information to improve security postures and reduce the likelihood of future incidents.

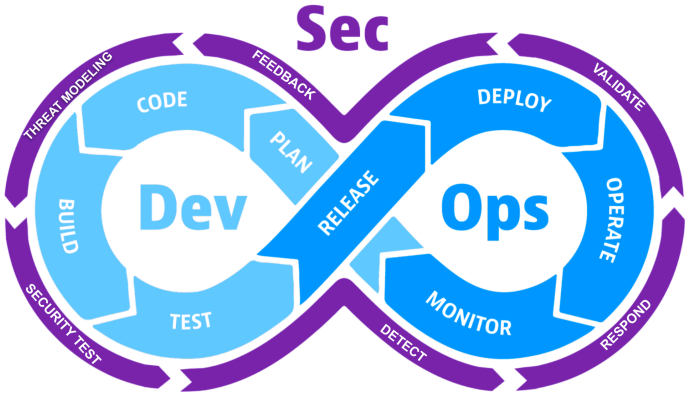


Figure 1.2.1 - *SecDevOps in the AIDOSec view*

Under the AIDOSec project, these activities will be considered the essential part of an effective cybersecurity strategy. **The AIDOSec Framework will be designed and developed in order to support these activities as the**

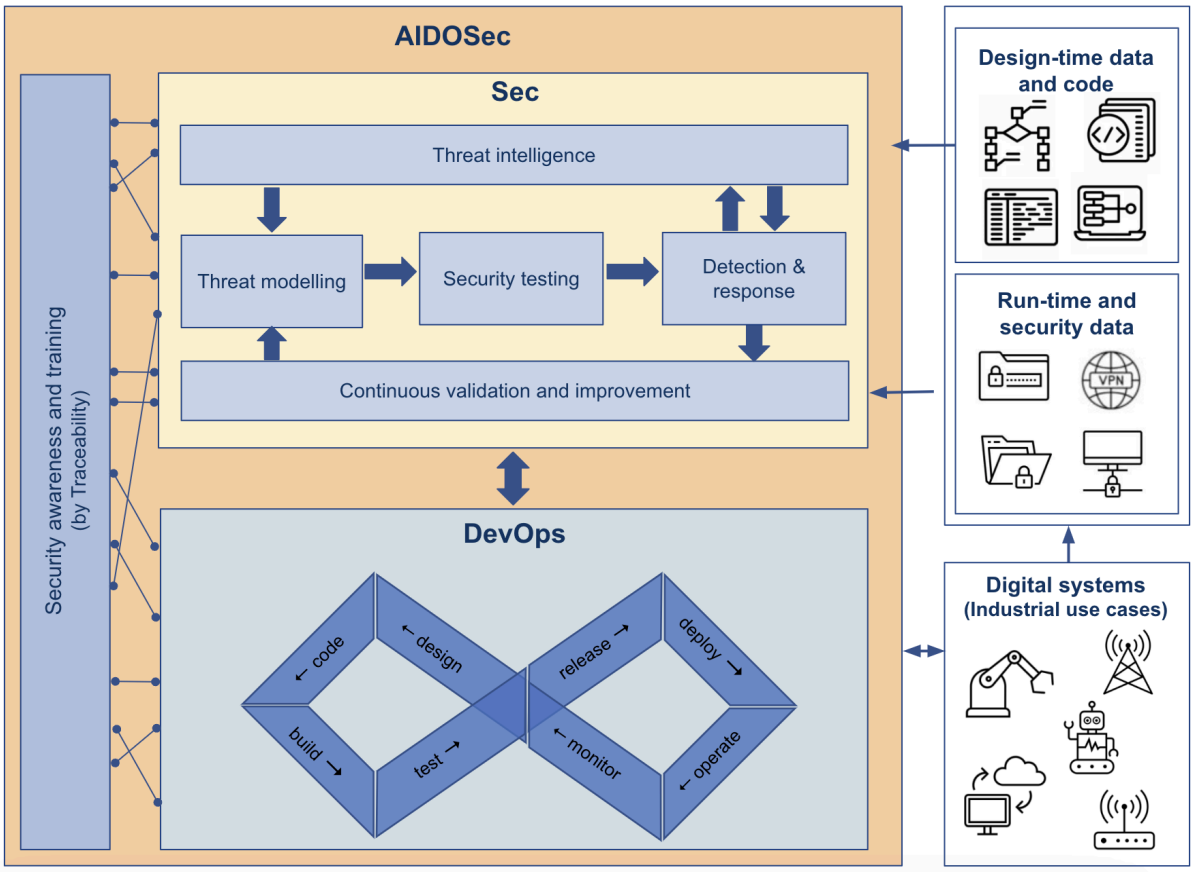
[37] Potter, Bruce, and Gary McGraw. "Software security testing." IEEE Security & Privacy 2.5 (2004): 81-85
[38] Felderer, Michael, et al. "Security testing: A survey." *Advances in Computers*. Vol. 101. Elsevier, 2016. 1-51
[39] https://owasp.org/www-project-web-security-testing-guide/v42/

core capabilities to be provided in the context of the project. It is the practical foundation of the AIDOSec conceptual approach and corresponding technical solutions.

1.2.2 AIDOSec approach

The framework will mainly rely on model-based methods and intelligent techniques. Thus, Model-driven Engineering (MDE)[40] and Artificial Intelligence (AI) will have a key role in the proposed framework. MDE will contribute by (i) providing better abstraction principles and techniques, (ii) facilitating activities automation (for instance, in threat modelling at design time), (iii) providing a new landscape for dealing with traceability, and (iv) supporting technology integration among all the covered design and development activities. AI will contribute by (i) automating repetitive and time-consuming cybersecurity tasks (e.g., static/dynamic analysis, vulnerability assessments, and detecting and responding to attacks), and (ii) incorporating ML into the security workflow, so that organisations can accomplish tasks faster, and act on and remediate threats at a rate that would not be possible with manual human capability alone. The overall framework should be tools/environment-agnostic (i.e., it can be exploited independently from the SecDevOps platform tools adopted). To cover all these topics and deal with the complete value chain, AIDOSec will bring together prominent tool vendors and research organisations with SOTA methods and tools that will be validated in highly relevant European industry case studies. The end users from the space, automotive, railway, smart sensors, health monitoring, digital industry, manufacturing and connectivity industry domains will drive the project by providing real-world requirements and case studies as well as by validating and endorsing the AIDOSec research and technical results.

Figure 1.2.2 provides an overview of the AIDOSec global approach and emphasises its key principles and concepts, relating them to corresponding WPs (see Section 3.1.2 for details). The overall AIDOSec infrastructure works with different kinds of data, including security data collected at runtime (e.g., IT monitoring, log events, etc.), along with data produced during the design phase of the software development process (e.g., software models, design documentation, traceability information, source code, etc.), as depicted in the right-hand side of the Figure.



[40] M. Brambilla, J. Cabot, M. Wimmer, Model-Driven Software Engineering in Practice, Second Edition, Morgan & Claypool Publishers, 2017

Figure 1.2.2 - *The AIDOSec overall approach*

All data from these sources will be used as input for the *Sec* component of the *AIDOSec* framework. The *Threat modelling* component is intended to support related activities, such as defining security requirements, identifying threats, identifying mitigation actions, etc. This component will use mainly architectural and software design models. The *Security testing* component is intended to support several kinds of security tests (such as static analysis, vulnerability assessment, penetration test, etc.). The *Detection & response* component aims to support all activities aimed at providing detection, investigation, threat hunting, and response capabilities. The *Threat Intelligence* component supports the injection of intelligence information into the *Threat Modelling* and *Detection & response* components. Then, the *Continuous validation and improvement* component aims at providing specific capabilities for the analysis of the cybersecurity activities (as defined and implemented in the previous components) based on continuously observed results. Moreover, the feedback loop thus generated will allow for improved security activities. These components will act in specific phases of the DevOps pipeline. Finally, all these activities will be traced by means of a *Traceability* model and related support enabling the correlation and reuse among the different development phases. This traceability support will also allow it to identify and handle root causes, as well as to make predictions in the early design phases that can guide subsequent analyses. The AIDOSec model-based framework and its technologies will be applied and validated through complementary *Digital systems (Industrial use cases)*.

1.2.2.1 AIDOSec Model-based Architecture and Traceability

The AIDOSec solution architecture will be defined by a core team in terms of engineering activities. These activities combine principles and practices from DevOps and Cybersecurity, relying on MDE and AI/ML automation. Concretely, we will define the architecture in terms of a hierarchy of components and subcomponents, offering or consuming services, and we will define their capabilities as functional interfaces. On the most practical level, we will identify components and interfaces related to capabilities for the various Cybersecurity activities in the DevOps phases (i.e., threat modelling, security testing, detection & response, threat intelligence, and continuous improvement). The AIDOSec solution's architecture will allow tracing a first integration link between the framework and the partners' use case and solutions capabilities through their relations to a set of generic requirements. Moreover, it will enable the implementation and integration of the AIDOSec capabilities.

At this architectural level, we will define the AIDOSec traceability methodology, which concerns maintaining links (sometimes conceptual or implicit) existing between the elements involved in the AIDOSec framework, i.e.:

- Links between different cybersecurity components (e.g., categorised threats can be directly related to mitigation measures and actions to address them)
- Links between cybersecurity components and DevOps phases (e.g., threats that can breach security requirements, mitigation measures that can be implemented on the code or can impact the design of the system)

The idea is to make explicit the causal links that govern security decisions: for instance, downward causality when changes to threat specifications or mitigation actions affecting the actions to be executed against attacks; ascending causality when it comes to updating threat specifications or mitigation actions as a result of feedback obtained by observing the results of response actions.

This component will enable to deliver the project's objective *O1 - AIDOSec global model-based framework for SecDevOps* (see Table 1.1.2.a).

1.2.2.2 AIDOSec Threat Modelling

The AIDOSec Threat Modelling will support the design and development of specific solutions. As there are several threat modelling methodologies, this component aims at being agnostic with respect to the specific methodology being adopted. The objective is rather to support the integration of existing or new methods within the AIDOSec framework.

In AIDOSec, secure architecture and design are considered an integral part of the project. From a security perspective, architecture and design are considered critical phases of the system and software development lifecycle. In fact, the decisions made during these phases can lead to a more resilient and resistant to attack approach and structure, and they can also prescribe and guide decisions in later phases, such as code and test. On

the other hand, bad decisions made during these stages can lead to design flaws that can never be overcome or fixed by even the smartest and most disciplined coding and testing efforts.
The AIDOSec Threat Modelling component is closely related to the architecture and design, and it contributes to the continuous feedback loop (see Section 1.2.2.6), which aims to improve the secure architecture and design. In particular, this component will identify the architectural components and analyse the interaction between these components, considering as input artefacts like architectural models and behavioural models, but also survey and interviews to software architects.

Among other activities, this component is interested in the identification of possible **threats** to which the software under control is potentially subject, related **countermeasures**, and **evaluation of risks**. This can be augmented via additional information coming from other sources, internals, like the threat intelligence component, or externals (e.g., the interaction with external frameworks providing knowledge of adversary tactics and techniques based on real-world observations - like the ATT&CK[41] framework).

This component will contribute to delivering the project's objective *O2 - AIDOSec cybersecurity toolkit* (see Table 1.1.2.a).

1.2.2.3 AIDOSec Security testing

The AIDOSec Security testing will support several kinds of **testing**, depending on the part of the DevOps loop in which they will act: e.g. Static Code Analysis and Software Component analysis during the build and/or test phase; Dynamic Analysis and Vulnerability Assessment during the Test Phase; limited Penetration Test during the Operate phase. The common goal of all of these tests is to find weaknesses and vulnerabilities before they pose a risk to the company: a weakness, typically found during the coding phase by a static analysis, will not necessarily be a vulnerability, but it will certainly be its precursor. The solution should ensure a low percentage of false positives found during testing, through a learning process supported by ML.

This component will contribute to delivering the project's objective *O2 - AIDOSec cybersecurity toolkit* (see Table 1.1.2.a).

1.2.2.4 AIDOSec Detection & response

AIDOSec Detection & response component aims to support activities aimed at providing **detection**, investigation, threat hunting and **response** capabilities. This component will provide solutions able to detect and respond to cyber threats in real-time, including the continuous monitoring of endpoint devices in the network to detect signs of cyberattack and resolve them either through automated remediation or by alerting a human stakeholder.

This component will contribute to delivering the project's objective *O2 - AIDOSec cybersecurity toolkit* (see Table 1.1.2.a).

1.2.2.5 AIDOSec Threat intelligence

The AIDOSec Threat Intelligence will support the injection of intelligence information to the Threat Modelling and to the Detection & response components.

In alignment with Gartner's definition of threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets", AIDOSec's Threat Intelligence component aims to incorporate a diverse array of data types to effectively identify and understand potential threats. The data categories include:

- **Indicator of Compromise (IoC) Data:** These crucial pieces of evidence, demonstrating the occurrence of a cyber-attack, encompass specific malicious activity patterns, such as IP addresses, domains, malware file hashes, suspicious URLs, and email addresses.
- **Tactical Data:** To formulate robust defensive strategies, understanding the specific Techniques, Tactics, and Procedures (TTPs) employed by attackers is imperative.
- **Strategic Data:** The assimilation of comprehensive information concerning threat trends and emergent cybersecurity risks is critical. Such data may include an analysis of the motivations and targets of specific threat actors or groups as well as knowledge about known and unknown (zero-day) vulnerabilities.
- **Operational Data:** The data encapsulates specific details about a threat or attack, such as the infrastructure used by an attacker or the specifics of a phishing campaign.

[41] ATT&CK: https://attack.mitre.org/

- **Open-source Intelligence (OSINT):** This data type includes publicly accessible information gathered from blogs, forums, social media, and other public platforms.
- **Darkweb and Underground Forum Data:** Data from such illicit online communities, where cybercriminals often trade information, tools, and services, provide a deeper understanding of their *modus operandi*.
- **Incident Reports and Logs:** The inclusion of data from past incidents and logs from network devices, servers, and other infrastructures provide valuable insights for future preventive measures.
- **Threat Intelligence Feeds:** Such services supply real-time or near-real-time information about potential threats and vulnerabilities, sourced from various entities such as commercial vendors, industry groups, government organisations, or open-source projects.
- **Data from CERTs and CSIRTs:** The shared information from these organisations about past attacks, vulnerabilities, and potential threats is essential to fortifying our cybersecurity measures.

The gathered intelligence information will serve a dual role: firstly, to augment the threat model, making it more contextually appropriate, to provide a more sound risk evaluation; and secondly, to feed the detection and response component, providing the data necessary to better identify possible attacks. As new data is discovered by the response component, it will be used to enhance the overall threat intelligence information.

This component will contribute to delivering the project's objective *O2 - AIDOSec cybersecurity toolkit* (see Table 1.1.2.a).

1.2.2.6 AIDOSec Continuous validation and improvement

The goal of this component is to verify that the system is working as expected, i.e., the AIDOSec security solutions do not affect the system operation while improving the whole security posture. It implies the observation of the system activity and the analysis of run-time data to verify, for instance, that security controls are working as expected and that the system is compliant with security requirements. Also, validation may involve other functional or non-functional requirements, for instance, related to the various DevOps phases affected by the Security process. It includes the use of AI/ML techniques for the analysis of both historical and real-time data involved in the process.

Moreover, this component will support the **continuous feedback loop**, based on involving the output generated so far, to make improvements to the whole security process. This phase will make use of the AIDOSec Traceability methodology (see Section 1.2.2.1) to exploit the links between cybersecurity solutions and/or the DevOps phases. Hereafter some examples:

- Cybersecurity activities performed during Development (e.g., threat modelling, security testing, ...) can exchange feedback with each other to improve threat identification, threat prioritisation, and design of effective risk mitigation, as well as improve the application of security testing;
- In addition, cybersecurity activities performed during Development can share feedback with cybersecurity activities performed during Operation (e.g., detect & respond, validate, etc.). For example, modelled threats can be linked to response actions, and response actions and validation results can be used to improve threat modelling;
- Finally, cybersecurity activities performed during Operation can generate relevant feedback that can be applied back to the system development phase. For example, response actions and validation results can be used to improve system design or apply code changes.

By continuously repeating this feedback loop, organisations can improve their cybersecurity posture over time and reduce the likelihood and impact of security incidents (see Section 1.2.3 for further details).

The feedback obtained at this stage can also contribute to the training of developers. They can improve their knowledge by contributing to the quality of their work. Thus, the proposed cycle suggests both automatic mitigation actions and automated training actions for developers, with the aim of reducing vulnerabilities (which are in fact mostly created by developers). See Section 1.2.2.7 for further details.

This component will contribute to deliver the project's objective *O3 - AIDOSec continuous validation and improvement* (see Table 1.1.2.a).

1.2.2.7 Awareness, training and security culture

According to the ECS SRIA 2024's vision, orchestrated system development requires holistic design processes where multifaceted developer communities jointly work together to achieve acceptable, safe, and trustworthy products (*CST 2.4 Quality Reliability, Safety and Cyber-Security, Major Challenge 5: Human systems integration).*

The OWASP top 10 project[42] shows how, for years, the weaknesses present in the code are always of the same kind, except for small deviations in the ranking positions. **A large percentage of vulnerabilities are due to a lack of developer knowledge, awareness, or more generally, security culture**.
AIDOSec envisions a component that deals specifically with **bridging this gap**: using ML, through the analysis of the countermeasures identified in the modelling phase, the weaknesses identified in the code analysis phase, and the vulnerabilities actually found in the subsequent testing phases.

In particular, this component aims at proposing content to be submitted to developers. These contents may take various forms:

- Generated content to create customised training sessions and workshops for developers, focusing on secure coding practices, common vulnerabilities, and mitigation strategies. This will help them understand the importance of security and build a security mindset.
- AI-driven gamified learning platforms that adapt to each developer's skill level, providing tailored security challenges, capture the flag (CTF) competitions, or bug bounty programs. This encourages developers to learn about security and apply their knowledge in a fun and engaging way.
- Tools that analyse code and provide real-time, contextual feedback on the security of their work. This helps developers understand the security implications of their code and encourages them to fix issues promptly.
- Secure coding guidelines and best practices, developed exploiting AI and tailored to the organisation's specific needs. Encouraging developers to follow these guidelines, will hold them accountable for any security issues that arise due to non-compliance.

Moreover, this component aims at leveraging AI to conduct regular assessments evaluating developers' security awareness through quizzes, tests, or practical exercises. An objective is to analyse the results in order to identify areas where developers may need further training or support.

Implementing Segregation of Duties (SoD) in a SecDevOps methodology is essential to maintain security, reduce risks, and prevent insider threats. SoD ensures that no single individual has excessive control over critical processes, and that responsibilities are distributed across different team members. However, in order to prevent SoD from being an obstacle to what SecDevOps aims to achieve, i.e. to create a more efficient, agile, and secure development pipeline, some traditional SoD concepts may need to be adapted or reinterpreted within the context of a SecDevOps environment. Thus, AIDOSec will support SoD through:

- **Role-based access control:** Implementing role-based access control (RBAC) to enforce SoD within the SecDevOps environment. This will allow team members to collaborate effectively while still maintaining appropriate access restrictions based on their roles and responsibilities.
- **Automation:** Leveraging ML to enforce SoD policies and perform routine tasks, with code analysis, vulnerability scanning, and deployment. This reduces the risk of human error and ensures consistent adherence to SoD principles.
- **Continuous monitoring and auditing:** Implement continuous monitoring and auditing of SecDevOps processes to detect potential SoD violations and maintain compliance. This provides visibility into the activities of team members and helps identify any potential conflicts of interest or abuse of privileges.

This component will contribute to delivering the project's objective *O3 - AIDOSec continuous validation and improvement* as well as the objective *O6 - AIDOSec Market uptake* (see Table 1.1.2.a).

1.2.2.8 AI-based solutions, analysis and automation

AI-based solutions, analysis, and automation will support the AIDOSec process in several ways. In AIDOSec in general, we will employ AI-based solutions to enable automation, optimization, and bring intelligence in the development process of software-intensive industrial systems, and in particular, as part of their security engineering activities. In other words, the intention is not to necessarily make the end products more intelligent by adding AIDOSec AI components in them, but rather to use AI to improve their development process, and analyse and mitigate security threats and remove vulnerabilities as part of a continuous engineering process. In this regard, the intended users of AIDOSec solutions will mainly be developers, testers, security engineers and analysts, and product managers who are involved in the development and quality assurance of software-intensive products. Therefore, in terms of risks, any potential inaccuracies or robustness issues in the implementation of the AI-based

[42] OWASP top 10, standard awareness project for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. (https://owasp.org/www-project-top-ten/)

solutions of AIDOSec will not have impact (i.e., cause harm) on the end users of the products, and may only lead to suboptimal results in uncovering additional security threats or improving the security engineering process of systems as intended in AIDOSec.

Nevertheless, there are certain characteristics of AIDOSec solutions, and also various measures that we take into account in the project that will help to ensure and improve accuracy, robustness, reproducibility, and explainability of our AI-solutions in AIDOSec. Firstly, some of the AI algorithms that are planned to be used in AIDOSec as the baseline have been designed in previous projects such as AIDOaRt (ECSEL), InSecTT (KDT), MegaMart2 (ECSEL) and IVVES (ITEA3) - to name a few (see Section 1.2.5). Those AI solutions have already been extensively applied and evaluated in the context of several industrial use-cases in those projects, and are planned to be extended and further improved in AIDOSec particularly to target security aspects. Such previous evaluations and successful applications increase our trust in the behaviour, robustness, and accuracy of those solutions, and their feasibility to achieve the objectives of AIDOSec. There are also several specific techniques and established procedures that are considered for implementation of AIDOSec AI solutions to ensure and improve their quality characteristics. For instance, various accuracy metrics (e.g., F-score measurement), implementation of traceability mechanisms for our AI models, and also use of techniques such as Local Interpretable Model-agnostic Explanations (LIME) to improve decision understanding, transparency, and explainability are also considered. For robustness, analysis of data with respect to data drift, concept drift, bias, and noise, among other techniques, will be incorporated as part of AIDOSec AI pipelines to ensure stable performance.

Moreover, in AIDOSec we will publish and make available (many of) the datasets that are going to be used for training of our AI solutions along with the implementation of AI algorithms (either as open source or special licences, e.g., for researchers and evaluation authorities). This greatly helps other researchers and practitioners beyond the project consortium as well as external authorities to understand the decision making process of our AI algorithms in detail, and evaluate and assess their robustness and impact independently in their own contexts. In particular, a determinant factor in the performance and behaviour of AI algorithms is the datasets on which they are trained on and the quality of data.

In this regard, the concept of ‘garbage-in, garbage-out’ is well understood and acknowledged in the AI community, emphasising the fact that the decisions and conclusions made by AI algorithms are only as good as the quality of data fed into those algorithms. This is particularly evident and important in AI solutions that offer transfer learning and reuse of pre-trained models such as in reinforcement learning, NLP and language models, and deep neural networks. Therefore, in AIDOSec we are also considering various anonymization techniques to be able to make available, to the extent possible, different datasets of the use-cases on which AIDOSec AI algorithms are trained on and evaluated. We believe this can greatly help with the explainability and transparency of our AI solutions and their detailed decision making steps, as well as their reproducibility and further evaluations in other contexts, ultimately increasing the adoption and exploitation capacity of AIDOSec results and innovations beyond the project consortium.

Considering the above points and described context, in this section we highlight how AIDOSec envisions to apply various AI techniques to improve the security engineering process, and in which areas different AI-based techniques and algorithms are to be used in the project.

AI can significantly improve threat modelling and threat intelligence by leveraging machine learning, natural language processing, and other advanced techniques. For instance:

- **Automated data collection and analysis:** AI can gather and analyse vast amounts of data from various sources, including security logs, network traffic, code repositories, and open-source intelligence feeds. This enables a comprehensive and up-to-date understanding of the system's threat landscape.
- **Enhanced threat identification:** AI algorithms can identify potential threats, vulnerabilities, and attack patterns within the analysed data by learning from historical events and recognizing patterns. This leads to more accurate and timely threat identification.
- **Threat prioritisation:** AI can prioritise threats based on factors such as their potential impact, the likelihood of occurrence, or the system's susceptibility to the identified vulnerabilities. This allows organisations to allocate resources efficiently and focus on addressing the most critical threats.
- **Continuous threat modelling:** AI enables continuous monitoring and updating of the threat model, ensuring it remains current and relevant as new data becomes available. This helps organisations stay ahead of emerging threats and maintain a robust security posture.

- **Correlating threat intelligence:** AI can correlate threat intelligence data from various sources, connecting seemingly unrelated events, and providing a more comprehensive view of the threat landscape. This can help organisations better understand the relationships between different threats and develop more effective mitigation strategies.
- **Predictive threat modelling:** By analysing historical data and trends, AI can predict potential future threats and attack scenarios. This proactive approach enables organisations to take preventive measures and better prepare for potential security incidents.
- **Generating actionable insights:** AI can provide actionable recommendations for mitigating identified threats and vulnerabilities, tailored to the specific context of the system. This can include patch management, configuration changes, or other defensive measures.
- **Integration with security tools:** AI can be integrated with other security tools, such as vulnerability scanners, intrusion detection systems, and Security Information and Event Management (SIEM) systems, to provide a more holistic view of the security landscape and enable faster response to threats.

Other examples are:

- **Threat detection:** AI can be used to detect and identify potential security threats by analysing large amounts of data and identifying patterns that may indicate an attack or breach. AI-powered threat detection systems can help security teams respond to incidents quickly and proactively.
- **Malware analysis:** AI can analyse malware and detect new variations of existing malware, identifying patterns and behaviours that may be missed by traditional security solutions.
- **Automated response:** AI can be used to automate responses to security incidents, including isolating affected systems, blocking malicious traffic, and even patching vulnerabilities.
- **Fraud detection:** AI can be used to detect fraudulent activities and transactions, such as payment fraud, identity theft, and phishing attacks.
- **Predictive analytics:** AI can analyse data to predict potential security threats, enabling security teams to take proactive measures to prevent attacks before they occur.
- **Training activities:** AI can be exploited to develop guidelines to share with developers and conduct regular assessments.

In summary, within the project, AI will primarily enhance the AIDOSec solutions and framework according to the specific use case requirements and solution providers' interests. However, this augmented AIDOSec framework, and related toolkit, can then be also applied in the context of other use cases in different domains.

This component will crosswise contribute to delivering the technical objectives *O1-O2-O3* (see Table 1.1.2.a).

1.2.2.9 AIDOSec integration

In order to apply and evaluate in practice the AIDOSec overall solution and its components, an integration approach will be specified and developed. The proposed integration will notably be based on the use of modelling standards for sharing the various underlying models and data and for efficiently combining the different tools implementing the AIDOSec technical components (described in the previous sections).

The use of MDE artefacts and methodologies does not limit the integration patterns to be used. On the contrary, the use of model-based representations of the data provides a common understanding no matter how the data is exposed and consumed (data lakes, APIs, etc.). For instance, existing APIs can be refactored (e.g., extended, reduced, combined, or split) by discovering and linking the models behind each individual API.

In addition, our model-based approach for requirements engineering and solutions specification would allow us to identify potential vertical and horizontal integration links between use cases and technology solutions. These links would also help in identifying potential collaborations between case study providers and technology providers.

The integration approach, including methods and tools, will then be applied in practice in the context of the AIDOSec project use cases. Two main activities will be accomplished:

1. Providing the required underlying support and developing testbeds for validating the AIDOSec technologies. To this end, we will notably rely on both the existing infrastructures from the use case providers and the results of the different activities carried out in the project.
2. Performing the validation and evaluation of the AIDOSec technologies in the context of the proposed industrial use cases. To this end, we will rely on the previously mentioned validation infrastructure and testbeds and on the evaluation of the technical KPIs defined in Table 1.1.2.a.

As discussed above, the global integration approach will be defined during the early phases of the project to identify the associated constraints and requirements. To tame the risk of a complex technical integration (e.g., due to a high technological heterogeneity), the integration will explicitly take into account customizable engineering processes sharing common MDE principles and practices (based on common metamodels, transformations, etc.). For this purpose, technology transfer will be enabled through the tight collaboration between the academics, the technology providers, and the industrial partners composing the project consortium.

This component will enable the realisation of the project's objective *O4 - AIDOSec demonstrators validation* (see Table 1.1.2.a).

1.2.3 AIDOSec process

Figure 1.2.3 illustrates the process behind the AIDOSec approach and offers an overview of how components can interact with each other; the figure uses rectangles to represent input/output data or artefacts, and ovals to represent the cybersecurity activities. In particular, such activities are those related to the specific solutions (methods and tools) that will be developed within the AIDOSec project (i.e., solutions for threat modelling, security testing, detection & response, threat intelligence, and related actions/measures) . The elements in the process are grouped by the traditional DevOps phases in which the security activities are performed, in particular:

- **During design**: *Threat modelling* takes as input *Design time data* and gives as output *Threat and countermeasures*. These are used to define *Design and code improvement actions* and obtain *Improved design* and *Improved code.* Moreover, *Context data* (i.e., data concerning the system and involved relations) are given as initial input of the *Threat intelligence* activity, while its output is represented by *Contextualized threat data* (i.e., threats specific to the context). *Contextualised threat data* are being exploited by the *Threat modelling* activity.
- **During code, build, testing, and release**: The source *Code* is the input for the *Security testing* activity (including static and dynamic code analysis, for instance); the correspondent output is represented by *Weakness and remediations*, used to perform *code securitization* and obtain *Improved code.*
- **Deploy, operate, monitor phase**: *Run-time data* (i.e., security data observed at run-time) are used to *Detect Events and anomalies*, which are needed for the *Response* activity and generate *Response actions* to be applied to the running *System*. As a consequence, *Updated run-time data* will be available.

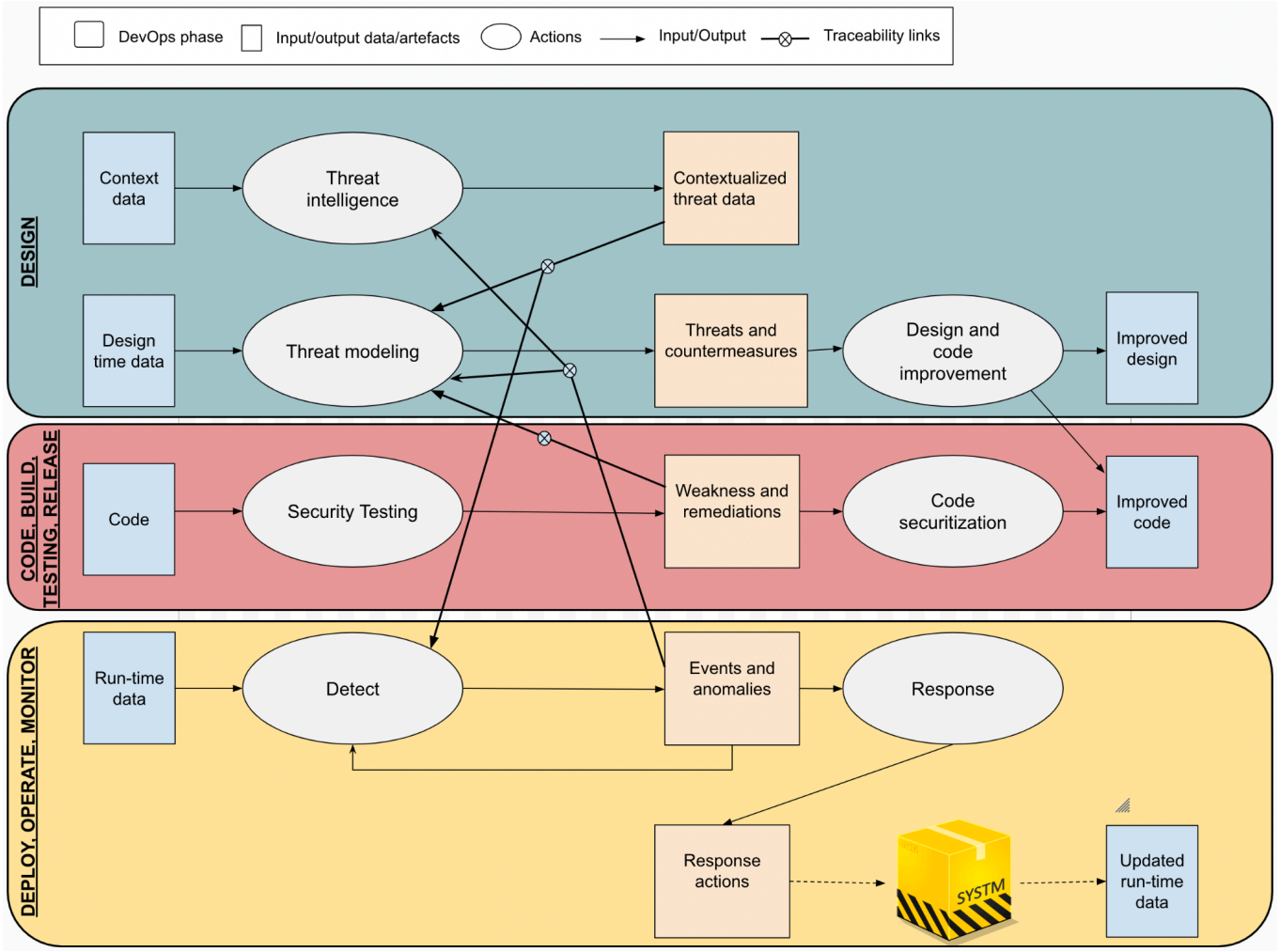


Figure 1.2.3 - *The AIDOSec process*

Key elements of the process are the *traceability links* that identify how the output of the activity can be used as input of other activities, enabling the communication among components and making possible the realisation of the feedback loop. Note that, these links were identified during the initial analysis of the process, but they will be extended during the project activities and made further extensible as well as reusable by the framework end-users.(notably, links between Threat modelling and Security testing)

To better explain the potential application of the process, let us consider a hypothetical example of a software designed to control CPS, such as a smart manufacturing system, to illustrate the AIDOSec workflow.

- **Threat modelling and intelligence:** The threat intelligence components gather data from various sources, such as open-source intelligence feeds, past security incidents, and other industry-specific data sources. The AI system then analyses this information to create a comprehensive threat model for the smart manufacturing system, identifying potential attack vectors, vulnerabilities, and risk factors. Some examples of threats identified might include unauthorised access, man-in-the-middle attacks, exposure of the device on the internet, a rogue master, data tampering and so on.
- **Countermeasures implementation:** Based on the output of the threat model, architects and developers receive a list of countermeasures to implement in the architecture or in their code. These countermeasures might involve secure communication protocols, an architectural change, stronger authentication and authorization mechanisms, or data integrity checks to mitigate the identified threats.
- **Security testing:** Once the developers have implemented the countermeasures, the software undergoes security testing. Automated static and dynamic analysis tools are used to scan the code and the running application, identifying any remaining vulnerabilities or potential security issues.
- **Deployment:** If the security tests are successful and no critical vulnerabilities are found, the software is automatically deployed to the production environment, in this case, the smart manufacturing system.

Otherwise, developers address the identified issues, and the software undergoes further testing before deployment.

- **Operations phase:** During the Ops phase, the AI system continuously monitors the software controlling the CPS for potential attacks and intrusions. Security tools, such as intrusion detection systems, log analyzers, and SIEM solutions, are used as possible sources of data to detect anomalies, minimise possible false positives, and respond to possible threats in real-time. The response will be contextualised to the environment, to avoid possible blocks that could be harmful for the business.
- **Continuous improvement:** Throughout the Ops phase, the AI system collects data on incidents, Indicators of Compromise (IoCs), and attacker behaviour. This information is fed back into the ML-driven threat modelling and intelligence components to continuously update and refine the threat model. As new threats or vulnerabilities are discovered, developers receive updated countermeasures to implement, and the process repeats.

In this particular example, the AIDOSec workflow helps the software for controlling the smart manufacturing system maintain a strong security posture throughout its lifecycle. It ensures that the software is developed and deployed securely, while continuously monitoring and adapting to new threats and vulnerabilities in the ever-evolving security landscape.

1.2.4 Industrial use cases

In this section, we introduce the industrial use cases on which the AIDOSec framework will be applied and validated. The proposed use cases are heterogeneous in terms of requirements and capabilities required, overall they will allow the project results to be fully validated. Table 1.2.4 reports the main information regarding the use cases: name, KAA and provider.

Table 1.2.4 - *The AIDOSec Use Cases and related Key Application Areas.*

Use Case number	Use Case	KAA	Use Case provider
1	Resilient New Concept Cars	Mobility (Automotive)	ABI
2	Dependable AI for Railway Traction Operation and E-Mobility Testing	Mobility (Railway)	AR
3	Secure Smart Sensors for Traffic Monitoring	Mobility (Traffic Monitoring)	CAMEA
4	AI/ML for optimization the CloudRAN products	Digital Society (Connectivity)	EAB
5	SecDevOps in Medical IoT Applications	Health & Wellbeing (Health monitoring)	HIB
6	Secure Smart Port Solutions by Design	Mobility (Maritime)	PRO
7	Wireless Communication Security	Digital Society (Connectivity)	TEK
8	Tooled-Up Distributed Real-Time Drone Application	Mobility (Aerospace)	THA
9	Collaborative Research and Development of Security-Critical AI-Based Solutions for ThingLink XR Trainings Platform	Digital Industry (Manufacturing)	TL
10	AI and Model-Based Approaches for Industrial Communication Products	Digital Industry (Industry Networks)	WMO
11	AI supported secure solution development life-cycle for critical infrastructure	Mobility (Traffic Monitoring)	KAPSCH
12	Railway operation in the cloud	Mobility (Railway)	GTS

13	Harmonized EU-CyberBridge: Aligning EU Cybersecurity Standards and Regulations for Enhanced Cybersecurity Protection	Mobility (Automotive)	MSG

In the following Sections, a description of each Use Case, with the technological and business goals and motivating scenarios are provided.

Use Case 1. Resilient New Concept Cars [ABI]
The Resilient New Concept Cars Case Study involves a virtual rear-view mirror scenario in which four cooperative cameras are used to capture the context outside the vehicle. Self-adaptation and AI at the edge are necessary to enable self-awareness of the system, as well as robustness and security with respect to cyber threats. Being aware means understanding the specific cyber threats to the automotive ecosystems and the potential impact of cyber threats on vehicles. A new concept in the car means new cyber threats and impacts that need to be fully understood. The starting point for this case study is an already existing Virtual Rear Mirror PoC implementing object detection and depth estimation algorithms. Abinsula is going to investigate and understand which could be the new frontiers of the cyber attacks (e.g. drawing on road signs could lead the AI-powered cameras to misinterpret its meaning), and to carry out rigorous investigation of new methods that could loosen the current technological limitations and enable the possibility of freely playing with all the available technology in the development of new concept cars. The goal is to address cybersecurity since the concept phase, as suggested by ISO 21434, and to define new procedures and study the new possible attacks and solutions.
Goals
Business: Abinsula will exploit AIDOSec Cybersecurity Solutions (e.g., threat modelling) to consolidate and enrich its software offering with solutions for safety and (cyber) security-relevant systems in the automotive context, with new methods and technologies, and with semi-products to be customised according to customers' needs.
Technological: The main technological goal is to: 1) investigate and understand the new frontiers of cyber attacks, due to the replacement of mirrors with AI-powered cameras that can create new safety- and (cyber)security-critical scenarios; 2) demonstrate how AIDOSec technologies can address the new scenarios since the beginning of the system development.
Motivating Scenario
Modern cars can be considered CPSs. They embed a large number of sensors and actuators and are equipped with advanced computational capabilities. These vehicles are connected systems that exchange data about the local environment, traffic situation, emergency alerts, and weather conditions. This enables cars to continuously generate and process a large variety of data to analyse their geographical position, condition of the traffic, state of the vehicle, passenger comfort, and safety. Therefore, more and more features require edge computing near the sensors, especially when offering driving assistance, and an intelligent edge is taking place. However, regulations limit the usage of AI or virtual mirrors. AI is a recognised innovative technology, but it is still far from being applied in real safety-critical applications, as cameras are far from completely replacing mirrors. This is something allowed only in concept cars and small productions that do not apply the same regulations applicable in large productions. In particular, it is necessary to consider that, when AI is involved, it might be necessary to update the networks over the air. This might even include a substantial change in the network's weights. The attack surface might increase and new challenging attacks strictly related to the usage of AI can appear. In this Case Study we will adhere to the recent ISO 21434[43], which helps the automotive industry to focus on practice to address cybersecurity in a systematic and consistent way.

Use Case 2. Dependable AI for Railway Traction Operation and E-Mobility Testing [AR]
AI-based solutions have the potential to improve operational efficiency in railway traction operation. However, the rigorous safety, security, reliability and availability standards in the market need to be met. Thus, one facet of the Alstom use case aims to ensure the dependability of AI when implemented in safety-critical railway real-time traction control systems. Aspects of Cybersecurity, Safety, and Reliability need to be addressed, not least from the perspective of verification in a manner that will be accepted by customers.
A similar challenge occurs in open test environments such as Alstom’s electric powertrain test lab, which is being made accessible to external clients and partners within e-mobility. To accomplish this, a shared data infrastructure

[43] Road vehicles - Cybersecurity engineering, ISO/SAE 21434:2021, 2021. https://www.iso.org/standard/70918.html

is required. Therefore, Alstom intends to develop and provide AI solutions for data analysis and verification support. In this context, cybersecurity is vital to ensure trustworthiness.

Goals

Business: Alstom envisions that dependable AI in railway traction systems will result in improved operational efficiency, not least concerning energy efficiency. Similarly, dependable AI in open testing environments will result in increased lab test capacity for a greater number of clients.

Technological: To achieve the business goals, dependable AI solutions that address railway traction relevant requirements for Cybersecurity, Safety, Reliability, and Availability need to be developed alongside AI solutions that ensure trustworthiness in shared testing environments.

Motivating Scenario

Sustainability is a key transportation factor, as Europe seeks to realise its net-zero goals. Rail generates approximately 4 to 6 times less CO2 emissions than travel by car (with an internal combustion engine), depending on the length of the journey. Even compared to electric vehicles, rail has a lower carbon footprint per passenger kilometre, at 6 to 41 grams, compared to 46 to 77 grams for electric vehicles. Compared to air travel, rail is also the greener option, generating about 10 to 15 times less CO2 emissions per passenger. Increasing urbanisation and population growth lead to more congestion in cities; rail can help relieve road traffic congestion and reduce air pollution. Urbanisation has been steadily increasing in Europe, from approximately 64 percent to 75 percent over the past 50 years. Even though the EU's population is expected to peak by 2025, several countries, including Sweden, Switzerland, France, Spain, and the Netherlands, are showing positive population growth. As a result of these macrotrends, rail is seen as one of the safest, most innovative, and sustainable modes of transport. By increasing the operational efficiency of rail traction through the implementation of AI-augmented real-time control, the necessary modal shift to rail can be boosted. At the same time, the capabilities within electric railway traction can be shared with other e-mobility actors to help accelerate the overall transformation of mobility.

Use Case 3. Secure Smart Sensors [CAMEA]

CAMEA develops, manufactures and services traffic monitoring systems from the Unicam family. These can serve as section speed enforcement, red-light enforcement, or weigh-in-motion systems. They are mostly camera-based and also radar-based, with optional addition of other sensors. As these sensors can operate as standalone and they can capture evidence (e.g., licence plates or measured speed of vehicles), the information transferred to the server needs to be credible. This use case focuses on the security of the sensor itself. As well, we are interested in non-repudiability of transferred data. For any evidence, we need to prove that it has been captured at a certain place and at a certain time and that it was not altered by any means. This is very critical for our applications.

Goals

Business: To develop and bring to the market secure smart sensors (definitely a big competitive advantage). Also, to satisfy increasing demand from municipalities for various traffic monitoring systems based on cameras and radars. Sales increase based on having good products for traffic monitoring tasks.

Technological: Reduction of power consumption on the site using smart standalone smart sensors (allowing battery or solar power operation of the sensors). Implementation of advanced features for sensor security and data non-repudiability (increasing credibility).

Motivating Scenario

In CAMEA, we develop and install many smart traffic cameras and radars for traffic monitoring systems. These sensors have a certain level of intelligence allowing data preprocessing. It could be licence plate detection in the case of an intelligent camera or speed measurements of individual tracked vehicles in the case of smart radar. These sensors then report information to the server or superior computer nearby. As has been stated, non-repudiability of evidence is critical for credible systems that can be used for traffic enforcement (e.g., at the court). Therefore, the security of the sensor and also a mechanism for the detection of any changes in source data needs to be present.

Use Case 4. AI/ML for Optimization the CloudRAN products [EAB]

On the Intent-based Management, the work is progressing on the programmatic approach for the Radio Access Networks software deployment engine, using a greedy resource allocation algorithm to place cells, sector carriers and the hosting Distributed Unit, Centralised Unit and Centralised Unit Control Plane (CU-UP) software on the available cloud infrastructure sites. In parallel, the cooperation with Ericsson Research to realise a Reinforcement Learning-based method for the same deployment engine is continuing, with the goal to compare this with the programmatic method as the next step.

Goals

Technological: The case study applies the AIDOSec methodology on 5G/6G Cloud RAN to address the expanding threat surfaces in the cloud-native stack and the complexity/dynamics of distributing the CloudRAN system over the cloud/edge with consideration of the Research and Development (R&D) efficiency and operational efficiency in the DevOps loop. Furthermore, the case study focuses specifically on ML-based analysis at run-time to detect anomalies of the system behaviour. This can be applied both in the development of the system in combination with symbiotic verification, and in the operations of the system. The designed case study in this proposal will focus more on the development. However, the Operations and Processes can also be covered via analysing data from live networks and also dynamically gathering feedback from the end-users e.g. operators.

Business: The CloudRAN solution has some built-in security however we need to ensure it maintains security and improves it with regard to well-known requirements for Telecom security. Also employing AIDOSec methodology can help Ericsson to increase the quality of the CloudRAN applications via reducing the time to release the products to the market.

Motivating Scenario

The advances in virtualization and automation technology have enabled cloud-based deployments of mobile cores, while also creating opportunities for cloud-based deployments of open Radio Access Networks (RAN). CloudRAN (Cloud Radio Access Networks) is part of this major technological shift in the industry. This cloud-based deployment option is an important step towards more open Radio Access Networks architectures. The primary security objectives in any Radio Access Networks implementation are to protect data and to ensure performance and availability. Cloud-based deployments can provide inherent security advantages such as isolation and geographical redundancy. However, the cloud also introduces new security risks that must be considered for open Radio Access Networks, the industry's generic term for open radio access network architectures. The threat surface in Cloud deployments is expanded compared to traditional solutions due to: (i) decoupling of software from hardware, (ii) separation of software layers, (iii) multiple organisations potentially sharing the same hardware, (iv) 3rd party organisations managing the cloud infrastructure, and (v) use of open-source software components. At the same time, the dynamics and complexity of the system increase resulting in a higher threshold to understand what is happening in the system, while there are challenges to have the full perspective of the system. Internal and external threat actors share the same attack vectors to exploit vulnerabilities in the cloud. Figure 1.2.5 shows threat surfaces of the cloud-native stack and it shows the attack vectors internal to the cloud, from devices inside the network and the public internet.

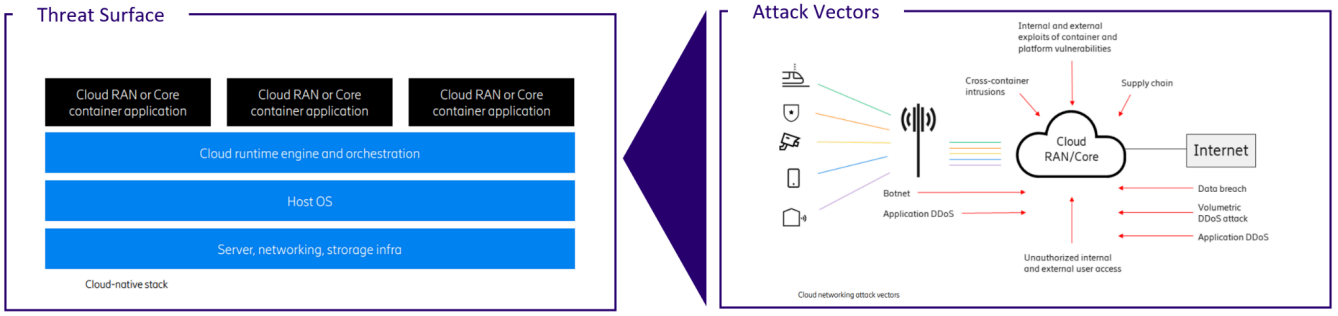


Figure 1.2.4.a. - *Security Considerations of Cloud Radio Access Networks*[44]

These challenges demand a new approach beyond traditional formal verification. In order to analyse the feasibility and generalizability of the AIDOSec methodology, a case study in a Telecom domain with a CloudRAN application needs to be examined.

Use Case 5. SecDevOps in Medical IoT Applications [HIB]

HI Iberia has a commercial product (REVITA[45]) that is used for remote monitoring of home-hospitalised patients by hospitals in Spain. The patient receives a kit of sensors and a gateway/interactive device to gather data for the hospital and perform Edge AI locally. The hospital receives the data, and the medical staff can use it for monitoring/diagnosis, etc. The sensor kit has many options (e.g., different sensors such as heart rate monitors, smart

[44] https://www.ericsson.com/4a67b7/assets/local/reports-papers/further-insights/doc/02092021-12911-security-considerations-for-cloud-ran.pdf
[45] https://revita.hi-iberia.es/

scales or breath analyzers for different patients and monitoring different conditions). The current REVITA system is in commercial use in several major hospitals in Spain. There is some built-in security but it requires improvements and the adherence to an established software development paradigm. The system is certified by the health system and the maximum care is taken by developers to ensure that all of the relevant security standards and procedures are followed. However, this for now requires the dedicated participation of specialist developers who apply their knowledge using mostly manual means (e.g., connection to several Health Information Systems such as eHospital or Caresoft HIS). This makes the production of new versions of the system very effort-intensive from the security point of view with new difficulties for each one of the new customizations. With the innovation in AIDOSec we aim to increase the security while simultaneously making the development system more streamlined and traceable by means of using a unified security workflow that is able to encompass health but also general software engineering standards such as OWASP IoT[46] and its associated verification system ISVS[47] as well as ISO/IEC 27400:2022[48] and the ENISA Guidelines for IoT applications[49], which strongly influence products in IoT domains dealing with data as sensitive as REVITA.

Goals

The overall goal for integrating SecDevOps in REVITA is to build security into the software development process, reducing the risk of security vulnerabilities. Introducing SecDevOps in a complex, customizable IoT product such as REVITA involves incorporating security best practices and principles into the development and deployment of the solution, such as the definition of security requirements, conducting threat modelling and using secure development practices.

The use case would consist of the different stages of the process of transition from an informal DevOps model to an integrated SecDevOps with emphasis on better testing of the hardware/software assets.

Technological: the technology goal is to offer a more secure application, with traceability that can prove that security requirements are followed during all stages of software production so that in a CI/CD production workflow can be certified at all stages to conform to security standards and maintain fit within the GDPR.

Business: from a business perspective, it is important to maintain the overall development and operation costs under check and not tie ourselves to a very expensive security framework. It is important that the achieved workflow is achievable with open source or own products and solutions and not rely on solutions from external parties.

Motivating Scenario

Security is a critical concern in telemonitoring health solutions, as they deal with sensitive patient data and are often subject to regulatory requirements. There are different common security problems in telemonitoring solutions like data breaches (telemonitoring health solutions deal with sensitive patient data, such as medical records and personal information, which makes them an attractive target for cybercriminals), unauthorised access, lack of device security, compliance issues, etc. Different security measures could improve the current REVITA solution like: data encryption, multi-factor authentication, auditing and logging, continuous monitoring and threat detection. The final objective is to ensure the confidentiality, integrity and availability of patient data and that it maintains security and to improve it with regard to well-known requirements for IoT security. Since REVITA is a health application that deals with the most critical of personal data and also with elements such as personal actions and activities, we will also endeavour to ensure that any AI techniques applied during AIDOSec are not only scientifically useful but also according to the highest standards of engineering factors such as robustness and reliability as well as AI specific metrics such as reproducibility and explainability. This will allow us to validate user acceptability and increase trust in the proposed solutions.

Use Case 6. Secure Smart Port Solutions by Design [PRO]

Prodevelop is a medium-sized company that develops a wide range of solutions mainly for the port environment. These solutions range from the development of management applications to the development of big data solutions where the processing of large amounts of information in real time is the key. Additionally, ports are customers that require highly customised solutions, implemented with the technologies that each port uses and with many integrations. In other words, customised projects require highly qualified personnel capable of handling a wide range of solutions.

[46] OWASP IoT security Top10 https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
[47] OWASP ISVS IoT security verification standard. https://owasp.org/www-project-internet-of-things/
[48] ISO/IEC 27400 IoT security standard https://www.iso.org/standard/44373.html
[49] ENISA Guidelines for IoT https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/@@download/fullReport

In relation to the quality and security of port applications, ports are strategic infrastructures for a country and require companies and solutions to have certificates that ensure their security. Proof of this has been that in the recent COVID crisis, ports have continued to operate to guarantee the supply of food and goods to the population. Thanks to the project , it is expected to improve the security and resilience of applications to increase their 24/7 availability and avoid security problems.

Goals

Business: The business objectives are to provide quality and secure solutions that meet the customer's security requirements and to have high credibility in providing secure and robust solutions. The productivity of developing such solutions can be increased by incorporating tools and methodologies to help ensure quality. This is currently a manual task.

Technological: On a technological level, it is vital that Prodevelop's solutions are secure in the different environments in which they are to be deployed, and it is also important to incorporate innovative tools that help ensure quality throughout the life cycle

Motivating Scenario

The development of port solutions without security vulnerabilities is difficult to achieve for the following reasons:

- They are complex solutions that require many customisations and adaptations specific to each client, as well as integrations with third parties
- They are heterogeneous solutions involving many technologies and deployments on different platforms.
- Different security measures and regulations for customers in different locations.
- Lack of qualified security personnel able to support the large heterogeneity of projects that arise.

These problems could be solved by applying innovative methodologies and solutions following the SecDevOps philosophy that allows security to be considered from the design phase through to the operations phase. Including automatic security validations of the libraries used and solution code and integrations in the design phase, construction of secure containers in the build phase and use of Infrastructure as Code (IaC) techniques to ensure the infrastructure is secure in different types of deployments and use of monitoring tools in the operations phase of the solution

Use Case 7. Wireless Communication Security. [TEK]

Wireless communications have a central role in most fields of modern human activities. Although at different levels of criticality, all applications require reliable and secure connectivity to provide their services with the expected performance and safety. TEKNE (https://en.tekne.it/) offers systems for telecommunication, for situation awareness, and for critical infrastructure protection. Moreover, TEKNE offers solutions that strengthen the security of these systems, through detection, classification, and identification of attacks that target the lower OSI layers—physical and datalink. The case study revolves around the improvement of these wireless security solutions and of their development cycle. The case study moves from two aspects. On one side, there is a complex and dynamic environment, in terms of heterogeneity, density, and mobility of communication nodes as well as sources of possible attacks. On the other side, to deal with these complexities, there is the employment of AI/ML technologies, which, however, can require a continuous adaptation to the environment dynamicity.

Goals

The case study addresses the following goals, through the development of an AI-based detector/classifier of attacks on wireless communications.

Business: TEKNE wants to consolidate and enlarge its offer of systems for situation awareness and critical infrastructure protection.

Technological: system adaptability, that is the "degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments" with focus on the adaptability of the AI models. Of course, the case study also wants to demonstrate an improvement in the detector/classifier performances.

Productivity: to use DevOps and to implement an effective development pipeline specific for AI/ML.

Motivating Scenario

The performance of AI models can degrade due to the dynamicity of the environment. In the specific case of the case study demonstrator, that is a detector/classifier of attacks to physical/datalink OSI layers, examples can be communication and sensing systems, with different compositions, used for a limited time span in great events scenarios with different installations, propagation characteristics, and crowd movements. Models must be updated frequently, rapidly and, in some cases, heavily if compared to the possibility of new data collections. In the pure AI field, the problem can be reconducted to the *Model Drift* phenomenon and the methods to detect and solve it, as

well as to *Transfer Learning* techniques that use fresh but limited target data to re-tune an AI model that was trained with large training datasets. In the software engineering field, the problem can be reconducted to the continuous development and the solutions that DevOps offers. Two of them are emphasised here: *Monitoring and Feedback*, to ensure that models are performing as expected and, in case di degradation, to trigger the execution of the pipeline that starts identifying areas for improvement; *Collaboration and Communication*, because, for AI system, the data scientists group adds to the developers and the operations teams. Consideration of the privacy issues completes the case study, regarding data that are collected to feed data-driven Machine Learning algorithms both at training and operating time.

Use Case 8. Real-Time Communication Network in a Civil Drone for Electric Lines Inspection [THA]

The use-case consists of a real-time communication network in a civil drone for the inspection of electric lines. Such an inspection drone embeds avionics applications, cameras, sensors and actuators. All these components need to interact with each other and with the ground control station in real-time. The communication requirements in terms of criticality between the different components vary from best effort to highly critical. Such variability is handled in commercial aircrafts by deploying several communication networks, each responding to specific communication needs. However, due to SWAP constraints (Size, Weight and Power) this is not applicable in modern drones. Rather, for such drones we need networks able to support mixed critical real-time communication.

The IEEE standard Time Sensitive Networking (TSN) is a promising network technology that provides safety guarantees for mixed critical real-time communication. In order to use TSN in the electric lines inspection drones, we need to develop appropriate security solutions to ensure secure TSN communication. The use case will demonstrate the applicability of the model-based approach to TSN. From a system architecture, we will generate both the components interface code, and the TSN network configuration. We will apply the solution to a drone application that will include the functional components of the drone and the base station as well as the simulation of the drone physical environment. The drone communication will be achieved using the Time-Aware Scheduler standard (TAS a.k.a. 802.1Qbv) of TSN. We propose to put in place gPTP (gPTP a.k.a. 802.1AS) and TAS on the physical platform, which is based on Linux and TSN-compatible hardware (mainly from NXP).

Goals

Business: One of the main objectives in avionics (civil drones and commercial aircrafts) is to reduce the SWAP costs (Size, Weight And Power). Today, communication between avionics systems in commercial aircrafts is performed by several networks, each one responding to the specific communication needs of the connected systems in terms of timing criticality. As a consequence, hundreds of kilometres of cables are needed (up to 500 km in an A380 aircraft). The weight and volume of cables can be drastically reduced if the various networks can be merged in one single network enabling mixed-critical communication. This will also allow reducing the maintenance costs of the networks. TSN (Time Sensitive Networking) seems to be the appropriate candidate to replace existing networks in aircrafts. Achieving the objective of reducing the SWAP and the maintenance costs will increase the competitiveness of THALES avionics products. Similar benefits are applicable to other Thales products such as satellites and radars.

Technological: The main technological goal is to demonstrate the capabilities of a TSN network to provide secure and dependable real-time communication for civil drones and commercial aircrafts. In particular, we will address the real-time performance of a mixed-critical network with critical and non-critical traffic and verify the capability to monitor in real-time the traffic to detect security attacks.

Motivating scenario

For civil drones and in avionics systems in general, the communication traffic becomes the more sensitive infrastructure in terms of security and dependability due to its interactions with external infrastructures and equipment. Therefore, we need to use an innovative solution to solve the security issues but also to handle the growing of the communication volume while saving volume and weight of cables and energy consumption. TSN (Time Sensitive Networking) seems to be the appropriate technology to meet these requirements.

Figure 1.2.4.b - ***A figure representing a civil drone exploited to inspect electric lines.***

Use Case 9. Collaborative Research and Development of Security-Critical AI-Based Solutions for ThinkLink XR Trainings Platform [TL]

The global manufacturing industry increasingly demands security-critical and efficient monitoring/maintenance solutions for automated systems. Our approach involves utilising novel security-critical AI-Based, MDE-Based, EDGE-Intelligence-Based, and VR/AR/MR/XR-Based technologies to design and develop Digital Solutions of various products. Rapid changes in security architectures, technologies, and components require sophisticated modern security-critical methods to keep Digital Solutions continuously running and evolving securely. We will provide an AI-based framework to facilitate the design and development of Digital Solutions for complex security-critical industrial systems in the global manufacturing domain.

Goals

Business: to increase productivity, reduce development costs, and improve security and software quality through security-critical AI-based MDE practices; to provide staff and stakeholders with scalable, secure, efficient, intuitive, and faster training/education related to end-products/machines/factories; to reduce training time and ensure faster and more secure onboarding of new employees, leading to reduced downtime, improved productivity, and enhanced security; to achieve ambitious project goals and improve the competitiveness of the global industry in the security-critical manufacturing industry domain; to simplify the development of security-critical AI-based systems in multiple domains, enabling scalable, secure, and efficient training for staff and stakeholders.

Technological: to develop security-critical AI-based Digital Solutions to optimise manufacturing processes by monitoring and simulating production conditions, identifying unexpected events, and mitigating security issues; to research and develop security-critical AI-based V&V services, fault localization, monitoring, and prediction of quality patterns; to demonstrate and evaluate the global use case with a focus on cybersecurity, traceability, federation, and continuous AI-based V&V services through integrated feedback loops.

Motivating Scenario

The global manufacturing industry increasingly demands security-critical and efficient monitoring/maintenance solutions for automated systems. Our approach involves utilising novel security-critical AI-Based, MDE-Based, EDGE-Intelligence-Based, and VR/AR/MR/XR-Based technologies to design and develop Digital Solutions of various products. Rapid changes in security architectures, technologies, and components require sophisticated modern security-critical methods to keep developed Digital Solutions continuously running and evolving securely. We will provide an AI-based framework to facilitate the design and development of Digital Solutions for complex security-critical industrial systems in the global manufacturing domain.

Use Case 10. AI and Model-Based Approaches for Industrial Communication Product[WMO]

Westermo (WMO) is a manufacturer of robust industrial communication equipment, e.g. routers and switches. WMO targets applications such as on-board rail, track-side rail, power distribution or industry automation on an international market.

Requirements in natural language play an important role in the negotiation with customers and in internal communication. Supporting the requirements process with AI techniques has a great potential and, in this project, we aim at incorporating such technologies for improving the quality of the requirements, for identifying ambiguous or duplicated requirements.

When designing new products, many aspects of a product need to be managed, often by teams of diverse colleagues

with niche competences, e.g. a decision on processor could impact software architecture as well as power consumption, heat dissipation and therefore also chassis geometry. By incorporating a model-based systems engineering approach we will strive to support cross-domain communication in early validation, as well as using models to enable simulations for supporting design validation. We would also like to experiment with the use of generative AI for going from one level of abstraction to the next.
In the DevOps process at WMO, a continuous and iterative process leads to the compilation of a large code base into an operating system running on an embedded device. In the previous AIDOaRt project, WMO improved the DevOps process and focused on AI for monitoring and cyber-security by improving security-related observability. E.g., one of two open data sets that WMO released in AIDOaRt is related to advancing this field. In this project, we aim to continue to improve AI for monitoring by continuing to improve how data is exported from deployed devices, both in terms of the amount of information as well as the format of it. In particular, we will export security-related data such as active processes and services, and we will publish at least one open data set to support research on this topic.
Goals
Business: WMO aims to accelerate and enhance the product lifecycle. First, increased pace and confidence in the development process through improved requirements engineering. Second, model-based approaches enables cross-disciplinary validation as well as simulation of relevant scenarios in early stages of product design. Third, enhancements in the system-testing and operations phases through improved monitoring and cyber-security confidence.
Technological: WMO aims to support innovation in and evaluation of AI algorithms for requirements management, monitoring and cyber-security, by working closely with academic partners and by sharing data. WMO also aims at introducing some model-based approaches in some processes or products. By improving the data export of our products, we aim to make cyber-security improvements with AI-powered monitoring. By striving towards these goals, WMO will reduce technical uncertainty, while improving robustness of the products as well as time-to-market.
Motivating Scenario
WMO products are aimed for complex environments with diverse needs of network topologies, redundancy protocols, performance, as well as strict hardware requirements in terms of acceptable temperature ranges, vibration, dust, or inconsistent power supply. Over time, customers in these domains require stricter and stricter robustness in both support for communication protocols, while also requiring stricter and stricter compliance with new sustainability or cyber-security directives as well as domain-specific standards. In order to remain competitive in this moving market, the processes for designing new hardware product platforms cannot be too long, and the software processes cannot allow for security-related issues to slip through safety nets. For this reason, WMO aims at enhancing the requirements processes with AI, to fortify the early product design phases with model-based approaches, and to explore AI-powered monitoring when products are up and running.

Use Case 11 – AI supported secure solution development life-cycle for critical infrastructure [KAPSCH]
Kapsch TrafficCom AG is a globally renowned provider of transportation solutions for sustainable mobility with successful projects in more than 50 countries. Serving both government (B2G) and business (B2B) sectors, our solutions are implemented in over 130 projects across the EU alone and play a considerable role in developing and maintaining the critical infrastructure of Europe. The Kapsch TrafficCom portfolio consists of solution design, hardware, software, services and integration that enable innovative solutions in the area of tolling, traffic management, smart urban mobility, and connected vehicles. We focus on leveraging technology ranging from well-established to cutting-edge such as DSRC, RFID, GNSS, video and V2X (ITS-G5 and LTE-V2X) to establish services that include centralized systems housed in secure environments as well as remote systems positioned on the roadside, which use public networks. In addition to their critical mission, these systems manage and exchange sensitive personally identifiable information (PII) including license plate numbers, driver identities, positional data etc. Given the integration of numerous in-house and third-party components such as cameras, sensors, and software, the potential for vulnerabilities is high and attack surfaces are significant. Besides an effective information security management system on corporate level (reflected in our ISO 27001 certification) and project specific security services to safeguard customer specific security needs this highlights the need for a comprehensive and robust secure development life-cycle. The Kapsch current secure development life-cycle is based on the industry best practice OWASP Software Assurance Maturity Model.
Goals

Business

- Integrate penetration testing early in the secure development life-cycle using the shift-left methodology to secure all layers of product development prior product release to reduce total solution life-cycle costing while increasing security.
- Enhance the overall framework, ensuring continuous improvement in security practices to enable the secure operation of critical infrastructure in an increasingly harsh environment.

Technological

- Assess and compare existing large language models (LLMs) for automated penetration testing to reduce the time required for additional manual security evaluations.
- Apply and integrate advanced AI driven penetration testing tools to the Kapsch development environment to identify as well as prevent potential vulnerabilities from the initial stages of product development.
- Develop strategies to address the cyber-attacks facilitated by AI technologies, ensuring our systems are resilient against both their completeness in attack scenarios as well as their increased volume.

Industry

- Suppliers of critical infrastructure in the transportation sector could benefit from our learnings regarding the cost effectiveness of AI-supported secure solution development lifecycle

Motivating Scenario

Consider a scenario where a tolling or traffic management system, equipped with various integrated components, faces a potential threat vector through an externally accessible roadside system. An attacker could exploit a vulnerability e.g. in a third-party camera firmware or an integrated software to access the network and extract sensitive PII data, leading to significant privacy breaches and / or operational disruption

To minimise such threats, our use case proposes the deployment of an AI-driven penetration testing tool tailored for certain hardware and software configurations. This tool will use advanced LLMs to conduct both semi-automated and fully automated tests at various stages of our product development and solution integration. By integrating these tests early in the development cycle (shift-left approach), potential vulnerabilities can be identified and managed, significantly reducing the risk of exploitation and total product / solution life-cycle costing. This approach not only addresses the immediate vulnerabilities but also prepares our systems to withstand attacks supported by AI technologies.

By comparing the effectiveness of various open-source LLMs designed for penetration testing, we can select the most efficient model that reduces testing time and enhances security measures.

Use Case 12. Railway operation in the cloud [GTS]

Railway operation is about to move to cloud environments to better fulfil the needs for increased scalability (dynamic deployment), higher availability and geographical redundancy, and improved maintainability and diagnosis.

GTS is currently developing an Integrated-Platform-Signaling (IPS) cloud platform environment for cloud operation of safety critical systems (new interlocking/OMC) with a specific focus on observability and maintainability.

This includes hosting the safety critical applications themselves using the well-established TAS Platform for SIL4 operation and beyond that support for operation and maintenance of the underlying infrastructure. The IPS cloud will support over 1000 safety critical instances and location independent operation (geo redundancy).

Goals

Business:

- Ensure compliance with current/future standards (EULYNX, IEC 62443, NIST, etc.)
- Reduce overall CO2 footprint of safety-critical interlocking systems by providing virtualized, cloud-centric solutions by maintaining observability using DevSecOps practices
- Decrease service disruptions, MTTR and needed manual service interventions by increasing continuous improvement loops and automation facilitating state-of-the-art AI and DevSecOps principles

Technological:

- Establish AI-enhanced observability capabilities, risk assessment incl. vuln management and service operations practices for IPS cloud on IT relevant and application specific data
- Evaluate application of ML approaches in air-gapped Cyber-physical-system environment as required by critical infrastructure operators
- Automated approach to comply security requirements defined in IEC 62443, EULYNX and CENELEC highly integrated in our current agile and DevOps development and operations end-to-end processes

Motivating Scenario
Today's safety critical railway operation is largely run on embedded HW. This local operation with low scalability requires dedicated housing air conditioning for small areas leading to comparatively high energy consumption and cost.
Cloud based railway operation helps alleviate the cost through central housing and reduced energy consumption due to massively improved scalability. However, this cloud based operation introduces new security and safety concerns which can be countered by new methods to detect and mitigate threats as well as a sound geo-redundancy solution. The IPS cloud environment will be developed to tackle these points focussing on the necessary observability and maintainability.

Use Case 13. Harmonized EU-CyberBridge: Aligning EU Cybersecurity Standards and Regulations for Enhanced Cybersecurity Protection [MSG]
Cybersecurity is essential in today's interconnected world, providing vital protection for economic and social activities. Despite the European Union's proactive efforts to bolster cybersecurity through comprehensive regulations, industries continue to face significant challenges in compliance, due to the rapid evolution and complexity of these regulations.

msg Plaut, with its strong foundation in automotive cybersecurity, safety, engineering, and homologation, addresses the regulatory challenges by proposing the Harmonized EU-CyberBridge Case Study. This initiative aims to analyze and align cybersecurity standards and regulations across various sectors, fostering a unified approach to compliance and security enhancement.

In particular, the case study will focus primarily on the automotive cybersecurity domain, including key standards such as UN R155 CSMS and ISO 21434. Additionally, it will tackle broader, cross-domain security concerns, as highlighted in the Cyber Resilience Act, a crucial component of the EU's Digital Decade Strategy.

Goals
Business: The Harmonized EU-CyberBridge case study initiative seeks to distil and integrate cybersecurity knowledge that is applicable across different domains. This integration will support the development of a robust, comprehensive cybersecurity framework. By leveraging our harmonized standards database, we aim to streamline the compliance processes and enhance the operational efficiency of client projects, thereby reducing cybersecurity risks and compliance costs.
Technological: Our primary technological objective is to develop a sophisticated database that systematically connects, analyzes, and identifies overlaps among various cybersecurity standards and regulations (e.g., UN R155 CSMS and ISO 21434). This analysis will enable us to determine key commonalities and differences, thereby assisting in the creation of unified compliance protocols that can be effectively applied across multiple sectors.
Motivating Scenario: An European corporation must comply with diverse cybersecurity regulations in multiple European markets. The current landscape requires separate compliance strategies for each regulation, significantly increasing complexity and cost. Through the EU-CyberBridge Use Case, msg Plaut will develop a database that not only maps these varied standards but also highlights commonalities and potential synergies. This resource will enable the corporation to adopt a streamlined, harmonized approach to cybersecurity compliance, reducing both the time and resources needed to meet diverse regulatory requirements.

1.2.5 Building on the results from previous and ongoing European and national research projects

In the following table we present a list of the main ongoing and past research collaborations that are related to AIDOSec. In particular, we distinguish projects providing the foundations in terms of research agenda and solutions, and projects that are relevant for AIDOSec with respect to specific sub-problems to be tackled.

Table 1.2.5 - *The AIDOSec consortium previous projects*

Project	Relevant Results	Usage and improvements in AIDOSec	Liaison partners
Foundations of AIDOSec			
AIDOaRt *ECSEL* 2021 - 2024 https://www.aidoart.eu/	Model-based framework to more efficiently support the continuous software and system engineering of CPSs and CPSoS via AI-augmentation. Reliable monitoring solution for critical infrastructures (e.g, ports) over computing continuum architecture. AI-assisted simulation, performance and anomalies analysis	AIDOSec is the follow-up of AIDOaRt. The AIDOaRt model-based framework will be the foundation of DevOps in the AIDOSec SecDevOps approach, and it is planned to be used as a basis for developing the AIDOSec dedicated framework, which will include a security layer to address cybersecurity issues in DevOps. Moreover, the AIDOaRt methods and tools will be enhanced to support the latest best practices in terms of AI/ML and DevOps.	ABI, ABO, ACORDE ,AIT, AR, BUT, CAMEA, DT, HIB, IMT,INT, JKU, MDU, PRO, RISE, SOFT, TEK, UNICAN, UNISS, UNIVAQ, UOC, WMO
MegaM@ Rt2 *ECSEL* 2017 - 2020 https://megamart2-ecsel.eu/	MegaM@art2 (MM2) provided a model-based framework for continuous development and runtime validation of complex systems. Overall, 28 model driven software tools have been developed, mostly open source. The tools can be divided into three categories: • Holistic system engineering, that integrate and verify existing industrial practices • Runtime monitoring, testing and validation. • Traceability and mega-modelling.	MM2, as the predecessor of AIDOaRt, also represents a foundational element of AIDOSec. AIDOSec inherits the model-based methodology on which the MM2 framework is based. Furthermore, the MM2 methods and tools covered three complementary dimensions of system engineering, i.e., design time engineering, runtime analysis, and traceability management (in particular between design time and runtime). Part of these methods and tools will be enhanced to consider security-related needs in DevOps.	ABO, AR, BUT, CAMEA, IMT, INT, MDU, RISE, SOFT, TEKNE, THA, UNICAN, UNIVAQ, UOC
Other projects relevant for AIDOSec			
VeriDevOps *H2020* 2020-2023 https://www.veridevops.eu/	Methodology and tools for automated analysis and verification of security requirements in DevOps context.	VeriDevOps methods and tools can contribute to the corresponding core areas of the AIDOSec project, including security requirements analysis with NLP, anomalies detection, vulnerability localisation, testing and DevSecOps.	ABO, MDU, SOFT,
Lowcomote *MSCA* *H2020*	Lowcode Engineering Platforms (LCEPs) are open, interoperable, scalable (supporting very large engineering models and social networks of	The low-code paradigm and low-code engineering platforms and latest related research results could be used to better support the specification of security	IMT, INT, JKU, LIE, UNIVAQ

2019 - 2023 https://www.lowcomote.eu/	developers) and smart (simplifying the development for citizen developers by ML and recommendation techniques). LCDPs rely on the framework defined by recent research in MDE, augmented with Cloud Computing and ML techniques.	properties, generate specific corresponding software components/code, etc.	
SCRATCH *ITEA3* 2020 - 2022 https://scratch-itea3.eu/	SCRATCh proposed a set of interoperable tools (toolkit) based on a common conceptual architecture and consisting of the following elements: ● Security foundation for strong device identity. ● DevOps IoT tools integrating processes and technologies that accelerate development and deployment of IoT solutions. ● A SecDevOps-inspired process consisting of procedures that actively promote continuous deployment of incremental system upgrades that facilitate security and reliability, based on real-world operational metrics.	Analysis of applicable security standards for IoT and DevOps is available as a project output directly on SCRATCh's website and the overall DevSecOps methodology (based on the Essence method) was also a public result put forward in deliverable D2.1[50]. In AIDOSec we will take these as a basis for the development of secure IoT components for the Health and Wellbeing use case and improve upon them with novel AI techniques (e.g., integrated AI-empowered requirements analysis and task generation for developers).	HIB
VALU3S *ECSEL* 2020 - 2023 https://valu3s.eu/	Research on how to use AI to improve model-based (design time and runtime) verification technology, especially for automated systems. Design, implement and evaluate SOTA V&V methods and tools in order to reduce the time and cost to verify and validate automated systems with respect to safety, cybersecurity and privacy requirements.	AIDOSec could use Methods and Tools developed in the VALU3S project for the evaluation of the cybersecurity.	AIT , AR, BUT, CAMEA, INT, LIE, RISE, UNIVAQ
AQUAS *ECSEL* 2017 - 2020 https://aquas-project.eu/	Efficient solutions for the entire product life-cycle considering inter-dependence of safety, security and performance of systems. In this project, the HEPSYCODE methodology (and related toolchain) was extended to support trade-off performance and safety.	In AIDOSec, HEPSYCODE will be further extended to manage security-related requirements.	AIT, BUT, INT, THA, UNIVAQ
SAFECOP *ECSEL* 2016 - 2019 http://www.safecop.eu/	ML-based approaches for SW testing and cooperative function verification.	Possible exploitation of the ML-based approaches for SW testing inside the AI for testing goals into AIDOSec.	INT, MDU, UNIVAQ
SECURED *HE* 2023 - 2025 https://secu	The goal of the SECURED project is to scale up multiparty computation, data anonymization and synthetic data generation, by increasing efficiency and	Possible exploitation of the AI techniques used for synthetic data generation and attack classification	THA, UNISS,

[50] https://scratch-itea3.eu/wp-content/uploads/2022/03/D2.1v5-IoT-Toolkit.pdf

red-project.eu/	improving security, with a focus on private and unbiased artificial intelligence and data analytics, health-related data and data hubs, and cross-border cooperation.		
PRESECREL *Spanish National fundings* 2022 - 2025 https://www.ai2.upv.es/proyecto/presecrelciberseguridad-para-el-vehiculo-autonomo/	PRESECREL contributes to industrial digitalisation by facilitating the development of predictable, reliable and secure industrial computing systems through the development and/or integration of models, middleware and specific platforms. The aim is to integrate these methodologies and techniques in an industrial environment guided by the technology of the IoT, cloud computing and Big Data analysis and processing in which modelling and cybersecurity drive the project forward.	The project may make it possible to model complex applications with different levels of criticality and security, to provide platforms for their execution and to integrate at a high level the capacity for the intelligent processing of high volumes of information in industrial environments.	UNICAN
NextPerception *ECSEL* 2020 - 2023 https://www.nextperception.eu/	Development of the next generation smart perception sensors and enhance the distributed intelligence paradigm to build versatile, secure, reliable, and proactive human monitoring solutions for the health, wellbeing, and automotive domains. ACORDE developed a novel, versatil edge-platform suited for the novel sensor data collection, and AI/ML supported fusion at the edge. It also provided implementation for anonymization algorithms.	In AIDOSec, security can be put at the forefront of the DevOps of the edge platform design. Moreover, edge platform design can be revisited with security in mind, e.g., Versatile security acceleration based on ISA versatile architecture, i.e. RISC-V based.	ACORDE BUT, CAMEA, HIB
C4D *ECSEL* 2019 - 2022 www.comp4drones.eu	COMP4DRONES (C4D) brings a holistically designed ecosystem from application to electronic components, realised as a tightly integrated multi-vendor and compositional UAV embedded architecture solution and a tool chain complementing the compositional architecture principles. In C4D ACORDE brought novel indoor/outdoor positioning solutions, with some incipient integration of security to react low-level attacks (jamming & spoofing) C4D developed a set of models and tools for mechatronic CPS system design.	In AIDOSec, design and implementation of positioning solutions would become holistic, in the sense that security can be considered along the whole design process (from models to implementation), at different implementation layers. AIDOSec could benefit from the mechatronic modelling and design methods developed in C4D when the Cyber-Physical interaction is relevant in the whole security of the system. Tools, solutions and methodologies inherited from C4D will be further extended to consider security-related needs.	ABI, ACORDE AIT, BUT, HIB, TEKNE, UNICAN, UNISS, UNIVAQ
FitOptiVis *ECSEL* 2018 - 2021 https://fitoptivis.eu/	FitOptiVis is an Ecsel JU project with the objective of developing a cross-domain approach covering a reference architecture, supported by low-power, high-performance smart devices, and by	Dynamic workload allocation may open security breaches in the system. Some of the techniques developed in FitOptiVis could be of interest in AIDOSec when dealing with systems with dynamic	ABI, BUT, CAMEA, HIB, UNICA,

	methods and tools for combined design-time and run-time multi-objective optimisation within system and environment constraints.	resource allocation. Tools, solutions and methodologies inherited from FitOptiVis (e.g., HEPSYCODE, knowledge related to reasoning techniques for verification) will be further extended to consider security-related needs.	UNICAN, UNISS, UNIVAQ
InSecTT *ECSEL* 2020 - 2023 https://www.insectt.eu/	InSecTT aims to develop solutions for intelligent, secure, trustable things for European industry throughout the whole Supply Chain. Artificial Intelligence of Things (AIoT) is the natural evolution for both AI and IoT: AI increases the value of the IoT through ML by transforming the data into useful information, while the IoT increases the value of AI through connectivity and data exchange.	InSecTT delivers results relevant for security, and Ops. E.g. how could an AI in a CPS- (IoT-) device monitor itself or its surroundings wrt. anomalies or security events.	JKU, MDU, RISE, WMO
PIACERE *H2020* 2020 - 2023 https://www.piacere-project.eu https://cordis.europa.eu/project/id/101000162/	PIACERE enables the automation of several DevSecOps tasks that otherwise would have to be performed manually by an operator. PIACERE consists of an integrated DevSecOps framework to model, verify, configure, provision, and monitor IT solutions based on IaC.	AIDOSec may face similar challenges than the PIACERE project when dealing with security during the Operations phase of the DevOps loop. Lessons learnt and tools developed in PIACERE may form a valuable source of information and inspiration for tools developed in the AIDOSec.	PRO
TRANSACT *ECSEL* 2021 - 2024 https://transact-ecsel.eu https://cordis.europa.eu/project/id/101007260	TRANSACT aims to develop a universal distributed solution architecture for the transformation of safety-critical CPS from local, stand-alone systems into safe and secure distributed solutions. To that end, TRANSACT will provide a reference architecture, together with a transition methodology, for safety-critical CPS that rely on edge and cloud computing, ensuring that performance, safety, security, and data privacy are guaranteed.	Lessons learnt from the application of the TRANSACT methodology, where safety, security, data privacy and performance are fundamental aspects considered in the transition, are of direct application in the AIDOSec project and the solutions developed in its context.	UOC
SACSys *KK-stiftelsen* 2019 - 2023 https://sacsys.github.io/main/	SACSys provides run-time guarantees of safety and cyber-security for time-critical collaborative adaptive systems by recognizing and defining continuous safety and security requirements, and designing behavioural models, running on cloud-based platforms, to analyse and check at run-time conformance of those requirements.	Since cybersecurity solutions for detection and response are one of the tasks that AIDOSec is considering, the proposed methods in SACSys will contribute to AIDOSec as well (analysis of design as well as runtime security threats).	MDU
Serendipity *SFSR*[51]	Serendipity develops technologies and a platform for safety critical connected	Since cybersecurity solutions for detection and response are one of the tasks that	MDU

2018 - 2023 https://www.es.mdu.se/projects/494-Serendipity	CPS that leverage existing techniques for dependable systems and augment them with scalable security solutions for open and heterogeneous systems.	AIDOSec is considering, the proposed methods in Serendipity will contribute to AIDOSec as well (analysis of design as well as runtime security threats).	
LoLiPoP IoT *KDT JU* 2023 - 2026 https://cordis.europa.eu/project/id/101112286	The project develops Long Life Power Platforms for Internet of Things, it focuses on low- and ultra-low-power computing components and energy harvesting.	The projects will run in parallel, COG, as the coordinator of LoLiPoP IoT, will take part in cross-project collaborations, especially on the low-power processing, to which AIDOSec will add the security and data communication efficiency levels.	BUT COG
Cyber Trainer *POR FESR Abruzzo*[52] *2014 - 2020.* 2018-2020 https://en.tekne.it/N34/cybertrainer-tekne-with-leonardo-in-cyber-security-field.html	Integrated platform (a *Cyber Range*) for training cybersecurity operators and for testing equipment and systems.	AI technology exploitation. DevOps for AI systems development.	TEK UNIVAQ
MYRTUS *Horizon Europe* 2024-2026 https://myrtus-project.eu/	MYRTUS primary goal is to provide efficient computing continuum management, leveraging advanced technologies such as federated learning and swarm intelligence techniques.	In AIDOsec we will reuse and extend the toolchain for dataflow-based AI coprocessor generation and the YOCTO-based node manager within the ABI lead UC.	ABI, SOFT, UNICA,
MATISSE HORIZON-KDT-JU-2023	This project aims to develop a model-based framework addressing the following challenges by i) To automize the creation of digital twins for the simulation, monitoring and testing of functional and non-functional properties ii) continuous validating digital twins to meet the required properties and iii) developing a multidomain and automated digital twin toolchain for the verification and validation of complex industrial	Collaboration on some technologies developed in the two projects, mutualization of some applications in the specific context of handling security aspects within Digital Twins	IMT, INNO RIV, MDU, SOFT UNITE

[51] Swedish Foundation for Strategic Research, it supports research in science, technology and medicine.
[52] European Regional Development Fund, Abruzzo region, Italy.

	systems based on digital twins.		

1.2.6 Interdisciplinarity

AIDOSec will provide a holistic framework relying on model-based methods and intelligent techniques that can support the entire cybersecurity process and its practices. Thus, it is at the crossroads of several disciplines, which require an interdisciplinary interplay of the involved expertise of the partners. Figure 1.6 illustrates the disciplines and sub disciplines involved in the project' activities. The project deals with modern and complex systems including electronic components and systems, information systems, embedded systems, and cyber-physical systems. Specifically, AIDOSec includes industrial Use Cases in the areas of mobility, digital society, health and wellness, and digital industry. The project involves important branches of computer science that are studied and applied for the purposes of developing the AIDOSec holistic model-based framework, that are Artificial Intelligence and Machine Learning, and Software Engineering practices including Model Driven Engineering and automation and traceability mechanisms. The project focuses on Security and Cybersecurity, in particular it aims at providing efficient solutions of Threat modelling and Threat intelligence, Security testing, Detection and Response. Such solutions will be employed for the continuous validation and improvement of the security posture of complex industrial systems, and for supporting DevOps with cybersecurity.

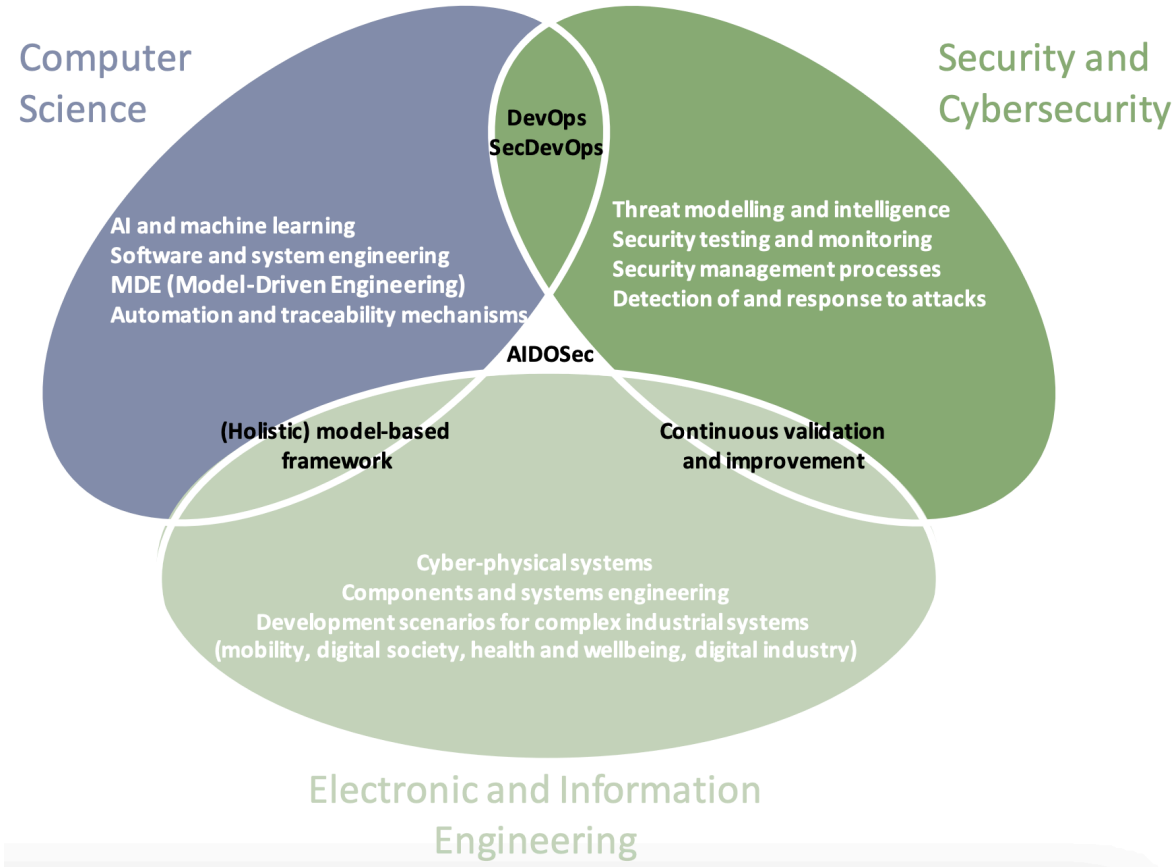


Figure 1.6: AIDOSec Interdisciplinary approach

1.2.7 The gender dimension

AIDOSec aims to apply a gender sensitive approach throughout all its activities from the conceptualisation to the reporting and delivery of the results, in which gender will not be an isolated category of identification, but intersected with the ones of ethnicity, class, age and citizenship. This approach will include: a) monitoring on the adoption of gender sensitive procedures at every stage of investigation and implementation; b) engaging in collecting qualitative information in stakeholders groups by aiming to assess the expectations and perceptions of

women and men; c) participation in social innovation and participatory processes will be analysed taking into account the different groups of women, including their socio economic circumstances such as pay, property, employment, work life balance and other important criteria such as family context and age (e.g., menopause) that may encourage or impede their participation; d) introduction, in the research, of explicit facilitation rules to avoid behaviour that may result in the detriment of the participation of women.

1.2.8 Open Science practices

Adapting the open science practices to the nature of the work to be carried out will increase the chances of achieving the desired objectives and provide opportunities for future collaborations. The consortium has carefully selected appropriate open science practices, which will be integrated into the project methodology. In particular, the consortium will seek to promote open cooperative work and systematic sharing of knowledge and tools both within itself and with the scientific and stakeholder communities, starting with appropriate planning and setting up of relevant processes already in the first project month. All researchers will have an ORCID-ID. The adopted open science practices will at a minimum include the following: Pre-registration of the research protocol(s) and (statistical) analysis plan(s) (e.g. OSF, Figshare). Use of the open repositories for early results (e.g., arxiv.org, SSRN, Figshare, Dataverse, Zenodo) and code that can be reused (e.g., Github). This will allow early, quick, rigorous and open sharing of the research results. In particular, the consortium commits to bringing scientific results closer to the public as means to adhere to the Open Access guidelines set by the Horizon Europe Programme. Therefore, all produced scientific publications and other research materials (e.g. datasets) will be available as Open Access through compliant repositories and the Open Research Europe publishing platform (i.e., OpenAIRE). The project's open access practices will impact accessibility on other scientific repositories such as DataCite, Datalib, Scopus and ORDA. Furthermore, the project will make available its findings through the European Open Science Cloud in order to support the openness, reusability, and discoverability of open science data. Finally, the EU data collection legislation will be employed along with the General Data Protection Regulation (GDPR) 2016/679 before making any data openly available. In addition, the new initiative Open Research Europe allows to immediately publish articles, following transparent, invited, and open peer-review with the inclusion of all supporting data and materials. Generally, open-access venues that are fully compliant with the EU open science practice policies will be preferred.

1.2.9 Data management

The project may exhibit potential data and/or ethics issues concerning the following categories:
1. Humans: Human participants will be involved in the project. User requirements will be defined based on human participants and the digital products of the project will be evaluated with the help of humans. All human participants will be *recruited on a voluntary basis.* There are no medical or biological studies implied, though some physiological and psychological measures will be taken (e.g., heart rate, oxygen level, EEG data, questionnaire on stress or anxiety) to study the impact of the pilots on physical and mental health. All participants are healthy people, with no medical issues. Human participation is only considered from the perspective of human sciences research. Informed consent documents will be signed by the participants, stating, among others, the background and purpose of the study, responsibilities, potential risks, procedures related to data storage, and that participants can withdraw from the study at any point during the pilot activities without any obligations whatsoever. Such standards will also be applied to the design and implementation of applications. Overall, the related aspects will follow the guidelines of the GDPR (EU) 2016/67. The experiments will be designed in accordance with the Declaration of Helsinki and submitted to the approval of the local, institutional ethics committees.
2. Personal data: Given the complexities of data protection legislation across Europe, all involved partners will agree upon a data protection policy aligned with relevant European, national and local policies. All the data will be anonymised. The raw data will be stored in a key file that only the researchers involved in the research can access.
3. Artificial Intelligence: To ensure the trustworthiness and transparency of the proposed ecosystem, all proposed AI-powered components will explicitly exhibit the following qualities and behaviour with respect to the EU Ethical AI requirements: (i) Human agency and oversight, (ii) Privacy and data governance, (iii) Transparency, (iv) Diversity, non-discrimination, and fairness, (v) Environmental and societal wellbeing, and (vi) Accountability. In any case, the proposal specifies dedicated tasks and deliverables for data and ethics management, and any relevant issue that may be raised will be resolved properly.
4. Findability: The consortium will publish data and codes, along with published articles, using well-known and certified data repositories, such as Zenodo. Dataset publications will have DOIs and keywords for future findability.

The research data will thus be searchable online (e.g., harvested by OpenAIRE). The data not associated with scientific publications will also be made publicly available, via an online database maintained by the coordinator.
5. Accessibility: All data with personal identifiers will be stored within the most secured data drives with very limited access rights, and all accesses will be logged and can be later identified. AIDOSec will also publicly share datasets not underlying the published articles, making them openly and freely available.
6. Interoperability: Each type of dataset will be stored and accompanied with a README file describing the datasets. The README files along with supplementary metadata files will provide key information related to datasets: origin and characteristics of the collected data, authors, licence, version, filename convention, data type, collection methods, measuring techniques and used standards, ownership, etc. The published data will also be mainly in open or widely used formats to boost interoperability.
7. Reusability: Published datasets will have a licence such as e.g., the CC-BY, and will be accompanied by the metadata and documentation useful for future reusability. During the project, all data will be stored on the centralised file storage system at the coordinator.
A data management plan (DMP) will be released at M6 and revised at the end of the project.The consortium will set up an Ethics and Privacy board, to oversee all relevant processes and aspects of the project.

#§CON-MET-CM§# #§COM-PLE-CP§# #§REL-EVA-RE§#

2. Impact

#@IMP-ACT-IA@#

2.1 Project's pathways towards impact

#@COM-DIS-VIS-CDV@#

AIDOSec will directly contribute to the expected impacts indicated in the ECS SRIA 2024 and SDG Goals of the UN Sustainable Development Agenda 2030 (UN SDG 2030) that share the common goals of promoting sustainable development and growth through research and innovation. Hence, the AIDOSec project results will contribute to the call's expected impacts, as outlined in the following sections.

Quantitative evaluations. Whenever possible, the AIDOSec achievements will be measured using quantitative and rigorous parameters based on: i) indicators defined in the *Study to support the monitoring and evaluation of the Framework Programme for research and innovation along Key Impact Pathways - The Indicator methodology and metadata handbook*[53]; ii) metrics from literature; and iii) data collected during the project development.

Qualitative measures. AIDOSec technologies will offer many improvements that can be challenging to quantify due to their subjective nature and the influence of factors such as industrial domain, capabilities, and previous experience of evaluators. Nevertheless, defining quantifiable measures is crucial as they often represent key aspects (e.g., ease of use, maturity) that can significantly impact the adoption of AIDOSec results by the industry. These improvements are expected to be quantified using satisfaction measures, typically calculated through a questionnaire format where questions are asked about specific capabilities and experiences related to the AIDOSec framework. A common feature of all satisfaction measures for AIDOSec evaluations should be using a four-point Likert scale with a "forced choice" method, requiring evaluators to take a favourable or unfavourable stance towards the improvement or advancement provided by AIDOSec solutions.
Industrial partners typically expect the following scale to be used for questionnaire responses:

- Fully achieved/fully agree/excellence
- Largely achieved/largely agree/good
- Partially achieved/partially agree/sufficient
- Not achieved/not agree/insufficient

A neutral position is not included in this five-point scale as the project's intended use of success criteria and supporting evaluation measures is to validate results and motivate industrial adoption of AIDOSec while identifying areas for future improvement. As such, capturing the positive and negative positions of industrial evaluators is of higher importance.

The Impact pathway of the AIDOSec project is outlined and discussed as follows. Section 2.1.1 defines the relations between AIDOSec and the expected outcomes and impacts defined in the ECS SRIA 2024, together with an analysis of the main markets related to the ECS SRIA dimensions (FTLs, CSTs and KAAs). These outcomes and impacts are linked to the Key Impact Pathways (KIPs) defined in the next European Research and Innovation Investment Programme. Therefore, an overview of AIDOSec impacts in terms of scientific, technological/economic and societal impact is illustrated in Section 2.1.2. Finally, in Section 2.1.3 we describe the impact that AIDOSec will have on the project's partners. Overall, AIDOSec outcomes and impacts contribute to ***Strengthening European excellence in Continuous System Engineering and notably SecDevOps*** (see AIDOSec objective O5 in Section 1.1.2), a hint of this contribution is given by the indicators used to describe the project scale and significance (Section 2.1.4).

2.1.1 AIDOSec contributions to the ECS SRIA 2024

As described in Section 1.1.3, AIDOSec technology results map specific FTLs, CSTs and KAAs from the ECS SRIA 2024. However, such results have a wider impact, embracing other dimensions, such as CST 2.1 (contributing to reducing energy consumption) and CST 2.2 (contributing to more secure communications). In this

[53] European Commission, Directorate-General for Research and Innovation, Nixon, J., Study to support the monitoring and evaluation of the framework programme for research and innovation along key impact pathways – Indicator methodology and metadata handbook, Nixon, J.(editor), Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2777/44653

section, we report in italics the excerpts from the ECS SRIA 2024 with the expected outcomes and impacts that we address, and discuss the AIDOSec contributions.

2.1.1.1 AIDOSec contribution to FTLs and CSTs expected outcomes and impacts

In this section, for each FTL and CST addressed by AIDOSec, we report an excerpt of the dimension (in italics), the list of expected outcomes to which AIDOSec contributes (with tags [#] to define if they have scientific, technology/economic and societal impacts), and then how AIDOSec is going to contribute to them.

FTL 1.3 - Embedded Software and Beyond

"Embedded software enables embedded and cyber-physical systems (ECPS) in a way that they can play a key role in solutions for digitalisation in almost every application domain."

"The efficiency and flexibility of embedded software, in conjunction with the hardware capabilities of the ECPS, allows for ***embedded intelligence on the edge*** *(edge AI), opening unprecedented opportunities for many applications that currently rely on the human acting involvement (e.g.* ***automated driving, security and surveillance, process monitoring****). Moreover, digitalisation platforms exploit embedded software flexibility and ECPS features to* ***automate their remote management and control through continuous engineering across their entire lifecycle*** *(e.g. provisioning, bugs identification, firmware and software updates, configuration management). It is the requirement of embedded software to improve sustainability of these platforms."*

In this FTL, AIDOSec contributes to the following **expected outcomes**:

I. **[#scientific, #technological/economic] -** From embedded software engineering to cyber physical systems engineering (*from MCH1*).
II. **[#scientific, #technological/economic] -** Ensuring there is a methodology to support the integration from which the engineers of such systems can benefit (*from MCH2*).
III. **[#technological/economic, #societal] -** Keep embedded systems relevant and sustainable across their complete lifecycle (*from MCH3*).
IV. **[#scientific, #technological/economic] -** Develop and make available to a wider audience, software libraries, software frameworks and reference architectures that enable interoperability and integration of products developed on distributed computing architectures (*from MCH6*).

The AIDOSec engineering approach enables **customizable SecDevOps processes** that are suitable for the **systematic analysis of edge components via MDE approaches**, supporting **secure heterogeneous software and hardware** (see AIDOSec contributions to CST 2.1) and contributing to "*strengthen the digitalisation advance in the EU and the European position in embedded intelligence and ECPS*". **AIDOSec model-based architecture facilitates integration, interoperability and automation**, responding to the need for "*integration at the higher abstraction levels and in a systematic way* **[III]**" and managing "*the complexity of ECPS and their quality properties* **[II]**", while its tools and methods contribute to **support the evolution of embedded software engineering** towards ECPS **[I]** (see AIDOSec contributions to CST 2.3) that keep into consideration **security in every step** of design, deployment and management of the system **[IV]** (see AIDOSec contributions to CST 2.4) and providing therefore "*tools to support the integration of different engineering artefacts and enable, by default, effective development with quality requirements in mind – such as safety, security, reliability, dependability, sustainability, trustworthiness, and interoperability* **[I]**". This further contributes to keep "*embedded systems relevant and sustainable across their complete lifecycle, and to maintain, update and upgrade embedded systems in a safe and secure, yet cost-effective way* **[III]**". The assessment of AIDOSec technologies is carried out in **different UCs** in which **quality, reliability, safety and security** are a must, and in many of them **edge processing and AI at the edge** are exploited to **improve performance and save energy** by bringing data processing on the device (see AIDOSec contributions to the ECS KAAs in Section 2.1.1.2.). This contributes to consolidating the position of Europe in the market of microcontrollers and low-end microprocessors for embedded systems, with solutions suitable for high-performance demanding applications.

FTL 1.4 - System of Systems

"The System of Systems (SoS) technology layer represents the upper layer of ECS technology stack for digitalisation solutions. This technology layer emerges from the composition of ECPS, connectivity and distributed software platforms."

"To create added value, a SoS needs to be ***trustable****, and here* ***end-to-end security issues have to be properly taken into account****. A secure SoS should be able to* ***defend against both deliberate attacks and accidental***

***threats**, and also its misuse. Moreover, it is not enough to ensure that each of the constituent systems is **secure in the pre-deployment phase**, but also that **the evolved/composed/integrated SoS, whose exact composition may be not known in advance, is secure**. **Dynamically adapting security requirements** and **risks mitigations** should be considered over time, and in handling emergent functionalities, properties and behaviours arising due to the complex interactions among the constituents of the SoS. **New methodology and tools for risk and vulnerability assessment and threat modelling are needed**."*

In this FTL, AIDOSec contributes to the following **expected outcomes**:

I. **[#technological/economic, #societal] -** Extension of components lifetime within the evolution of the SoS during its lifecycle (*from MCH3*).
II. **[#scientific, #technological/economic] -** Possibility that SoS will easily evolve, adapting to new contexts, new requirements and new objectives (*from MCH3*).

In the era of smart everything everywhere, there is a strong market pull for complex systems with very physical interaction - e.g., smart cities, smart traffic management and autonomous vehicles, efficient remote management etc. AIDOSec provides AI-based **key enabling technologies** that can support the issues related to security of complex systems and SoS (see AIDOSec contributions to CST 2.1, CST 2.2, CST 2.3 and CST 2.4).
AIDOSec framework addresses **security since the pre-deployment phase** with methods and tools for **threat modelling, security testing, detection & response, and threat intelligence** contributing to addressing "*complexity, variability and fuzziness of composability results* **[II]**". The AIDOSec **traceability** approach, together with the **continuous validation and improvements** component, enables the **dynamic adaptation** of security requirements and risk mitigation, providing continuous support and a feedback loop to methods and tools for risk and vulnerability assessment that can be applied **through the lifecycle of the evolving system [I]**. Challenges and issues related to specific domains, and AIDOSec impact on them, are discussed in the Section 2.1.1.2.

CST 2.1 - Edge computing and embedded Artificial Intelligence

*"Our world is drastically changing with the deployment of digital technologies that provide ever **increasing performance and autonomy** to existing and new applications at a constant or **decreasing cost** but with a big challenge concerning **energy consumption**."*

*"The introduction of AI at the edge for data analytics brings important benefits for a multitude of applications. ... One of the mainstream uses of AI is to allow an **easier and better interpretation of the data** (unstructured data such as image files, audio files, or environmental data) coming from the physical world. Being able to **interpret data** from the environment **locally** triggers new applications such as autonomous vehicles. The use of **AI in the edge** will contribute to **automate complex and advanced tasks** and represents one of the most important innovations being introduced by the **digital transformation**."*

In this CST, AIDOSec contributes to the following **expected outcomes**:

I. **[#technological/economic, #societal] -** Increasing the energy efficiency of computing systems, especially in the field of systems for AI and Edge Computing (*from MCH1*).
II. **[#scientific, #technological/economic] -** At tools level, HW/SW co-design of system and their associated algorithms are mandatory to minimise the data moves and optimally exploit hardware resources, particularly if accelerators are available, and thus optimise the power consumption (*from MCH1*).
III. **[#scientific, #technological/economic] -** Promoting tool and components interoperability (*from MCH3*).

Nowadays, many application domains rely on distributed computation across the edge-fog-cloud continuum computing, to improve efficiency and reliability, as well as adaptation to internal and external constraints. Edge computing becomes a way to reduce latency, bandwidth and power consumption, bringing data close to source, and leaving the transmission to the upper layer for tasks that require more power, are more computation hungry and require higher storage capability. In such a context, edge intelligence becomes a powerful tool to process unstructured data near source contributing to **reduce data traffic, data storage and the carbon footprint** of ECPS **[I]**. AIDOSec model-based approach allows system-level analysis, and together with solutions for **model-to-model transformation [III]** (e.g., ATL from IMT) becomes a powerful tool that can be exploited by tools for **HW-SW co-design [II]** (e.g., Hepsycode from UNIVAQ) or commercial tools for HW code generation (e.g., HDL Coder from Simulink). This contributes to "*improve interoperability* **[III]**" and "*increasing the energy efficiency* **[I]**" of the systems (see also AIDOSec contributions to FTL 1.3 and FTL 1.4). Furthermore, AIDOSec contributes to

increasing security at the edge, providing AI-based solutions as **threat modelling** and **detection & response**. This, overall, contributes to "*enable synergies between domains: e.g., self-driving vehicles with higher reliability*" (see AIDOSec UCs in KAA 3.1) also considering the human in the loop, as in the case of medical systems, reducing "*the impact of health problems with a positive impact on the healthcare system costs, first-aid and insurance services*" (see AIDOSec UC in KAA 3.4). Section 2.1.1.2 details the impact of all the AIDOSec UCs.

CST 2.2 - Connectivity

*"The industrial transition to Industry 4.0, with its massive usage of automation and digitalization accompanied by AI-supported analytics, puts much higher demands on the **availability and reliability of high-speed, secure, low or guaranteed latency connectivity**."*

In this CST, AIDOSec contributes to the following **expected outcomes**:

I. **[#scientific, #technological/economic, #societal]** - Robust, dependable, secure and interoperable connectivity from application to application and prepared for interaction in System of Systems solutions are fundamental to market success (*from MCH3*).

Many of the complex ECPS rely on large and dispersed deployments of IoT sensors; data processors require that the connectivity proposed in the project is able to deal with regular security as well as connection uncertainty such as intermittent connectivity and unreliable channels. Although Connectivity is not a main target for AIDOSec, activities related to ensuring cyber-security and privacy (see contributions to CST 2.4) and technology provided by partners (see Section 1.1.5), contribute to addressing the expected outcomes in Major Challenges 3 **[I]**. For instance, many UCs in AIDOSec (see Section 1.2.4) deal with efficient and secure data transmission and communication . For instance, HIB (UC5) will propose communications with **built-in data correction mechanisms** (transparent CRCs), exploiting the usage of **private blockchain** systems to provide a reliable backbone for the data; TEK (UC7) focusses on the development of an **AI-based detector/classifier** of attacks on wireless communications; THA (UC8) will address the real-time performance of a **mixed-critical network** with critical and non-critical traffic. Security of data transmission is addressed also by technology providers in the project, for instance: UNIVAQ tool, HEPSYCODE, considers security-related requirements (such as **cryptography**) already at system-level of abstraction; INNORIV proposes a **Secure Platform**, considering both Wireless Sensor Networks (WSN) and Wired network; BUT contributes to explore secure channels, exploiting **homomorphic encryption**.

CST 2.3 - Architecture and design: methods and tools

*"To strengthen European industry's potential to transform new concepts and ideas cost- and effort-effectively into high-value and high-quality ECS-based innovations and applications, two assets are essential: **effective architectures and platforms at all levels of the design hierarchy; and structured and well-adapted design methods and development approaches supported by efficient engineering tools, design libraries and frameworks**. These assets are key enablers to produce ECS-based innovations that are: (i) beneficial for society; (ii) accepted and trusted by end-users; (iii) successful in the market."*

In this CST, AIDOSec contributes to the following **expected outcomes**:

I. **[#scientific, #technological/economic]** - Enable European engineers to extend design processes and methods to a point where they allow handling of future ECS-based systems with all their new functionalities and capabilities for the whole lifecycle (*from MCH1*).
II. **[#technological/economic, #societal]** - Enable the design of trustworthy systems, meaning systems that probably possess the desired quality properties of safety, security, and dependability (*from MCH1*).
III. **[#scientific, #technological/economic]** - Derive efficient and consistent methods for modelling, designing, and validating future ECS-based systems, supporting the different steps in the continuous development processes derived in *[CST 2.3]* Major Challenge 1 by 2026 (*from MCH2*).
IV. **[#scientific, #technological/economic]** - In the design phase of new connected highly autonomous and evolvable ECS, this complexity must be handled and analysed automatically to support engineers in generating best-in-class designs with respect to design productivity, efficiency and cost reduction (*from MCH3*).

AIDOSec provides a **model-based framework** that supports the **integration of security aspects** in the early stage of continuous system and software development, contributing to handle *"future ECS-based systems with all their*

new functionalities and capabilities for the whole lifecycle **[I]***"*. The framework brings MDE principles and practices in SecDevOps processes to support **seamless and scalable integration of heterogeneous software** technologies and compatible **heterogeneous hardware platforms**, considering **security since the beginning**, with the definition and analysis of security requirements, policies, and architectures. This enables *efficiency*, as well as "*the design of trustworthy systems, with the desired quality properties of safety, security, dependability, etc* **[II]***"*. Tools and models bring **transparency for engineers**, who can completely comprehend each process step to perform optimisations and error correction. AIDOSec tools, techniques and methods contribute to "*derive efficient and consistent methods for modelling, designing, and validating future ECS-based systems, supporting the different steps in the continuous development processes* **[III]**" and to "*support engineers in generating best-in-class designs with respect to design productivity, efficiency and cost reduction* **[IV]**" (see also AIDOSec contributions to FTL 1.3, FTL 1.4 and CST 2.3). They integrate AI/ML techniques to support **threat modelling and analysis, security testing, detection, and response** , as well as **learning and adaptation (threat intelligence)** to improve security solutions. This contributes to the "*creation of safe, secure and trustworthy products in Europe* **[II]**".

CST 2.4 - Quality, reliability, safety and cybersecurity

"Modern technologies and new digitised services are key to ***ensuring the stable growth and development of the European Union and its society****. These new technologies are largely based on smart electronic components and systems (ECS). Highly automated or autonomous transportation systems, improved healthcare, industrial production, information and communication networks, and energy grids all depend on the availability of electronic systems. The main societal functions and critical infrastructure are governed by the efficient accessibility of smart systems and the uninterrupted availability of services."*

In this CST, AIDOSec contributes to the following **expected outcomes**:

I. **[#scientific, #technological/economic, #societal] -** A robust root of trust system, with unique identification enabling security without interruption from the hardware level right up to the applications, including AI, involved in the accomplishment of the system's mission in dynamic unknown environments (*from MCH3*).
II. **[#scientific, #societal] -** Protection of the EU citizen's privacy and security while at the same keeping usability levels and operation in a competitive market where also industrial Intellectual Protection should be considered (*from MCH3*).
III. **[#technological/economic] -** Proof-of-concept demonstrators that are capable of simultaneously guaranteeing (a given level of) security and (a given level of) privacy, as well as potentially evolving in-reference designs that illustrate how practical solutions can be implemented (*from MCH3*).
IV. **[#scientific, #technological/economic, #societal] -** To translate a well-conceived system into orchestrated system development requires holistic design processes where multifaceted developer communities jointly work together to achieve acceptable, safe, and trustworthy products (*from MCH5*).

AIDOSec Cybersecurity Solutions address security since the pre-deployment phase and the AIDOSec **intelligent traceability** tackles security **from the root cause analysis of threats to security status and performance of the system through its lifecycle**. This contributes to supporting "*mission critical systems with lots of reliability, quality and safety & security concerns* **[I]**" (see also AIDOSec contributions to CST 2.3). AIDOSec **traceability** enables automation in both intra- and inter-development stages, which is strategic in **system design, and continuous validation and improvement**, as well as in its **operation and maintenance**, contributing to considering security while, at the same time, "*keeping usability levels and operation in a competitive market* **[II]**" (see also AIDOSec contributions to FTL 1.3 and FTL 1.4). Assessment is carried out in different **challenging use cases**, that require "*guaranteeing (a given level of) security and (a given level of) privacy* **[III]**" and address human system integration **[IV]**, and have an impact on big EU challenges, such as the Green Deal. Details about the impacts of AIDOSec UCs are reported in the following discussions related to the ECS KAAs.

2.1.1.2 AIDOSec contributions to the ECS KAAs expected outcomes and impacts

The following table depicts an overview of AIDOSec UCs mapped to the KAAs and their Major Challenges (MCHs). In the rest of this subsection, for each KAA addressed by AIDOSec UCs, we report an excerpt of the dimension (in italics), a brief description of the UCs contributions to the KAA, and their contributions to the expected outcomes to (with tags [#] to define if they have scientific, technology/economic and scientific impacts).

Table 2.1.2.2 - *map between UCs and relevant challenges for KAA*

Mapping Major Challenges (MCHs)/Use cases	1	2	3	4	5	6	7	8	9	10	11	12	13
UC13. MSG - Harmonized EU-CyberBridge: Aligning EU Cybersecurity Standards and Regulations for Enhanced Cybersecurity Protection													
UC12. GTS - Railway operation in the cloud													
UC11. KAPSCH - AI supported secure solution development life-cycle for critical infrastructure													
UC10. WMO - AI and Model-Based Approaches for Industrial Communication ProductsModel-based Testing and Fuzzing of Embedded Systems to Enhance Security and Robustness													
UC9. TL - Critical AI-Based Solutions for ThingLink XR Trainings Platform													
UC8. THA - Tooled-Up Distributed Real-Time Drone Application													
UC7. TEK - Wireless Communication Security													
UC6. PRO - Secure Smart Port Solutions by Design													
UC5. HIB - SecDevOps in Medical IoT Applications													
UC4. EAB - AI/ML for optimization the CloudRAN products													
UC3. CAMEA - Secure Smart Sensors for Traffic Monitoring													
UC2. AR - Dependable AI for Railway Traction Operation and E-Mobility Testing													
UC1. ABI - Resilient New Concept Cars													
KAA 3.1 - Mobility	**1**	**2**	**3**			**6**		**8**			**11**	**12**	**13**
MCH1: Enable CO2 neutral mobility and required energy transformation.		**X**										**X**	
MCH2: Enable affordable, automated and connected mobility for passengers and freight on or off road, rail, air and water.	**X**		**X**										
MCH4: Provide tools and methods for validation and certification of safety, security and comfort of embedded intelligence in mobility.	**X**	**X**				**X**		**X**			**X**	**X**	**X**
MCH5: Achieve real-time data handling for multimodal mobility and related services.								**X**					
KAA 3.3 - Digital Industry									**9**	**10**			
MCH1: Responsive and smart production.										**X**			
MCH4: Industrial service business, lifecycles, remote operations and teleoperation.									**X**	**X**			
MCH5: Digital twins, mixed or augmented reality, telepresence.									**X**				
KAA 3.4 - Health and Wellbeing					**5**								
MCH2: Enable the shift to value-based healthcare, enhancing access to 4P's game-changing technologies.					**X**								
MCH3: Support the development of the home as the central location of the patient, building a more integrated care delivery system.					**X**								
MCH5: Ensure more healthy life years for an ageing population.					**X**								
KAA 3.6 - Digital Society				**4**			**7**						
MCH4: Facilitate supportive infrastructures and sustainable environments.				**X**			**X**						

KAA 3.1 - Mobility

*"Our mobility is currently in a fundamental phase of change. Mobility is faced with great challenges and at the same time offers enormous potential to help solve essential problems of our world: global warming because of CO2 created by our society (**Green Deal**), an ageing society with special needs for an **easy and accident free mobility**."*

*"The first societal challenge, known as the **European Green Deal,** is at the forefront of the EU's priority list. ... This ECS-SRIA Chapter on mobility is aligned with the proposal for the partnership 'Towards zero emission road transport' (2Zero) programme by Horizon Europe to achieve carbon-neutrality in road transport by 2050. There are plans to continue and strengthen this cooperation between 2Zero and the ECS community."*

*"The second societal challenge focuses on the usage of smart perception, safety and automated mobility solutions and services to **provide safe and comfortable inclusive mobility** that is also suitable for the elderly as well as people with special needs. ... The ECS-SRIA Chapter on mobility is also closely aligned with the proposal for the partnership 'Connected, Cooperative and Automated Mobility' (CCAM) under Horizon Europe. Additional key aspects of the contribution by the ECS domain to the future of mobility are increasing user value, security, privacy protection features, affordability and human interaction. Particularly in urban areas, intermodality and technologies supporting the shared principles will be crucial."*

The mobility application area is addressed by the Abinsula, Alstom, Camea, Prodevelop, and Thales UCs.

ABI UC aims to enhance the human interaction and driving experience, contributing to providing safe and comfortable inclusive mobility. The proposed rear-view mirror gets data from an AI-powered cooperative multi-camera system and provides a rear image on a screen. Safety and cybersecurity are considered since the beginning of the development, adhering to the most recent standards related to security (e.g., ISO 21434) and regulations (e.g., 2019/2144), to deal with the new frontiers of cyber-attacks in AI-powered always connected vehicles (e.g. drawing on road signs could lead the AI-powered cameras to misinterpret their meaning), providing a more secure, safe and effective drive and inspire how to certify such systems.

AR UC aims at exploiting AI-augmented real-time control to increase the operation efficiency of the rail traction, and enable its sharing among several e-mobility actors, contributing to accelerating the overall transformation of mobility towards zero CO2 emission. Cybersecurity and safety need to be addressed, providing AI solutions for data analysis and verification support, to increase trustworthiness and acceptance from customers.

CAM UC proposes a traffic monitoring system based on secure smart sensors with processing capabilities. It focuses on an innovative and flexible infrastructure that gathers traffic-related information (e.g., licence plates or speed of the vehicle) and sends it to the server or a micro-data centre on the premise, guaranteeing the security of the sensor itself, mechanism to detect changes of source data and their non-repudiability when transferred.

PRO UC focuses on providing quality and secure solutions that meet the customer's security requirements and to have high credibility in providing secure and robust solutions. The productivity of developing such solutions can be increased by incorporating tools and methodologies to help ensure quality.

THA UC consists of a communication network for an autonomous system (drone and ground station). It will investigate the issue of transmitting mixed critical data within one single physical network while meeting the timing and security constraints. Runtime monitoring will detect security attacks and prevent timing issues.

KAPSCH UC involves a comprehensive transportation and tolling solution framework, focusing on the integration of advanced security measures within the secure development life-cycle. It aims to leverage AI-driven penetration testing tools and industry best practices to enhance the security of critical infrastructure, ensuring the protection of sensitive personally identifiable information and the resilience of systems against potential cyber-attacks. This approach not only mitigates immediate vulnerabilities but also prepares the infrastructure to withstand future threats, thereby safeguarding the operation of essential transportation and tolling systems.

GTS UC encompasses a cloud-based platform for railway operations, aiming to address the challenges of hosting safety-critical applications with stringent requirements for scalability, availability, and maintainability. It will explore the integration of AI and DevSecOps principles to enhance observability and ensure compliance with security standards, while also facilitating geo-redundant operations and reducing the CO2 footprint of interlocking systems.

MSG Plaut UC proposes the Harmonized EU-CyberBridge to streamline EU cybersecurity compliance by systematically analysing, connecting, and identifying overlaps among various cybersecurity standards and regulations This reduces complexity and costs for European corporations dealing with diverse regulations across multiple markets.

In this KAA, AIDOSec UCs contribute to the following **expected outcomes**:

I. **[#societal] - Energy consumption and CO2-neutral mobility** *(from MCH 1)*- The introduction of AI in the rail traction control systems (Alstom UC) and operations (GTS UC) improves efficiency and allows for sharing the rail tractions and operations among different actors. This enables a boost in the necessary modal shift to rail, contributing to reducing the use of combustion-engine powered cars and, in turn, reducing the CO2 footprint, being demonstrated that the rail option is one of the most efficient in terms of energy consumption per passenger per kilometre.

II. **[#societal] - Interaction between humans and vehicles** *(from MCH 2)* **-** virtual mirrors, traffic monitoring, and railway control open a plethora of new possible types of interaction between humans and machines, with autonomous capabilities for risks prevention and vehicle resource optimization, e.g., correlating of different images from different points of view and predicting of possible critical events and possible countermeasures (ABI and CAM UCs), sharing rail tractions among several e-mobility actors (AR UC).

III. **[#scientific, #technological] - Verification**, **Validation,** and **Certification** *(from MCH 4)*– verification and validation methodology are integral parts of the design activities, especially if systems must be certified for operation. The UCs related to Mobility will define the relevant scenarios and their conversion for virtual testing, considering the generation of the optimal test set that complies with possible certification constraints. Similarly, the UCs related to Mobility focus on enhancing EU cybersecurity compliance by connecting, analysing, and identifying overlaps among various cybersecurity standards and regulations. The approach supports the certification process by ensuring consistency and adherence to cybersecurity regulations (MSG Plaut UC).

IV. **[#scientific, #technological] - Real-time data handling** *(from MCH 5)* – Alstom UC to ensure the dependability of AI when implemented in safety-critical railway real-time traction control systems. Thales UC aims to demonstrate the capabilities of a TSN network to provide secure and dependable real-time communication for drones and avionics systems.

V. **[#scientific, #technological/economic, #societal] - Security** and **safety** *(transversal to the Mobility KAA MCHs)* - when interconnected systems are involved, vulnerability to possible cyber-attack is there. The introduction of AI in Mobility, as it happens in ABI and CAM UCs (video systems with AI processing capabilities), in the TEL UC (AI for data analytics), in KAPSCH UC (AI for penetration testing), or in the AR UC (AI-augmented control systems for rail tractions), opens new surfaces to cyber-attacks (e.g., changing the AI network's weights when it is updated over the air). Safety is also crucial when possible safety-critical interaction with human beings is involved.

KAA 3.3 - Digital Industry

"The Industry 4.0 changes to the mode of operation have a profound impact on how are managed and operated the factories, construction zones and processes. Powerful networked digital tools are needed to ***achieve the necessary Situational Awareness and control of autonomous vehicles, robots and processes at various autonomy levels****."*

"The business environment is changing. Through specialisation in new or niche end products, production is becoming more ***demand-driven and agile****, while production is increasingly geographically* ***distributed****. In addition, the outsourcing of auxiliary business functions such as* ***condition monitoring and maintenance*** *is gaining in popularity, leading to highly networked businesses."*

The digital industry application area is addressed by WMO UC and TL UC.

WMO UC deals with industrial communication in harsh an environment, supporting the transitioning from low levels of automation and digitalisation to highly digital industries and enabling connected, automated and reactive production, as a way to scale up and enable remote operations, e.g. by connecting to a windmill in a remote area. In this UC, Westermo aims at enhancing the quality of the software in the products by means of model-based and AI-powered approaches, which will improve the quality of software in Westermo products.

TL UC tackles the collaborative research and development of security-critical AI-based solutions for TL XR Trainings Platform, to utilise novel AI-based, MDE-based, EDGE-intelligence-based, and VR/AR/MR/XR-based technologies to design and develop digital solutions of various products for the global manufacturing industry.

In this KAA, AIDOSec UCs contributes to the following **expected outcomes**:

I. **[#technological/economic] - Robust, resilient and adaptive production** *(from MCH 1)* - in such a context, responsiveness, flexibility, and smartness are at the base for automation technology. The products adopted in the WMO UC are meant not only to handle changing networks but also to respond well to invalid inputs.
II. **[#technological/economic] - Remote operations, teleoperation** *(from MCH 4)* - with the increasing importance of megatrends like internet-of-things, we can expect networks in digital industries to be more dynamic, and also to include low-cost devices such as sensors etc., where protocol compliance or robustness may be low. Westermo provides products, such as switches and routers, that enable communication networks in domains like on-board rail, track-side rail, power distribution and factory automation in general.
III. **[#technological/economic] - Tracking & simulator-based design** *(from MCH 5)* - Extended Reality (XR) is an umbrella term that encompasses Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) technologies. These technologies enable users to experience immersive and interactive digital environments that can enhance their perception of reality. In the digital industry, XR has various applications that can benefit different sectors and domains. In AIDOSec, TL aims to leverage XR to provide products that monitor and simulate production conditions to increase productivity, reduce development costs, and improve security and software quality through security-critical AI-based MDE practices.

KAA 3.4 - Health and Wellbeing

"The healthcare industry is facing radical change, enabled by its current digital transformation in combination with a change towards personalized medicine. ***Data will play an increasingly important role*** *in providing a better understanding of consumer needs in terms of health, and to enhance and tailor a more* ***cost-efficient health*** *offering that delivers the right care at the right time and in the right place."*

"Care solutions need to be integrated, ***combining information across all phases of the continuum of care from many sources*** *– preventing, preparing, and providing care based on person-specific characteristics. This will support the development of applicable biomedical models for specific disease groups, for customer groups and for populations, taking* ***heterogeneous data*** *involving history, context, or population information into account."*

The health and wellbeing application area is addressed by the HIB UC.
HIB UC deals with the improvement and increase of security practices in the production of a remote health platform for home hospitalisation purposes. Such platforms are used to monitor the health parameters of persons under monitoring using a variety of sensors (wearables such as activity trackers, smart medical devices such as pulse oximeters and even IoT sensors at the home of the patients such as movement detectors) that gather data that is then analysed using AI algorithms at the Edge or Cloud. The GDPR recognises data concerning health as a special category of data and provides a definition for health data for data protection purposes that applications such as those modelled in the HIB UC need to consider in all of the stages of the DevOps process. In the current post COVID-19 health environment, these systems are on the rise with great growth and a very fragmented marketplace of solutions. Adherence to a trusted, security-oriented brand such as AIDOSec will increase the impact of the results of the Use Case in future exploitation.

In this KAA, the HIB AIDOSec UC contributes to the following **expected outcomes**:

I. **[#technological, #societal] - Data protection, anonymization and traceability** *(from MCH2 and MCH3)* – A high level of digital trust is required for executing transactions in healthcare and wellbeing and enable P4 healthcare. All of the generated data in this domain is of critical consideration, and as such, it requires specific protections that start with a correct development practice for applications. In AIDOSec, we will propose for the HIB UC the highest level of data protection not only in static scenarios but also in the transmission of such data from the sensors to the data platform and beyond. Data privacy and security will be major drivers, but connections to other elements, such as data ownership, will be explored with the tools provided by AIDOSec (e.g., encryption, safe enclaves and data traceability using blockchain).
II. **[#technological, #societal] - Data interoperability** *(from MCH2 and MCH3)* – different health systems in the EU and beyond use a plethora of different data formats connected to the particulars of Health Information Systems (HIS). Providing solutions that are able to interact with not just one but a wider array of subsystems

presents an engineering challenge but also one of future legal dimension: the proposal for a European Health Data Space (EHDS) defines clear priorities for data ownership, usage in AI applications, the movements of such data in the EU and other related challenges. In the HIB UC in AIDOSec, we will propose development workflows and tools that help identify such data challenges and provide protection and verification tools to ensure that they align with standards and best practices.

III. **[#economic, #societal] - Supporting the consideration of the home as the central location for the patient** *(from MCH3 and MCH5)* – in intimate connection with the challenge MCH2 and the reduction of overall costs, HIB will propose solutions for home hospitalisation and the effective work of clinicians with patients that are away from the hospital premises. This implies even more challenging environments for data transmission, so technical elements such as the aforementioned secure enclaves and data traceability are paramount. The Use Case is constructed around an existing product for home hospitalisation management (REVITA by HI Iberia), so this will evolve naturally from the current product requirements and challenges.

KAA 3.6 - Digital Society

"Europe needs digital solutions that support the individual, and at the collective level to empower society as a whole. ... Future digital innovations will therefore need to address societal concerns in a sustainable way, guaranteeing participation and reducing inequality. A human-centred approach is therefore a key aspect of the EU's approach to technology development. It is part of European social and ethical values, (social) inclusiveness, and the creation of sustainable, high-quality jobs through social innovation"

*"...providing a **reliable and resilient digital infrastructure** (with ubiquitous and continuous connectivity), protecting society against destabilising forces and establishing a sustainable environment."*

The digital society application area is addressed by the TEK UC and the EAB UC.

TEK UC demonstrator is an AI-based detector and classifier of security attacks on wireless communications, to allow timely countermeasures for greater availability. The UC wants to demonstrate that artificial intelligence techniques increase the adaptability of the demonstrator to the dynamic and heterogeneous environments in which it operates, as well as its effectiveness. The demonstrator will be experimented with different scenarios of critical infrastructure protection that belong to the KAA theme "Digital Society". The other theme characterising the UC is the CST "*Quality, reliability, safety and cybersecurity*". Major Challenge 3 "Cybersecurity and privacy" of the latter theme, is strictly related to Major Challenge 4 "Supportive infrastructure" of the former theme, and deals with "real-time monitoring to manage the *dynamicity* and *variability* of systems" and with "new approaches, methodologies and tools *empowered by AI*" that are the main demonstrator properties that the UC aims at.

EAB UC is based on CloudRAN, a cloud-based deployment option for Radio Access Networks (RAN) architectures. It provides security advantages such as isolation and geographical redundancy but also introduces new security risks. The threat surface in Cloud RAN deployments is expanded compared to traditional RAN solutions. A new approach beyond traditional formal verification is needed to address these challenges.

In this KAA, both AIDOSec UCs contributes to the following **expected outcome**:

I. **[#scientific, #technological/economic, #societal] - Provide reliable and resilient communication infrastructure** *(from MCH 4)* – All aspects of Digital Society rely on dependable communications systems that provide ubiquitous and continuous connectivity. TEK UC addresses the availability of communications under link interference or destruction, accidental or intentional. EAB UC focuses on securing Cloud RAN deployments against evolving threats and takes a comprehensive stance, safeguarding communication infrastructure's reliability, resilience, and continuity. Through innovative solutions and collaborative efforts, these use cases contribute to building a foundation for a Digital Society that thrives on dependable and secure communication systems. For instance, it can be employed for network security and fraud detection, predictive maintenance, resource optimization, and data-driven decision-making.

2.1.1.3 Market Analysis

Analysis of technology markets (related to the foundational and cross-layer technologies) and the markets related to the UC domains (KAA). In the following, we provide additional market analysis overviews beyond the market analyses provided by the ECS SRIA 2024 document.

FTL 1.3 - Embedded Software and Beyond

According to the "Embedded System Market Share | Global Report, 2023-2032"[54], the **Embedded System Market** size is worth more than **USD 140 billion in 2022** and is projected to witness over **6% Compound Annual Growth Rate (CAGR) from 2023-2032**. The growth of the industry is attributed to rising sales of smart devices and wearables and a steady increase in the use of automated solutions in the industrial sector. AI/ML solutions are expected to boost the need for more complex embedded systems over the estimated timeframe. Similarly, In the "Embedded Software Market Size, Global Forecasts Report 2032"[55] According to a report by Global Market Insights, the **Embedded Software Market** exceeded **USD 15 billion in 2022** and is poised to exhibit over **9% CAGR from 2023 to 2032**, due to the rapid rise in AI and ML tech innovations. With steady technological advancement, the deployment of deep and machine-learning models in device software has increased. Embedded sensor-power systems, when fed with real-time data, can be trained to help recognize potential issues in hardware devices. The adoption of ML and AI tech in embedded software systems will therefore rise, to track and inspect defects and production assets of interconnected facilities. In "Embedded Systems Market Size, Share, Growth, & Forecast Analysis By 2029"[56] by Data Bridge Market Research, the **embedded systems market** was valued at **USD 91.86 billion in 2021** and is expected to reach **USD 148.64 billion by 2029**, registering a **CAGR of 6.20%** during the forecast **period of 2022 to 2029**. The growth of the market is attributed to the growth of computer technology and the wide range of applications for electronic systems. The "Global Embedded System Market Report 2024 Edition"[57] by Cognitive Market Research further supports the projected growth in the embedded systems market. The report estimates the market size to be **USD 90.65 billion in 2022**, with an expected increase to **USD 160.86 billion by 2030**. The industry's **CAGR** is forecasted to be **6.1% from 2023 to 2030**, indicating a steady growth trajectory. This growth is driven by the increasing demand for Advanced Driver-Assistance Systems (ADAS) in electric and hybrid vehicles and the rising automation in various industries.

The four reports projected **growth in the embedded systems and embedded software markets** over the next several years. The growth is **attributed to the rise in AI and ML** tech innovations, steady technological advancement, and the deployment of deep and machine-learning models in device software. Their adoption in embedded systems is expected to rise, to track and inspect defects and production assets of interconnected facilities.

FTL 1.4 - System of Systems

System of Systems (SoS), intended as an integrated and self-regulating system beyond brands, industries, and vertical domain boundaries is a crucial technology (an enabler) for digitalization and for the European Digital Era. The **Internet of Things (IoT) is the main enabler.** In this regard, the CAGR of the **IoT market** varies depending on the source. In its whitepaper[58], ARTEMIS states that the **IoT global market** is a rapidly growing sector The global Internet of Things (IoT) market was valued at **USD 190.0 billion in 2018** and is projected to reach USD **1,102.6 billion by 2025**, exhibiting a **CAGR of 24.7%** in the forecast period.
Similarly, according to Fortune Business Insights, the global IoT market size was valued at **USD 544.38 billion in 2022** and is projected to grow from **USD 662.21 billion in 2023** to USD **3,352.97 billion by 2030**, exhibiting a **CAGR of 26.1%** during the forecast period[59].
According to a report by Mordor Intelligence, the Internet of Things (IoT) market size is estimated at **USD 1.17 trillion in 2024**, and is expected to reach **USD 2.37 trillion by 2029**, growing at a **CAGR of 15.12%** during the forecast period (2024-2029)[60]. IoT Analytics[61] highlights that the IoT market remains a top-three corporate technology priority and estimates a **robust growth of 17% per annum** through 2030. This growth is fueled by an increase in connected assets and corresponding investments in AI and cybersecurity within the IoT sector.
Another source, Expert Market Research, reports for 2024[62] that the global IoT market size attained a value of about **USD 2.18 trillion in 2023**. The market is further expected to grow at a **CAGR of 15.9%** to reach nearly **USD 8.20 trillion by 2032**.

---

[54] Embedded System Market Share | Global Report, 2023-2032 (gminsights.com)
[55] Embedded Software Market Size, Global Forecasts Report 2032 (gminsights.com)
[56] Embedded Systems Market Size, Share, Growth, & Forecast Analysis By 2029 (databridgemarketresearch.com)
[57] Embedded System market size was $90.65 billion in 2022! (cognitivemarketresearch.com)
[58] Artemis-IA · News · ARTEMIS Whitepaper 'From the Internet of Things to System of Systems'
[59] Internet of Things [IoT] Market Size, Share & Growth by 2030.
https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307 Accessed 5/2/2023 .
[60] IoT Market - Size, Growth & Trends - Internet of Things (mordorintelligence.com)
[61] INSIGHTS-RELEASE-State-of-IoT-Spring-2024-10-emerging-IoT-trends-driving-market-growth.pdf (iot-analytics.com)
[62] IoT Market Size, Share, Growth, Demand, Analysis 2024-2032 (expertmarketresearch.com)

These reports indicate a significant growth trajectory for the IoT market, driven by technological advancements and increased adoption across various industries. The **CAGR** figures vary slightly between sources but consistently show a **double-digit growth rate**, underscoring the dynamic nature of the IoT sector.

CST 2.1 - Edge computing and embedded Artificial Intelligence

According to a report by Future Market Insights, the **global embedded intelligence market** is projected to reach a market value of **USD 86,215.9 million in 2032**, increasing **from USD 25,405.8 million in 2022**, expanding at a **CAGR of 13.0%** during the forecast period. As reported by a McKinsey Global Survey on AI in 2022, **AI adoption has more than doubled** between 2017 and 2022, **with an increasing level of investment**. Still, there is a rising **need for intelligent machines** with self-reflection skills and the demand for speedy, accurate, and intelligent technologies that can function without human intervention are some of the major **factors projected to drive the demand** for embedded intelligence in the future. According to a report by Grand View Research[63], the global **edge computing market** size was valued at **USD 11.24 billion in 2022** and is expected to expand at a **CAGR of 37.9% from 2023 to 2030**. The **global embedded intelligence market** is projected to reach a market value of **USD 86,215.9 million in 2032**, increasing from **USD 25,405.8 million in 2022**, expanding at a **CAGR of 13.0%** during the forecast period[64]. **In 2024**, the market size is reported to be **USD 28,057.6 million**, with a forecasted growth to USD 86,135.67 million by 2033, at a slightly adjusted **CAGR of 11.2%**[65]. The **global edge computing market** was valued at **USD 11.24 billion in 2022** and is expected to expand at a **CAGR of 37.9% from 2023 to 2030**, according to Cognitive Market Research.
As of 2024, the market size is estimated at **USD 15.59 billion**, and it is anticipated to reach **USD 32.19 billion by 2029**, growing at a **CAGR of 15.60%** during the forecast period[66], according to Mordor Intelligence.

CST 2.2 - Connectivity

A report by Expert Market Research[67], the global IoT connectivity market attained a value of about **USD 163 billion in 2020** and is expected to grow at a **CAGR of 20.9%** to reach approximately **USD 493 billion by 2026**. The IoT connectivity market is being driven by the rising demand for high-speed network connectivity.
Several market studies show huge potential, with 1.2 billion devices capable of on-device AI inference expected to be shipped in 2023, and the market size for Application-Specific Integrated Circuit (**ASIC**) responsible for edge inference expected to reach **USD 4.3 billion by 2024.** The **market for AI-related semiconductors** is also expected to grow significantly, with potential use cases requiring tailored solutions. By 2025, **AI-related semiconductors** (i.e., chips that are designed to enable and facilitate AI applications) could account for almost 20 percent of all demand, translating into about USD 65 billion in revenue. The global **AI chip market** is expected to **grow to USD 253.30 billion by 2030**, with a **CAGR** of **35.0%** from 2020-2030.

CST 2.3 - Architecture and design: methods and tools

Methods and tools for Cybersecurity, DevOps[68], MDE, and AI/ML are cornerstone contributions of AIDOSec. The market analysis for embedded intelligence has already been discussed in CST 2.1 and the market analysis for cybersecurity is outlined in CST 2.4. In addition to these, market analysis figures are provided for the remaining AIDOSec pillars, which include DevOps and MDE. The "**DevSecOps Market** Overview, Industry Trends, & Market Size By Forecast"[69] by Data Bridge Market Research report on the global DevSecOps market. The report provides an overview of the market by deployment type, component, organisation size, and vertical. It states that the global DevSecOps market was valued at **USD 2.59 billion in 2021** and is expected to reach **USD 23.16 billion by 2029,** registering a **CAGR of 31.50%** during the **forecast period of 2022-2029**. The report discusses how businesses are utilising DevSecOps software more frequently to achieve more agile development techniques with

[63] Edge Computing Market Size, Share & Growth Report, 2030 (grandviewresearch.com)
[64] Embedded Intelligence Market Report 2024, Market Size, Share, Growth, CAGR, Forecast, Revenue (cognitivemarketresearch.com)
[65] Embedded Intelligence Market Trends & Demand to 2033 (futuremarketinsights.com)
[66] Edge Computing Market - Companies, Size & Industry Growth (mordorintelligence.com)
[67] Global IoT Connectivity Market Outlook - Expert Market Research.
https://www.expertmarketresearch.com/reports/iot-connectivity-market Accessed 5/2/2023.
[68] We consider here DevOps as an umbrella term for all security-oriented variants (DevSecOps, SecDevOps).
[69] DevSecOps Market Overview, Industry Trends, & Market Size By Forecast (databridgemarketresearch.com)
https://www.databridgemarketresearch.com/reports/global-devsecops-market

improved security due to the rising concern for **data security**. The report also highlights some of the factors driving the growth of the DevSecOps market such as the growing internet penetration rate and increasing need for highly secure and faster application delivery. In its report, Grand View Research[70] states that the global **DevSecOps market** size was valued at **USD 2.79 billion in 2020** and is expected to expand at a **CAGR of 24.1% from 2021 to 2028**. Similarly, **other market research firms**, with their reports[71] [72] [73] agree on a **two-digit CAGR** for the DevSecOps market, highlightening the growth and importance of DevSecOps in ensuring secure and efficient software development practices.

Concerning **MDE**, it received a recent boost by its reincarnation in low-code development technologies. As reported by Gartner[74], the worldwide **market for low-code development technologies is projected to total $26.9 billion in 2023**, an increase of **19.6% from 2022**. A rise in business technologists and a growing number of enterprise-wide hyper automation and composable business initiatives will be the key drivers accelerating the adoption of low-code technologies through 2026. Low-code application or development platforms (**LCAPs/ LCDPs**) are projected to be the largest component of the low-code development technology market, growing 25% to reach nearly **$10 billion in 2023**. Gartner predicts that by 2026, developers outside formal IT departments will account for at least 80% of the user base for low-code development tools, up from 60% in 2021. **In 2024**, Mordor Intelligence[75] stated that the **LCDP market size** is estimated at **USD 16.17 billion in 2024**, and is expected to reach **USD 62.15 billion by 2029**, growing at a **CAGR of 30.90%** during the forecast period.

CST 2.4 - Quality, reliability, safety and cybersecurity

According to a report by Fortune Business Insights, the **global cyber security market size** was valued at **USD 153.65 billion in 2022**. The market is projected to grow from **USD 172.32 billion in 2023** to **USD 424.97 billion in 2030**, exhibiting a **CAGR of 13.8%** during the forecast period. The global cybersecurity market is projected to continue its growth trajectory in 2024, where, according to Statista, the revenue in the cybersecurity market is expected to reach **USD 183.10 billion**. The **market is dominated by Security Services**, which is projected to have a market volume of **USD 92.91** billion in 2024[76]. The overall market is expected to exhibit a **CAGR of 10.56% from 2024 to 2028**, resulting in a **market volume of USD 273.60 billion by 2028**.

Cyber security is a method of protecting systems, networks, and programs from digital attacks. The increasing adoption of enterprise security solutions in manufacturing, Banking, Financial Services, and Insurance (BFSI), and healthcare is expected to drive the cybersecurity market growth in the forthcoming years. The **COVID-19** pandemic severely affected the overall behaviour of consumers and providers but the demand for healthcare, manufacturing, and government cybersecurity services grew exponentially during the pandemic. Similarly, according to an article by Harvard Business Review[77], the **conflict in Ukraine** presents perhaps the most acute cyber risk U.S. and western corporations have ever faced. The invasion by Russia led to the most comprehensive and dramatic sanctions ever imposed on Russia, which views such measures as economic warfare. Russia will not stand by, but will instead respond asymmetrically using its considerable cyber capability. It represents a factor that is driving and will drive the growth of the **cybersecurity market** in the next few years.

KAA 3.1 - Mobility

[70] Global DevSecOps Market Share Report, 2021-2028 - Grand View Research.
https://www.grandviewresearch.com/industry-analysis/development-security-operation-market-report
[71] DevSecOps Market Size, Share, Trends & Outlook by 2033 | FMI (futuremarketinsights.com)
[72] DevSecOps Market Trends 2023-2032, Global Analysis Report (gminsights.com)
[73] DevSecOps Market Share, Size and Industry Growth Analysis 2024 - 2030 (industryarc.com)
[74] Gartner Forecasts Worldwide Low-Code Development Technologies Market to Grow 20% in 2023
https://www.gartner.com/en/newsroom/press-releases/2022-12-13-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-20-percent-in-2023
[75] Low Code Development Platform Market - Size, Share & Growth (mordorintelligence.com)
[76] Cybersecurity - Worldwide | Statista Market Forecast
[77] The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict (hbr.org)
https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict

In **2023**, the global **automotive cybersecurity market** was valued at **USD 3.13 billion** and is projected to grow significantly in the forecast period[78]. **By 2024**, the market is expected to reach **USD 8.86 billion**, and by 2029, it could expand further to USD 14.80 billion at a **CAGR of 10.8%**[79] [80].
A report by Market Research Future[81] discusses the projected growth of the Automotive Industry, which is expected to grow to **USD 6,070.4 billion by 2030**, with a **CAGR of 6.9% during the forecast period (2023-2030)**. The growth is driven by factors such as increasing demand for high-end passenger vehicles, urbanisation, and rising infrastructure spending. The commercial vehicle sales growth is driven by rapid population growth, urbanisation, infrastructure, and industrial expansion. E-commerce and digital transformation are also important in improving the transportation and logistics sector. The Automotive market segmentation includes Vehicle Type (Passenger Car and Commercial Vehicle) and Propulsion Type (ICE Vehicle and Electric Vehicle).
If we consider the market for automotive cybersecurity, it is growing rapidly due to the increasing number of connected and autonomous vehicles on the road. According to a report by MarketsandMarkets, the global market for automotive cybersecurity is expected to grow from **USD 1.34 billion in 2020** to **USD 4.09 billion by 2025**, at a **CAGR of 25.5%** during the forecast period. Automotive manufacturers, suppliers, and cybersecurity companies are the main players in this market, and they are working together to develop innovative solutions to address the unique challenges posed by cybersecurity threats in the automotive industry.

Similarly, the market for railway cybersecurity is growing due to the increasing digitization and connectivity of railway systems, which has led to an increase in cyber threats. According to a report by MarketsandMarkets, the **global market for railway cybersecurity** is expected to grow from **USD 6.0 billion in 2020** to **USD 12.6 billion by 2025**, at a **CAGR of 16.3%** during the forecast period. According to Market Research Future[82], in 2023, the **global railway cybersecurity market was valued at USD 6.60 billion** and is projected to reach **USD 16.68 billion by 2030** at a **CAGR of 8.80%**. **By 2024**, the market is estimated to be **USD 8.96 billion** with a **CAGR of 9.4%**, according to the Business Research Company[83].
Railway operators, suppliers, and cybersecurity companies are the main players in this market, and they are working together to develop innovative solutions to address the unique challenges posed by cybersecurity threats in the railway industry posed by **digitalization** and **urbanization**, among others.

KAA 3.3 - Digital Industry

The digital industry is a broad term that encompasses various technologies and markets. For example, the global digital marketing market reached a value of nearly **USD 321 billion in 2022** and is expected to grow at a **CAGR of 13.1% between 2023 and 2028 to reach** a value of around **USD 671.86 billion by 2028**[84]. The market size reached **USD 363.05 billion in 2023**[85] The global **digital transformation market** size was evaluated at **USD 731.13 billion in 2022** while the market size was valued at **USD 880.28 billion in 2023**[86]. It is expected to grow at a **CAGR** of **27.6% from 2024 to 2030**
The market growth can be attributed to the growing adoption of cutting-edge technologies such as cloud, big data analytics, and Artificial Intelligence (AI), among others.

KAA 3.4 - Health and Wellbeing

McKinsey's research indicates that the **global wellness market has reached USD 1.8 trillion.** The market continues to grow at **CAGR of 5% to 10%**, with consumers increasingly seeking effective, data-driven, science-backed health and wellness solutions[87].

[78] Automotive Cyber Security Market Size, Analysis 2024-2032 (expertmarketresearch.com)
[79] Automotive Cybersecurity Market Size, Trends, Outlook 2034 (transparencymarketresearch.com)
[80] Automotive Cyber Security Market Size, Share & Growth 2024-32 (reportsandinsights.com)
[81] Automotive Industry 2024 - Market Size, Company, Growth 2030 (marketresearchfuture.com)
[82] Railway Cybersecurity Market 2024 | Size, Share, Growth 2032 (marketresearchfuture.com)
[83] Railway Cybersecurity Market Size,Trends And Forecast 2024-2033 (thebusinessresearchcompany.com)
[84] Digital Marketing Market Share. https://www.expertmarketresearch.com/reports/digital-marketing-market
[85] Digital Marketing Market Size & Industry Report | 2032 (expertmarketresearch.com)
[86] Digital Transformation Market Size, Trends Report, 2023-2030 (grandviewresearch.com)
[87] The top wellness trends in 2024 | McKinsey

Another report by Statista estimates that the health and wellness market size worldwide was over **USD 4.3 trillion in 2020** and is set to increase to almost **USD 7 trillion by 2025**[88]. Deloitte's 2024 Global Health Care Sector Outlook[89] emphasizes the sector's transformation driven by technological advancements, demographic shifts, and evolving patient needs. Key trends shaping the future of health care include the integration of AI, sustainability, social care integration, cost management, and workforce adaptation.

KAA 3.6 - Digital Society

The report by Grand View Research[90] discusses the growth of the global telecom services market, which was valued at **USD 1,805.61 billion in 2022** and is expected to expand at a **CAGR of 6.2% from 2023 to 2030**. The growth is driven by factors such as rising spending on the deployment of 5G infrastructures, increasing number of mobile subscribers, and soaring demand for high-speed data connectivity.

Cybersecurity in the communication market is a growing and dynamic sector that encompasses various technologies, services and solutions to protect data and systems from cyberattacks. According to a report by MarketsandMarkets[91], the global cybersecurity in communication market size is expected to grow from **USD 31.4 billion in 2020** to **USD 51.6 billion by 2025**, at a **CAGR of 10.4%** . Some of the key factors driving this growth are the increasing adoption of cloud-based services, the rising demand for secure and reliable communication networks, and the growing awareness of cyber threats among enterprises and consumers.

2.1.2 Contribution to Horizon Europe Key Impact Pathways

In Section 2.1.1 we described the AIDOSec contributions to the ECS SRIa 2024, describing for each expected outcome the nature of AIDOSec impact (scientific, technological/economic, societal) and, therefore, map them to the Horizon Europe Key Impact Pathways (KIPs). In this section we change the point of view and focus on these ones, to give a complete overview of the outcomes that AIDOSec will have in the medium-term period and the impact it will have beyond the immediate scope and duration of the project, in terms of scientific, technological/economic and societal impacts. Figure 2.1.2 shows the KIPs that are affected by AIDOSec and its results.

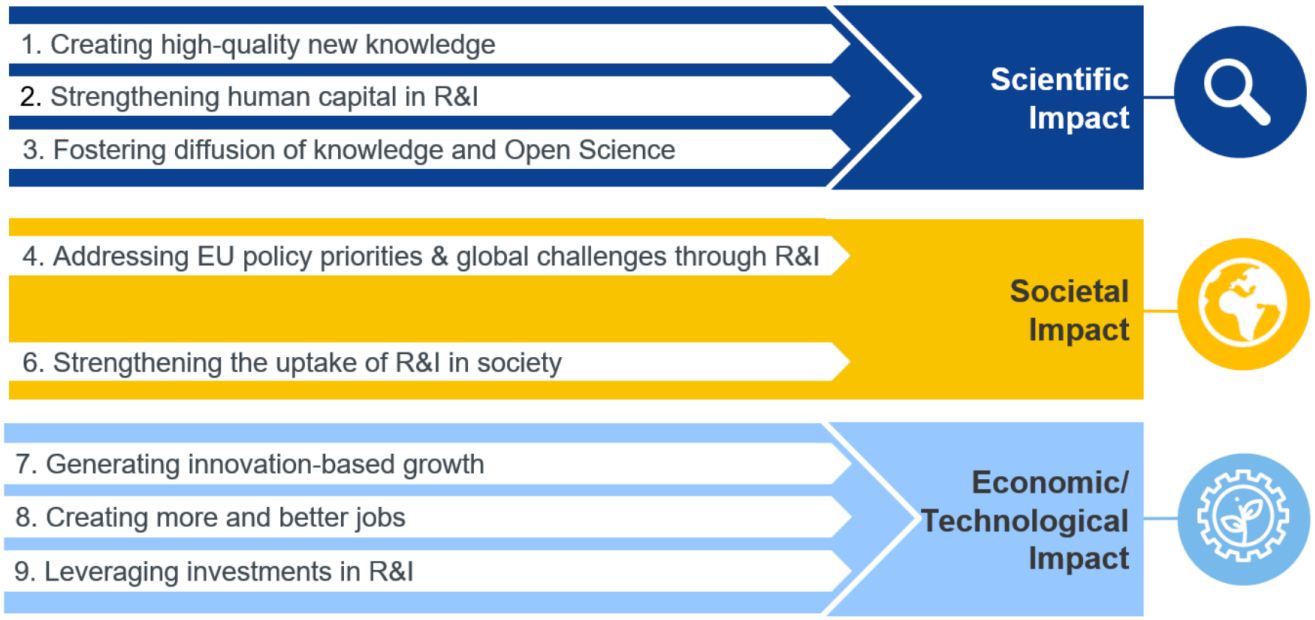


Figure 2.1.2 - ***AIDOSec contributions towards the KIPs***

2.1.2.1 Scientific Impact

[88] Wellness industry - Statistics & Facts | Statista. https://www.statista.com/topics/1336/wellness-and-spa/
[89] 2024 Global Health Care Sector Outlook (deloitte.com)
[90] https://www.grandviewresearch.com/industry-analysis/global-telecom-services-market
[91] Cyber Security Market Size, Share, Growth Drivers, Opportunities & Statistics (marketsandmarkets.com)

AIDOSec contributes to advanced knowledge in the MDE, and AI applied to DevOps, with a focus on security (SecDevOps). The interdisciplinary nature of AIDOSec (cybersecurity, SecDevOps, MDE, AI/ML) is a key enabler for contributing to the strategic ***Main Common Objective 1: boost industrial competitiveness through interdisciplinary technology innovation.*** Furthermore, AIDOSec, as their direct successor, contributes to the mid and long-term impact of the MegaMart2 and AIDOaRt ECSEL JU projects.

1. **Creating high-quality new knowledge.**

From a scientific point of view, the project will advance the SOTA in cybersecurity of complex systems by leveraging SecDevOps, MDE and AI/ML techniques and practices. The project will produce novel methods, techniques, and tools for modelling, analysing, verifying and testing security aspects in SecDevOps processes (see AIDOSec contributions to FTL 1.3 and FTL 1.4). By leveraging the innovation potentials of ongoing industrial and research activities by involved partners (see Section 1.1.5), the project will also develop innovative AI solutions for automating security tasks and enhancing security decision-making (see AIDOSec contributions to CST 2.3 and CST 2.4). The project will contribute to the scientific literature by publishing high-quality papers in relevant journals and conferences.

The AIDOSec project proposal aims to **advance the SOTA in SecDevOps** by combining MDE and AI principles and techniques. The project will contribute to the ***Horizon Europe objectives of enhancing cybersecurity, digital sovereignty, and innovation capacity in Europe***. As a preliminary indicator of the potential scientific impact of AIDOSec, it is worth noting i) how the AIDOSec consortium involves partners whose members are active researchers on Cybersecurity, MDE, DevOps, and AI/ML, and ii) the current low number of peer-reviewed scientific publications and, at the same time recent scientific venues interested in the interdisciplinary area targeted by AIDOSec, as witnessed by querying two of the most reputable scientific indexing systems and databases, the ACM Digital Library[92], and IEEE Xplore[93].

2. **Strengthening human capital in research and innovation**

From a societal point of view, the project will enhance security awareness and culture among DevOps practitioners and stakeholders. The project will promote the adoption of security best practices and standards in DevOps processes (see AIDOSec contributions to CST 2.3 and CST 2.4).

AIDOSec will also foster collaboration and communication among different roles and teams involved in DevOps projects. The project will disseminate its results and outcomes to various target groups, such as academia (communities working on cybersecurity, MDE, DevOps, and AI/ML as well as communities related to embedded systems and edge computing), industry (focussing both on AIDOSec industrial partners and on the external ones), policymakers, and the general public. In order to develop cybersecurity skills among AIDOSec organisations, AIDOSec will promote internal campaigns on cybersecurity concerns, focussing on specific target groups (use-case specific stakeholders, industrial experts, and researchers).

3. **Fostering diffusion of knowledge and Open Science.**

AIDOSec project will adopt the Open Science practices described in the programme guide[94], such as:

- Making the research data generated by the project FAIR (findable, accessible, interoperable and reusable) and open by default unless there are legitimate reasons to protect them, adhering to the *'as open as possible, as closed as necessary'* principle. The project will use the European Open Science Cloud (EOSC) as the preferred platform for storing and sharing the data and will follow the guidelines and standards for data management and metadata. The project will also define a Data Management Plan (DMP) that will specify what data will be collected, processed, and generated; what methodology and standards will be applied; how data will be curated and preserved; and how data will be shared and made open (i.e., through OpenAIRE). For details related to AIDOSec actions towards OpenScience.
- Providing (Green or Gold) open access to scientific publications resulting from the project, either by publishing in open-access journals or platforms or by depositing a copy of the accepted manuscript in a trusted repository (e.g., arxiv.org, Zenodo, FigShare, and online libraries of academic partners).
- Developing and using open-source software for the AIDOSec framework, and making it available under appropriate licences that allow reuse and modification. The project will use existing standards, open-source

[92] ACM Search Results
[93] IEEE Xplore Search Results
[94] Horizon Europe (HORIZON), Programme Guide. Version 3.0 01 April 2023.

tools (e.g., Modelio counts a community of 80k users), and open-source platforms (e.g., Eclipse[95] for MDE, Keptn[96] for continuous delivery) whenever possible, and will contribute to their improvement and maintenance. The project will also document the software code and provide clear instructions on installing, running and using it.

By implementing these Open Science practices, ***AIDOSec aims to increase the transparency, reproducibility and quality of its research outputs, as well as to foster collaboration, innovation and societal impact***.

2.1.2.2 Societal Impact

AIDOSec provides key enabling technologies to address security of digital systems, contributing to their uptake. This, in turn, contributes to lowering the global energy footprint at all the levels of the economy and supporting European strategic autonomy in terms of sustainability and resilience addressing the ***Main Common Objective 3: establish and strengthen sustainable and resilient ECS value chains supporting the Green Deal***. The security supported by AIDOSec also contributes to improving trust in (AI-based) digital systems, supporting autonomous and remote work and contributing to ***Main Common Objective 4: unleash the full potential of intelligent and autonomous ECS-based systems for the European digital era***. Here we discuss an overview of the AIDOSec impact with respect to societal challenges, details related to specific application domains are discussed in Section 2.1.2.2.

4. Addressing EU policy priorities and global challenges through research and innovation

The European Union proposed a **Green Deal**, a set of policy initiatives aimed at achieving climate neutrality by 2050. Some of the key goals include reducing greenhouse gas emissions, investing in research and innovation, preserving the natural environment, promoting energy efficiency, providing healthy food and clean energy, and creating jobs and skills training for the transition. In this respect, AIDOSec will contribute to promoting sustainable industrialization, i) by improving the efficiency of the engineering process via automation supported by MDE and AI/ML techniques (see AIDOSec contributions to CST 2.1 and CST 2.3) and quality of the engineered systems (see AIDOSec contributions to CST 2.2 and the contributions of AIDOSec use cases to the ECS SRIA KAAa in Section 2.1.2.2).

Similarly to the Green Deal proposed by the European Union, the Sustainable Development Goals (SDGs) set in the 2030 Agenda for Sustainable Development by the United Nations and related Targets are considered by AIDOSec:

- **SDG 9** (Industry, Innovation and Infrastructure), **Target 1** (Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all) improving wireless security solutions and their development cycle towards developing quality and reliable infrastructure in the field of telecommunications; **Target 4** (By 2030, upgrade infrastructure and retrofit industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies and industrial processes, with all countries taking action in accordance with their respective capabilities) by aiming to reduce SWAP costs (Size, Weight And Power) in avionics making it more sustainable; **Target 5** (Enhance scientific research, upgrade the technological capabilities of industrial sectors in all countries, in particular developing countries, including, by 2030, encouraging innovation and substantially increasing the number of research and development workers per 1 million people and public and private research and development spending) by enhancing research and encouraging innovation in the automotive industry (virtual rear-view mirrors, safety-critical railway real-time traction control systems, secure smart sensors for traffic monitoring systems, secure port applications). See AIDOSec contributions to KAA 3.1 - Mobility and KAA 3.2 - Digital Industry.
- **SDG 11** (Sustainable Cities and Communities), **Target 2** (By 2030, provide access to safe, affordable, accessible and sustainable transport systems for all, improving road safety, notably by expanding public transport, with special attention to the needs of those in vulnerable situations, women, children, persons with disabilities and older persons) by contributing to i) traffic monitoring via secure smart sensors for traffic

[95] www.eclipse.org
[96] www.keptn.sh

monitoring systems, and ii) maritime mobility enhancing the quality and security of port applications. See AIDOSec contributions to KAA 3.6 - Digital Society.

- **SDG 3 (**Ensure healthy lives and promote well-being for all at all ages), **Target 8** (Achieve universal health coverage, including financial risk protection, access to quality essential health-care services and access to safe, effective, quality and affordable essential medicines and vaccines for all) by streamlining the development of secure health-care services. See AIDOSec contributions to KAA 3.4 - Health and Wellbeing.

6. **Strengthening the uptake of research and innovation in society**

Horizon Europe aims to involve citizens in research, building a knowledge-based society. Open science promotes citizen participation, increasing societal relevance and trust. R&I missions mobilise citizens in co-design and co-creation, stimulating societal uptake of innovative solutions. In AIDOSec, industrial use cases (see the contribution of AIDOSec use cases to the ECS SRIA KAAa described in Section 2.1.2.2) target different groups including auto/train drivers, auto/train passengers , pedestrians, doctors and patients, port personnel, and, more in general, people connected in safety and security-critical scenarios (a detailed descriptions of AIDOSec target groups will be provided in the FPP). Due to the increased data processing capabilities of complex industrial systems (vehicles, ships, ports, roads, and communication infrastructure), AIDOSec will contribute to promoting the awareness of cyber-security threats among the involved target groups. In this regard, MDE and AI/ML techniques will help automating complex tasks to tame the complexity of engineering tasks[97].

2.1.2.3 Economic/Technological Impact

AIDOSec technology facilitates the design and development of secure, safe, reliable and adaptive systems (see contributions to the ECS SRIA 2024 in Section 2.1.1). The Project fosters innovation in different domains, and in particular it is expected to contribute to the impacts on Automotive, Railway, Traffic Monitoring, Maritime, Public Security, Aerospace, Health Monitoring, Secure Communication, and Efficient Testing, (according to the partners' business as described in Section 2.1.1.2) supporting the ***Main Common Objective 2: ensure EU digital autonomy through secure, safe and reliable ECS supporting key European application domains*** and ensuring "*security, privacy-by-design and strategic autonomy all along the industrial and digital value chains*". Besides the expected wider impact, AIDOSec is expected to have an immediate impact at consortium level:

- ***AIDOSec is an enabler for Large Enterprises*** since the average expected impact on human resources for new personnel hired.
- ***AIDOSec is an enabler for SMEs*** since it improves competitiveness in terms of the quality of products and services offered, responsiveness to customers' needs, and time to market.
- ***AIDOSec is an enabler and opportunity for Academia*** to improve their presence, research and activities in SecDevOps-related areas.

In the following, we briefly discuss a summary of AIDOSec economic and technological impacts. Details with reference to the ECS SRIA 2024 are reported in the Section 2.1.1, while details at the partner level are reported in the Section 2.1.3.

7. **Generating innovation-based growth**

AIDOSec is an enabler for strengthening competitiveness and growth. Academic and Research institutes are particularly interested in **improving their scientific and technology competencies**, **enriching their expertise**, increasing their **teaching offering** and consolidating their **position in the scientific communities**. The most mature results are exploited through **technology transfer activities**, to foster new collaborations and research projects. For industrial partners, AIDOSec is a way to **improve their industrial position**, enriching their **technology offering** to customers and **entering new markets**.

8. **Creating more and better jobs**

[97] The positive market forecast for Low-Code Development Platform (LCDP) suggests a growing interest and benefit of MDE techniques in involving citizen developers into software engineering tasks (Gartner Forecasts Worldwide Low-Code Development Technologies Market to Grow 20% in 2023) .

Innovative technologies lead to complex systems (e.g., embedded and cyber-physical systems (ECPS) and embedded and cyber-physical systems of systems (ECPSoS)) that need fewer operators (due to AI and automation) but require higher levels of personnel skills. The activities in AIDOSec contribute to the **acquisition of new skills and competencies** that allow companies to **create better jobs**. At the consortium level, AIDOSec contributes both to **favouring the growth of companies**, allowing them to hire new employees, and **increasing the network of universities** that, in turn, can have **more and better collaboration** in the context of research projects and can attract the **interest of new researchers and PhD students**. AIDOSec will organise training activities about cyber-security (see Section 1.2.2.6) and AI (see Section 1.2.2.7) to promote awareness and study the interplay between these two aspects.

9. **Leveraging investment in research and innovation**

AIDOSec is leveraging MDE, which is a foundational practice to reduce complexity by **raising the level of abstraction**. This approach can be **tailored to different target groups** ranging from experts (e.g., software/system engineers) to citizen developers (via Low Code Development Platforms (LCDP), being **flexible with respect to their needs** and their expertise. This contributes to **facilitating systems designs and development, and the update of legacy systems**. To support the uptake of new methods and technologies, the AIDOSec project will include **training activities to transfer new knowledge** to the personnel, system producers and technology end-users, preparing the next generation of knowledge-workers that will take over the use of the new technologies, **improving skills of the labour force on innovative technologies**.

2.1.3 Impact on consortium partners

This section collects the evaluation and the expectation of each partner about the impact of the AIDOSec project on each one's business. Among the 40 partners involved in the project there are 9 Large Companies, 14 SMEs, 13 Academia and R&D Organisations institutes creating the right balance between the consolidated experience of the industrial partners and the knowledge base of research and academic partners. The discussion addresses the required themes of competitiveness, growth, sustainability and innovation.

Competitiveness, growth, sustainability and innovation for LEs. In summary:

- **Competitiveness**: The AIDOSec project is expected to help partners strengthen their competitiveness by improving product quality, reducing time to market, and increasing market share. The secure and dependable AI-based DevOps framework will enhance cyber-security and support digital transformation.
- **Growth**: Partners expect the AIDOSec project to support their growth by enabling them to develop new products and services, enter new markets, and attract new customers. The project will also help partners to increase their revenue and profitability.
- **Sustainability**: The AIDOSec project is expected to help partners reduce their environmental impact by optimising resource usage, reducing waste, and promoting sustainable practices. The project will also support partners in meeting their sustainability goals and complying with environmental regulations.
- **Innovation**: Partners expect the AIDOSec project to enhance their innovation capacity by providing them with new tools and methodologies for developing AI-based solutions. The project will also support partners in fostering a culture of innovation and collaboration within their organisations.

Large Enterprise (LE)
AR

Strengthen competitiveness 1. Dependability is necessary for any real-time AI implementation in a railway context. AI can enable data-driven control insights to augment physics-based control methods, thereby taking into account population variance in fleets of trains and operational variance between train mission profiles. This could help usher in unprecedented possibilities for train performance, energy and resource consumption, and overall life cycle costs, providing a strong competitive advantage in the market. 2. In a shared electric powertrain test lab environment that Alstom is developing, cybersecurity is a key concern, not least when AI is used to process measurement data etc., to avoid malicious or human error-driven security breaches. A trustworthy data-sharing infrastructure among clients and partners will improve both the attractiveness of the test facilities and help accelerate e-mobility transformation.
Strengthen growth By offering new control solutions based on dependable AI for railways as well as expanding the test lab capacity and capability, Alstom could strengthen its position in markets where whole life cycle cost is a key buying criteria such as Europe. The adoption of new data-driven real-time control technologies will also require new capabilities and competencies among existing employees and the possibility for new recruitment.
Strengthen sustainability Railways is the most sustainable mode of transportation in terms of capacity efficiency. By increasing the energy efficiency, performance, reliability and life cycle cost, a more rapid shift to this mode of transportation could be achieved, which in turn would reduce the environmental footprint of the whole transportation sector. Alstom's open electric powertrain test lab with dependable shared data infrastructure will help accelerate the transition to electrification in other modes of transportation, not least for heavy road transports.
Improving innovation capacity and the integration of new knowledge Alstom envisions that dependable AI in railway traction systems will result in improved operational efficiency, not least concerning energy efficiency. Similarly, dependable AI in open testing environments will result in increased lab test capacity for a greater number of clients.
DT
Strengthen competitiveness AIDOSec will help Dynatrace to better understand the requirements of SecDevOps in industrial environments, specifically regarding the analysis and management of known vulnerabilities in software. Dynatrace aims to strengthen its knowledge in this space and transfer it into novel product features.
Strengthen growth AIDOSec will help Dynatrace’s industrial growth by providing insights and learning about the requirements of SecDevOps within other industries and organisations. Those insights can then be used to develop novel product features that will help Dynatrace to increase its market share within that space.
Strengthen sustainability The prevention of cyber-attacks, especially at an early stage, has a significant positive impact in terms of sustainability, by protecting critical infrastructure and saving the resources otherwise required to recover from a cyber-attack.
Improving innovation capacity and the integration of new knowledge AIDOSec will help Dynatrace to research base technologies for the development of innovative product features in the area of SecDevOps.
GTS
Strengthen competitiveness With extensive international experience in all aspects of transport automation, GTS is a world leading supplier of railway safety technology, such as train control, train management systems and integrated communications technology for trains. The product range includes interlocking systems, train protection in line with the ERTMS/ETCS specifications, automatic shunting systems, CheckPoints for automatic trackside condition monitoring of trains and maintenance and repair systems. The novel IPS cloud to be developed for supporting cloud readiness of the above mentioned products is a significant step for ensuring the competitiveness of these products in the future, as the market is now shifting

into the direction of cloud operation. Technologies developed in AIDOSec specifically related to Objective 3 on observability and diagnosability will strengthen this approach and thereby the position of GTS on the global market.
Strengthen growth The rail transport market is expected to grow at a compound annual growth rate (CAGR) of 6.5% over the next five years. A major driver behind this is the ongoing increase in competitiveness against other transportation markets is the reduction in carbon footprint as well as reduction in operational cost, where again a major driver is the ability to operate large networks in the cloud. Technologies developed in AIDOSec will ensure the uptake of such safe and secure railway cloud operation.
Strengthen sustainability Railway cloud operation is a large booster to sustainability due to the highly reduced carbon footprint as well as reduced amount of server housing. This is paired with the sustainability aspect of the railway domain itself, where growth in terms of shift from other transportation domains such as automotive or avionics automatically leads to a reduction in carbon footprint.
Improving innovation capacity and the integration of new knowledge GTS plans to integrate technologies, tools and methodologies developed in AIDOSec into their development process enabling the uptake of the innovation capacity from the different technology providers into the railway domain.
INT
Strengthen competitiveness Intecs Solutions (INT) is mainly active in the vulnerability assessment in the automotive domain, commonly referred to as Automotive Cybersecurity. This market includes various services that aim to protect vehicles from cyber threats, such as vulnerability assessment, penetration testing, risk assessment, and incident response. In particular, Intecs is providing professional services for vulnerability assessment and risk assessment for its customers. The tools that will be developed in this project will improve the efficiency of the services and will contribute to expanding the same services in different domains such as railway.
Strengthen growth INT will exploit AIDOSec project results and the acquired knowledge for increasing its technical lead and competitive edge in its core domains, and for opening up domains where AIDOSec technologies are essential for the development of trusted and reliable systems. In fact, the tool can be applied to different domains, and it will help INT in extending its core domains, but also its product portfolio. Thus, INT expects AIDOSec to increase its visibility, competitiveness and the returns in terms of service offers for the usage, support, training, tutoring and provision of customizations and extensions in the Automotive and Railway cyber security markets.
Strengthen sustainability The project will provide enabling technologies and will enrich the company portfolio in the cybersecurity domain.
Improving innovation capacity and the integration of new knowledge The Innovation introduced by AIDOSec will enlarge INT's portfolio, and it will open up to new domains. In addition to strengthening the skills and the competencies in the domains in which INT is already active, and thus to enlarge its business in these domains, it will increase its business by applying the innovation in other new domains, such as the railway one.
KAPSCH
Strengthen competitiveness Integration of penetration testing early in the secure development life-cycle using the shift-left methodology to secure all layers of product development prior product release leads to a reduction of total solution life-cycle costing while increasing security.
Strengthen growth Innovation in security practices is essential for securing growth, as they enable secure operation of critical infrastructure in an increasingly harsh environment.

Strengthen sustainability
Intelligent Transportation Systems have a positive impact on reducing traffic related emissions. Securing these solutions is part of the critical infrastructure to ensure uninterrupted operation strengthens environmental sustainability.

Improving innovation capacity and the integration of new knowledge
This project will allow us to develop strategies to address the cyber-attacks facilitated by AI technologies, ensuring our systems are resilient against both their completeness in attack scenarios as well as their increased volume.

MSG

Strengthen competitiveness
To strengthen our competitiveness, our strategic objective is to leverage our in-house fundamental cybersecurity knowledge across various domains, given that core cybersecurity principles are universally applicable. This cross-domain expertise underpins our initiative in the Harmonised EU-CyberBridge Case Study.

The Harmonised EU-CyberBridge Case Study conducted by msg Plaut is designed to systematically analyze Cybersecurity Standards and Regulations to identify commonalities that can be leveraged for enhanced compliance and cybersecurity across different sectors. The results of this case study will pinpoint aspects of cybersecurity knowledge that are transferable between domains, aiding in the development of a robust cybersecurity framework that supports all cybersecurity-relevant sectors.

Strengthen growth
msg Plaut’s participation in the AIDOSec project is strategically aimed at strengthening our growth through two main avenues:

1. Develop Expertise: We will build on our existing capabilities by training new cybersecurity experts, ensuring our team is proficient with the latest technologies and approaches.
2. Increase Visibility: Our involvement will enhance msg Plaut's recognition within the research community, helping to forge new partnerships and open up additional business opportunities.

Strengthen sustainability
Through the AIDOSec project, msg Plaut will strengthen its market sustainability thanks to the efforts to expand our expertise and establish new partnerships.

Improving innovation capacity and the integration of new knowledge
msg Plaut aims to innovate its cybersecurity standard and regulation database, facilitating the discovery of synergies and enabling efficient knowledge transfer. Currently, these tasks are managed through basic, non-efficient Excel tables. This improvement will not only help reduce human errors by considering a more comprehensive set of regulatory frameworks but will also decrease work effort through automation.

SOFT

Strengthen competitiveness
SOFTEAM and its parent company DocaPoste invests in Modelio, eCitiz, HEVA products and GAIA-X, SecNumCloud initiatives. The project will have a direct impact on those products as it provides enabling technologies and novelties in cyber-security.

Strengthen growth
SOFTEAM and DocaPoste have an ambitious growth goal (10%-20% per year). For that DocaPoste have joined several initiatives such as GAIA-X and SecNumCloud with the renowned expert Guillaume Poupard as the head. AIDOSec will contribute to the growth objectives by improving the company's capabilities, product and service offering. In particular, SOFTEAM will develop tools for modelling and threat analysis, automation of security requirements analysis and compliance validation. In addition, SOFTEAM will promote the AIDOSec framework that provides complementary solutions on monitoring and detection of security vulnerabilities and anomalies in a continuous manner.

Strengthen sustainability The project provides enabling technologies and strengthens the company's capacities in cyber-security.
Improving innovation capacity and the integration of new knowledge SOFTEAM strives to produce trustable products and services for citizens, government agencies and other organisations. The project contributes to strengthening SOFTEAM positions in its core markets and enables new services in the cyber-security domain. In particular, the development in the AIDOSec will contribute to the novel product line by DocaPoste on intelligent secure backup and archiving addressing the SME market.
THA
Strengthen competitiveness AIDOSec will provide the needed technology to introduce mixed critical communication in THALES real-time systems, while providing security guarantees. This technology will be introduced in the space domain (satellites, ground stations), in avionics, in maritime domain and air traffic management.
Strengthen growth We expect to reduce the cost of the deployment of our embedded networks by 50%, thanks to the merging of various networks of different communication criticality levels. This will reduce the certification and maintenance costs. This will also address the specific needs of new customers and markets (e.g drones).
Strengthen sustainability Merging several networks in one single safe and secure network will allow to significantly reduce the weight and volume in several critical real-time systems. As an example, today there are more than 500 km cables in an airbus 380. As a direct consequence, the need for energy to operate the aeroplane will be drastically reduced.
Improving innovation capacity and the integration of new knowledge The innovation introduced by AIDOSec will bring a breakthrough to design and to maintain secure mixed critical networks, which allows THALES to develop innovative products and reduce our impact on the environment.
UST
Strengthen competitiveness CyberSecurity Framework based on tactics, technical and procedures that cybercriminals use. As developments become more reliable, the speed of delivery will improve the time to market of software assets produced. In a production phase, downtime expected from successful attacks should be reduced to minimal, resulting in better availability than without AIDOsec methodologies used.
Strengthen growth UST expects a 30% growth margin due to a newly opened opportunity that lies in the development and improvement of a strategic roadmap that defines the type of tests and tools to be used adapted to be further replicated to our client's needs and restrictions.
Strengthen sustainability Throughout the complete SecDevOps transformation framework, UST can achieve an optimization use of the human workforce.
Improving innovation capacity and the integration of new knowledge Addressing the various use cases presented by the other partners will allow UST to introduce and validate new tools that provide solutions for the diverse needs posed by the rest of the partners. It will also enable participants from UST in the project to acquire and foster a culture focused on security. As experts in security testing, this will allow us to create a knowledge ecosystem that can be extended to the rest of the teams at UST.
WMO
Strengthen competitiveness In the project, WMO aims to speed up the requirements, design, and validation feedback processes. After the project, WMO will develop new products faster, they will be better tested, and they will be more secure. This will reduce time-to-market and increase competitiveness in a changing market.

Strengthen growth Customers in market segments such as energy or rail require a rigorous software development process. Here, compliance to cyber security standards such as IEC 62443 will likely be mandatory in the coming years. By strengthening the development process while also fortifying cybersecurity, WMO will be able to continue to grow in these markets
Strengthen sustainability One of the main sustainability perspectives of WMOs use case is that of reduced waste. Typical customer installations are in the areas of digitalization (e.g. energy market), or urbanization (e.g. public transport) that drive society's green transition. From a company-internal perspective, improving requirements processes, less time is needed to understand what the correct product ought to be. With model-based approaches and earlier simulations in the design phase, fewer incorrect design decisions will be made, and fewer rounds of prototyping will be needed. Finally, from a cyber-security perspective, if a security issue would make its way to a customer installation, then a security hotfix is needed. If the site is remote or active, then shutting it down for patching can be costly or mean loss of productivity and thus waste. In the end, improved cybersecurity leads to decreased downtime, and reduced waste
Improving innovation capacity and the integration of new knowledge Through the project, WMO expects to learn about, prototype, implement and/or integrate AI-powered tools for requirements and monitoring. WMO also aims at introducing model-based systems engineering for early validation in the product design phase. WMO also strives for increased knowledge among colleagues not involved in the project, e.g. by active participation in project Hackathons, by supervising thesis students, and by inviting guest lecturers from project partners to present results that are not our focus area in the project.

Competitiveness, growth, sustainability and innovation for SMEs. In summary:

- **Competitiveness**: By adopting SecDevOps practices, SMEs can improve their competitiveness by delivering high-quality, secure software at a faster pace. This can help them stay ahead of their competitors and meet the demands of their customers.
- **Growth**: The adoption of SecDevOps practices can also help SMEs grow by enabling them to scale their operations and deliver more software products at a faster pace. This can help them expand their customer base and increase their revenue.
- **Sustainability**: By integrating security into the development process, SMEs can reduce the risk of security breaches and improve the sustainability of their operations. This can help them avoid costly security incidents and maintain the trust of their customers.
- **Innovation**: The adoption of SecDevOps practices can also help SMEs foster a culture of innovation by encouraging collaboration and communication between developers and operations teams. This can help them develop new ideas and improve the way they code and operate their software.

Small and Medium Enterprises (SME)
ABI

Strengthen competitiveness
In AIDOSec, Abinsula targets the automotive market, in which the current Abinsula's offering covers all systems from the low level up to the entire infotainment system. In recent years, at least at demonstration or prototype level, the demand for 'video' technologies inside the passenger compartment has grown enormously, often requiring the union of cluster systems with those of infotainment, with consequent problems of security, safety and optimised management of resources.
One of Abinsula's goals is to bring innovation ready for the market: the current Virtual Rear Mirror PoC is meant to be enriched with new features for the adaptive and cyber-secure vision, based on the AIDOSec Cybersecurity Solutions (e.g., AIDOSec threat modelling) and the know-how acquired in the project. The results obtained by Abinsula in the AIDOSec project will be another step, in line with Abinsula strategy, for the competition of the new commercial offer for secure automotive systems based on smart cameras. This new offer will allow Abinsula to consolidate itself in the automotive market through innovative solutions that will then be verticalized for the various customers. Results will then be exploited also in other markets as the precision agriculture and healthcare markets. The main considered target groups will be:
Tier 1 and car makers in the automotive market

Tier 1 for precise agriculture market

Strengthen growth
Abinsula is a TIER 2 in the automotive market, and it is an official supplier of embedded software for important world leaders in this market (e.g., Magneti Marelli, FCA, CNHi, TATA, BMW). Abinsula also counts among its customers, leading ICT companies (e.g., Topcon-Tierra, Applix, Seat, Pagine Gialle, Samsung, Tata Consulting). Abinsula is able to provide best in class service and to reduce cost and time to market thanks to its expertise and semi-products.
In 2021 (most recent official data currently available), Abinsula's turnover was around 7 million Euros (Abinsula group overall is more than 10 million Euros). AIDOSec results will contribute to strengthen Abinsula competitiveness and growth, allowing the company to increase its offering to customers and to open new business opportunities. This will lead, at the end of the project, to an estimated growth of 10% in terms of marginality and 25% in terms of profitability margins. Currently Abinsula counts around 80 employees, and it is expected to grow about 10% each year.

Strengthen sustainability
The demonstration of the cybersecurity technologies developed in the proposed AIDOSec project will allow Abinsula to reaffirm its presence in the automotive market with cutting edge and secure offerings, contributing to its sustainability.

Improving innovation capacity and the integration of new knowledge
Abinsula aims at innovating its processes with the new tools and methodologies that will be used, in the development phase, to formalise and model the possible threats and the attack surface of a system. Currently, these tasks need high human expertise and the aid of tools and methodologies could, on one hand, help to reduce human errors, considering a more complete set of threats, on the other hand, reduce the work effort by means of automation.

ACORDE

Strengthen competitiveness
While ACORDE is a recognized player in RF equipment design and manufacturing, recent research and development efforts have provided ACORDE with the capability to offer to different customers and partners different types of monitoring and positioning solutions. For ACORDE, it is imperative to adapt and improve its design and implementation processes to cover security in all phases, from solution conception to its final validation and operation, while keeping sufficiently efficient and cost-effective. This will enable ACORDE to keep their solutions competitive not only in performance and price, but also in the aforementioned terms of security, once security has become a necessity instead of an additional benefit.

Strengthen growth
AIDOSec is a chance to strengthen current researched solutions to offer monitoring/positioning solutions to stakeholders of critical infrastructures in different domains, e.g., renewable energy, ports, etc. In projects like AIDOaRt, resilient monitoring and positioning solutions are being developed, after investigating the options offered by different technologies for positioning and for AI/ML performance data analysis. A full resilience cannot be really offered without covering the security of the monitored and positioning data, with the holistic coverage aimed at AIDOSec.
Moreover, the participation of ACORDE in AIDOSec shall be an incentive to attract security experts to the company. The company is making an effort, in the process of interviewing and attracting these types of experts, which is an even bigger challenge for an SME. Participation in specific projects like AIDOSec, with high innovation potential, able to offer perspectives and challenges to this type of professionals is a clear help for a company like ACORDE to adhere to this necessary type of talent.

Strengthen sustainability
As mentioned, the innovations and know-how expected from AIDOSec will bring optimised resilience to the monitoring & control, and thus to overall systems in applications like renewable energies. This will have a direct impact in the immediate ACORDE environment, like the solar plants currently being serviced by ACORDE monitoring systems. The resilience of such monitoring systems will impact the resilience of these plants, and thus the perception of renewable energies as mature, robust and trustable energy sources.
More specifically, ACORDE monitors its own powering, which is expected to help the company to improve its own operation in terms of energy consumption and safety. At the same time, this is sensitive information that needs to be protected, and so where the technologies and lessons of AIDOSec can have direct application.

Improving innovation capacity and the integration of new knowledge
AIDOSec will help with an important transformation and enrichment of its knowledge profile and future targets. ACORDE systems/R&D division is used for the gradual and periodical enrichment of its expertise. However, this time, a clear gain in security expertise on an important part of the personnel, will have a clear traversal exploitation in the company. It shall help to cover a clear knowledge needed in the provision of IT services provided by the company (to third parties and to itself), and even to the growing demands on the monitoring & control of the RF equipment designed and manufactured in other divisions of the company. Moreover, as was explained, the AIDOSec know-how and experiences are perceived as enablers for truly competitive industrial monitoring and positioning solutions, thus with feasible exploitation.

CAMEA

Strengthen competitiveness
Having secure smart sensors is definitely a big competitive advantage. There is a big demand from municipalities for various traffic monitoring systems based on cameras and radars. Security and safety even in these systems is becoming a hot topic and it can be requested in tenders in the future.

Strengthen growth
The same way as industrial competitiveness, industrial growth is expected if we have good products for traffic monitoring tasks allowing us to win tenders.

Strengthen sustainability
Using smart standalone smart sensors can significantly reduce power consumption on the site. This allows battery or solar power operation of the sensors.

Improving innovation capacity and the integration of new knowledge
The biggest innovation expected is introduction of secure features and non-repudiability mechanisms embedded within the sensors.

COG

Strengthen competitiveness
AIDOSec will bring a new level of flexibility in the SCMP product line installed and operated by our customers. New products and services will take advantage of the secure communication and machine learning model updates that will guarantee a seamless and secure process of model regular adaptation and updates.

Strengthen growth
AIDOSec will enable Cognitechna to grow faster, the new security options will be primarily used in our own product lines and services. However, an opportunity also lies in offering the security-enhancing modules as a plug-in component for cooperating companies in industrial automation, agricultural business, healthcare, and social services. We will also be able to address specific requirements of the security/intelligence service customers (we have several established links to potential European customers through our cooperation with the Czech Ministry of Interior Affairs.

Strengthen sustainability
One of the key lines of the R&D activities in the project will involve energy-aware security processing. Indeed, current technology cannot employ even the basic algorithms on-site (e.g., on-edge devices collecting data from local IoT sensors) as this processing would consume too much processing power and energy. The AIDOSec development will enable optimising the security algorithms and methods for low-power devices, so it will lead to more sustainable solutions.

Improving innovation capacity and the integration of new knowledge
As Cognitechna is still a startup company, the project has a great potential to significantly boost our innovation capacity and integrate the newly developed knowledge to almost all our current and future product lines. Our company business will be able to keep the competitive edge in the area of secure computing, which is becoming more and more important, especially in non-European markets in which we operate (South Korea, Arabic countries, Kenya, etc.).

HAL

Strengthen competitiveness
Haltian will enhance its expertise and innovation capacity in the fields of AI, cybersecurity, and IoT. AIDOSec will also enable Haltian to offer more secure and reliable products and services to its customers, differentiate itself from its competitors, and access new markets and opportunities.
The AIDOSec program will address the main challenges and needs of the IoT market, such as data protection, privacy, trust, and resilience. The program will leverage the latest advances in AI techniques, such as deep learning, federated learning, and explainable AI, to provide intelligent and adaptive security solutions for IoT devices and data. The program will strengthen competitiveness by refining anomaly detection methodologies, enabling us to offer superior solutions to clients and setting us apart from competitors The program will also follow the best practices and standards for cybersecurity and IoT, such as the EU Cybersecurity Act, and the GDPR. By doing so, the program will ensure that the security solutions are compliant, interoperable, and scalable.
Through the AIDOSec program, Haltian will gain a competitive edge over its rivals in the IoT market. Haltian will be able to offer its customers state-of-the-art security solutions that are tailored to their specific needs and contexts. Haltian will also be able to demonstrate its commitment to security and trust, which are essential factors for customer satisfaction and loyalty. Moreover, Haltian will be able to expand its portfolio and reach new segments and regions, such as the public sector, the healthcare sector, and the US market. By participating in the AIDOSec program, Haltian will boost its competitiveness and growth potential in the IoT market.

Strengthen growth
The AIDOSec research program is a European initiative that aims to develop innovative and secure solutions for AI-driven cyber-physical systems, which are systems that integrate computational and physical components, such as smart buildings, smart cities, and smart factories. These systems are expected to play a key role in the digital transformation of various sectors, such as energy, mobility, health, and manufacturing. However, they also pose significant challenges in terms of security, reliability, privacy, and ethics.
By participating in this program, Haltian will benefit from the collaboration with leading research institutions and industry partners from different countries and domains. This will enable Haltian to access cutting-edge technologies and infrastructures, such as AI platforms, cyber-security tools, and testbeds, that will support its research and development activities. Furthermore, Haltian will gain increased visibility and reputation in the European market, as well as opportunities to network and establish strategic partnerships with potential customers and stakeholders. The project will strengthen Haltian’s growth by expanding our service offerings and providing access to new markets through its advanced capabilities of secure systems.
Moreover, Haltian will leverage its expertise in IoT device design and development, cloud services, and data

analytics to create new products and services that meet the needs and expectations of the end-users and customers of AI-driven cyber-physical systems. Haltian will apply its user-centric and co-creative approach to design and develop IoT devices that are secure, reliable, and easy to use, as well as cloud services that are scalable, interoperable, and compliant with data protection regulations. Haltian will also use its data analytics capabilities to provide insights and value-added services that enhance the performance, efficiency, and sustainability of AI-driven cyber-physical systems.
The AIDOSec research program will thus strengthen Haltian's growth by enhancing its innovation capacity, competitiveness, and differentiation in the IoT domain. Haltian will be able to offer solutions that address the current and future challenges and opportunities of AI-driven cyber-physical systems, and that create value for its customers and end-users. Haltian will also be able to expand its market share and reach new segments and regions, as well as to foster its organisational learning and development.

Strengthen sustainability
Haltian is committed to creating a positive impact on the environment, society and governance (ESG) through its innovative products and services. The AIDOSec research program, which aims to develop a novel AI-driven framework for secure and trustworthy IoT systems, aligns with Haltian's ESG goals in several ways. First, AIDOSec will enhance the energy efficiency and reliability of IoT devices, reducing their carbon footprint and environmental impact. Second, AIDOSec will improve the privacy and security of IoT data, protecting the rights and interests of users and stakeholders. Third, AIDOSec will foster the development of new IoT applications and solutions that can address societal challenges and create value for customers and partners. By participating in AIDOSec, Haltian will demonstrate its leadership and excellence in the field of IoT and contribute to the advancement of sustainable and responsible technology.

Improving innovation capacity and the integration of new knowledge
Haltian is a leading IoT and product development company that provides end-to-end solutions for smart devices, wireless sensors, and cloud services. Through the AIDOSec research program, Haltian aims to enhance its innovation capacity and the integration of new knowledge in the fields of AI, cybersecurity, and IoT. AIDOSec will enable Haltian to develop novel AI-based methods and tools for securing IoT devices and networks, as well as to create new value-added services and business models for its customers. By collaborating with leading research and industry partners in the AIDOSec consortium, Haltian will gain access to cutting-edge scientific and technological expertise, as well as to new markets and opportunities. AIDOSec will also foster Haltian's internal R&D capabilities and human resources, as well as its involvement in the European innovation ecosystem.
AIDOSec will improve Haltian's innovation capacity and the integration of new knowledge in several ways. First, AIDOSec will provide Haltian with a comprehensive framework and a set of best practices for developing secure and trustworthy AI solutions for IoT. This will enable Haltian to apply state-of-the-art AI techniques, such as machine learning, deep learning, and natural language processing, to enhance the functionality, performance, and usability of its IoT products and services. Second, AIDOSec will allow Haltian to leverage the latest advances in cybersecurity, such as encryption, authentication, and anomaly detection, to protect its IoT devices and networks from malicious attacks and unauthorized access. This will increase Haltian's reputation and credibility as a reliable and secure IoT provider, as well as its compliance with the relevant regulations and standards. Third, AIDOSec will help Haltian to create new value-added services and business models for its customers, such as predictive maintenance, data analytics, and smart automation. This will enable Haltian to offer more customized and differentiated solutions that meet the specific needs and preferences of its customers, as well as to generate new revenue streams and competitive advantages.

HIB

Strengthen competitiveness
HI Iberia will increase its industrial strength by improving its solution REVITA through its transition from an informal DevOps model to an integrated SecDevOps with an emphasis on better testing of the hardware/software assets and increased security by design .The solution has currently some built-in security, but since it is a medical device, we need to ensure it maintains security and improves it with regard to well-known requirements for IoT security (e.g., OWASP, ISO/IEC 27400:2022, ENISA).

Strengthen growth HI Iberia will increase its industrial growth by improving its telemonitoring solution. Adherence to a strong, security-focused branding such as AIDOSec that incorporates the most relevant security standards can be of much help for an SME to sell their products throughout the EU.
Strengthen sustainability The current product used as a basis for the Health and Wellbeing use case (REVITA) has security built in a manual manner and does not conform to a specific security-aware process. By its usage in AIDOSec, HIB expects that the product will be not only more secure but, by applying a consistent process, we will increase its sustainability in the longer run: less specific security effort that require particular skills by one specialist developer and a better process that enables all members of the team to contribute to security.
Improving innovation capacity and the integration of new knowledge AIDOSec will introduce innovative methodologies and solutions following the SecDecOps philosophy that allow security to be considered from the design phase through to the operations phase.
INNORIV
Strengthen competitiveness As a SME, Innovation River is interested in enhancing its competencies in technology point of view. Innovation River aims to mature and scale its current methodology and technology in the domain of Security DevOps. We expect that the AIDOSec Project will improve the competitiveness in InnovationRiver's industrial sector by optimising development processes on complex systems through the use of the paradigm of continuous development and continuous integration using security aspects in the early stage of continuous system and software development.
Strengthen growth INNORIV expects that the AIDOSec Project will strengthen the industrial growth in terms of opportunity in the cybersecurity market and will involve new specific customers.
Strengthen sustainability There will be an improvement in the environmental impact and energy savings because the production processes of complex industrial systems will be significantly reduced and simplified using distributed cloud secure environment solutions.
Improving innovation capacity and the integration of new knowledge Cybersecurity growth is not only a response to the escalating frequency and sophistication of cyber threats but also a proactive stance in safeguarding sensitive data and digital infrastructure. This growth encompasses the continual evolution of defensive strategies, the development of advanced encryption techniques, and the deployment of cutting-edge intrusion detection systems to fortify digital defences.
LIE
Strengthen competitiveness LIE globally available modelling tools will profit from the innovations that will be developed in the scope of this project. In particular, finding an efficient way for continuous engineering with DevOps will increase the efficiency of the modelling frameworks and infrastructure provided by LieberLieber. Also, the existing products, such as LemonTree (lifecycle management of models), can be expanded with AIDOSec methods, which will raise its competitiveness in the market.
Strengthen growth AIDOSec will improve the attractiveness of our professional MBSE services as well as our tools such as LemonTree. In particular, new business opportunities will open up due to the gained knowledge in engineering continuously in a model-based way. This will allow us to hire new personnel and implement our growth strategy.
Strengthen sustainability By using efficient engineering methods rather than a real duplicate of the system under development, a significant amount of raw material, energy and effort for the creation of a digital system can be saved. In addition, Continuous Engineering of complex systems using DevOps together with MBSE methods leads to shorter release cycles of products and thus reducing resources needed in the whole development cycle.

Improving innovation capacity and the integration of new knowledge Due to the gained knowledge of using DevSecOps in engineering complex systems our capacity for designing innovative solutions for our customers will be improved. The innovative results of AIDOSec can easily be disseminated inside LieberLieber via our global expert community and partner companies.
PG
Strengthen competitiveness AIDOSec helps PG to research and enhance the in-build cybersecurity capabilities in our product platform targeted to various industrial operators.
Strengthen growth AIDOSec can make improvements to their product, and possibly also creating partnerships across the consortium, training and hiring new personnel.
Strengthen sustainability PG customers use their platform for optimising their production and this way reducing the waste in material handling, energy and water consuming and other areas with environmental impact.
Improving innovation capacity and the integration of new knowledge Implementation of the AI supported communication framework for data sharing between different systems and services that can be used in security-critical infrastructure.
PRO
Strengthen competitiveness Thanks to AIDOSec, Prodevelop will be able to improve its application development cycle with the implementation of SecDevOps best practices and specific tools. Therefore, Prodevelop will not only produce better software at lower cost in a more agile way, but also develop higher quality, and more reliable and secure software. These advantages will enable us to be in a better competitive position with respect to our competitors.
Strengthen growth Most of the projects that Prodevelop carries out are obtained through tenders. It is increasingly common for clients to demand DevOps-based development cycles, cloud deployments and strict security measures throughout the development process and not just in the operations phase. Thanks to AIDOSec, Prodevelop will gain a great advantage over its competitors, which will allow it to be better valued in tenders and increase its success rate. In addition, Prodevelop is currently in a growth phase, and we are convinced that thanks to the knowledge gained in the project, this trend will continue and new employees will be recruited.
Strengthen sustainability Thanks to the SecDevOps methodology from AIDOSec, Prodevelop will be able to securely develop and deploy better software in fewer hours with the minimum computing resources. For instance, Prodevelop will be able to develop solutions that scale based on real-time demand, allowing it to optimise resources and reduce energy consumption and carbon footprint, as well as the cost of developing and maintaining solutions.
Improving innovation capacity and the integration of new knowledge Thanks to AIDOSec, Prodevelop will be able to improve its application development cycle with the implementation of SecDevOps best practices and specific tools, leading to a more agile methodology, and allowing the company to manage a larger amount of projects, products and customers.
SC

Strengthen competitiveness

AIDOSec will produce and enhance Use Case Analysis, the involvement in defining use case requirements, scenarios, and data collection for AI-based, CyberSecurity-Based, and XR-based solutions will allow SC to have a comprehensive understanding of the manufacturing industry's needs. This will enable them to tailor the products and services more effectively to meet industry demands.

Within advanced Threat Intelligence & Automation, SC contribution to the design and development of AI-based AIDOSec threat intelligence and analysis solutions will position them at the forefront of cybersecurity innovation. This will enhance product offerings, making SC more competitive in the market.
SC role in integrating the results of various work packages and developing use cases ensures that the solutions are holistic and encompassing. This integration capability can be a unique selling point, making their services more attractive to potential clients.
SC commitment to running various validation and evaluation scenarios for security-critical solutions/tools will ensure that the products are robust and reliable. This will boost the reputation in the market, leading to increased trust and credibility.

IPR Management: SC involvement in analyzing exploitable results and defining Intellectual Property Rights (IPRs) will ensure that we have a competitive edge in terms of proprietary technology and solutions. This can lead to market leadership as they can offer unique solutions that others cannot replicate easily.

Impacted Products/Services:
- AI-based solutions for threat intelligence and analysis.
- CyberSecurity-based solutions tailored for manufacturing industries.
- XR-based solutions for the Manufacturing Industries Use Case.

Expected Improvement:
- Enhanced security features in our products/services.
- More tailored solutions to meet the specific needs of the Manufacturing Industry.
- Integration capabilities that allow for a more holistic approach to CyberSecurity.

Market Competitiveness & Leadership:
- SC involvement in the AIDOSec project positions them as pioneers in AI-based, CyberSecurity-based, and XR-based solutions for the Manufacturing Industry.
- The commitment to validation, evaluation, and IPR management ensures that products/services are not only advanced but also reliable and unique.
- By addressing the specific needs of the Manufacturing Industries Use Case, SC can establish themselves as market leaders in this niche segment.

Summary: The AIDOSec project will significantly bolster the industrial competitiveness by enhancing the product offerings, ensuring robust validation and evaluation, and positioning us them as leaders in AI and cybersecurity solutions tailored for the Manufacturing Industry."

Strengthen growth

The AIDOSec project will play a pivotal role in strengthening SolidComp Ltd's industrial growth in several ways:

Opportunity to Increase Market Share:
The involvement in the AIDOSec project, particularly in the design and development of AI-based threat intelligence and analysis solutions, will allow them to offer advanced CyberSecurity solutions. This can lead to a competitive edge in the market, attracting more clients and increasing their market share.
By focusing on specific use cases, such as the Manufacturing Industries Use Case, SC can offer solutions that are more tailored to specific industry needs, making them a preferred choice for potential clients.
Opportunity to Involve New Customers:
- Diverse Solutions: their contributions to AI-based, CyberSecurity-based, and XR-based solutions will cater to a broader range of customer needs. This diversity in offerings can attract new customers looking for

comprehensive CyberSecurity solutions.
- Robust and Reliable Products: their commitment to running various validation and evaluation scenarios ensures that our products are dependable. This reliability can be a significant factor in attracting and retaining customers.
Opportunity for Personnel Growth:
- Training Existing Personnel: their involvement in the AIDOSec project will expose their team to cutting-edge technologies and methodologies in AI, CyberSecurity, and XR. This exposure can lead to upskilling and training opportunities for existing personnel, making them more adept at handling advanced projects.
- Hiring New Employees: The growth and expansion resulting from the AIDOSec project can lead to an increased workload and the need for specialized skills. This can result in opportunities to hire new employees, further strengthening our team and capabilities.

Market Competitiveness & Leadership:
- Unique Selling Proposition (USP): their role in analyzing exploitable results and defining Intellectual Property Rights (IPRs) can lead to the development of proprietary technologies and solutions. These unique offerings can set them apart from competitors, providing a strong USP.
- Reputation and Credibility: SC active role in a project as significant as AIDOSec can boost the reputation in the industry. Being associated with a project that aims to revolutionize CyberSecurity solutions can position SolidComp as a leader in the field.

Summary: The AIDOSec project offers SC a golden opportunity to enhance product offerings, expand the customer base, and grow the team. The project will not only increase our market share but also position them as leaders in the industry, offering cutting-edge CyberSecurity solutions.

Strengthen sustainability
The involvement in the AIDOSec project, particularly in AI-based threat intelligence and analysis solutions, will lead to more efficient and secure manufacturing processes. Efficient processes can lead to reduced waste, optimized energy consumption, and better utilization of raw materials.

By focusing on the Manufacturing Industries Use Case, SolidComp can offer solutions that are specifically tailored to the needs of the manufacturing sector. This can lead to optimized manufacturing processes, which in turn can result in reduced energy consumption, minimized waste, and efficient use of resources.

SC commitment to running various validation and evaluation scenarios ensures that the solutions are not only advanced but also reliable. Reliable solutions can prevent costly errors in manufacturing processes, leading to savings in terms of materials, energy, and time.
SC involvement in analyzing exploitable results and defining IPRs can lead to the development of proprietary technologies that are efficient and sustainable. Proprietary technologies can be optimized for reduced energy consumption, efficient use of raw materials, and minimized environmental impact.
The integration of AI-based, CyberSecurity-based, and XR-based solutions can lead to smart manufacturing processes. Smart manufacturing can optimize production lines, reduce waste, and ensure that resources are used efficiently. In addition to the technical and cybersecurity aspects of the AIDOSec project, the indirect implications for industrial sustainability are evident.

Improving innovation capacity and the integration of new knowledge
The involvement in the AIDOSec project, particularly in AI-based threat intelligence and analysis solutions, will allow them to offer advanced cybersecurity solutions tailored to the manufacturing industry's needs. This innovation will ensure more secure and efficient manufacturing processes, positioning SolidComp as a leader in cybersecurity solutions for manufacturing.

The focus on the Manufacturing Industries Use Case means developing solutions specifically tailored to this sector. This targeted approach is innovative as it ensures that the solutions are highly relevant and effective for the manufacturing industry.

The integration of AI-based, CyberSecurity-based, and XR-based solutions into SolidComp's offerings

represents a significant technological leap. These advanced technologies will enable smarter manufacturing processes, optimizing production lines, reducing waste, and ensuring efficient use of resources.

The commitment to running various validation and evaluation scenarios for security-critical solutions/tools ensures that the solutions we offer are not only advanced but also reliable. This rigorous validation process is an innovative approach that ensures the solutions are robust and effective.

SC involvement in analyzing exploitable results and defining IPRs means that they are at the forefront of developing proprietary technologies and solutions. This focus on IPRs ensures that we can offer unique solutions that others cannot easily replicate, giving us a competitive edge.

The integration of advanced technologies and the focus on efficient manufacturing processes means that SolidComp Ltd's solutions will likely lead to reduced waste and more sustainable manufacturing practices. The innovations introduced by the AIDOSec project will position SolidComp as a leader in cybersecurity solutions for manufacturing. The tailored solutions, rigorous validation processes, and focus on IPRs will give us a competitive edge, attracting more clients and increasing our market share.

Summary: The AIDOSec project introduces several key innovations to SC environment and business, positioning us as leaders in cybersecurity solutions for manufacturing and ensuring more sustainable manufacturing practices.

SWA

Strengthen competitiveness
Swascan wants to enrich its expertise in the use of Artificial Intelligence in cybersecurity operations, an area in which the company is a major player in Italy. The collaboration with AIDOSec would allow it to enrich and rethink its cybersecurity tools, currently on the market, with the integration of Machine Learning aimed at greater automation, in the search for vulnerabilities, in limiting false positives, and in interpreting the malicious behaviour of possible attackers.

Strengthen growth
As a cybersecurity company, we think that AIDOSec can be a great cue to develop new solutions for our customers who make significant use of DevOps.

Strengthen sustainability
The possibility of developing new cybersecurity solutions based on an innovative approach such as the one proposed by AIDOSec can be a driver for a greater presence of the company on the market, contributing to its sustainability.

Improving innovation capacity and the integration of new knowledge
AIDOSec aims to approach security in DevOps in a holistic manner, homogeneously addressing the critical aspects involved in this area, using AI and MDE as the glue of the whole process: the process characterised in this way is an important innovation with which Swascan wants to equip some products in its market proposition.

TEK

Strengthen competitiveness
TEKNE aims at perfectionating the industrial process to develop AI based systems. The aspects are technical and organisational, as well as about the security of the collected data. AIDOSec addresses all of them.

Strengthen growth
AIDOSec will improve the factors of industrial growth: technological capabilities, industrial processes, and products. TEKNE will demonstrate the progress in the case study, with an enhanced version of its AI based detectors/classifiers of security attacks on wireless communications, which will be developed using AIDOSec tools and components.

Strengthen sustainability
Not directly applicable, however, the products that the case study considers, detectors/classifiers of attack to

wireless communications, can have impact on safety aspects that depend on security (availability of communication links).

Improving innovation capacity and the integration of new knowledge
Innovative AI-empowered products that address wireless communication security, as well as innovation of industrial development process: DevOps and implementation of an effective pipeline for the continuous development of AI systems.

TL

Strengthen competitiveness
The participation in the AIDOSec project will enable them to contribute our expertise and resources to a collaborative research initiative, working alongside other project participants. TL aims to achieve the following through the collaboration:

- Joint research: Collaborate with other AIDOSec participants on research projects, sharing knowledge and resources to advance the state of security in the global manufacturing sector.
- Technology transfer: Contribute to the development and transfer of innovative technologies and practices related to AI-driven security automation, MDE, and continuous improvement.
- Networking and partnerships: Forge strategic partnerships with other AIDOSec participants, fostering long-term collaborations and strengthening our position within the global manufacturing industry.

Strengthen growth
ThingLink is an innovative platform enabling critical sector customers to create immersive XR (Extended Reality) trainings for safety and onboarding purposes. We recognize the value of collaboration in achieving global success and securing a strong competitive position in the market. To this end, we propose to actively participate and contribute to the AIDOSec project, an AI-driven framework supporting DevOps practices with a strong emphasis on security, tailored to the specific needs of the manufacturing industry worldwide.
By actively participating in the AIDOSec project, we will contribute to and benefit from the following innovations:

- Joint development of AI-driven security automation solutions: Collaborate with other AIDOSec participants to develop and implement advanced machine learning techniques that automate repetitive and time-consuming cybersecurity tasks.
- Collaboration on MDE and AI research: Work together with other AIDOSec participants to advance the state of MDE and AI research, sharing knowledge and best practices to improve abstraction, automation, and security in the manufacturing industry.
- Co-development of comprehensive traceability solutions: Collaborate on the development of advanced traceability solutions that correlate security controls across different DevOps phases, enabling better vulnerability prediction and root cause analysis.
- In collaboration with the AIDOSec project participants, we propose to conduct research, develop prototypes, and create proof-of-concept for security-critical AI-based Solutions tailored to the global manufacturing sector. This will include:
- Collaborative research on the implementation of MDE techniques to improve abstraction and automation in design and development activities.
- Joint development of AI and ML principles to automate cybersecurity tasks and enhance security workflow.
- Collaboration on the development of advanced traceability solutions that integrate with existing tools and processes.
- We envision the following improvements through our active participation and collaboration in the AIDOSec project:
- Enhanced security through joint research and development: Contribute to and benefit from the advancements made in the AIDOSec project to bolster our platform’s security.
- Strengthened partnerships and networking: Forge lasting relationships with other AIDOSec participants, opening up opportunities for future collaborations and joint initiatives.
- Shared innovation: Benefit from the exchange of ideas, knowledge, and best practices among AIDOSec participants, leading to a more secure and efficient manufacturing sector.

Strengthen sustainability

By actively participating in the AIDOSec project, ThingLink will collaborate with other project participants in research and development to create a security-focused, AI-driven XR trainings platform tailored to the needs of the global manufacturing sector. The platform will enable enterprises to accelerate learning, enhance employee experience, and save money while maintaining a strong emphasis on security and scalability. The commitment to collaborative research, development, and knowledge exchange with AIDOSec project participants will position ThingLink as a market leader in providing innovative and secure XR training solutions for the global manufacturing industry.
Improving innovation capacity and the integration of new knowledge Business Potential: ● Expansion of ThingLink's market reach within the global manufacturing industry through collaboration and strategic partnerships. ● Establishment of ThingLink as a trusted provider of secure XR training solutions. ● Increased client retention and attraction of new clients within the global manufacturing domain. By actively participating in the AIDOSec project, we will contribute to and benefit from the following innovations: ● Joint development of AI-driven security automation solutions: Collaborate with other AIDOSec participants to develop and implement advanced machine learning techniques that automate repetitive and time-consuming cybersecurity tasks. ● Collaboration on MDE and AI research: Work together with other AIDOSec participants to advance the state of MDE and AI research, sharing knowledge and best practices to improve abstraction, automation, and security in the manufacturing industry. ● Co-development of comprehensive traceability solutions: Collaborate on the development of advanced traceability solutions that correlate security controls across different DevOps phases, enabling better vulnerability prediction and root cause analysis.

Competitiveness, growth, sustainability and innovation for Universities (U) and Research Organizations (RO). In summary:

- **Competitiveness**: By participating in the AIDOSec project, Us and ROs can improve their competitiveness by conducting cutting-edge research in the field of SecDevOps. This can help them attract more funding and collaborations, enhance their reputation in the academic community, and stay at the forefront of their field.
- **Growth**: The AIDOSec project can also help Us and ROs grow by enabling them to expand their research programs, attract more students and researchers, and increase their research output. This can help them make a greater impact in their field and contribute to the advancement of knowledge.
- **Sustainability**: By conducting research on SecDevOps, Us and ROs can contribute to the sustainability of the software industry by developing new tools and practices that improve the security of software products. This can help reduce the risk of security breaches, improve the resilience of software systems, and promote responsible and sustainable development practices.
- **Innovation**: The AIDOSec project can also help Us and ROs foster a culture of innovation by encouraging collaboration between researchers from different disciplines, promoting interdisciplinary research, and developing new ideas and approaches to SecDevOps. This can help advance the state of the art in this field and drive innovation in the software industry.

Universities (U) and Research Organizations (RO)
ABO (U)
Strengthen competitiveness ABO will exploit its STGEM tool on new industrial UCs and will extend the tool with new capabilities that will allow for detection of vulnerabilities and anomalies and for generation of tests for security testing of complex CPS in a DevOps context. The new tool capabilities will allow STGEM to validate large, complex CPS more efficiently, to generate security tests with minimal human effort, and to detect vulnerabilities and anomalies at an early stage in product development.

Strengthen growth ABO will exploit new opportunities to collaborate with old and new industrial partners in Finland and Europe. The results of the scientific research carried out by ABO in collaboration with other project partners will be published in top software engineering conferences and journals. All software artefacts and tools developed as part of the research and development activities will be released as open-source software. ABO will also use the project results for technology transfer and to improve teaching.
Strengthen sustainability The AI/ML techniques used for vulnerability detection and security testing will reduce the time required to detect vulnerabilities and anomalies in software artefacts and generate tests for security testing of complex CPS. As a result, the overall productivity in DevOps practices for CPS will improve and the energy footprint will become smaller.
Improving innovation capacity and the integration of new knowledge The main innovation will be the new tool capabilities that will allow STGEM to detect vulnerabilities and anomalies at an early stage and the new tool capabilities for security testing of complex CPS in a DevOps context. ABO will also exploit new integration opportunities of test generation and monitoring solutions in CI/CD pipelines, will contribute to the integration of its tools into the AIDOSec framework, will assist with integrating its tools with the use cases targeted in the project, will contribute to evaluating the tools in the selected use cases and in collecting evaluation results.
AIT (RO)
Strengthen competitiveness AIDOSec will allow AIT to further strengthen and develop its position in research on risk and threat modelling such as modelling cascading effects thereof. This also includes the interplay of risk analysis and threat modelling in general and specifically in terms of DevOps. The integration of security with respect to risk and threat analysis into the life cycle of DevOps is of great interest for AIT. AIDOSec enables AIT to broaden its portfolio and, therefore, increase its competitiveness among other RTOs on a national and international level. AIT will use the gained know-how in follow-up contract research to continue transferring research results to industry.AIDOSec will pave the way for investigating the benefit of threat and risk modelling within the DevOps cycle.
Strengthen growth The newly developed solutions for SecDevOps will open up new groups of target customers and will lead to an increased portfolio for AIT. AIT will continue its work with academic and industrial partners from AIDOSEC and transfer research results to industrial partners (national and international). AIDOSEC will allow AIT to possibly hire researchers working on SecDevOps. This leads to an increase in research topics in the field of risk analysis, threat modelling and cascading effects thereof.
Strengthen sustainability Further development of existing software products and services for future projects and different application areas (reduced amount of resources required). AIDOSec will strengthen AITs position.
Improving innovation capacity and the integration of new knowledge New research topics that are relevant for industry (especially SecDevOps); adoption in specific domains possible
BUT (U)
Strengthen competitiveness As an academic institution, BUT will strengthen its position as a key research, development, and education institution combining the security topics with artificial intelligence and applied machine learning. This will attract new students and new young researchers, as well as new cooperation with our industrial partners.
Strengthen growth BUT plans to commercialise project results in the form of technology transfer and, potentially, the creation of a new startup - a recognised spin-off company of the team involved in the project. We have a long track of the establishing successful startups companies, Cognitechna was also established as a consequence of a previous research effort.

Strengthen sustainability
Involvement in innovative projects like AIDOSec enhances the reputation of research organisations and attracts high-quality students and researchers. This ensures the ongoing development of groundbreaking research and technology transfer.

Improving innovation capacity and the integration of new knowledge
The project will extend BUT's portfolio of European projects in the field of applied machine learning in cybersecurity and safe and secure HW/SW application development pipeline. We will explore and integrate new knowledge from the innovation in terms of homomorphic encoding and apply advanced mechanisms to optimise the secure AI development pipeline.

IMT (RO)

Strengthen competitiveness
As an academic/research organisation, IMT is particularly interested in improving the SOTA in terms of CPS engineering by relying on model-based solutions. In particular, they work on techniques for heterogeneous model transformation and federation, possibly combined with Machine Learning, to better support various activities of the CPS engineering process. In the specific context of AIDOSec, they want to further develop and deploy their novel approaches in order to more efficiently support the definition and enforcing of CPS security properties. To this end, they will extend their current model-based engineering expertise by collaborating on advanced solutions (e.g. Eclipse-based prototypes), and by publishing corresponding scientific results in relevant conferences and journals of the domain.

Strengthen growth
Around the various topics mentioned before, IMT expects to both continue the ongoing collaborations with partners (academic and industrial) from AIDOaRt but also significantly extend them via complementary fruitful collaborations with new partners from AIDOSec. In particular, IMT is seeking to work more deeply with partners having a solid expertise on Cyber-Security (for instance), and for partners interested in applying model-based approaches in the context of their industrial setups.

Strengthen sustainability
The project consolidates the IMT scientific and technological knowledge on model-based solutions. It also strengthens the organisation’s international visibility, as well as its research expertise in cyber-security.

Improving innovation capacity and the integration of new knowledge
From a research perspective, AIDOSec will further develop the existing model-based engineering expertise at IMT, notably by adding a novel security dimension to it.
From a teaching perspective, AIDOSec will allow completing the teaching currently performed in the context of our student programs by possibly adding a new focus on security aspects.
From an industrial dissemination perspective, AIDOSec will feed internal discussions on future collaborations around the trending topics of Cyber-Physical Systems and/or Security.

JKU (U)

Strengthen competitiveness
As an academic/research organisation, JKU is interested in improving the SOTA MDE and Cybersecurity principles and practices in SecDevOps and its adoption in the automotive and manufacturing systems application areas. Moreover, JKU is interested in the hybridization of MDE, DevOps, and Cybersecurity both on research and practical aspects, as well as the new challenges brought by AI augmentation from an engineering process and system under study perspectives. The goal is to improve and gain expertise in AIDOSec areas (MDE, AI, Cybersecurity, SecDevOps) by collaborating with partners and publishing corresponding scientific papers to relevant conferences and journals in these domains.

Strengthen growth
JKU expects to continue the ongoing collaborations with partners (academic and industrial) from AIDOSec. JKU seeks to work more deeply with partners in industrially relevant contexts. Results will be submitted to the top conferences and journals in the modelling software engineering, and industrial informatics fields. Moreover, JKU will encourage and supervise Ph.D. and M.Sc. theses in the project context. Co-supervisions with other project partners will be encouraged.

Strengthen sustainability
Participating in innovative European projects such as AIDOSec is crucial for the long-term sustainability of research organisations like JKU. AIDOSec will consolidate their scientific and technological knowledge on model-based and cybersecurity solutions and strengthen their international visibility. Participating in European projects attracts high-quality students and researchers at all levels, including entry-level, master's, PhD, and postdoctoral positions, ensuring ongoing development of cutting-edge research and technology transfer.

Improving innovation capacity and the integration of new knowledge
JKU will contribute to the research activities and implementation of academic solutions combining techniques and practices from different research areas (MDE, DevOps, AI/ML, cybersecurity). On the one hand, JKU will continue to extend existing solutions to make them more suitable to adoption in (controlled) industrial scenarios. Moreover, the collaboration with industrial and academic partners will foster the identification of industrial needs and possibilities to devise new solutions in one or more of the identified research areas.

MDU (U)

Strengthen competitiveness
The main competitive aspect for academia is growing knowledge/expertise in research fields that are expected to become, or already are becoming, the forefront of SOTA and practice. AIDOSec deals with the software engineering process of very complex systems and proposes corresponding solutions to tame such complexity by means of model-based engineering (MBSE) techniques and also allow for automated/iterative development through DevOps. These solutions are of paramount interest for MDU; it is enough to mention that INCOSE promotes MBSE as the future of development for industrial systems in its vision for 2030. To add to the general problem of complex systems development, AIDOSec targets security, which is a growing challenge for software systems. Also in this case, it is worth mentioning that MDU is strengthening its research profile for cybersecurity both through specific recruitments and also by means of an upcoming study program. Therefore, the experience matured due to the research in AIDOSec, and the opportunity of collaborating with both industrial and research partners in the project consortium, have a great potential to strengthen MDU competitiveness, both as a collaboration partner and as an education/research institution.

Strengthen growth
The project helps us to establish new collaborations with academia and industry, build the way and foundation for new projects, and also attract new funding. We expect that these research results developed in AIDOSec will open up opportunities for grants of over 1M € over three years after the end of the project.

Strengthen sustainability
MDU works to ensure the competitiveness of the academic and business communities and contribute to a sustainable society. MDU offers unique expertise and testbeds and demonstration facilities, instrumental in future-proofing technologies, products and services. MDU has a proven track record of disseminating and promoting industrial deployment of its research findings, including establishing spin-off companies and licensing of its software.

Improving innovation capacity and the integration of new knowledge
(MDU) is one of Sweden's large institutes of higher education. The University is characterised by its close cooperation with companies and with the public sector in the region, and by its distinct environmental profile. The objective of MDU is to innovate based on AIDOSec results and improve the current body of knowledge in software testing, in the traceability (meta-)model in the SecDevOps process. Moreover to disseminate our results with the broader research community as well as with our industrial partners. To achieve this, we regularly publish in the main software testing and software engineering venues and continuously engage in diverse academic and industrial collaboration.
(Testing related) With an emphasis on method and tool development, as well as industrial and practical real life case studies, our research focus includes (but is not limited to) test design, model-based testing, search-based software testing, decision-support for software testing, and test automation. In short, we develop, refine, and evaluate methods, theories and tools for testing of industrial software systems.

RISE (RO)

Strengthen competitiveness
As the leading research institute in Sweden , AIDOSec will help RISE to strengthen and enrich our expertise

in building intelligent security analysis solutions for the verification and validation of complex industrial systems. This, in turn, contributes to expanding our offerings to our partners in the area of cybersecurity. Moreover, cybersecurity is an area which is gaining ever-increasing importance and is of strategic significance for EU states, society and industry.

Strengthen growth
AIDOSec will enable us to build new partnerships, and expand our network of industrial and academic partners beyond Sweden and across Europe. Moreover, the project creates opportunities for our research organisation and group to open new Postdoc, doctoral student, as well as, master thesis positions. By involving our junior researchers to work alongside the senior ones in AIDOSec, the project also greatly helps with career advancement of junior researchers towards becoming senior by getting more familiar with the way of working in large-scale EU projects that entail close collaboration between industry and academia.

Strengthen sustainability
Use of intelligent and automated security analysis solutions is a critical and important step towards tackling cybersecurity issues in industrial settings, and for the reduction of resources for verification and validation of security-related issues in general. On the other hand, security issues in critical infrastructures such as power plants, hospitals, and water treatment facilities can directly impact the sustainability goals in the context of smart cities, as one example. Therefore, RISE as a research organisation will benefit from the results and experience of the AIDOSec project to offer a bigger portfolio of cybersecurity analysis solutions to our network of industrial and state partners (e.g., municipalities) helping them towards reaching their sustainability goals by creating more reliable infrastructures.

Improving innovation capacity and the integration of new knowledge
As a research partner, the new knowledge gained from AIDOSec in the area of cybersecurity and the novel solutions that we intend to develop for the project create new innovation opportunities in terms of contributing to the SOTA, and also state of the practice through knowledge transfer to our wide network of partners that we collaborate with. We will publish articles about our results and achievements in the project and present them at various scientific and industrial venues. Our results in AIDOSec can also build the baseline knowledge and technology for our future industrial research projects paving the way for us to build more solutions in the area of cybersecurity. AIDOSec project, in general, offers an excellent and unique opportunity for us to combine and extend our knowledge in the areas of AI, software engineering, and cybersecurity.

UEF (U)

Strengthen competitiveness
The global manufacturing industry increasingly demands security-critical and efficient monitoring/maintenance solutions for automated systems. Our approach involves utilising novel security-critical AI-Based, MDE-Based, EDGE-Intelligence-Based, CyberSecurity-Based, and VR/AR/MR/XR-Based technologies to design and develop Digital Twins of various products. Rapid changes in security architectures, technologies, and components require sophisticated modern security-critical methods to keep Digital Twins continuously running and evolving securely. We will provide an AI-based framework to facilitate the design and development of Digital Twins for complex security-critical industrial systems in the global manufacturing domain. UEF's participation in the AIDOSec will enable us to contribute our expertise and resources to a collaborative research initiative, working alongside other project participants. We aim to achieve the following through our collaboration: 1) Joint research: Collaborate with other AIDOSec participants on research projects, sharing knowledge and resources to advance the state-of-security in the global manufacturing sector; 2) Technology transfer: Contribute to the development and transfer of innovative technologies and practices related to AI-driven security automation, MDE, and continuous improvement; 3) Networking and partnerships: Establish strategic partnerships with other AIDOSec participants, fostering long-term collaborations and strengthening our position within the global manufacturing industry.

Strengthen growth
UEF conducts AI-based, CyberSecurity-based, Digital Twins based, CyberSecurity-Based, and VR/AR/MR/XR-based research work specifically tailored for the global consortium companies' needs. Our expected outcomes for solving the AIDOSec project related problems: 1) Development of security-critical AI-based Digital Twins to optimise manufacturing processes by monitoring and simulating production conditions, identifying unexpected events, security breaches, and testing various conditions; 2) Leveraging

security-critical AI-based MDE practices to increase productivity, reduce development costs, improve software quality, and enhance security; 3) Consortium partners contributing to the development of security-critical AI-based V&V services, fault localization, monitoring, and prediction of quality patterns; 4) Demonstrating and evaluating the global UC with a focus on cybersecurity, traceability, federation, and continuous AI-based V&V services of DTs through integrated feedback loops; 5) Providing staff and stakeholders with scalable, efficient, intuitive, secure, and faster training/education related to end-products/machines/factories; 6) Reducing training time and ensuring faster and more secure onboarding of new employees, reducing downtime, and improving productivity and security; 7) Achieving ambitious project goals and improving the competitiveness of the global industry in the security-critical manufacturing industry domain; 8) Simplifying the development of security-critical AI-based systems in multiple domains, enabling scalable, secure, and efficient training for staff and stakeholders.

Strengthen sustainability

Digital solutions that we will implement in the project will drive the industry towards sustainability. Our exploitation plans aim to maximise the impact of innovative products and services in the security-critical manufacturing industry related to Finland UC. UEF conducts security-critical AI-based, Digital Twins based, CyberSecurity-based, and VR/AR/MR/XR-based research work specifically tailored for Finland UC needs. The expected results include increased productivity, reduced development costs, improved security, greater engagement in XR training, and increased adoption of products/services. The aim is to make a significant impact in the security-critical manufacturing industry. In addition, we expect to create AI-based CyberSecurity patents as a result of our research work and integrate them into the Finland UC. Moreover, our aim is to simplify the development of security-critical AI-based systems in multiple domains (i.e., Finland UC can easily be extended into other domains) by utilising EDGE-Intelligence, AI-based CyberSecurity, and guaranteeing their quality while reducing the skill level required from the developer. The plan is expected to take 3 years and the goal is to make a significant impact in the security-critical manufacturing industry as well as in the research field.

Improving innovation capacity and the integration of new knowledge

UEF will spearhead the innovation and the integration of new knowledge in the security-critical manufacturing industry in Finland. Using cutting-edge technologies, such as AI and VR/AR/MR/XR, UEF will conduct security-critical research work that will produce novel solutions and insights for the industry. UEF will enhance the productivity, efficiency, security, and quality of the products and services in the manufacturing industry. UEF also anticipates to create new AI-based patents and integrate them into the Finland Use Case. Furthermore, UEF will enable the development of security-critical AI-based systems in multiple domains by utilising EDGE-Intelligence, AI-based CyberSecurity, and ensuring their quality while lowering the skill level required from the developer.

UNICA (U)

Strengthen competitiveness

UNICA is participating with the Microelectronics and Bioengineering lab of the Department of Electrical and Electronic Engineering. The group has an already established position in Europe related to Embedded and Cyber-Physical System Design and strategy/architectures for porting AI at the edge. With AIDOSec, the goal is to strengthen this position and to improve the visibility of the lab by improving the proposed technologies and extending the set of proof of concepts to a completely new application scenario like the automotive one.

Strengthen growth

UNICA aims to advance SOTA in the context of advanced computing architectures at the edge. The results will be submitted to relevant conferences and/or in professional journals. Any possible tool extension will be distributed Open Source (https://mdc-suite.github.io/).

Strengthen sustainability

UNICA participation to AIDOSec is meant not only to improve its developed tools and technologies, but also provides to UNICA a unique opportunity to carry-out technology and knowledge-transfer activities by means of visiting periods and active collaborations, as well as by means of dedicated tutorials for non hardware experts. All this together will positively affect the lab's attractiveness and will open opportunities for further exploitation activities of the proposed technologies (e.g. new proposal).

Improving innovation capacity and the integration of new knowledge
UNICA will encourage and supervise Ph.D., M.Sc., and Bach. theses in the context of the project. Co-supervisions with other project partners (also industrials such as ABI) are expected.

UNICAN (U)

Strengthen competitiveness
As an academic research institution, UNICAN competitiveness is measured on the basis of how well the technologies, methodologies and tools they openly provide to the community do match its needs and make its economic impulse more efficient in terms of usage of natural resources and human labour. AIDOSec will improve the ability to play this role by enlarging the platforms over which our analysis and design technologies may apply. Concretely, AIDOSec will positively impact our model- & ontology-based security by design methodologies, the MAST tool and the S3D Technology. The most competitive advantage is in the synergies among (1) the automated timing modelling and analysis of software with MAST deployed over hardware platforms whose (2) performance figures are obtained by simulation with S3D, and (3) the use of high-level security patterns deployable by code generation techniques that embed the most appropriate security assertions with respect to continuously improving threat models. Empowered by their integration in AIDOSec these will differentiate us from the competitors and colleagues in associated and related methodologies and research environments.
From the education perspective, AIDOSec will enhance and make more attractive our lectures at master level in UNICAN “Certification of quality and security in computing systems” subject

Strengthen growth
Traditional customers of UNICAN technologies and tools are in the avionics and space domains. Impact of the innovations that will be achieved with AIDOSec will expand the scope to several other key application areas. Some clear targets are Mobility, Digital Industry, and Digital Society, but others may well be impacted, since security by design is an enabling technology for design flows in many domains, and DevOps is a growingly adopted development paradigm.

Strengthen sustainability
The techniques they will include in the mainstream of the secure DevOps with AIDOSec follow an optimization strategy that may be also quite well applied over sustainability or environment friend-ability qualifiers, hence the use of these techniques at industrial level would be very neatly reused with these additional optimization vectors in mind. For example, the same approach used for characterising and finally recommending IOT devices with better security figures in a design/development process is suitable to be used to select better configurations, products or components with the most adequate levels of environmental impact.

Improving innovation capacity and the integration of new knowledge
The adaptation of the model-based analysis tools in MAST to SecDevOps and their combination with ontology-based security by design modelling methodologies will cross fertilise both areas of research. Quite wider space can be envisioned to accommodate even more of the techniques provided by the partners into a renewed architecture of competencies meant for cyber physical systems in the European IT engineering space.

UNISS (U)

Strengthen competitiveness
The main impact to be achieved for UNISS is to position the research activity of the Artificial Intelligence and Formal Methods Laboratory (AIMET) both at the local and international levels. With respect to the former, this can be achieved by improving the visibility of the Laboratory and strengthening its relationships with other research institutions and ICT funders locally. The latter can be achieved by leveraging tools and methods from AIDOSec activities for the international academic and industrial community.

Strengthen growth
UNISS will develop original research in the field of artificial intelligence and formal methods and contribute as much as possible to the SOTA. Original papers will be published at relevant conferences and/or in professional journals.

Strengthen sustainability
The participation of the University of Sassari in AIDOSec strengthens its sustainability by fostering

collaboration, knowledge exchange, and access to resources, thereby enabling AIMET to enhance its research capabilities, attract talented students and researchers, and ensure the transfer of groundbreaking technologies.
Improving innovation capacity and the integration of new knowledge In the case of UNISS, AIDOSec will provide the chance to improve our institution's capabilities in the area of cybersecurity, which is currently of utmost relevance and on which only a few people are working.
UNITE (U)
Strengthen competitiveness As a research organisation, UNITE is interested in enhancing its competencies both from a scientific research and a technology point of view. UNITE aims to mature and scale its current methodology and technology in the domain of Security and DevOps for software and system engineering, as well as the combination of model-based engineering and AI/ML. In general, the strong collaboration with industrial partners throughout the project offers a much more practical view of the actual industrial problems in the area, which will result in much more targeted research to be conducted by UNITE.
Strengthen growth Results will be submitted to the top conferences and journals in the software and system engineering and artificial intelligence fields. All prototype tools developed as part of the research activities will also be released as open source software. Both aspects will continue to enforce the UNITE position in the research areas of software and system engineering and artificial intelligence. We expect to be able to capitalise on the results obtained in AIDOSec in order to gain future research funding (both at the European and National levels) allowing us to hire new students or postdoc students in the future.
Strengthen sustainability Participation in innovative projects like AIDOSec is key for UNITE long-term sustainability as it helps to increase visibility and attract more and better students/researchers at all levels that will ensure the continuous development of innovative research and tech transfer.
Improving innovation capacity and the integration of new knowledge AIDOSec will contribute to enhance UNITE competencies both from a scientific research and a technology point of view: From a research perspective, AIDOSec will improve UNITE competencies and strengthen its position in the field of DevOps and Continuous Software and System Engineering by relying on model-based solutions and AI/ML. In AIDOSec, UNITE will contribute to the design of the general architecture and the traceability approach, also to develop novel cybersecurity solutions. To this end, UNITE will extend its current expertise by collaborating with industrial partners, and by publishing corresponding scientific results in relevant conferences and journals of the domain. From a technology transfer perspective, UNITE is interested in applying developed technologies in industrial cases and collaborating with solution providers (especially industrial partners) with the aim of integrating research efforts as part of existing or new software solutions and services.
UNIVAQ (U)
Strengthen competitiveness As a research organisation, UNIVAQ is interested in enhancing its competencies from a research point of view. UNIVAQ aims to mature and scale its current methodology in the domain of ESL HW/SW Co-Design by focusing on MDE and security. For this, the collaboration with industrial partners offers a view of the actual industrial problems in the area, which will result in much more targeted research.
Strengthen growth Results will be submitted to the top conferences and journals in the electronic design automation field. All prototype tools developed as part of the research activities will also be released as open source software. Both aspects will continue to enforce the UNIVAQ position in the research areas of electronic design automation with particular focus on ESL HW/SW Co-Design. We expect to be able to capitalise on the results obtained in AIDOSec in order to gain future research funding and collaborations.
Strengthen sustainability

For research organisations, participation in innovative projects like AIDOSec helps to increase the visibility of the organisation and attracts more and better students/researchers at all levels that will ensure the continuous development of innovative research and tech transfer.
Improving innovation capacity and the integration of new knowledge AIDOSec will contribute to enhance UNIVAQ competencies from both research and technology transfer points of view: from a research point of view, AIDOSec will improve UNIVAQ competencies and strengthen its position in the field of HW/SW co-design of secure dedicated/embedded systems. To this end, UNIVAQ will extend its current HESPSYCODE methodology (www.hepsycode.com) and will publish scientific results in relevant conferences and journals; from a technology transfer point of view, UNIVAQ is interested in industrial collaborations with solution providers in order to integrate research efforts as part of software solutions and services and/or to create university spin-offs.
UOC (U)
Strengthen competitiveness As a research organisation, UOC will exploit AIDOSec for scientific research but also for technology transfer and teaching purposes. From a research perspective, AIDOSec allows UOC to mature and scale its current techniques and prototypes on, mainly, software and systems design, AI for software engineering and verification/simulation for security analysis. Moreover, UOC plans to conduct innovative research on new fields, including verification of security properties using logics, secure model-based DevOps and life-cycle/continuous interoperability, and holistic CPS engineering. In general, the strong collaboration with industrial partners throughout the project offers a much more practical view of the actual industrial problems in the area, which will result in much more targeted (and therefore useful) research to be conducted by UOC. From a teaching perspective, UOC offers several degrees related to computer science plus some masters (e.g., especially its master on Industry 4.0 but there are also related masters on computer engineering, free software, information security, …), and one PhD programme in this area. Results of the project will be continuously integrated in the course contents, specially at the master level.
Strengthen growth Results will be submitted to the top conferences and journals in the modelling and software engineering field. All prototype tools developed as part of the research activities will also be released as open source software continuing the tradition of the team. Both aspects will continue to cement UOCs position as one of the important players in the software engineering research ecosystem.
Strengthen sustainability For research organisations, participation in innovative projects like AIDOSec is key for its long-term sustainability as it helps to increase the visibility of the organisation and attracts more and better students/researchers at all levels (entry level, master level, phd level, postdocs) that will ensure the continuous development of innovative research and tech transfer.
Improving innovation capacity and the integration of new knowledge UOC will encourage and supervise Ph.D. and M.Sc. theses in the context of the project. Co-supervisions with other project partners will be encouraged.

2.1.4 Scale and significance of the project's contribution

During project lifetime, AIDOSec results are disseminated through the target groups which count overall **thousands of members** (see Section 2.2.1). This allows AIDOSec to gain visibility and get a preliminary assessment of its technologies. Seminars, tutorials, and technology transfer activities will help reaching companies. The goal is to set the base for further dissemination of project results that, in 5 years after project end, will set a milestone in the advancement of SecDevOps. Table 2.1.4

reports the scale and significance of the AIDOSec Project. Quantitative metrics are inherited from the monitoring indicators by Nixon[98] and adapted to monitor AIDOSec-specific outcomes.

Table 2.1.4 - *Scale and significance: indicators and target metrics*

Scale			Significance
	Indicator (I)	**Target Metric (TM)**	
Scientific Outcomes and Impact			
1. Creating high-quality new knowledge			AIDOSec will contribute to the ECS SRIA 2024 ***Main Common Objective 1: boost industrial competitiveness through interdisciplinary technology innovation*** and to the ***Horizon Europe objectives of enhancing cybersecurity, digital sovereignty, and innovation capacity in Europe***. AIDOSec aims at becoming a **reference in the SecDevOps communities, acting as a bridge between academic research and industrial practices**. The scientific impact will be assessed by overperforming the average indicators of the projects funded by the KDT Programme. The main project result, the AIDOSec framework, should be used as reference for scientific publications. Scientific results should be published in peer-reviewed publications that contribute to upskill researchers and allow them to stabilise their academic career. AIDOSec will strive to **achieve the highest knowledge share through EU open knowledge infrastructures**, promoting the diffusion of the project results
1.1	**(short term) publications:** number of peer-reviewed scientific publications	> 80 publications Baseline: 0	
1.2	**(medium-term) citations:** citation index of peer-reviewed publications (at the end of the project)	>= 2 H-Index Baseline: 1.2	
2. Strengthening human capital in research and innovation			
2.1	**(short term) skills**: number of researchers involved in upskilling (training, mentoring/coaching, mobility and access to R&I infrastructures) activities in AIDOSec	>= 10 researcher Baseline: 0	
2.2	**(medium term) careers**: number and share of upskilled researchers involved in AIDOSec with increased individual impact in their R&I field.	> 10 researcher >= 0.3/year Baseline: annual increase in the H-index of researchers similar to FP researchers (increase of 0.29/year during 2015-2018).	
3. Fostering diffusion of knowledge and Open Science			
3.1	**(short term) shared knowledge**: share of research outputs (open data/publication/software etc.) of AIDOSec that are shared through open knowledge infrastructures.	> 50% Baseline: share of the EU's publications that are in OA (between 42 % and 46 % between 2016 and 2018).	
3.2	**(medium-term) knowledge diffusion:** share of open access research outputs resulting from AIDOSec actively used/cited.	Baseline: mean field-weighted citation score for H2020 non-OA publications (2.2)	
Societal Outcomes and Impact			
4. Addressing EU policy priorities and global challenges through research and innovation			AIDOSec will contribute to the ECS SRIA 2024 ***Main Common Objective 3: establish and strengthen sustainable and resilient ECS value chains supporting the Green Deal*** *and* ***Main Common Objective 4: unleash the full potential of***
4.1	**(short-term) results:** number and share of results aimed at addressing identified Union policy priorities and global challenges (including SDGs)	> 20 publications > 50% (of publications targeted at TM1.1) > Baseline: 0 publications	

[98] European Commission, Directorate-General for Research and Innovation, Nixon, J., Study to support the monitoring and evaluation of the framework programme for research and innovation along key impact pathways – Indicator methodology and metadata handbook, Nixon, J.(editor), Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2777/44653

		in the identified SDGs	***intelligent and autonomous ECS-based systems for the European digital era***. AIDOSec will **contribute to achieve the targets of the SDG goals**. Thanks to the adoption of automation capabilities supported by MDE and AI/ML techniques, together with well-defined DevOps engineering activities, AIDOSec aims at **contributing to the diffusion of a critical knowledge of cybersecurity threats** among researchers, industrial practitioners, and to the users of the industrial/software system under study/development.
4.2	**(medium-term) solutions**: AIDOSec innovations, including research outcomes and related solutions (e.g., improved version of partners' solutions, integrated solutions)	> TM1.1 + 10 solutions Baseline: 0 publications and solutions in the identified SDGs	
6. Strengthening the uptake of research and innovation in society			
6.1	**(short-term) co-creation:** Participation/ contribution of Union citizens and end-users to the co-creation of R&I content in AIDOSec	Yes/No (for each project result)	
6.2	**(medium-term) engagement**: end-user engagement mechanisms in place by beneficiary entities after AIDOSec	> 5 Baseline: 0	
Economic/Technological Outcomes and Impact			
7. Generating innovation-based growth			AIDOSec will contribute to the ECS SRIA 2024 ***Main Common Objective 2: ensure EU digital autonomy through secure, safe and reliable ECS supporting key European application domains.*** AIDOSec, through its innovative platform (Objective 1), aims to **create qualified jobs** (academic and industrial researchers, engineers) and **cybersecurity-aware citizens**. The AIDOSec framework is a research and innovation project and, as such, it needs further investments to scale up and improve the AIDOSec framework's capabilities
7.1	**(short-term) innovative results:** number of innovative products, processes or methods resulting from AIDOSec and intellectual property rights (IPR) applications.	> 20 (products, processes, methods) > 3 (IPR) Baseline: 0	
7.2	**(medium-term) innovations**: number of innovations resulting from AIDOSec, including from awarded IPRs.	> 3 (submitted innovations by all periodic reports)	
8. Creating more and better jobs			
8.1	**(short-term) supported employment:** number of full-time equivalent (FTE) jobs created, and jobs maintained in participating legal entities for AIDOSec	> 10 Baseline: 0	
8.2	**(medium-term) sustained employment:** increase of FTE jobs in participating legal entities following AIDOSec	> 2% Baseline: 0	
9. Leveraging investment in research and innovation			
9.1	**(short-term) co-investment:** amount of public and private investment mobilised with the initial investment in AIDOSec.	> 30% of AIDOSec budget Baseline: 0 euro	
9.2	**(medium-term) scaling up**: amount of public and private investment mobilised to exploit or scale up AIDOSec results (including foreign direct investments).	> 200% of the AIDOSec budget Baseline: 0 euro	

2.1.5 Requirements and potential barriers

AIDOSec impact strategy relies on the maximisation of project results towards expected outcomes and impacts. To avoid that external factors and barriers could jeopardise our plan, here we address the most significant ones to plan the necessary mitigation measures. The barriers related to AIDOSec and the respective mitigating measures are provided in Table 2.1.5.

Table 2.1.5 - *Potential barriers and mitigation measures*

Barriers	Proposed mitigation measures
Hesitation to overcome traditional workflows and pre-existing processes. Professionals are often sceptical about changes in their workflow that may add work effort.	The project will adopt a human-centred design approach, onboarding professionals into novel and experimental activities and tools, without increasing effort. Moreover, the project will consider already existing compliance requirements, policies, and procedures as well as security and development standards. The project will also develop transition/adoption guidelines elicited from the integration and technology transfer phases of the project.
Availability of content and tools in different EU languages	The project will ensure the translation of produced learning content through manual or automated means
Engaging and retaining stakeholder participation in the long term	The project will leverage intrinsic and extrinsic motivation factors and incentives, as proposed by EC's Data Act for a fair and innovative data economy, for continuous participation.
Competition, e.g. other platforms will appear in the market, with a functionality overlap	Besides the Communication, Dissemination, and Exploitation plan (D6.2) of the project, the modular approach of tangible outcomes, providing independent services along with the full solution, can provide flexibility in terms of coexisting with competitive projects. In this respect, the goal of the project is to make it possible to integrate alternative solutions, even available from outside the project, e.g. for security management.
Intellectual property rights barriers	The project has a solid plan for IPR management (PCA) and monetization. (D7.1)
Legal and ethical barriers	AIDOSec will rely on EU legislation, which is stated in Network Information Security (NIS) 2 Directive (EU 2022/2555), GDPR and eIDAS regulation. This will be tackled by following the ENISA cyber threat taxonomy in identifying requirements and specifications. GDPR and eIDAS regulations will be the guidelines to address issues like data minimization, consent, transparency, data protection, right to access and rectification, right to erasure, data portability, and accountability.

#§IMP-ACT-IA§#

3. Quality and efficiency of the implementation

#@QUA-LIT-QL@# #@WRK-PLA-WP@#

3.1 Work plan and consortium composition

According to the required brief presentation of the implementation section, the overall structure of the work plan and the consortium composition is presented. The AIDOSec consortium is well established from previous projects, which made it easy to produce even a more detailed description and a Gantt chart. The project is organised into seven work packages (WPs) containing logically connected activities. The first five WPs represent the major technical activities that have been scheduled in order to interact coherently with one another. The last two WPs ("Dissemination and Exploitation" and "Project Management") represent the horizontal activities that weave throughout the whole project and interact with each one of the technical WPs.

3.1.1 Overall Strategy of the work plan

The project will follow an iterative and incremental cycle of Plan-Do-Check-Act in software process improvement activities, identify the requirements, provide the methodology and tools to meet these requirements, validate the results and finalise the deliverables. The approach will further be iterative in order to allow reflection and optimal planning. The research and development in the project will follow an iterative and incremental approach that is divided into three phases as shown in Figure 3.1.1. Each phase ends with a project milestone. In addition, we have a first milestone at month 6 focusing on the establishment of the project management, project website and social

media presence and a first definition of the use cases.

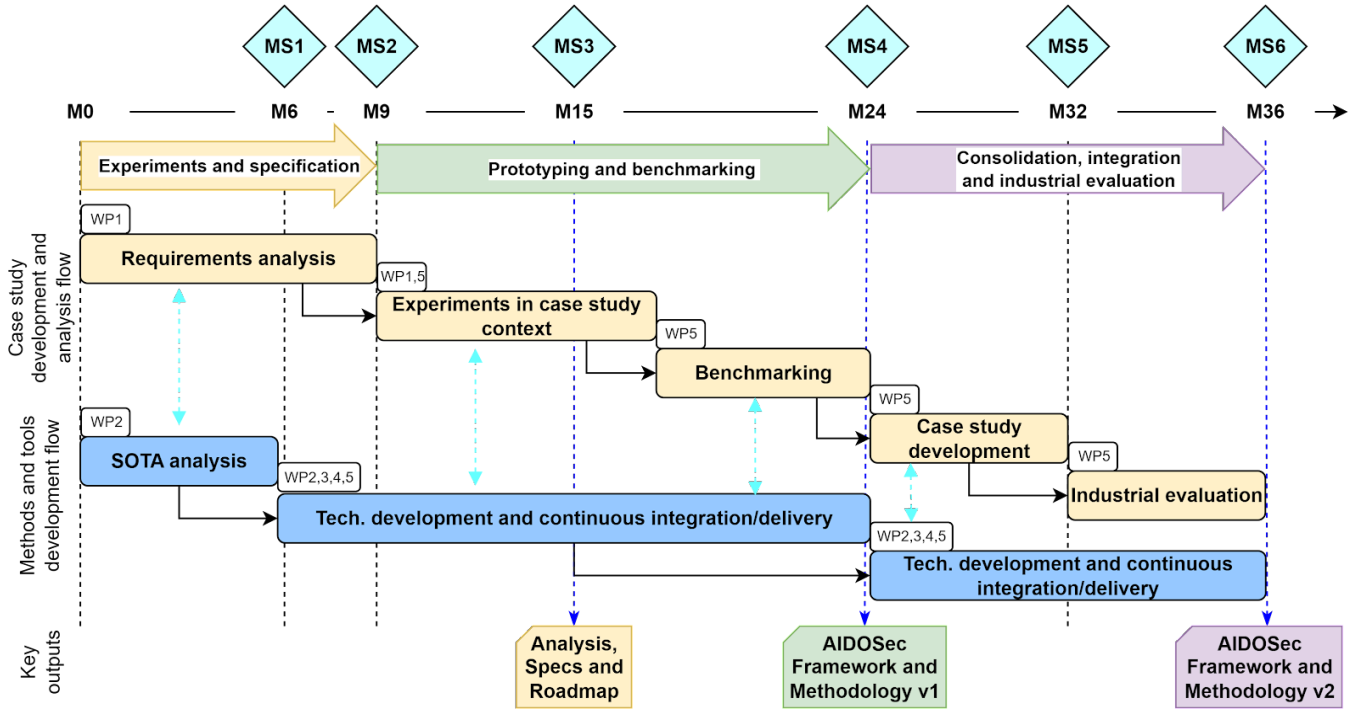


Fig. 3.1.1 AIDOSec project timeline

Phase 1 – Experiments and specification: In the first phase of the project, we will create an initial technical baseline. We will also define precisely the actual use cases and their requirements.

- **Milestone 1:** Initial baseline. An official kick-off meeting for the project has been held. The public website, the Project Handbook and the Consortium Agreement have been established. Use cases are defined.
- **Milestone 2:** Initial specification of AIDOSec Framework. Case Study activities start with baseline technologies evaluation and experimental development with a close feedback loop with technical development.

Phase 2 – Prototyping and benchmarking: In the second phase of the project we will improve and integrate the results from Phase 1 and perform a first round of evaluation by end-users.

- **Milestone 3: Prototyping.** Preliminary release of the AIDOSec results generalised from the baseline technologies. This version will focus on the first baseline results in the context of the use cases.
- **Milestone 4: Tech. benchmarking.** Interim public release of the AIDOSec integrated tool-supported infrastructure. First round of evaluation by end-users. The integration activities are executed in parallel with the case studies applications development for faster consolidation of the AIDOSec technologies. The technology development will continue with the new iteration of feature development.

Phase 3 – Consolidation, Integration and Industrial Evaluation: In the third phase of the project we will integrate and validate the technical results of the AIDOSec, provide final validation and experience reports from the two use cases and final management report.

- **Milestone 5: Consolidation.** Improved internal release of the AIDOSec integrated tool-supported framework.
- **Milestone 6: Final** public release of the AIDOSec integrated tool-supported framework and methodology, final validation and experience reports.

3.1.2 Work package structure

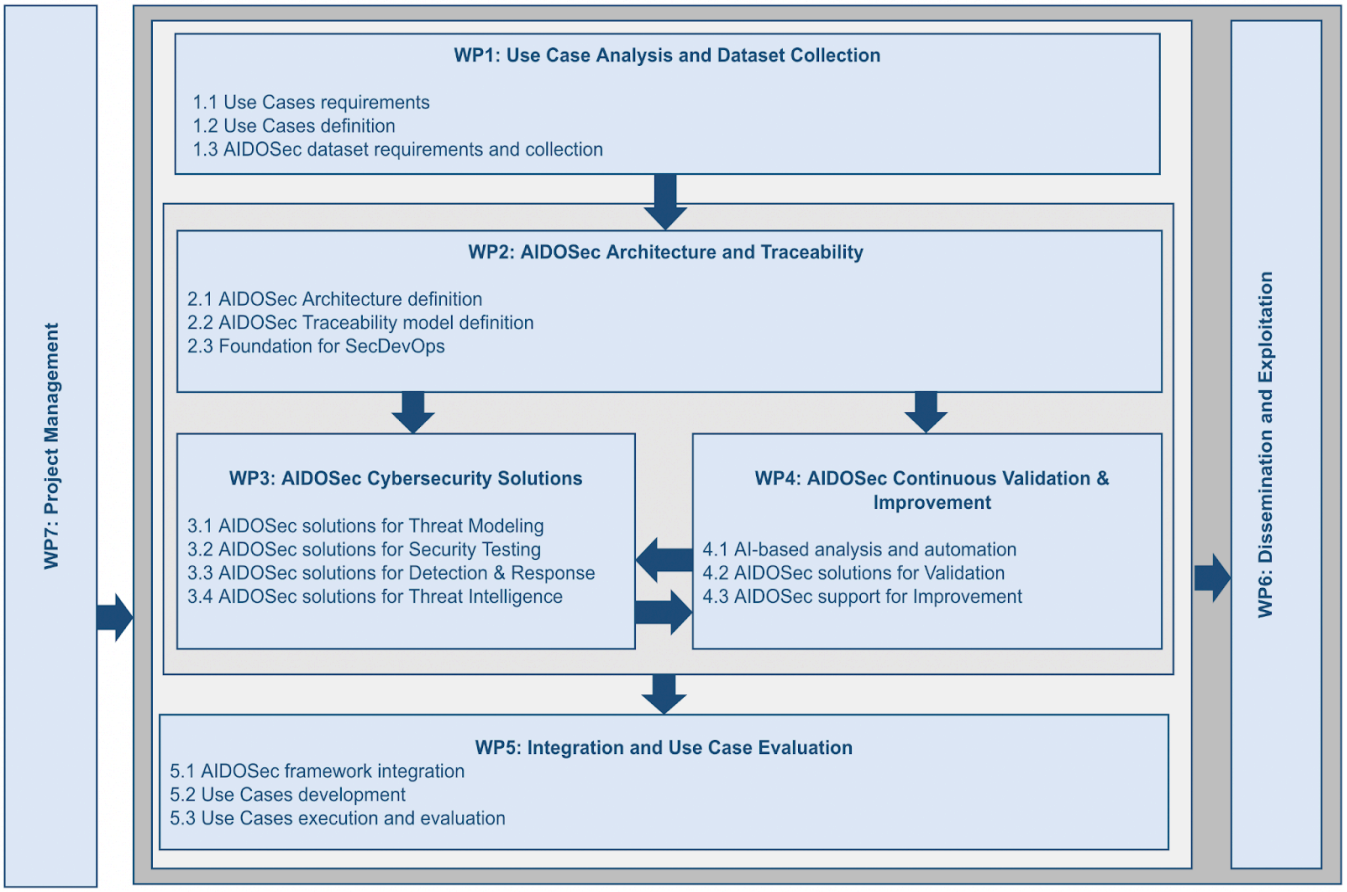


Fig. 3.1.2 AIDOSec Work package structure

WP1 Use Case Analysis and Dataset Collection addresses the use case requirements analysis and definitions as well as the dataset requirements definition and collection. The use case providers will define in detail the project use cases and establish the use case requirements that outline them. The results will be fed to the AIDOSec solution architecture (WP2) and to develop the AIDOSec technology solutions (WP3 and WP4). These use cases will also be used to check the applicability, universality and interoperability of the AIDOSec technical results across different domains (WP5). Distilled objectives of this work package are:

- To define real-life industrial use cases to ensure that WP3-5 deliver practical results;
- To define detailed requirements specification for WP2-5;
- To define means and plans for validation of results;
- To perform an initial check of the universal applicability of the technical work.

WP2 AIDOSec Architecture and Traceability is concerned with defining the AIDOSec solution architecture and the traceability metamodel by combining and harmonising principles and best practices of model-driven and SecDevOps engineering methodologies. WP2 will define the foundations from the scientific and technological standpoint. The goal is to set the engineering challenges AIDOSec addresses and figure out the impact/benefits that the AIDOSec capabilities can bring to the DevOps pipeline by addressing cybersecurity concerns and relying on AI/ML and MDE. Distilled objectives of this work package are:

- To specify the global architecture for the AIDOSec framework;
- To specify the traceability metamodel language;
- To study the foundations of SecDevOps methods and tools (together with the dimensions of MDE and AI/ML) to be considered in the context of the AIDOSec platform.

WP3 AIDOSec Cybersecurity Solutions supports the definition and development of the AIDOSec cybersecurity solutions (methods and tools) that will extend the AIDOSec framework (defined in WP2) according to the needs of the various kinds of systems under development (i.e., the use cases requirements defined in WP1). It will include solutions inherent in the various cybersecurity services we aim to cover, specifically *threat modelling*, *threat intelligence*, *security testing*, *detection and response*. WP3 aims at employing AI (and ML) techniques in multiple security-related aspects of the system development process by relying on the AIDOSec core model-based framework for SecDevOps.
WP3 concentrates on the definition and development of AIDOSec cybersecurity solutions (methods and tools), which expand the AIDOSec framework defined in WP2. It takes into consideration the specific needs of diverse systems under development, conforming to the use case requirements outlined in WP1. WP3 primarily focuses on four main cybersecurity services - threat modelling, threat intelligence, security testing, and detection and response, each aiming to leverage AI and ML techniques for enhancing the security aspects of system development.
In WP3, AIDOSec will develop threat modelling methods and tools to systematically identify, assess, and manage security threats throughout the DevOps pipeline. These methods, informed by threat intelligence and anomaly data, will adapt to the dynamic threat landscape. The associated tools will provide an intuitive interface for effective decision-making in preventative measures.
WP3 also focuses on proactive security testing, employing automated and manual tests at every DevOps stage, with tools for efficient execution, result analysis, and security measures implementation.
For real-time threat detection and response, WP3 uses ML algorithms and threat intelligence. The results inform threat modelling, creating a feedback loop. Tools automate these processes, enhancing security operations' speed and efficiency. Threat intelligence in WP3 collects, analyses, and applies threat information proactively. Data analysis and ML enable real-time alerts, trend analysis, and predictive modelling.

In summary, the distilled objectives of this work package are:

- To define cybersecurity solutions to improve the SecDevOps pipeline in the context of system development;
- To design and develop AI-augmented tools to support the various cybersecurity concerns;
- To refine the proposed solutions based on the feedback from their applications within use cases.

WP4 AIDOSec Continuous Validation and Improvement aims at providing specific capabilities for the *analysis and validation* of the cybersecurity solutions (as defined and implemented in WP3) based on continuously observed results. It allows to verify that the system is working as expected, i.e., the AIDOSec cybersecurity solutions do not affect the system operation while improving the whole security posture. It implies the observation of the system activity and the analysis of run-time data to verify, for instance, that security controls are working as expected and that the system is compliant with security requirements. Also, validation may involve other functional or non-functional requirements, for instance, related to the various DevOps phases affected by the security process. It includes the use of AI/ML techniques for the analysis of both historical and real-time data involved in the process.
Furthermore, it will support the *continuous feedback loop*, based on involving the output generated so far, to make improvements to the whole security process. This phase will make use of the AIDOSec traceability methodology (WP2) to exploit the links between cybersecurity solutions and/or the DevOps phases. By continuously repeating this feedback loop, organisations can *improve* their cybersecurity posture over time and reduce the likelihood and impact of security incidents. The feedback obtained at this stage can also contribute to the training of developers. They can improve their knowledge by contributing to the quality of their work. Thus, the proposed cycle proposes both automatic mitigation actions and automated training actions for developers, with the aim of reducing vulnerabilities (which are in fact mostly created by developers). Distilled objectives of this work package are:

- To define and develop solutions for the system security validation;
- To design and develop solutions to support system security improvement based on the feedback loop and traceability links;
- To support the improvement of the developers' security culture by means of dedicated activities;
- To provide AI-based support to all the activities of analysis, validation and improvement.

WP5 Integration and UC Evaluation provides specific industrial demonstrators as use cases from the Mobility, Health and Wellbeing, Digital Society and Digital Industry domains, such as Abisnula, Alstom, Camea, Prodevelo,

Thales in Mobility, HI Iberia in Health and Wellbeing, Tekne in Digital Society, Westermo and Thinglink in Digital Industry.
The WP5 will integrate technical developments from WP3 and WP4. according to the framework architecture defined in WP2. Besides this, WP5 will conduct controlled experiments on the case study partners' facilities defined in WP1. At that point, WP5 will perform a preliminary evaluation as feedback for WP3-WP4, strong interaction between use cases providers and technology providers is needed. Finally, WP5 will proceed to the final integration and consolidation phase and validate the AIDOSec results. Distilled objectives of this work package are:

- To define the integration approach for AIDOSec framework;
- To integrate the toolsets developed in WP3-4 in the AIDOSec framework (as defined in WP2);
- To develop the infrastructure and testbeds for validation of AIDOSec technologies - to validate the AIDOSec technologies by running industrial case studies.

WP6 Dissemination and Exploitation concentrates on the project impact activities and community building through several dedicated tasks. Distilled objectives of this work package are:

- To ensure wide adoption of the AIDOSec approach via various dissemination and exploitation activities - to establish scientific collaboration through conferences, workshops, summer schools and journal publications
- To coordinate and execute the standardisation activities for the increase of AIDOSec familiarity
- To build an ecosystem for AIDOSec by educating developers and engaging with the community via blogs, tutorials and demonstrations;
- To maintain constant dialogue with industry interests groups, prospective companies and decision makers;
- To prepare for joint exploitation of the AIDOSec results through planning and arrangements for co-marketing and co-distribution.

WP7 Management regroups all the project management activities. Distilled objectives of this work package are:

- to establish an effective project management structure;
- to encourage good interaction within the project and towards the EC;
- to ensure compliance with project plans and that the project activities meet the appropriate quality levels;
- to check and validate the correct scheduling of tasks;
- to manage risks;
- to perform overall legal, contractual, ethical, financial and administrative management of the consortium;
- to coordinate Intellectual Property Right (IPR) and other innovation-related activities at the consortium level;
- to manage science and society issues, related to the research activities conducted within the project.

3.1.3 Project Gantt chart

The figure below illustrates AIDOSec project's Gantt chart. This visual roadmap outlines the key milestones and deliverables providing a comprehensive overview of project tasks, their dependencies, and the projected completion dates.

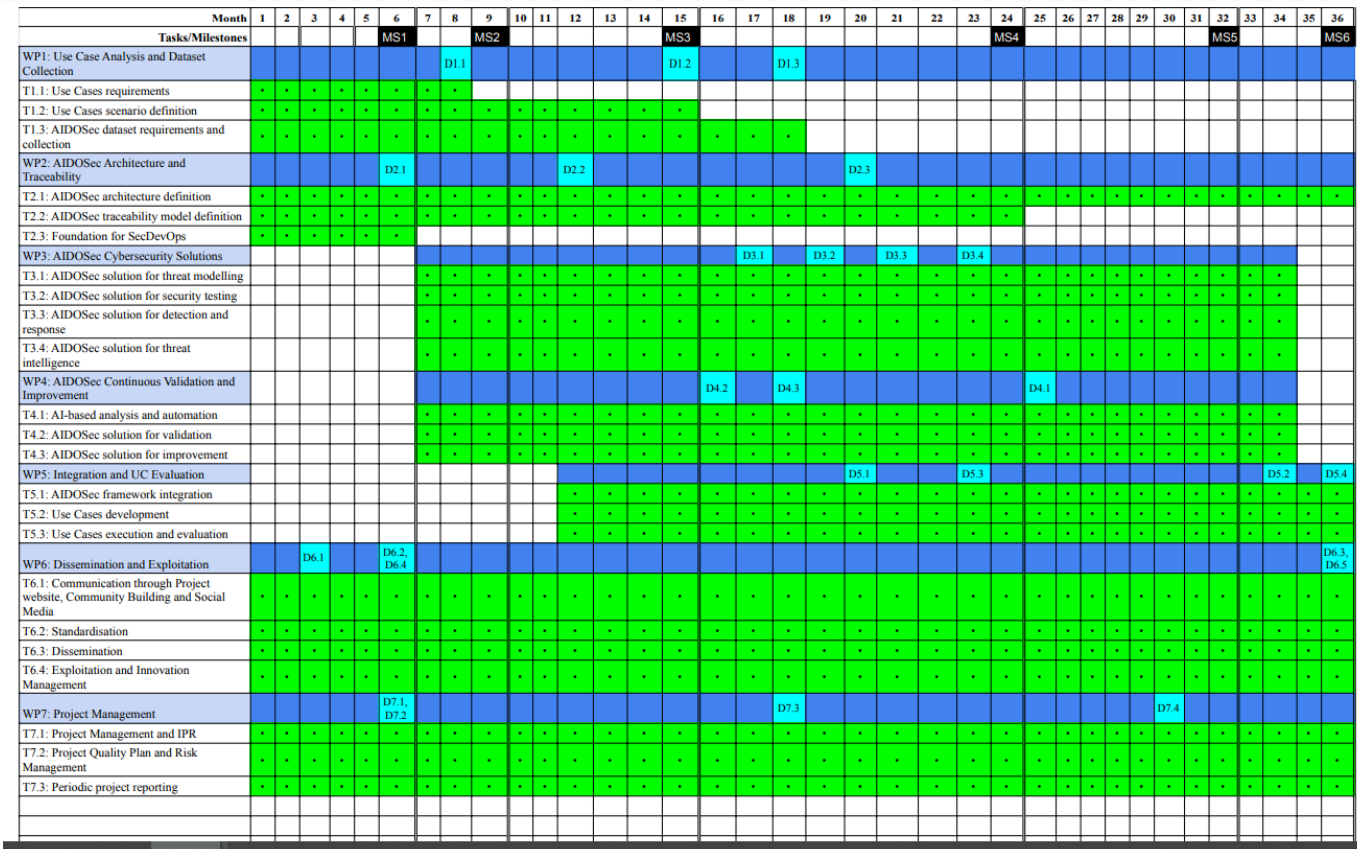


Fig. 3.1.3 AIDOSec Gantt chart

3.2 Consortium as a whole

3.2.1- Partners competencies and complementarities

AIDOSec requires a consortium consisting of companies and individuals having complementary skills, technology know-how and expertise. Scientific skills are required to develop theory innovations, a new scalable model persistence, test stories modelling and execution as well as cloud testing. Technological skills are essential when developing the proposed technologies and prototypes. Knowledge about end-user needs will enable us to identify adequate usage scenarios to derive reference requirements for AIDOSec technology. The AIDOSec consortium comprises a well-balanced combination of research, technology and end-user partners. It is visually shown on the following map.

The AIDOSec consortium consists of a well-balanced combination of:

- **Case study owners and end-user partners**: Providing knowledge of both end-users' needs and development scenarios for complex industrial systems.
- **Technology and service provider partners**: Providing knowledge and tools in DevSecOps, Threat modelling, Security Testing, Detection and Response to attacks, and AI technologies.
- **Research partners**: Providing knowledge in anomaly detection, fault localisation and foundational AI technologies.

Case study owners and end-user partners:

- **ABI** contributes to the project as a Use Case provider, bringing in its long-term experience in the automotive domain. ABI is a Tier 2 SME in the automotive market and an official supplier of embedded software for important world leaders in this market (e.g., Magneti Marelli, FCA, CNHi, TATA, BMW). ABI will contribute by offering embedded systems design covering the whole development cycle from idea and concept creation to cost-effective mass production arrangements. ABI can provide best-in-class service

and reduce cost and time to market thanks to its expertise and semi-product. ABI offices are fully equipped with desks, fibre and instrumentation for designing and testing embedded software and devices.

- **AR** is a Use Case provider in dependable AI for railway traction operation and e-mobility testing with potential solution provider partners RISE and MDU. AR intends to develop and provide AI solutions for data analysis and verification support. In this context, cybersecurity is vital to ensure trustworthiness.
- **CAM** will enhance its own camera-based and radar-based traffic systems, relying on standalone sensors with embedded processing, with mechanisms ensuring the credibility of information transferred to the server. This is partly about the security of the sensor itself and also about the non-repudiability of transferred data – the mechanism that needs to be developed in cooperation with BUT.
- **HIB** has extensive experience in health applications as manufacturers of the REVITA solution for hospitals, and in setting up private blockchain environments for their use in the managing of hospital data. HIB has experience in AI and the management of medical solutions and testing their solutions
- **PRO** will contribute with its expertise in providing requirements for its Use Case. PRO has experience defining and evaluating processes to improve the development/operations lifecycle, in this task, the objective will be to integrate security tools created or evaluated during the execution of the project. PRO has expertise in developing Use Cases using methodologies, frameworks and tools developed during the execution of R&D projects.
- **TEK**, as a Use Case provider, will contribute to defining the requirements of AIDOSec technological solutions that it will use to develop the demonstrator: an AI-based detector and classifier of security attacks on wireless communications. An iterative approach is planned, for tight cooperation with solution providers. TEK will contribute to evaluating the project results. TEK will lead the task T1.2.
- **THA** will provide a Use Case consisting of a drone platform focusing on secure communication with the ground station and the cloud. In addition, THA will develop a solution to detect security attacks over the network. THALES will also participate in exploitation, dissemination and standardisation activities. THALES is leading the TASK 5.2 on use-cases development.
- **TL** will provide a Use Case for manufacturing industries in which we will develop security-critical AI-based and XR-based Solutions to optimise manufacturing processes in the industry. By monitoring and simulating production conditions, we can identify unexpected events, and security breaches, test various conditions, and identify/mitigate unexpected security issues.
- **WMO** is a Use Case provider with existing automation in both a mature test framework (developed and maintained in-house over more than a decade) and a mature DevOps process (almost as mature as the test framework). In previous projects, InSecTT and AIDOaRt, WMO has used these frameworks to give input to research collaborations and extended automation. WMO also has previous experience in releasing datasets (e.g. publicly and in tight collaborations with individual NDAs) and has participated in similar projects previously (e.g. InSecTT and AIDOaRt). WMO will lead the task T1.3.
- **KAPSCH** will share learnings regarding the cost effectiveness of AI-supported secure solution development lifecycle with other partners of the AIDOsec project.
- **GTS** has the role in this project of one of a domain expert and industrial case study provider, bringing rail expertise into the project. With its role as a railway solutions provider for international markets, GTS will be able to provide the domain knowledge, safety background and prototyping infrastructure to show the applicability of the technologies developed in AIDOSec to their solutions.
- **MSG** contributes to the project as a Use Case provider with the Harmonized EU-CyberBridge Case Study. As a specialised firm in cybersecurity services, msg Plaut will collaborate within the case study alongside AIT to leverage and extend our expertise in cybersecurity standards and regulations.

Technology and service providers partners:

- **ABO** will contribute to UC requirements analysis and feedback, to UC scenario analysis and feedback, and to the definition and analysis of the requirements data sets. ABO will investigate ML/AI-based techniques for security test generation and will extend their previous work on ML/AI-based techniques for attack and intrusion detection in real time. ABO will also investigate the integration of test generation and monitoring solutions in CI/CD pipelines, will contribute to the integration of its tools into the AIDOSec framework, will assist with integrating its tools with the use cases targeted in the project, will contribute to evaluating the tools in the selected use cases and in collecting evaluation results. ABO will contribute to the dissemination effort on social media and in the local press, will disseminate the results of their work in

highly ranked academic journals and venues, will coordinate the Finnish cluster and contribute to the overall coordination of the project, and will submit periodic project reports to EC and national funding authority.

- **ACORDE** will contribute to a qualitative improvement in the security of the sensor and edge sides of industrial monitoring systems, as demonstrated in the maritime use case. ACORDE has wide experience in these subjects, and it will build up on the results of AIDOaRt. ACORDE is the leader of Task 4.2 "AIDOSec solution and validation".
- **COG** will provide its technologies for secure and efficient dynamic offloading of a part of machine-learning-based information processing from the edge to the cloud and will help Camea define and successfully validate its use case.
- **DT** will contribute to the detection and analysis of vulnerabilities in software systems throughout a SecDevOps engineering process.
- **HAL** plans to advance anomaly detection methodologies applicable across multisensory environments for comprehensive anomaly detection and analysis. Leveraging established one-class classification techniques, such as Subspace-Support Vector Data Description, we aim to enhance their efficiency in handling both uni and multimodal data for enhanced anomaly detection for improved performance of anomaly detection algorithms.
- **HIB** will collaborate with other AIDOSec participants to develop and implement advanced machine-learning techniques that automate repetitive and time-consuming cybersecurity tasks. Co-development of comprehensive traceability solutions: Collaborate on developing advanced traceability solutions that correlate security controls across different DevOps phases, enabling better vulnerability prediction and root cause analysis. As a Solution/Technology provider, we would be using the testing tools (developed by other partners in the project) in the development work of our remote control environment. On the other hand, we offer our environment to other partners as a place where they can test and develop their testing tools
- **INNORIV** will contribute to the project by exploiting new frontiers in cloud security aspects. Thanks to the active collaboration with some National service providers, Innoriv will explore new security requirements methodology, already improved in several previous EU projects, moreover, it can contribute to traceability model requirements. Thanks to expertise in the design and execution of tests and validation in complex systems, INNORIV can implement automatic tests.
- **INT** is a company developing AI tools in several domains. INT will contribute with its expertise in AI and ML. It will contribute with its expertise in automotive and railway cybersecurity and AI/ML.
- **LIE** will contribute to optimising the DevOps toolchain (pipeline, continuous integration, DevOps), offering LemonTree for model-based versioning integrated with the Enterprise Architect modelling tool.
- **PG** will contribute to the AI-based solutions by utilising Genius Core Platform, which is a web-based service that enables the creation and management of process models and simulations of industrial systems and workflows. The Platform uses AI-based techniques to optimise the performance, efficiency, and quality of the systems and workflows as well as to detect and prevent security threats. This solution will be applied to the Finnish use case for Manufacturing Industries as well as other potential cross-border use cases in collaboration with other partners.
- **SC,** as a leader in smart manufacturing innovations, is shaping security-critical AI-based solutions for AIDOSec in which they go beyond traditional methods by integrating 3D Laser Scanning and Photogrammetry for unmatched precision. These technologies combined with AI and CyberSecurity will transform data visualisation and position them to elevate smart manufacturing standards, focusing on precision, safety, and novel innovations integrated into the smart Manufacturing Industries Use Case.
- **SOFT** technology provider, will contribute with its expertise and tools for security threats modelling, security requirements analysis and automated recommendations for countermeasures. SOFT will be responsible for AIDOSec architecture and apply its best practices in model-based requirements engineering for large collaborative research projects. will apply the AIDOSec framework in its cyber-security offerings.
- **SWA** is an Italian cybersecurity company and would like to contribute with its expertise in vulnerability research and management to help achieve the project goals and, in turn, leverage the machine learning and MDE knowledge of the other consortium members to improve the quality and features of some of its solutions.
- **UNICA** is a technology provider and will mainly cooperate with ABI in porting at the edge the AI algorithms considered for the scenario on dedicated dataflow coprocessors.

- **UST** has vast experience working on Cloud and DevOps projects in different industries such as banking and finance, retail, logistics, and others, in which it has defined cloud architectures and adapted DevOps methodologies to the needs of its clients' workforces and to the most recent security requirements we are currently facing.

Research partners:

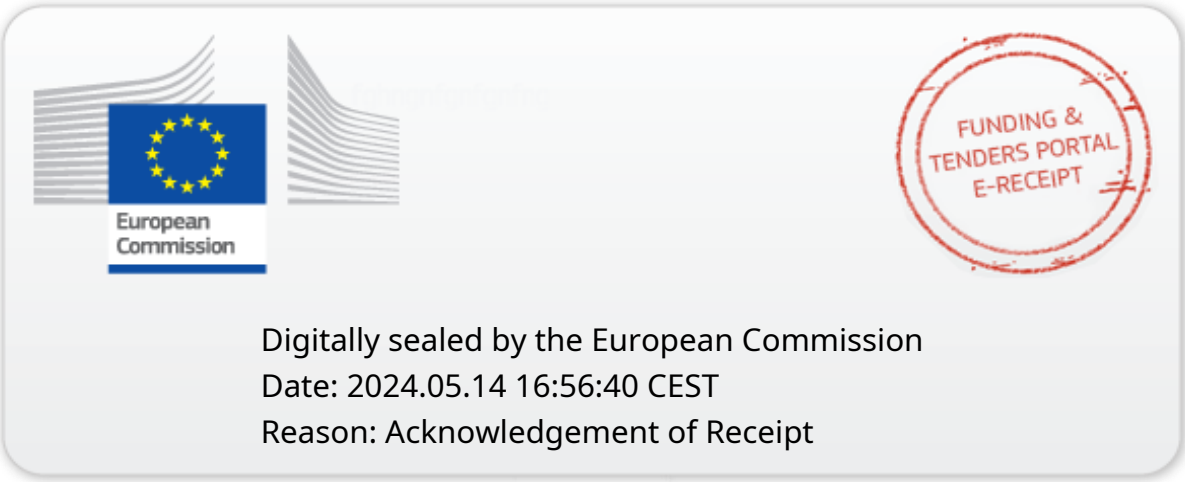
- **MDU** is the project coordinator of AIDOSec and the country coordinator of the Swedish sub-consortium. Thanks to its extensive experience in project coordination of ECSEL and Horizon projects, MDU is well equipped to steer the project coordination. Furthermore, MDU will lead WP7 on project management and WP6 on Dissemination and exploitation, as well as the tasks of communication and dissemination. Moreover, MDU contributes to AIDOSec with its expertise and technical solutions in continuous model-based system engineering, cybersecurity handling for CPSs, and smart/automated testing techniques for industrial systems.
- **AIT** will contribute to integrating security approaches in DevOps processes providing solutions for threat identification, impact and cascading effect estimation.
- **BUT** will contribute by exploring secure channels for processing and learning from data collected on-site, using, among others, homomorphic encryption, as well as secure monitoring and updating the models and the infrastructure.
- **IMT** will actively contribute to AIDOSec as both a research partner and a (research) solution provider. Notably, they will bring their long-term expertise in designing and developing model-based architectures and solutions to be applied to large and complex software-intensive systems from various domains. They will also bring their solid experience working within such large European projects (in particular ECSEL/KDT ones). Moreover, as the French consortium coordinator and the T2.2 leader, they will be strongly involved in the project management as a whole and thus act as a regular member of the project's core team.
- **JKU** will contribute to defining the overall architecture by promoting the integration of components and capabilities to support AI-augmented MDE capabilities for DevOps processes. JKU will contribute by proposing security threats, modelling and analysis, and support for MDE approaches (e.g., architecture modelling, and traceability mechanisms).
- **RISE** will lead Task 4.1 on AI-based security analysis and automation. RISE generally contributes to the project with expertise in Natural Language Processing (NLP) and Machine Learning (ML) for threat classification. In particular, RISE will build on the already developed prototypes in the failure log clustering with extensions to identify security-relevant failures in the nightly test execution log. In addition, RISE also plans to extend this solution to execution trace analysis to determine if an execution path/log is malicious or legitimate. Finally, RISE will also utilise its expertise in ML to explore anomaly detection algorithms in identifying potential security anomalies.
- **UEF** will contribute to the reliable safety-critical AI-based solutions for AIDOSec in the Manufacturing Industries domain. We will utilise sophisticated data analysis and machine learning techniques to track and evaluate the security level of complex systems and environments as well as to offer automated suggestions and feedback for enhancement. Our solutions will be used for the Finnish use case for Manufacturing Industries and other possible cross-border use cases in cooperation with other partners.
- **UOC** will contribute its expertise and experience from past projects in defining use case requirements, considering its intended contribution to the technical work packages, UOC is familiar with the needs of use case providers due to previous ECSEL projects. Its experience is based on MDE tools, processes and, in particular, in modelling traceability. UOC has extended competencies in the formalisation of datasets for AI, including the definition of a DSL and tool for this purpose (DescribeML). UOC has experience in modelling complex scenarios in a diversity of fields (including security) as well as validating and testing properties on models. As a tool provider, UOC will work to ensure the integration of its tools within the AIDOSec framework.

- **UNIVAQ** will contribute to the project by exploiting its expertise in ESL HW/SW co-design. UNIVAQ will extend and integrate a methodology, HEPSYCODE, that has been improved in several ways in past projects. This time the focus will be on security requirements at the system level.
- **UNISS** will contribute to the project by exploiting its expertise in formal modelling and verification as well as in AI and Deep Learning.
- **UNITE** will contribute to the solution for continuous validation and improvement. Specifically, UNITE will provide extensive knowledge regarding software engineering and artificial intelligence.

Competence Matrix	Sweden				Austria							Czech Republic			Spain						Finland						France			Italy								
Major Role	MDU	AR	RISE	WMO	AIT	GTS	DT	JKU	KAPSCH	MSG	LIE	BUT	CAMEA	COG	ACORDE	HIB	PRO	UNICAN	UOC	UST	ABO	HAL	PG	TL	UEF	SC	IMTA	SOFT	THA	ABI	INT	INNORIV	SWA	TEKNE	UNICA	UNISS	UNITE	UNIVAQ
Case study owners		·		·		·			·	·			·			·	·							·					·	·				·				
Technology and service providers					·		·				·			·	·	·		·	·	·	·	·	·	·		·	·	·			·	·	·					
Final user				·																																		
Research	·		·	·	·			·				·						·	·		·	·			·		·								·	·	·	·
Specific Areas																																						
Transportation		·				·			·	·																			·	·								
Telecom				·									·		·			·											·					·				
Manufacturing Industry				·						·													·	·	·	·												
SecDevOps	·		·	·		·	·	·		·	·					·		·		·	·	·						·								·		
Threat modelling	·		·		·			·			·								·			·			·			·		·								
Security testing	·			·		·			·			·			·						·							·										
Fault localization																											·											
Attack/anomalies detection and response	·		·				·								·						·	·			·													
AI technologies	·	·	·		·		·					·		·		·			·		·	·	·	·	·	·	·	·	·		·				·	·	·	
Standardization	·				·	·			·	·								·				·						·	·									
Tool publishing	·										·										·				·			·	·					·				·

Fig. 3.2.2 Competence Matrix

#§QUA-LIT-QL§# #§WRK-PLA-WP§#



This electronic receipt is a digitally signed version of the document submitted by your organisation. Both the content of the document and a set of metadata have been digitally sealed.

This digital signature mechanism, using a public-private key pair mechanism, uniquely binds this eReceipt to the modules of the Funding & Tenders Portal of the European Commission, to the transaction for which it was generated and ensures its full integrity. Therefore a complete digitally signed trail of the transaction is available both for your organisation and for the issuer of the eReceipt.

Any attempt to modify the content will lead to a break of the integrity of the electronic signature, which can be verified at any time by clicking on the eReceipt validation symbol.

More info about eReceipts can be found in the FAQ page of the Funding & Tenders Portal.

(https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq)