Topic: HORIZON-MSCA-2022-SE-01-01
Call: HORIZON-MSCA-2022-SE-01
Type of Action: HORIZON-TMA-MSCA-SE

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

WP1 – Project Coordination and Management
D1.1 Quality Assurance

Editors	UPRC
Authors	Christos Xenakis
Dissemination Level	PU
Type	R
Version	1.3

Project Profile	
Contract Number	101131292
Acronym	AIAS
Title	AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks
Start Date	Jan 1st, 2024
Duration	48 Months

Partners

University of Piraeus Research Center	EL
BEIA CONSULT INTERNATIONAL SRL	RO
UNIVERSIDAD DE MALAGA	ES
K3Y	BG
ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS	EL
SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED	CY
CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI	IT
FOGUS INNOVATIONS & SERVICES P.C	EL
UNIVERSITAT POLITECNICA DE VALENCIA	ES
PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA	PT

Document History

VERSIONS

Table 1 Document history

Version	Date	Author	Remarks
0.1	29/4/2024	UPRC	Table of Contents
0.2	15/05/2024	UPRC	Quality Assurance Plan section
0.3	24/05/2024	UPRC	Project Overview subsection
0.4	31/05/2024	UPRC	Subsections 2.1 - 2.4
1	14/06/2024	UPRC	First version
1.1	24/6/2024	Cristina Alcaraz (UMA), Javier Lopez (UMA)	Review
1.2	27/06/2024	UPRC	Revised version based on internal reviewer feedback.
1.3	28/6/2024	UPRC	Final version

AIAS message

Executive Summary

This deliverable details the quality assurance plan and project management handbook for the AIAS project. It is divided into two primary sections: the Management Handbook and the Quality Assurance Plan.

The Management Handbook begins by providing an overview of the project, including its budget, the consortium members, and the project's aims and objectives. It also offers a high-level description of the AIAS platform architecture. Following this, the document elaborates on the project management approach, detailing the methodology, deliverables, milestones, and resource commitments. This section also introduces the project management platform, focusing on the tools used for collaboration, task monitoring, and communication. Additionally, the handbook outlines the decision-making and conflict resolution mechanisms in place for the project. It concludes with a discussion on risk management, identifying potential risks and describing strategies to mitigate them.

The Quality Assurance Plan section emphasizes the project's communication strategies, including the presentation of the AIAS project logo, its website, and social media accounts. It outlines the protocols for arranging and conducting meetings, as well as the follow-up activities necessary to ensure effective communication and coordination. This section also details the standards for document naming and versioning, publication guidelines, and project reporting, all of which are essential for maintaining high-quality outputs and consistency throughout the project.

Overall, this document serves as a crucial guide for managing the AIAS project effectively and ensuring rigorous quality assurance at every stage.

Table of Contents

List of Figures

List of Tables

Abbreviations Table

Abbreviation	Description
CA	Consortium Agreement
DLT	Distributed Ledger Technology
EC	European Commission
ER	Experienced Researcher
ESR	Early-Stage Researcher
EC-GA	European Commission – Grant Agreement
ExC	Exploitation Committee
IPFS	Inter Planetary File System
PC	Project Coordinator
PM	Project Management
RTO	Research Technical Objective
SC	Scientific Coordinator
ToK	Transfer of Knowledge
WPL	WP Leaders
XAI	Explainable AI

Management Handbook

1 Project Overview

1.1 Project Profile

Table 2 AIAS Project profile

Programme	HORIZON.1.2 - Marie Skłodowska-Curie Actions (MSCA)
Call	HORIZON-MSCA-2022-SE-01
Topic	HORIZON-MSCA-2022-SE-01-01
Number	101131292
Acronym	AIAS
Title	AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks
Start Date	1 January 2024
Funding Scheme	HORIZON-TMA-MSCA-SE - HORIZON TMA MSCA Staff Exchanges
Funded under	Marie Skłodowska-Curie Actions (MSCA)
Overall Budget	1 564 000,00 EUR
EU contribution	1 564 000,00 EUR

1.2 List of beneficiaries

Table 3 AIAS project list of Beneficiaries

No.	Partner full name	Short name	Country
1	UNIVERSITY OF PIRAEUS RESEARCH CENTER	UPRC	GREECE
2	BEIA CONSULT INTERNATIONAL SRL	BEIA	ROMANIA
3	UNIVERSIDAD DE MALAGA	UMA	SPAIN
4	K3Y	K3Y	BULGARIA
5	ATHINA EREVNTIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS	ISI	GREECE
6	SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED	S5	CYPRUS
7	CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI	CNIT	ITALY
8	FOGUS INNOVATIONS & SERVICES P.C.	FOG	GREECE
9	UNIVERSITAT POLITECNICA DE VALENCIA	UPV	SPAIN
10	PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA	PDM E FC LDA	PORTUGAL

1.3 Aims and objectives

AIAS envisions a sustainable secure environment for AI systems employing a long-term, international and cross discipline research scheme to develop a novel platform for securing industries against AI adversarial attacks. AIAS aspires to design, develop, and validate a holistic platform for monitoring, protecting, and improving the robustness of AI systems against threat actors, while providing comprehensive and transparent explanations to administrators (i.e., via XAI) to configure their AI systems and mitigate adversarial AI attacks. The proposed solution aims to solidify the strategies to improve AI system’s resilience to cyberattacks safeguarding the confidentiality, integrity, and availability of their operations. AIAS’s training aims at providing the opportunity to Experienced Researchers/Early-Stage Researchers (ERs/ESRs) Transfer of Knowledge (ToK), and practical skills that will stimulate their professional growth through carefully planned cross partner training activities and interactions with the partner organisations and their respective networks in the markets of cybersecurity and AI. The ERs/ESRs will dive into State of the Art (SotA) and innovative research challenges, collaborate in a multicultural environment, and develop new hard and soft skills to become leaders in the employment market.

The objectives, denoted as RTOs, of the AIAS project are the following:

RTO 1: Conceptualize and develop a service architecture integrating AI-empowered applications, deception mechanisms, and mitigation techniques towards the holistic protection of organizations against cyberattacks and adversarial AI.
RTO 2: Design and develop a novel adversarial AI engine for creating attack scenarios tailored to the characteristics of the targeted organisations’ hardware and software infrastructure.
RTO 3: Design and implement novel intelligent deception methods based on high-interaction honeypots, digital twins, and virtual personas.
RTO 4: Design, develop, and assess AI-based methods for the detection and mitigation of cyberattacks including adversarial AI attacks as well as conceptualize and implement data collection and fusion methods.
RTO 5: Develop and verify explainable AI (XAI)-based recommendation engine empowering human in-the-loop proactive decisions to thoroughly mitigate adversarial AI attacks.
RTO 6: Assess the functionality, effectiveness and efficiency of AIAS in real-life scenarios.

1.4 AIAS platform

The AIAS platform comprises a number of components which along with their interdependencies are shown in Figure 1. Figure 1 depicts the basic system architecture to be further refined and documented in D2.1 Requirements & Reference Architecture as the project progresses. The integrated AIAS platform will rely on an architecture composed by Six distinct modules.

- The **Deception Layer** implements deception mechanisms based on high-interaction honeypots, digital twins and virtual personas to create a virtual imitation of the organization in order to deceive adversaries and lure potential attacks on the organization’s AI models and AI-based systems.

- The **Adversarial AI Engine Module (A2IEM)** generates adversarial AI attacks that will be deployed to test the robustness of the organizations AI systems.

- The **AI-based Detection Module (AIDM)** will employ *Life-long Reinforcement Learning* to detect known and unknown adversarial AI attacks and cyberattacks. Life-long reinforcement learning’s goal is to continuously and dynamically train the Reinforcement Learning model using the new information acquired from the ***Data Security Fusion base*** and the ***AIAS Decentralized Knowledge Base***.

- The **Mitigation of Adversarial AI Attacks Module (MIAIM)** will utilize the data from already detected attacks to recommend mitigation actions to human operators, based on comprehensible, transparent and explainable recommendations empowering security teams with a game theory-based and XAI recommendation engine for mitigation actions. A part of this module is the **Adversarial AI Mitigator (AIM)** that exploits game theory methods to collect and learn all possible mitigation techniques that can deal with each adversarial AI attack.

- The **Security Data Fusion** base is a data pool that gathers all the security data regarding the attacks that have occurred in the organization and were captured by the deception mechanisms, the attacks that have been detected by the AI-based Detection Module, the generated adversarial AI attacks, as well as it preserves the deployed mitigation methods.

- The **AIAS Decentralized Knowledge Base** *is* a Distributed Ledger Technology (DLT)-based InterPlanetary File System (IPFS) that collects all the security data from various instances of AIAS that have been installed in different organizations in a decentralized and distributed knowledge base.

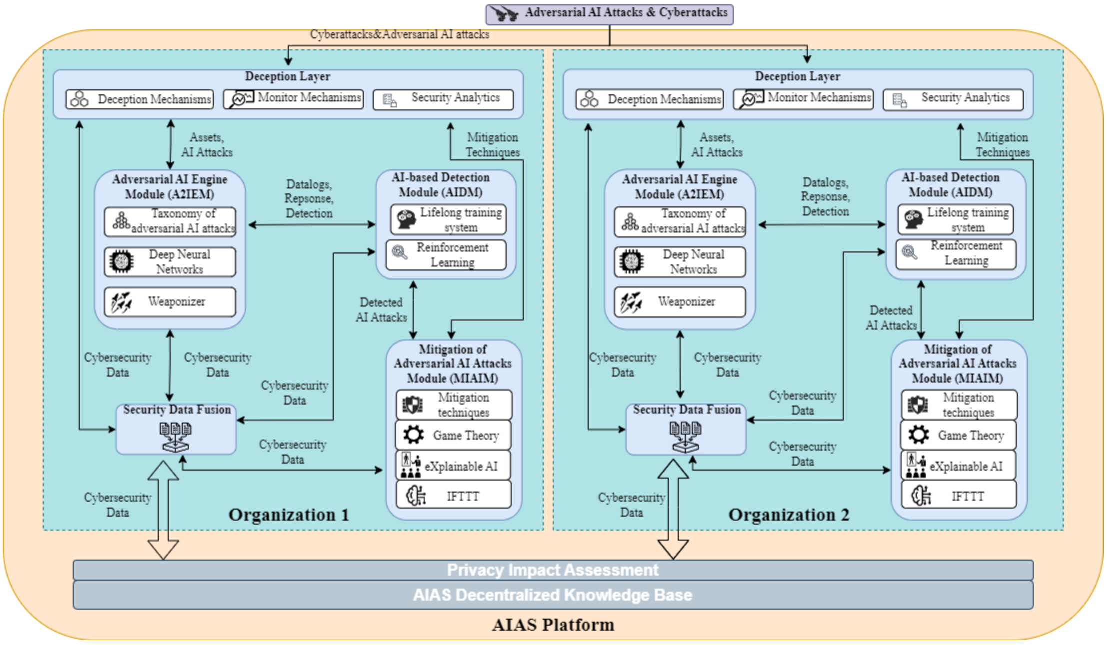

Figure 1 The AIAS Platform envisioned architecture (extracted from the GA)

2 Project Management

2.1 Gantt Chart

In Figure 2 the AIAS project Gantt Chart is depicted which indicates the duration of each task and Work Package while it indicates with a capital “D” the time in the project’s lifetime a deliverable is due.

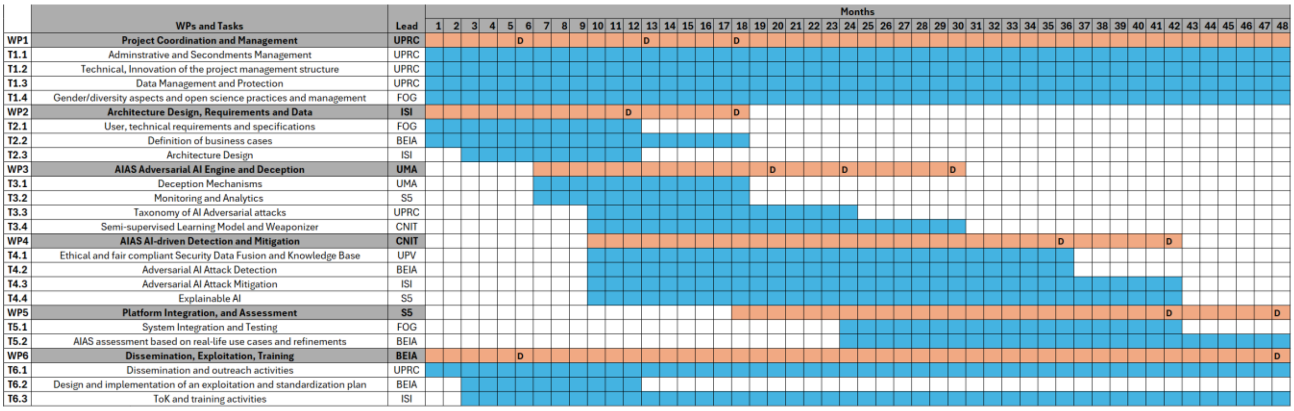

Figure 2 AIAS Project Gantt Chart

2.2 List of Deliverables

Table 4 lists the deliverables of the AIAS project along with the Work Package they belong to, the dissemination level and the due date.

Table 4 AIAS Project List of Deliverables

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	Quality Assurance	WP1	1 - UPRC	R - Document, report	PU - Public	6
D1.2	Data Management Plan	WP1	1 - UPRC	R — Document, report	PU – Public	6
D1.3	Progress Report	WP1	1 – UPRC	R – Document, report	SEN - Sensitive	13
D1.4	Mid-term Meeting	WP1	1 – UPRC	R – Document, report	SEN – Sensitive	18
D2.1	Requirements & Reference Architecture	WP2	8 – FOG	R – Document, report	PU - Public	12
D2.2	Specification & Business cases	WP2	5 - ISI	R – Document, report	PU - Public	18
D3.1	AIAS Deception Layer	WP3	3 – UMA	R- Document, report	PU – Public	20
D3.2	Taxonomy of Adversarial AI attacks	WP3	1 – UPRC	R – Document, report	PU – Public	24
D3.3	Adversarial AI Engine	WP3	7 – CNIT	R – Document, report	PU - Public	30

D4.1	AI-based Detection of Adversarial AI Attacks	WP4	9 – UPV	R – Document, report	PU – Public	36
D4.2	Mitigation of Adversarial AI Attacks & XAI	WP4	5 – ISI	R – Document, report	PU – Public	42
D5.1	Platform Integration	WP5	8 - FOG	R – Document, report	PU – Public	42
D5.2	Platform Evaluation	WP5	2 – BEIA	R – Document report	PU - Public	48
D6.1	Dissemination plan	WP6	1 – UPRC	R – Document, report	SEN – Sensitive	6
D6.2	Dissemination and Standardization Activities, Market Analysis and Exploitation Plan	WP6	2 - BEIA	R — Document, report	PU - Public	48

2.3 List of Milestones

The AIAS project Description of Action contains milestones for each Work Package that help verify and monitor the progress of the work towards the project’s objectives. Even though milestones do not constitute separate deliverables, they are crucial to the project’s internal organization. The milestones identified for AIAS are listed in Table 5.

Table 5 List of AIAS project milestones

#	Title	Related WPs	Due Date	Means of Verification
1	Consortium Agreement	1	M1	CA completed
2	Kick-off meeting	1	M1	Kick-off meeting held
3	Requirements definition and initial dissemination networking activities	1,2,6	M12	D1.1, D1.2, D2.1, D6.1 submitted, social media and project website up and running, 2 newsletter issued, 1st brochure released, at least 8% of the secondments started, >1 public talks, 1st workshop
4	Development started, and planned actions completed	1,3,6	M24	D1.3, D1.4, D2.2, D3.1, D3.2 submitted, 1st trailer release, 3 newsletters issued, 2nd brochure released, at least 45% of the secondments have started, >1 public talks, 1st open day, FAQ released, 2nd workshop, 1st hackathon
5	Half of the AIAS modules completed	3,4,6	M36	D3.3, D4,1 submitted, 3 newsletters issued,1st video released, 3rd brochure released, 1st article, 1st industrial exhibition, 2nd open day, at least 75% of the secondments started

6	AIAS modules individually implemented and tested, and first version of AIAS module platform delivered	3,4,5	M44	D4.2, D5.1 submitted, as least 96% of secondments started, 2 newsletters issued, 2nd video released, 3rd brochure released, 2md article, 1 white paper released, 2nd industrial exhibition
7	Final version of AIAS module platform delivered	5,6	M48	D5.2, D6.2 submitted, secondments completed, 1 newsletter issued, 2nd trailer released

2.4 Resources to be Committed

The realisation of the objectives of AIAS requires commitment of human (Person-Months) and other (equipment, workshops, travel costs, etc.) resources. All in all, the project’s total budget is **€1,564,000.00**, which is equal to the total EU requested contribution. The consortium aims to minimize travel requirements by utilizing the following strategies: (i) conducting conference calls and videoconferences, (ii) coordinating events to coincide with other gatherings that many partners are already attending, and (iii) using partners' VPN facilities for remote integration tasks without incurring extra costs. The budget also includes auditing expenses for partners who need to obtain certificates.

Table 6 Staff effort per participant

Participant	WP1	WP2	WP3	WP4	WP5	WP6	Total Person-Months
1 – UPRC		7	16	15	12		50
2 – BEIA		7	7	8	8		30
3 – UMA		8	18	7	9		42
4 – K3Y		8	6	4	6		24
5 – ISI		15	9	6	5		35
6 – S5		5	7	3	15		30
7 – CNIT		9	10	20	6		45
8 – FOG		6	8	6	10		30
9 – UPV		9	7	7	7		30
10 - PDM		4	4	7	9		24
Total Person - Months	0.00	78.00	92.00	83.00	87.00	0.00	340

2.5 Governance structure and procedures

The organisational structure of the consortium comprised by the following Consortium Bodies:

- The **Project Coordinator Christos Xenakis (UPRC)** is the legal entity acting as the intermediary between the Parties and the Granting Authority. The Project Coordinator shall, in addition to its responsibilities as a Party, perform the tasks assigned to it as described in the EC-GA and the Consortium Agreement (CA).

- The **Steering Board** is the decision-making body of the Consortium. The Steering Board shall consist of one representative of each Party (referred to as “*Member*”) as Table 5 indicates.

Table 7 Steering Board of AIAS

No.	Partner Full Name	Member (Name /Surname)
1	UNIVERSITY OF PIRAEUS RESEARCH CENTER	Christos Xenakis
2	BEIA CONSULT INTERNATIONAL SRL	George Suciu
3	UNIVERSIDAD DE MALAGA	Cristina Alcaraz

4	K3Y	Panagiotis Radoglou-Grammatikis
5	ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS	Ilias Politis
6	SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED	Sotiris Koussouris
7	CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI	Giuseppe Bianchi
8	FOGUS INNOVATIONS & SERVICES P.C.	Dimitris Tsolkas
9	UNIVERSITAT POLITECNICA DE VALENCIA	Carlos E. Palau
10	PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA	Luís Miguel Campos

- The **Project Technical Manager Ilias Politis (ISI)** shall chair all meetings of the Steering Board (“chairperson”). The Project Technical Manager is designated initially by the Project Coordinator, and any subsequent change requires approval of the Steering Board.

- The **Scientific Coordinator Christos Xenakis (UPRC)** is responsible for overseeing the Project technical work. The mandate of the Scientific Coordinator is to: i) Accomplish the technical objectives of the Project; ii) Supervise, plan and progress the Project’s technical output; iii) Promote, in association with the Project Technical Manager, Project’s visibility in the international forums; iv) Ensure the overall technical co-ordination and technical content of the Project; v) Ensure that technical decisions are made in time; vi) Monitor the overall technical progress; vii) Identify potential problems with intersections between different functions; viii) Give technical presentations both internally and externally; ix) Support the Project Coordinator to manage the total Project.

- The **Exploitation Committee (ExC)** will be in charge of ensuring that the results are efficiently disseminated and exploited. It will consist of representatives from each beneficiary. The ExC's tasks will be coordinated by the PC and approved by the SC. The ExC's primary responsibilities will be to develop plans for exploitation and knowledge exchange.

- **WP Leaders (WPL)**: They will oversee all WP operations. They will submit reports to the PC, schedule regular technical meetings, assure program punctuality, and manage people and resources effectively. The PC will immediately note any discrepancies in the signed contract. WPLs will take the lead in preparing deliverables and ensuring that objectives and milestones are met on schedule.

- The **Participant Managers (PMs)**, represent each partner in the Granting Authority and participate in voting procedures as regards administrative or technical issues of the project.

- The **External Advisory Board (EAB)** consists of four well known external, independent experts coming from the business spectrum. The EAB will offer high-end consultation services to the consortium to ensure that the project results will match the community’s and stakeholders’ needs. ANNEX 1 presents the signed NDA among the EAB members. Table 8 lists the members of the EAB.

Table 8 EAB member of AIAS

No.	Member (Name /Surname)	Organization	Email
1	Panagiotis Bountakas	Sphynx Technology Solutions AG	p.bountakas@sphynx.ch

2	Evangelos Kotsifakos	Lstech Espana SL	ekotsifakos@lstech.io
3	Konstantinos Papadamou	Trinomial Technologies Ltd.	kostantinos.papadamou@trinomial.xyz
4	Styliani Tsitsoula	Hellenic Cybersecurity Institute	st@hcsi.gr

2.6 Project Management Platform

2.6.1 Microsoft SharePoint

The consortium agreed to use Microsoft SharePoint to facilitate collaboration in the authoring of deliverables and reports in real time and to achieve consistency. Additionally, the Microsoft SharePoint is used among the consortium as the project’s document repository.

2.6.2 Gitlab

Gitlab was chosen by the consortium as the development collaboration tool and the project’s code repository. The main incentives behind this decision were:

- Integrated CI/CD: which offers built-in continuous integration and continuous deployment (CI/CD) capabilities without needing third-party integrations. Making it easy to automate testing and deployment processes within the same platform.
- Self-Hosting: This allows organizations to run their GitLab instance on their own servers, providing full control over their codebase and data.
- DevOps Lifecycle Management: GitLab offers tools for every stage of the software development lifecycle, from planning and source code management to CI/CD, monitoring, and security.
- Issue Tracking and Project Management: GitLab allows issue tracking and project management features.
- Free Private Repositories.
- Security Features: Built-in security testing tools, including static application security testing, dynamic application security testing, container scanning and dependency scanning as part of its CI/CD pipeline.
- Open Source: The community Edition of GitLab is open-source which facilitates transparency and control.

2.6.3 ClickUp

To monitor the progress of each task and deliverable within the project the coordinator has setup an instantiation of the Click Up project management and monitoring tool. The Click Up tool enables setting deadlines, beginning of tasks and deliverables, assign tasks to consortium members and set end-points.

2.7 Internal Communication

2.7.1 Mailing List

To facilitate communication among the AIAS consortium partners, a general email list (aias-project@ssl-unipi.gr) has been established. If a consortium member wishes to be added to or removed from this general communication list, they should reach out to the AIAS project consortium coordinator, UPRC, who manages the mailing list.

2.7.2 Communication Tools

A crucial element for a project’s successful management, is the continuous and effective communication between the members of the consortium. For that reason, from day one in the AIAS project life, the coordinator has provided to the consortium members the necessary tools/software to facilitate their work and effective communications among them. One of these tools is the virtual meeting platform Microsoft Teams for organizing and hosting online meetings. Other communication tools include but are not limited to the project’s mailing list.

2.8 Decision making mechanism and Conflict Resolution

The AIAS consortium members will seek consensus of all involved or affected parties to reach a decision. However, in case after considerable amount of effort this cannot be achieved and to avoid dead-ends in project operational progress, a majority vote of 2/3 would be sufficient for approving a decision. In the extreme case that the decision taken is unacceptable according to the partners found in the minority, the resolution of the conflict will be escalated to each partners higher executive, and if still a consensus is not feasible, the coordinator will forward the issue to the EC Project Officer. Finally, the process is concluded by signing a CA among the involved consortium members for guaranteeing the compliance with selected decisions and tasks/obligations.

2.9 Risk management approach

In the AIAS project risks may arise in different areas or stages of its evolution including but not limited to technology maturity, the availability of data and information, risks related to integration, business use cases, and commitment. One of the key responsibilities of the Project Coordinator and the Project Coordination Team is the scientific and technical risk management of the project. Therefore, the AIAS risk management framework includes:

- Identifying risks with adverse effects or impacts.
- Evaluating and quantifying the risks, rating the likelihood of occurrence, and level of severity.
- Contingency Planning and contingency actions.
- Control and monitoring of risks and related documentation.
- Managing outcomes and minimising negative impact.

Additionally, the AIAS project risk analysis framework classifies risks per category and prioritizes risk monitoring according to their level of likelihood (low, medium and high) and their Level of Severity (low, medium and high).

- Low: risks that potentially can affect the success of a Task. The AIAS project foresees that the Task leader will manage the risk and the WP leader is informed.
- Medium: risks that potentially affect the success indicators of a particular work package. WP leader manages risk, the project leader is informed, and the risk is brough to the attention of the Project Coordination Team.
- High: risks with high impact are risks that may seriously affect the success of indicators of the whole project. The risk is brought to the attention of the Project Officer (EC).

Finally, based on the experience accumulated during previous pertinent projects and AIAS project’s unique nature an early identification and assessment of possible risks and mitigation measures has been carried out and presented in Table 9.

Table 9 : Critical risks & risk management strategy (PM : Project Management, TEC : Technical, L: Likelihood, S: Severity, L: Low, M: Medium, H: High)

Risk number	Description	Work Packages No (s)	Proposed Mitigation Measures
1	Secondments of researchers may affect dynamics in SMEs.	WP2, WP3, WP4, WP5	**[Level of Likelihood: Medium | Level of Severity: High]** Mitigation: There are scientists and engineers inside SMEs who guarantee employee secondments. Contingence Plan: The SMEs will recruit new researchers and engineers.
2	Intellectual Property issues	WP1, WP6	**[Level of likelihood: Low | Level of Severity: Medium]** Mitigation: Define detailed IP rights in the CA. Contingency Plan: Escalate critical issues to GA and CA.
3	Too loose system requirements and architecture in accordance with the technical challenges individuated by the project proposal	WP2, WP3, WP4, WP5	**[Level of Likelihood: Medium | Level of Severity: High]** Mitigation: Beneficiaries from the industrial sector will be actively engaged in the system design process. Their knowledge will aid in preventing such issues. Contingency Plan: In our strategy, we anticipate a review of partner criteria for the implementation WPs. Solicit input from stakeholders in order to expand and modify requirements.
4	Selected business use cases do not cover the complete spectrum of solutions	WP2, WP5	**[Level of Likelihood: Low | Level of Severity: High]** Mitigation: Using an iterative process, the use cases and accompanying technological solutions will be established early on in the project. Contingency Plan: Possible use case versus offered solution gaps will be identified and addressed with new or revised business use cases.
5	One or more AIAS modules do not achieve the expected quality	WP3, WP4	**[Level of Likelihood: Low | Level of Severity: High]** Mitigation: AIAS will use agile software development to allow the project coordinator and steering committee to promptly detect such a risk if it materializes and to implement appropriate mitigation measures to address the problem. Contingency Plan: Another partner will be responsible for enhancing the module.
6	Interface difficulties between WPs and difficulties in the integration process. Causing delays, degraded quality of deliverables and/or reduced functionality of the system.	WP3, WP4, WP5	**[Level of Likelihood: Low | Level of Severity: Critical]** Mitigation: The development of modules will adhere to WP2-specifications and architecture, including the interface requirements between them. In WP3, WP the various modules will be tested against these requirements to reduce the possibility of integration issues. In addition, a comprehensive integration strategy will be prepared. Contingency Plan: The majority of the consortium's AIAS partners have expertise with development and integration activities, allowing them to assume responsibility for a partner who may encounter issues during integration.
7	No achievement of the anticipated degree of dissemination/standardization	WP6	**[Level of Likelihood: Low | Level of Severity: High]** A plan for standardizing and distribution has been developed. These actions will be regularly monitored to

			ensure that the desired levels are met. Negative comments will result in rapid improvement measures, even if they extend beyond the project's lifespan
8	Delay in the execution of secondments	WP1, WP2, WP3, WP4, WP5, WP6	**[Level of Likelihood: Medium | Level of Severity: High]** Mitigation: A designated individual will oversee the execution of secondments at the level of each partner. At the project level, the Coordinator will organize teleconferences every one to two months to evaluate the tracking of secondments and gather information about any discovered delays at the participant and sending institution level. On the other hand, each Partner is responsible for ensuring that the secondments occur as planned and must notify the Coordinator of any potential deviations immediately or no later than two months before the scheduled secondment. After a possible delay has been detected, the Consortium or the Steering Committee will establish action plans (where is the case). Contingency Plan: The Coordinator will notify REA of the solution discovered.
9	Withdrawal of participants	WP1, WP2, WP3, WP4, WP5, WP6	**[Level of Likelihood: Low | Level of Severity: High]** Mitigation: Another partner will lead the tasks/WP of the departing partner. Contingency Plan: If not, REA might agree to incorporate a new partner with the same exact competence in the project.
10	Staff turnover	WP1	**[Level of Likelihood: High | Level of Severity: Low]** Mitigation: All partners include high-skilled employees. Contingency Plan: All participants will identify extra employees with the required expertise who are not originally meant to be seconded to the project activity to mitigate risk.
11	Fellows fail to meet the target RTOs, MVOs, KPIs of the projects	WP1, WP2, WP3, WP4, WP5, WP6	**[Level of Likelihood: Low| Level of Severity: Low]** Mitigation: Fellows will be able to stay on track due to the cross-sectoral two-supervision provided by experienced professionals and the SotA research facilities of beneficiaries. Contingency Plan: If required, R&T funding will be utilized to acquire new instruments, software, hardware, or fellows will get extra training.
12	Inadequate coordination	WP1, WP2, WP3, WP4, WP5, WP6	**[Level of Likelihood: Low| Level of Severity: High]** Mitigation: As coordinator for previous experience in coordinating with MSCA programmes. Contingency Plan: The CA will also provide a method for replacing PC to reduce this risk.
13	Dataset not available for testing	WP3, WP4, WP5	**[Level of Likelihood: Medium | Level of Severity: Medium]** Mitigation: Participants have already identified existing datasets. Contingency Plan: If necessary, fellows will exploit existing and open-access datasets.
14	Significant and unresolved potential risks	WP1, WP2, WP3, WP4, WP5, WP6	**[Level of Likelihood: Low | Level of Severity: High]** Mitigation: Thorough list of risks together with mitigations and contingency plan. Contingency Plan: Escalate critical issues to GA and CA.

Quality Assurance Plan

1 Communication

The project's communication strategy aims to attract potential endorsers, end users, and consumers through a series of activities that effectively convey the project's outcomes to the appropriate target audiences. The central objective of communication operations within AIAS will be to augment project awareness by utilizing non-electronic and electronic channels. Furthermore, interactive and non-interactive efforts will be used, including the upkeep of the project website and the delivery of social media presentations.

The next objects and tools are among the most pivotal in the realm of communications:

- **Build a visual representation of the AIAS identity**. Creating the AIAS logo and textual communication templates, which all project partners will use in their distribution and communication efforts. This will make it easier to establish a unique brand. Below, the official AIAS logo is presented:

Figure 3 Official AIAS logo

- **The development and maintenance of the project website** is essential for efficient communication and distribution of information throughout the project's lifecycle. The website is overseen by S5 and will remain accessible online for at least two years following the completion of the project. The website will disseminate publicly available information, including comprehensive project details, activities, consortium partners, and public deliverables, as well as the project's significant outcomes (e.g., scientific publications). The AIAS website was established in M02 and can be visited by following the specified link: https://www.aias-project.eu/
- **Utilizing social media platforms to disseminate information**. The AIAS consortium plans to initiate a social media campaign by establishing Facebook, LinkedIn, Threads, YouTube, and X/Twitter accounts. The purpose is to disseminate vital information to the general public. S5 oversees the management of all social media platforms and maintains consistent updates to maintain up-to-date content and direct people to the primary project website. Below are the official social media profiles of the AIAS project:
    - **Facebook**: AIAS MSCA: https://www.facebook.com/aias.msca/ [FBA]
    - **LinkedIn**: account AIAS MSCA https://www.linkedin.com/in/aias-msca-0a19382b8/ [LNA]
    - **X/Twitter**: account AIAS_MSCA: https://twitter.com/AIAS_MSCA [XTA]

- **YouTube**: Channel of AIAS: https://www.youtube.com/@AIAS-project [YTA]

2 Project Meetings

The Project Coordinator (UPRC) holds a crucial role in overseeing all meetings of the General Assembly, unless the General Assembly decides otherwise. It is mandatory for all members of the General Assembly to attend or be represented at any meeting. They have the option to nominate a substitute or proxy to attend and vote on their behalf. Moreover, their active and cooperative participation throughout the meetings is expected. The chairperson is mandated to organize regular sessions of the General Assembly at least twice a year.

The chairperson must also organize special meetings whenever a Member submits a written request. The chairperson must provide written notification of a meeting to each Member promptly, no later than 14 calendar days before an ordinary meeting and 7 calendar days before an exceptional meeting. The chairperson must create and deliver an agenda to each Member at least 14 calendar days before the meeting, or 7 calendar days before an exceptional meeting. Any agenda item that necessitates a decision by the Members must be indicated as such on the agenda. Any Member has the authority to include an item in the initial agenda by providing written notice to all other Members at least 7 calendar days before and 2 days before an extraordinary meeting. At a General Assembly meeting, the attending or represented Members can unanimously consent to including a new item in the initial agenda. The General Assembly can conduct meetings using tele- or videoconferencing, as well as other telecommunication methods. The Coordinator can make decisions without convening a meeting if the Coordinator shares a proposed decision with all Members of the General Assembly and sets a deadline for responses of at least 7 calendar days. The decision will be considered agreed upon if at least 51% of Responding Parties agree, and in case of a tie, the Coordinator's vote will have the final say. The chairperson is responsible for creating minutes for each meeting, which serve as the official record of all decisions made. The individual must distribute a preliminary version of the meeting minutes to all participants within 10 days following the meeting. The minutes will be deemed acceptable if, within 7 calendar days after receiving them, no Party has raised a complaint to the chairperson regarding the accuracy of the draft minutes through written notice. If an objection is raised, the chairman will address it by engaging with the opposing party. If necessary, the chairperson will then conduct a vote among the members present at the meeting. The ultimate determination will be reached through a voting process requiring a simple majority.

The Coordinator's responsibilities include

- Organizing meetings.
- Suggesting decisions.
- Creating the agenda for General Assembly meetings.
- Leading the meetings.
- Documenting the minutes.
- Overseeing the execution of decisions made during the sessions.

3 Document naming and versioning

Most of this project's output will comprise documentation, encompassing deliverables and publications. The naming and version control systems are presented below. Figure 4 serves as template for naming internal non-deliverable project documents.

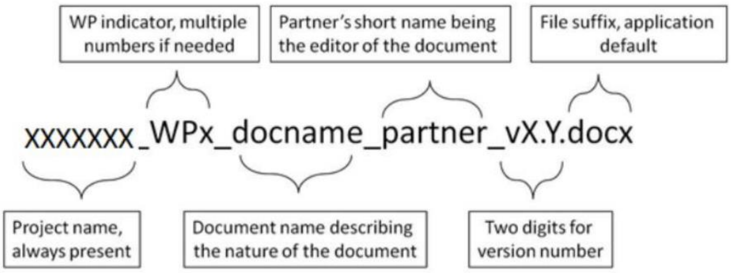
WP indicator, multiple numbers if needed
Partner’s short name being the editor of the document
File suffix, application default
xxxxxxx_WPx_docname_partner_vX.Y.docx
Project name, always present
Document name describing the nature of the document
Two digits for version number

Figure 4 Internal AIAS Document Naming

A representation of the minutes from the kick-off meeting is depicted in figure 5.

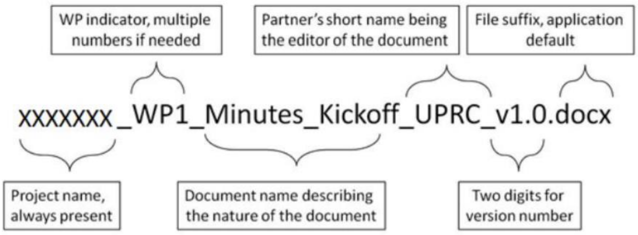
WP indicator, multiple numbers if needed
Partner’s short name being the editor of the document
File suffix, application default
xxxxxxx_WP1_Minutes_Kickoff_UPRC_v1.0.docx
Project name, always present
Document name describing the nature of the document
Two digits for version number

Figure 5 Internal AIAS Document Name Example – Minutes of Kick-off Meeting

To avoid the irreversible loss of past information as the review process progresses, it is necessary to increment the minor variant number each time a document is evaluated, even if the author reviews it.

Deliverables to the Commission will be given a unique name style, as it is shown in figure 6.

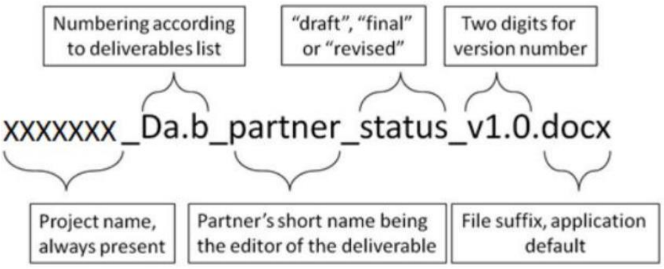
Numbering according to deliverables list
“draft”, “final” or “revised”
Two digits for version number
xxxxxxx_Da.b_partner_status_v1.0.docx
Project name, always present
Partner’s short name being the editor of the deliverable
File suffix, application default

Figure 6 Naming of AIAS Deliverable

An example –first draft version of D1.1 - is shown in figure 7.

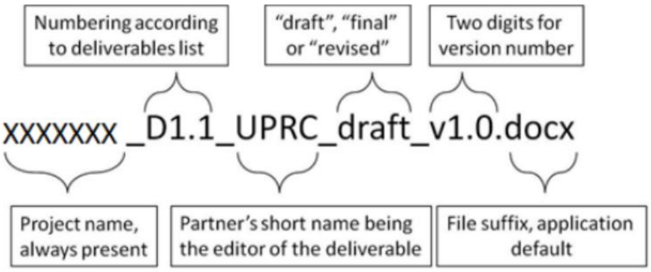
Numbering according to deliverables list
“draft”, “final” or “revised”
Two digits for version number
XXXXXXX _D1.1_UPRC_draft_v1.0.docx
Project name, always present
Partner’s short name being the editor of the deliverable
File suffix, application default

Figure 7 AIAS Deliverable Name Example – First Draft Version of Deliverable D1.1

4 Publication guidelines

Partners in the project can publish publications based on their contributions. These publications will be submitted to journals that allow open access, as stipulated by the EC. Scholarly publications that provide unrestricted access to their papers are often preferred. When project participants are required to submit articles to journals or proceedings with a lower level of open-access, which necessitates either parallel publication or an embargo period, the requirement will be evaluated based on the delay and level of audience access provided by the specific publication method.

An acknowledgment of AIAS support must be included in all related publications, using the following statement: “*The research has received funding from the European Commission’s Horizon research and innovation programme under grant agreement No. 101131292*.”

5 Project reporting

The Project Coordinator must submit regular activity reports to the EC, at month 24th month and on 28th month. The reports provide a detailed summary of the partners' activity, including accomplishments, cooperation, resource allocations, and plans. They and the financial statements will serve as the principal project management documents. The processes stated in the Grant Agreement clearly describe the steps that will be taken.

References

FBA	Facebook page of AIAS https://www.facebook.com/aias.msca/
LNA	LinkedIn account of AIAS https://www.linkedin.com/in/aias-msca-0a19382b8/
XTA	X/Twitter account of AIAS: https://twitter.com/AIAS_MSCA
DSN	Dropbox Sign https://sign.dropbox.com/
GA	AIAS Grant Agreement
YTA	AIAS YouTube channel https://www.youtube.com/@AIAS-project

Annex 1

Below the signed NDA is presented. The DropboxSign [DSN] has been used as a tool to request and collect signatures.

NDA for AIAS External Advisory Board

This confidentiality declaration (hereinafter the “Declaration”) is made effective as of the date of signature of this Declaration by

The undersigned:

1. Panagiotis Bountakas, Sphynx Technology Solutions AG., p.bountakas@sphynx.ch
2. Evangelos Kotsifakos, Lstech Espana SL, ekotsifakos@lstech.io
3. Konstantinos Papadamou, Trinomial Technologies Ltd., kostantinos.papadamou@trinomial.xyz
4. Styliani Tsitsoula, Hellenic Cybersecurity Institute, st@hcsi.gr

Declares towards:

5. UNIVERSITY OF PIRAEUS RESEARCH CENTER – UPRC
6. BEIA CONSULT INTERNATIONAL SRL – BEIA
7. UNIVERSIDAD DE MALAGA – UMA
8. K3Y – K3Y
9. ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS – ISI
10. SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED – S5
11. CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI – CNIT
12. FOGUS INNOVATIONS & SERVICES P.C. – FOGUS
13. UNIVERSITAT POLITECNICA DE VALENCIA – UPV
14. PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA - MDPFC

Hereinafter individually referred to as the “Project Partner” and collectively as “Project Partners”,

Whereas:

- Project Partners collaborate in the project “AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks” (AIAS);

- External Advisory Board (EAB) Member will be part of the EAB and will in that role potentially become aware of any confidential information of Project Partners;

- Project Partners therefore ask the Member to execute this Declaration;

Declares as follows:

1. Confidential information is understood to mean: all information, documents and data of Project Partner or Project Partners and/or related to the Project which is designated as ‘confidential’.

2. EAB Member undertakes:

    a) to use any Confidential Information that he/she/they becomes aware of in the context of his/her/their work as EAB Member for the AIAS consortium (the “Work”) exclusively in the context of the Work;

    b) to observe secrecy with respect to the Confidential information;

c) not to disclose Confidential Information to third parties without the permission of the Project Partner who owns the Confidential Information;

d) to take all reasonable steps to ensure that the Confidential Information shall be protected against loss and unauthorized access.

3. The confidentiality obligations referred to in paragraph 2 shall not apply to Confidential Information of which EAB Member can sufficiently provide evidence that it:

a) was already in the public domain before the disclosure to EAB Member or later on becomes public without the direct or indirect responsibility of EAB Member;

b) was already known by EAB Member or was in EAB Member's possession prior to the disclosure;

c) was independently developed by EAB Member without recourse to the Confidential Information;

d) was received by the EAB Member from a third party who was legally entitled to disclose that information;

e) is required under a statutory duty and/or court order to be disclosed, provided that prompt advance notice is given to the respective Project Partner or Project Partners and such disclosure shall be as limited as possible.

4. The obligations referred to in paragraph 2 will remain in effect for ten years after the Work has ended.

5. All Confidential Information (including all copies thereof) shall remain the sole and exclusive property of the owning Project Partner and shall be returned to this Project Partner or destroyed upon request of this Project Partner, and in any event after the Work has ended. However, EAB Member may retain one copy of the Confidential Information for compliance purposes. For the avoidance of doubt, the confidentiality obligations of this Declaration shall remain applicable for this copy.

6. No warranties, representation, rights, title, interest or licenses to trademarks, inventions, copyrights or patents are implied or granted under this Declaration and the Confidential Information is provided "as is". EAB Member is not allowed to apply for intellectual property rights related to Confidential Information.

7. This Declaration is governed by the laws of Belgium. All disputes arising out of or in connection with this Declaration, which cannot be solved amicably, shall be finally settled by the courts of Brussels.

Name: Panagiotis Bountakas
Organization: Sphynx Technology Solutions AG
Signature:

Date:05 / 15 / 2024

Name: Evangelos Kotsifakos
Organization: Lstech Espana SL
Signature:

Date: 05 / 13 / 2024

Name: Konstantinos Papadamou
Organization: Trinomial Technologies Ltd.
Signature:

Date: 05 / 13 / 2024

Name: Styliani Tsitsoula
Organization: Hellenic Cybersecurity Institute
Signature:

Date: 05 / 13 / 2024