Grant Agreement No.: 101093069
Call: HORIZON-CL4-2022-DATA-01
Topic: HORIZON-CL4-2022-DATA-01-03
Type of action: HORIZON-RIA

Programming Platform for Intelligent Collaborative
Deployments over Heterogeneous Edge-IoT Environments

D6.2 Mid-Term Dissemination-Communication-Exploitation report

Work package	WP6
Task	T6.1, T6.2, T6.3
Due date	30/06/2024
Submission date	02/07/2024
Deliverable lead	POLIMI
Version	1.0
Authors	Walter Quadrini (POLIMI), Jean-Baptiste Milon (MARTEL)
Reviewers	Galileo Disperati (MARTEL), Fernando López (FIWARE)

Abstract	Mid-term report including D-C-E achievements and plans, exploitable artefacts and mapping of stakeholders to them. The document also includes evaluation of communication actions and of strategic collaborations with other research projects.
Keywords	Dissemination; Communication; Exploitation

Document revision history

Version	Date	Description of change	List of contributor(s)
V0.1	29/05/2024	Table of Contents	Walter Quadrini (POLIMI), Galileo Disperati (MARTEL)
V0.2	03/06/2024	Collection of contribution to SDOs	Walter Quadrini (POLIMI), all partners
V0.3	05/06/2024	Introduction	Kevin Keyaert (MARTEL)
V0.4	15/06/202	Collection of contribution to Exploitation	Jean-Baptiste Milon (MARTEL), all partners
V0.5	17/06/2024	Collection of contributions to Dissemination	Walter Quadrini (POLIMI), all partners
V0.6	24/06/2024	Final harmonization, Executive Summary, Conclusions (in opposite order)	Walter Quadrini (POLIMI)
V0.7	28/06/2024	Internal review	Galileo Disperati (MARTEL), Fernando López (FIWARE)
V0.8	02/07/2024	Final version	Walter Quadrini (POLIMI), Galileo Disperati (MARTEL),
V1.0	02/07/2024	Final review & submission	Stavroula-Isidora Giannakandropoulou (UNIS)

Disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the other granting authorities. Neither the European Union nor the granting authorities can be held responsible for them.

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme	
Nature of the deliverable:	Document, report

Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	

Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc.
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Executive summary

This document is supposed to support whom it may concern about the dissemination, communication and exploitation activities related to the project for the reporting period ending at M18 (June 2024). To this aim, it serves as an integration and a follow-up to what already reported in the Communication and Dissemination Plan delivered at M09.

The overall results for the Communication and Dissemination activities are aligned with the roadmap agreed in the Description of Action (part B) for most of the items and the related KPIs. In some cases, the expected results have been slightly overperformed and some of the KPIs have been already reached, demonstrating a general commitment of the consortium partners with respect to the project itself (apart from the validity of the technical achievements subjects of these dissemination and communication activities). The grounds to reach the entire set of KPIs seem furthermore solid, and the strategy to fulfil these gaps has been defined, as well as the means to convey it.

For what concerns the Exploitation activities, the consortium has listed several software assets which have been identified as potential heritage of the project beyond the end of the funding. The identification of IP owners also testifies the intention of the partners to continue on the road the project has paved, in order to increase the technical maturity of the solutions and contribute to the pan-European ecosystem, providing it additional tools enabling new businesses opportunities or strengthening existing ones.

Co-funded by
the European Union

Table of contents

Co-funded by the European Union

Co-funded by
the European Union

List of figures

Co-funded by the European Union

List of tables

Co-funded by
the European Union

Abbreviations

Please note that the full name of the project (Programming Platform for Intelligent Collaborative Deployments over Heterogeneous Edge-IoT Environments) may be sometime abbreviated using the acronym **INCODE**, for practicality, although the consortium is in the process to change it (the change has not been finalised at the time of writing).

Acronym	Description
6G-IA	6G Smart Networks and Services Industry Association
AA	Application Area
ACM	Association for Computing Machinery
AES	Audio Engineering Society
AI	Artificial Intelligence
AIDA	Awareness, Interest, Desire and Action
AIOTI	Alliance for IoT and Edge Computing Innovation
AMM	Attack Mitigation Component
APEL	Applied Electronics Laboratory – Univ. of Patras
BDVA	Big Data Value Association
CCS	Computer and Communications Security
CEI	Cloud, Edge and IoT
CIM	Context Information Management
CSA	Coordination and Support Action
DIH	Digital Innovation Hubs
DOI	Digital Object Identifier
DRTD	Department of Research, Technology and Development – IPTO
DSO	Distribution System Operator
EBDVF	European Big Data Value Forum
ECESCON	Electrical and Computer Engineering Student Conference of Greece

ECG	Electrocardiogram
EMG	Electromyography
ETSI	European Telecommunications Standards Institute
EUCEU	European Cloud Edge and IoT
EuCNC	European Conference on Networks and Communications
gNB	gNodeB
HIPEAC	High Performance, Edge And Cloud computing
HV	High Voltage
IAFA	Impact Assessment and Facilitation Action
ICT	Information and Communication Technology
IDP	Internal Developer Platform
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Intellectual Property
IPR	Intellectual Property Rights
ISG	Industry Specification Group
ISO	International Organization for Standardization
ITU	The International Telecommunication Union
KoM	Kick-off Meeting
KPI	Key Performance Indicator
MDC	Malware Detection Component
ML	Machine Learning
MLTK	Machine Learning Toolkit
MNO	Mobile Network Operator
N/A	Not Applicable

Co-funded by
the European Union

NDR	Network Detection and Response
NDSS	Network and Distributed System Security
NGO	Non-Governmental Organization
NGSI-LD	Next Generation Service Interfaces – Linked Data
NLE	NEC Laboratories Europe
NLP	Natural Language Processing
NsaaA	Network Slice as a Service
NTNU	Norges teknisk-naturvitenskapelige universitet
OSL	Software Development Group for OpenSlice
OSS	Operations Support System
PLM	Product Lifecycle Management
PPDR	Public Protection and Disaster Relief
R&D	Research and Development
RBAC	Role-Based Access Control
SDG	Software Development Group
SDO	Standard Developing Organisation
SLA	Service Level Agreement
SME	Small and Medium Enterprise
SNS	European Smart Networks and Services Joint Undertaking
TBA	To Be Announced
TDB	To Be Defined
TMF	TMForum
TRL	Technology Readiness Level
TSO	Transmission System Operator
TTF	Testing Task Force

Co-funded by the European Union

TX.Y	Task X.Y
UC	Use Case
UI	User Interface
UN	United Nations
UXL	Unified Acceleration Foundation
VAR	Value-Added Reseller
WP	Work Package

Co-funded by
the European Union

1 Introduction

1.1 Purpose of the document

Prepared in the context of Work Package 6 (WP6), this deliverable serves two major purposes:

1. Report on the progress and key achievements of the project's outreach and impact creation activities held from month 1 to month 18 (January 2023 to June 2024).
2. Lay out a plan of outreach and impact creation activities for month 19 to month 36 (July 2024 to December 2025) to ensure the fulfilment of targets and supporting the successful conclusion of the project.

1.2 Structure of the document

The sections of this deliverable are organised as follows: After the introductory **Section 1, Section 2** depicts communication activities and tools used during the first half of the project (M01-M18), work dedicated to synergies in parallel, and the plan for the second half of the project (M19-M36). Similarly, **Section 3** outlines the current status of dissemination actions and their planning for the second reporting period, as well as it depicts a perspective over the potential contact points with SDOs and regulation entities. **Section 4** offers a comprehensive report on events (organised, participated to, planned) while **Section 5** offers a breakdown of the individual partners' exploitation plans. Wrapping up the deliverable are a full summary of all Key Exploitable Results (**Section 6**) and a brief set of conclusions.

1.3 Communication and Dissemination strategy in a nutshell

The plan for communication and dissemination activities was outlined earlier in the first half of the project, through the dedicated document, and such activities are closely coordinated among all the work packages to ensure a coherent plan of action that will have a significant impact on the European IoT, Swarm and Continuum Computing ecosystem. The consortium pursues and ensures close coordination with the European Commission, other ongoing IoT and Swarm projects, and other pertinent initiatives in closely related domains, such as the EUCloudEdgeIoT initiative, BDVA, AIOTI, GAIA-X, in order to increase the reach of the project's efforts and maximize the impact its activities will have.

By closely combining the communication and dissemination efforts with the exploitation and sustainability activity, the project implements a comprehensive set of measures with the goal of maximizing its expected impact.

The following project objectives will be achieved through a series of focused outreach and communication initiatives:

Create a unique and recognizable brand identity to support in marketing and promotional initiatives.

Raise awareness of the project's results and advantages to ensure the project's widespread visibility and adoption throughout the European continuum computing community.

To ensure that the project outcomes are effectively presented and that the generated technologies and concepts are adopted further, an important amount of pertinent stakeholders is to be reached, stimulated and engaged.

Co-funded by the European Union

Support the main stakeholders' engagement strategies and initiatives while giving the continuum and swarm computing community visibility and resonance within the European ecosystem and beyond.

Establish and expand the project's community and promote relationships with other initiatives, with a focus on Open Continuum and EU-funded projects on related subjects to encourage discussion, expansion, and knowledge exchange.

Encourage significant contributions to important scientific fields, open-source projects, and standardization bodies as necessary.

Co-funded by the European Union

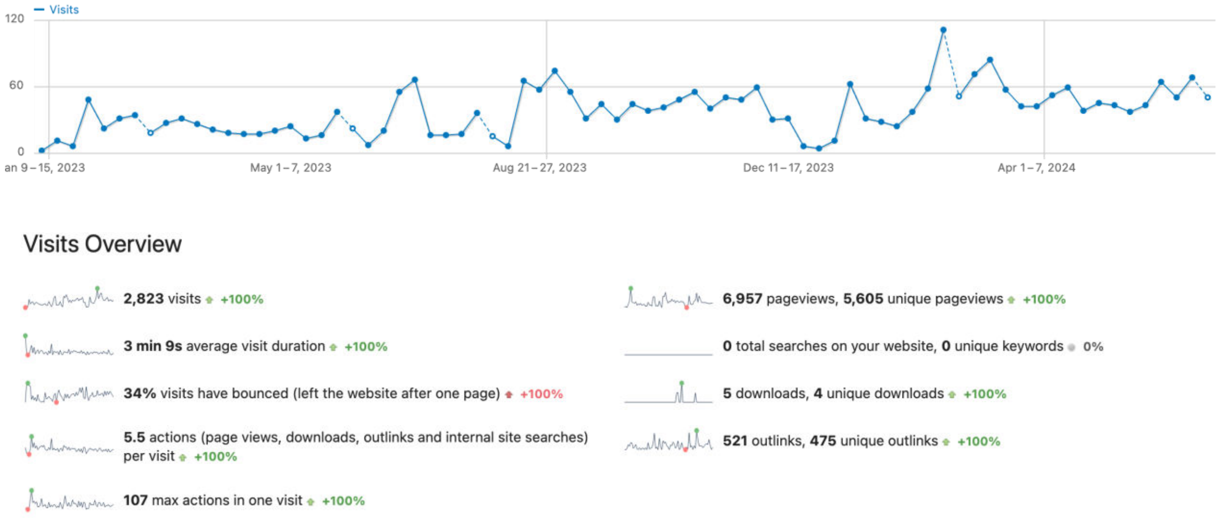
2 Communication activities

2.1 Project website

Since its initial development in January 2023, the project website has formed a central hub for information and engagement among the community and network of diverse stakeholders. It is developed and structured to collect and display the project's goals, activities and achievements as they unfold in correspondence to the set timeline for implementation efforts. This requires a continuous investment to update all relevant information related to INCODE's developments from its inception until completion. Beyond this timeframe, the website also acts as a public repository and virtual recollection of project activities. The content features the following elements:

- General information about the project, its vision and objectives.
- Introduction of the consortium and synergistic liaisons with other projects under umbrella initiatives.
- News items and press releases.
- List of relevant events.
- A repository of resources, such as publications, presentations/talks, promotional materials, videos, and public deliverables.
- Dedicated pages on the various application areas.
- Contact information.
- An acknowledgment and reference to relevant initiatives on swarm computing and the Cloud-Edge-IoT continuum in Europe.

The website is being periodically updated according to the progress of the project. Until today (end of June 2024, Figure 1), the website counts around **2,800 unique visitors**, who generated around **5,600 unique page views** on an **average visit duration of 3'09"**. Drilling down into specific pages, the most popular pages - alongside the homepage – are the dedicated pages on the various Application Areas, counting a total of 733 views, as reported in Figure 2.



Visits Overview

2,823 visits +100%

3 min 9s average visit duration +100%

34% visits have bounced (left the website after one page) +100%

5.5 actions (page views, downloads, outlinks and internal site searches) per visit +100%

107 max actions in one visit +100%

6,957 pageviews, **5,605** unique pageviews +100%

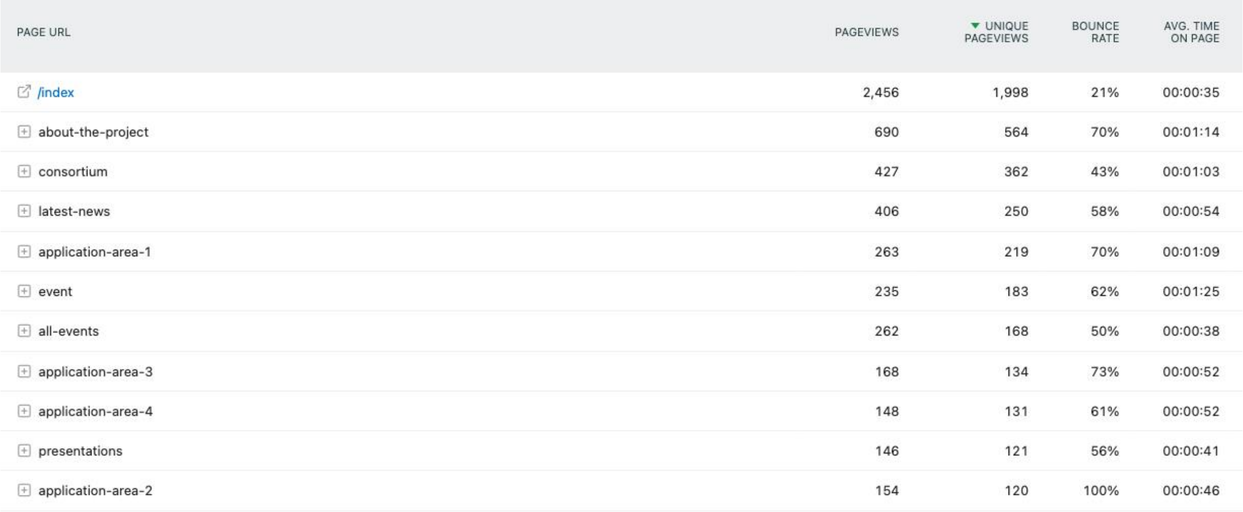
0 total searches on your website, **0** unique keywords 0%

5 downloads, **4** unique downloads +100%

521 outlinks, **475** unique outlinks +100%

Figure 1: Project website analytics – Visits overview

Co-funded by the European Union



PAGE URL	PAGEVIEWS	▼ UNIQUE PAGEVIEWS	BOUNCE RATE	AVG. TIME ON PAGE
/index	2,456	1,998	21%	00:00:35
about-the-project	690	564	70%	00:01:14
consortium	427	362	43%	00:01:03
latest-news	406	250	58%	00:00:54
application-area-1	263	219	70%	00:01:09
event	235	183	62%	00:01:25
all-events	262	168	50%	00:00:38
application-area-3	168	134	73%	00:00:52
application-area-4	148	131	61%	00:00:52
presentations	146	121	56%	00:00:41
application-area-2	154	120	100%	00:00:46

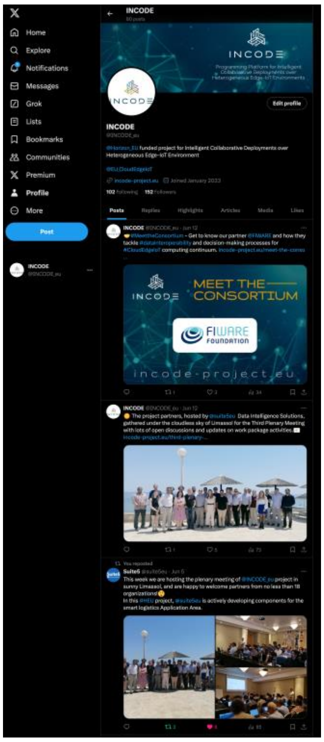
Figure 2: Most visited pages

2.2 Social media channels

INCODE has established an active presence on social media channels to regularly promote the project activities and output while encouraging a wider promotion of innovative applications within the IoT-edge-cloud computing continuum. The project has built a fair follower base on several social media channels, namely X (formerly Twitter) and LinkedIn, which are all linked to the project's website.

2.2.1 X

INCODE uses X as a social network to cover the news in real-time, cross-share relevant and interesting initiatives, and to establish meaningful connections with targeted groups of stakeholders, including policy makers, industry, and the general public. So far, the INCODE X account has reached **152 followers** (including project partners, similar projects, interested stakeholders, etc.). In total, around **80 tweets** have been posted. The project also follows 86 accounts, mostly projects and initiatives in similar fields or of approximate nature where partners have been involved.



INCODE
80 posts

INCODE
@INCODE_eu

@Horizon_EU funded project for Intelligent Collaborative Deployments over Heterogeneous Edge-IoT Environment

@EU_CloudEdgeIoT

incode-project.eu Joined January 2023

102 Following 152 Followers

INCODE @INCODE_eu · Jun 12
🤝 #MeettheConsortium - Get to know our partner @FIWARE and how they tackle #datainteroperability and decision-making processes for #CloudEdgeIoT computing continuum. incode-project.eu/meet-the-conso…

1 3 34

INCODE @INCODE_eu · Jun 12
😊 The project partners, hosted by @suite5eu Data Intelligence Solutions, gathered under the cloudless sky of Limassol for the Third Plenary Meeting with lots of open discussions and updates on work package activities.
incode-project.eu/third-plenary-…

1 5 73

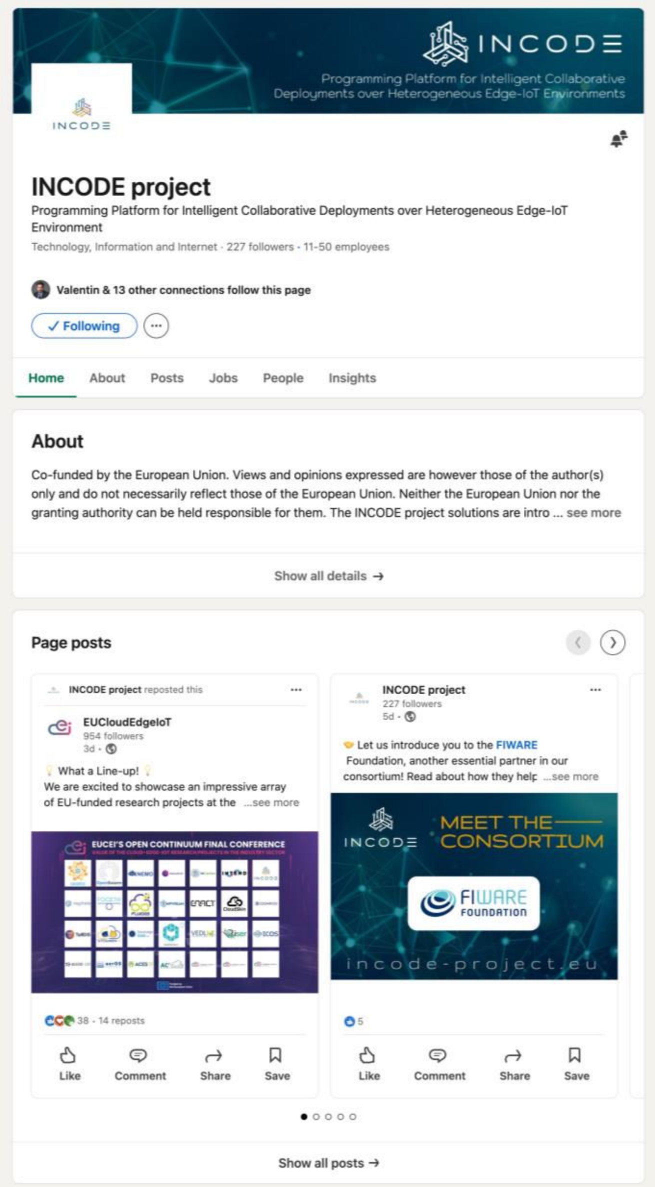
You reposted
Suite5 @suite5eu · Jun 6
This week we are hosting the plenary meeting of @INCODE_eu project in sunny Limassol, and are happy to welcome partners from no less than 18 organizations😊
In this #HEU project, @suite5eu is actively developing components for the smart logistics Application Area.

Figure 3: Project X account

2.2.2 LinkedIn

LinkedIn allows the INCODE project to network with individuals and organizations within the media industry and beyond, share crucial information about project activities, and stay up to date on the latest developments in the field. The LinkedIn account has gathered **227 followers** so far. Similarly to X, the LinkedIn account is mostly used to share the latest progress of INCODE, echoing key promotional messages from the project website and sharing relevant news from the project's partners, pertinent projects and the European Commission.

Co-funded by the European Union



INCODE
Programming Platform for Intelligent Collaborative Deployments over Heterogeneous Edge-IoT Environments

INCODE project

Programming Platform for Intelligent Collaborative Deployments over Heterogeneous Edge-IoT Environment

Technology, Information and Internet · 227 followers · 11-50 employees

Valentin & 13 other connections follow this page

✓ Following
Home
About
Posts
Jobs
People
Insights

About

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. The INCODE project solutions are intro ... see more

Page posts

INCODE project reposted this

EUCloudEdgeIoT
954 followers
3d ·

What a Line-up!
We are excited to showcase an impressive array of EU-funded research projects at the ...see more

38 · 14 reposts

INCODE project
227 followers
5d ·

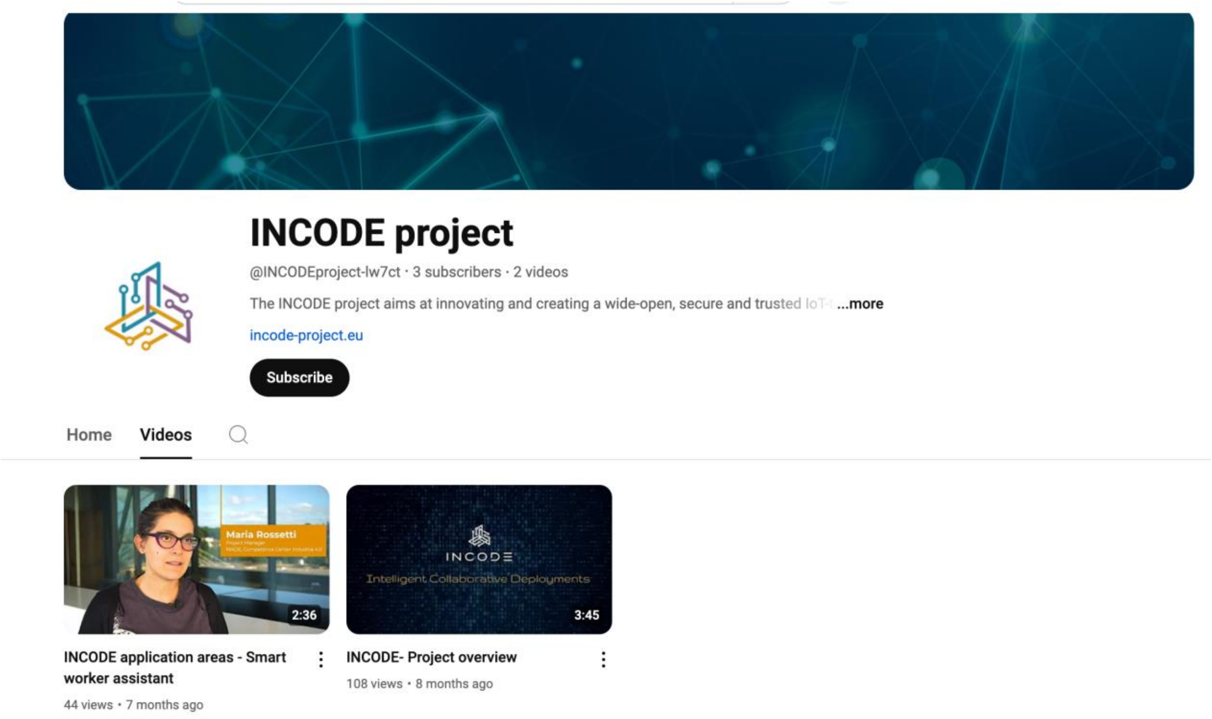
Let us introduce you to the FIWARE Foundation, another essential partner in our consortium! Read about how they help ...see more

5

Figure 4: Project LinkedIn account

2.2.3 YouTube

INCODE has also created an channel on YouTube, one of the leading video-sharing platforms. This channel has been opened at the early project stages to disseminate the first project video. Since then, the project has released a total of **2 videos** on the channel depicted in Figure 5.



INCODE project

@INCODEproject-lw7ct · 3 subscribers · 2 videos

The INCODE project aims at innovating and creating a wide-open, secure and trusted IoT-C ...more

incode-project.eu

INCODE application areas - Smart worker assistant

44 views • 7 months ago

INCODE- Project overview

108 views • 8 months ago

Figure 5: Project YouTube account

2.3 Promotional material

2.3.1 Videos

INCODE released **2 videos** which have been uploaded on the project’s YouTube channel and mirrored on the project website. So far, the YouTube Channel reached a total of **153 views**. With content on the application areas being expanded and deepened in the coming period, more videos will be produced to populate the media channels for greater substantive exposure of the specific project activities.

- The video titled *Project Overview,* produced at the start of the project, offers a glimpse into the aim, activities, challenges and organisation of INCODE, as well as the benefits in terms of application potential. The video is presented by the project coordinator and project manager in interview form to share a personal and first-hand account from the people who coordinate the daily activities of the project.

Lina Giannakandropoulou
Research Projects Delivery Manager
Uni Systems
they're also connected to the cloud via
wireless or wired communication channels.

Figure 6: Screenshot of video INCODE – Project overview

- The video titled *INCODE application areas – Smart worker assistant* provides a closer look into one of the project application areas. The interview form allows for bringing attention to the consortium partners (in this case, Maria Rossetti from MADE, as per Figure 7) who manage the specific work package tasks related to this topic.

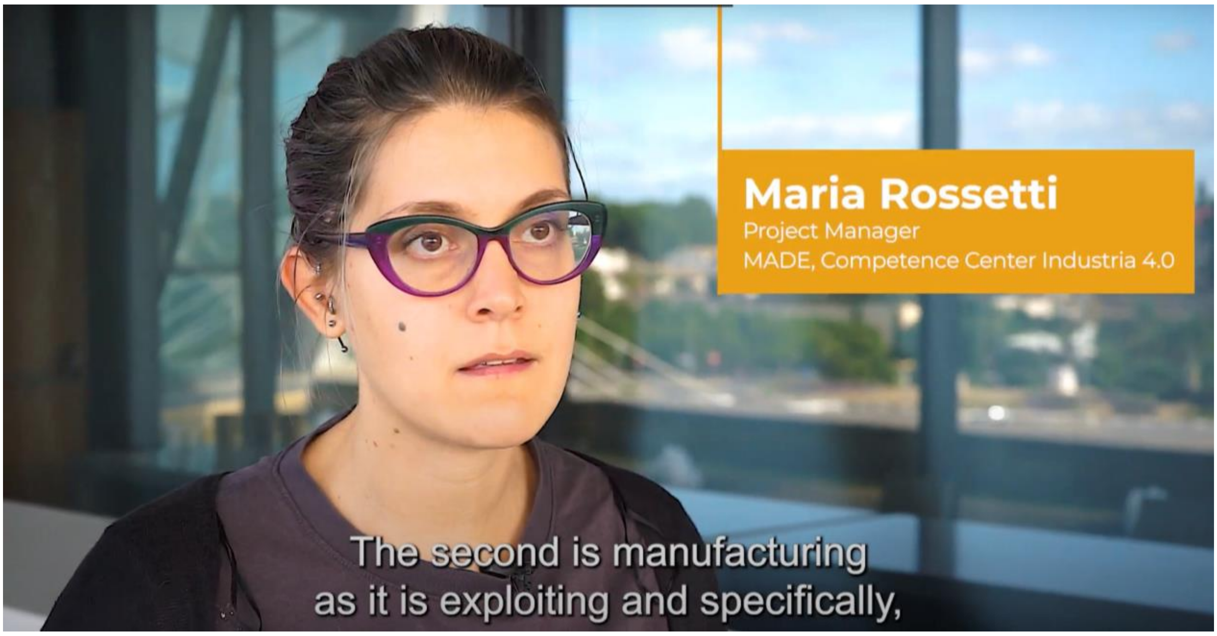

Maria Rossetti
Project Manager
MADE, Competence Center Industria 4.0
The second is manufacturing
as it is exploiting and specifically,

Figure 7: Screenshot of video INCODE application areas – Smart worker assistant

2.3.2 Print

For visual in-person exposure at events, INCODE created two main print materials. One is a roll-up which states the main objectives of the project with a dedicated QR-code for interested audiences to visit the project website (Figure 8). A second is a flyer (Figure 9) which states those same objectives, but also highlights the various application areas that the project champions, i.e. smart logistics, smart worker assistant, utilities inception, and smart PPDR.

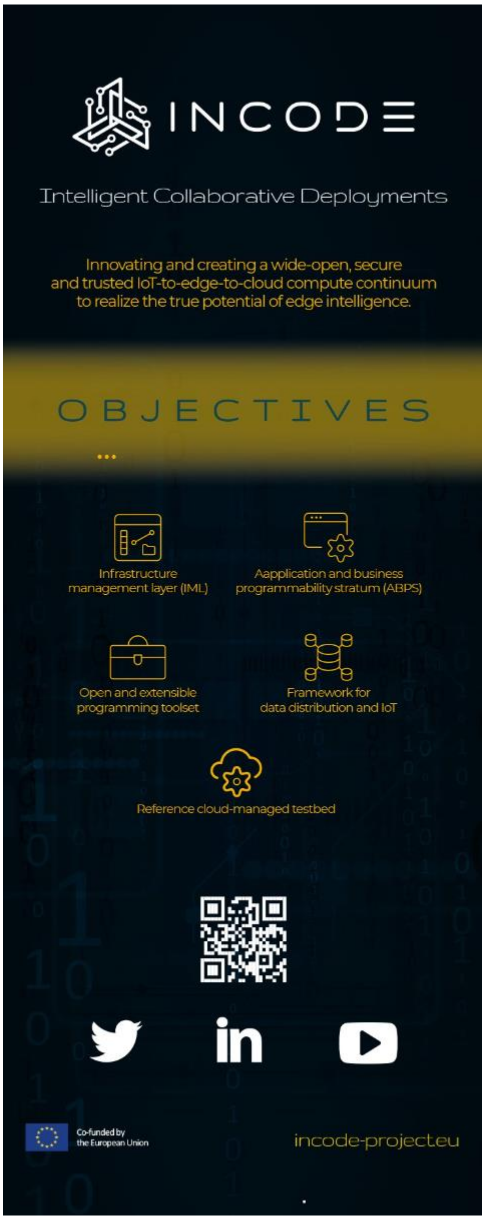
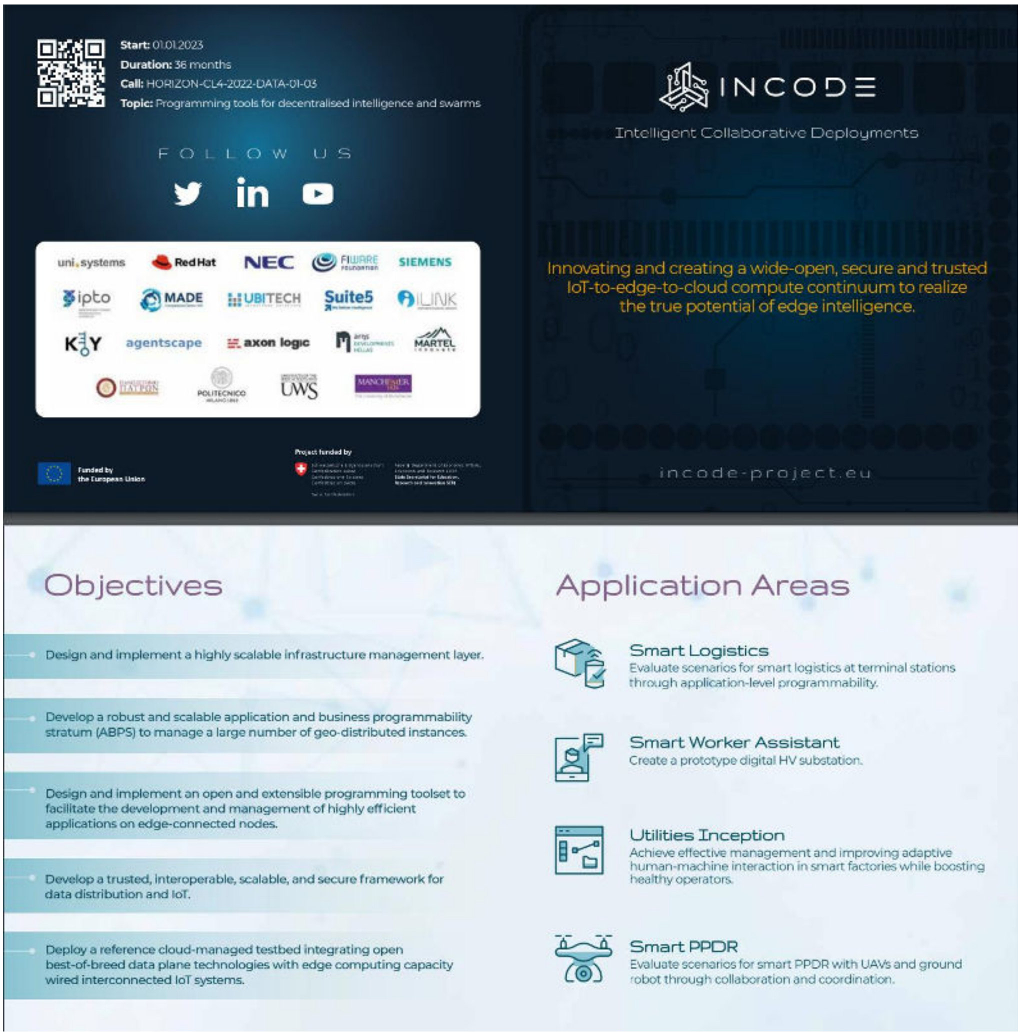

INCODE
Intelligent Collaborative Deployments
Innovating and creating a wide-open, secure and trusted IoT-to-edge-to-cloud compute continuum to realize the true potential of edge intelligence.
OBJECTIVES
Infrastructure management layer (IML)
Application and business programmability stratum (ABPS)
Open and extensible programming toolset
Framework for data distribution and IoT
Reference cloud-managed testbed
Co-funded by the European Union
incode-project.eu

Figure 8: Project roll-up


INCODE
uni.systems
Red Hat
NEC
FIWARE Foundation
SIEMENS
ipto
MADE
UBITECH
Suite5
ILINK
KEY
agentscape
axon logic
arys developments hellas
MARTEL
POLITECNICO MILANO 1863
UWS
MANCHESTER 1824

Start: 01.01.2023
Duration: 36 months
Call: HORIZON-CL4-2022-DATA-01-03
Topic: Programming tools for decentralised intelligence and swarms

FOLLOW US

Funded by
the European Union

Project funded by

INCODE

Intelligent Collaborative Deployments

Innovating and creating a wide-open, secure and trusted IoT-to-edge-to-cloud compute continuum to realize the true potential of edge intelligence.

incode-project.eu

Objectives

- Design and implement a highly scalable infrastructure management layer.
- Develop a robust and scalable application and business programmability stratum (ABPS) to manage a large number of geo-distributed instances.
- Design and implement an open and extensible programming toolset to facilitate the development and management of highly efficient applications on edge-connected nodes.
- Develop a trusted, interoperable, scalable, and secure framework for data distribution and IoT.
- Deploy a reference cloud-managed testbed integrating open best-of-breed data plane technologies with edge computing capacity wired interconnected IoT systems.

Application Areas

Smart Logistics
Evaluate scenarios for smart logistics at terminal stations through application-level programmability.

Smart Worker Assistant
Create a prototype digital HV substation.

Utilities Inception
Achieve effective management and improving adaptive human-machine interaction in smart factories while boosting healthy operators.

Smart PPDR
Evaluate scenarios for smart PPDR with UAVs and ground robot through collaboration and coordination.

Figure 9: Project flyer

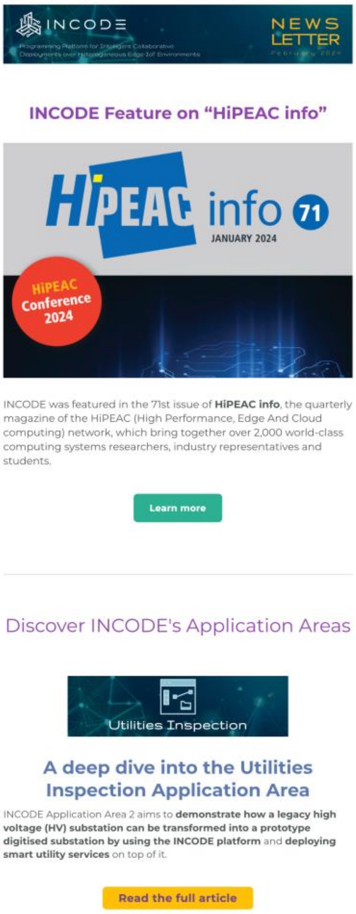
2.4 News items, newsletters & press releases

In terms of news outlets to date, project communication channels have issued 1 press release (and 1 press clipping item), 3 periodic newsletters, and 22 news items (published on the website and echoed on social media) offering insight on the consortium, its activity and the ecosystem they operate within.

Press releases & clipping

The first project press release was issued on the occasion of its kick-off (February 2023), offering an overview of the project's vision, objective, and parties involved. Our press clipping, so far, counts the feature that the project received on HIPEAC info (Nr. 71) – released in January 2024 – once again offering a bird's eye view of the project, with a breakdown of the envisioned four application areas. Both items can be found in Annex A, in the document's coda.

Newsletters


INCODE
Programming Platform for Intelligent Collaborative Deployments over Heterogeneous Edge-IoT Environments
NEWS LETTER
February 2024
HiPEAC info 71
JANUARY 2024
HiPEAC Conference 2024
Utilities Inspection

INCODE Feature on “HiPEAC info”

INCODE was featured in the 71st issue of **HiPEAC info**, the quarterly magazine of the HiPEAC (High Performance, Edge And Cloud computing) network, which bring together over 2,000 world-class computing systems researchers, industry representatives and students.

Learn more

Discover INCODE's Application Areas

A deep dive into the Utilities Inspection Application Area

INCODE Application Area 2 aims to **demonstrate how a legacy high voltage (HV) substation can be transformed into a prototype digitised substation by using the INCODE platform** and **deploying smart utility services** on top of it.

Read the full article

Figure 10: Screenshot from the February 2024 project newsletter

The 1st newsletter (June 2023) was sent to 10 subscribers (50% opens / 20% clicks); the issue introduced the project’s vision, objectives and consortium members (also sporting the dedicated overview video), and covered, notably, the launch of the EU Cloud-Edge-IoT initiative we are part of, and project partners’ presence at the Concertation and Consultation on Computing Continuum Meeting; finally, it offered a space to promote upcoming events participations/ecosystem events.

The 2nd newsletter (October 2024) was sent to 12 subscribers (83% opens / 17% clicks); the issue promoted the (then) upcoming participation to EBDVF 2023 (alongside other events) and launched our series of deep-dive articles on the project Application Areas.

The 3rd newsletter (February 2024) was sent to 17 subscribers (60% opens / 6% clicks); the issue highlighted the project being featured on HIPEAC info, collected the continuation of the articles on the Application Areas, and reports on the EBDVF 2023 and DISCOVER-US events participations; finally, it covered the presentation of application area 3 to the European Smart Networks and Services Joint Undertaking (SNS) community and promoted upcoming events participations/ecosystem events.

A 4th issue is in preparation at the time of writing, scheduled for release at the end of June/early July 2024: the content will cover the Smart Computing webinar organised within the EUCloudEdgeIoT initiative in May 2024, the consortium meeting held in early June 2024, and promote any upcoming events in the pipeline.

2.5 Synergies and liaisons with relevant initiatives

Liaison activities with other projects (particularly those of the same call) for common actions have been pursued, through co-organised workshops and knowledge exchange with the goal to create a common ground of understanding and mutual support. Although falling under the Communication task (T6.2), and therefore reported here in this sub-section, such endeavours entice direct interaction with T6.1 for the promotion of material and the planning of collaboration actions. Here below, a breakdown of all activities conducted within the reporting period.

EUCloudEdgeIoT initiative/Open Continuum CSA

As briefly touched upon in the section about newsletters, our project is part of the Open Continuum CSA and the EU Cloud Edge IoT Initiative. The EUCloudEdgeIoT.eu initiative aims to realise a pathway for the understanding and development of the Cloud, Edge and IoT (CEI) Continuum by promoting cooperation between a wide range of research projects, developers and suppliers, business users and potential adopters of this new technological paradigm.

Through the participation to the initiative, the project not only had the chance to access a wider platform for collaboration and communication purposes - by featuring on their online outlets and attending their launch event, their Concertation and Consultation on Computing Continuum Meeting, and their final conference - but also established a collaboration with the other projects operating under the Swarm Computing cluster of the initiative. The project are **TaRDIS**, **OASEES**, **OpenSwarm** and **SMARTEDGE**, with which we kicked off a fruitful exchange, materialising in an active "echo chamber" of news and announcements coming from all projects, and in the joint organisation of the "Tackling the ever-increasing complexities of developing efficient heterogeneous swarm systems" EUCloudEdgeIoT Webinar (where we took the lead, together with TaRDIS, but featured all respective Project Coordinators as panelists). The collaboration with some of these projects will continue in the second half of the project, as detailed in the following Section (2.6).

More details on all related and aforementioned events can be found in Section 4.

Computing Continuum Cluster

The Computing Continuum cluster coordinated by HIPEAC and initiated in 2023 is a network of initiatives interesting in exchanging knowledge and experiences around the continuum, from IoT to edge to cloud to HPC. The main purpose is to share the research and innovation agendas of the initiatives to identify which can be the future challenges in the topic, contributing so to the future research programs, finding synergies for future projects and sharing the position with the research community. The FIWARE Foundation has joining this cluster to contribute with the vision of the FIWARE community about distributing data management and the integration between IoT, cloud and edge worlds. The initiative is also interesting for FIWARE to explore other technologies and partners which can enrich its innovation roadmap and ecosystem.

More details on all related and aforementioned events can be found in Section 4.

Other initiatives

It must also be noted that within the reporting period, the project established links with other six initiatives, including associations, clusters and CSAs (BDVA, AIOTI, EFFRA, 6G-IA/SNS, UNLOCK CEI) through participating, networking and presenting our objectives and progress at events organised by them.

2.6 Communication plan (M19-M36)

2.6.1 Amendments to branding

Due to a necessary acronym change (which is under finalisation at the time of writing) a complete review of logo, logotype and branding will affect website, social media, promo material, reporting and presentations templates. The actions dedicated to this effort are planned to take place within summer 2024.

2.6.2 Dedicated web and video content

Due to the central role of the project Application Areas (i.e. logistics, worker assistance, PPDR, and utilities inspection), specific efforts will be placed on developing content that sheds more light on each area individually. This will entail an expansion on the webpages illustrating the specifics of these areas with videos and news items that will subsequently be shared on social media as a campaign over the space of a few months.

2.6.3 Future event participation

WP6 and the consortium have worked together to pinpoint and prepare some event participations for the second half of the project, often as a result of our interaction with fellow EU-funded projects and initiatives. More details can be found in Section 4 of the present document.

2.6.4 Synergies

WP6 intends to continue and expand upon all synergies reached so far: in particular, the virtuous circle kickstarted by the collaboration with the EUCloudEdgeIoT Swarm Computing cluster of projects mentioned in Section 2.5. To this end, T6.2, after finalising the project application to the Horizon Results Booster platform in spring 2024, has invited some of the cluster's projects to join us in receiving feedback and consultation from the Booster team as a group (as suggested by the team itself), in order to optimise and maximise reach. Meetings to initiate the process have been arranged for the end of June 2024.

Co-funded by
the European Union

3 Dissemination activities

For what concerns the dissemination activities, performed under the banner of the task T6.1, followed the marketing-derived AIDA model, which is based on four consecutive stages (Awareness, Interest, Desire, and Action). The project activities have been hence divided as it follows:

Awareness (M01-M12): where efforts had been focused on raising awareness for the project itself among scientific and practitioners' audiences. The consortium worked indeed on the identification of the specific communities to address, and on the scientific dissemination means which could best receive the scientific outcome of INCODE project. A series of scientific events (~conferences) and publications are hence identified to intercept the attention of these communities.

Interest (M13-M24): the INCODE consortium is now focusing on the available project outcomes and on their proposition to the identified communities. Peer-reviewed publications in scientific conferences have been deemed the most effective mean to raise interest of such communities, and the academic partners provided material for these events.

Desire (M25-M36): this third phase is supposed to proceed together with the integration of the tools provided by technical Work Packages in Application Areas, which are expected to serve as case studies and demonstrators for higher level publications and events.

Action (M37-M48): this last phase is supposed to take place beyond the formal ending of the project. In this stage, early strategies connected to the exploitation activities of different partners are supposed to further generate interest and to permanently position themselves in the targeted communities. Furthermore, the long iterations which usually characterises peer-reviewed journals will allow to submit to valuable publications the most interesting scientific outcome of INCODE.

3.1 Report on dissemination activities (M01-M18)

According to the aforementioned considerations, the first period of the project has been mainly devoted to the creation of awareness and interest in the identified communities. The identification of such communities has been realised thanks to the creation of a document, shared in the internal project repository that every partner updates with relevant scientific events (e.g., conferences and workshops). Pertaining the scientific areas of involved partners, these events are supposed to be the entry point for the related community. Table 1 reports an instance of this living document.

Table 1: Living document

Name of the event	Type of event	Location and date	Focus/target stakeholders	URL	Project contact point	Relevance to INCODE	Comments
Global IoT and Edge Computing Summit	Scientific Conference	Brussels, 24-25 September 2024	ICT Engineering community	https://giecs.eu/call-for-papers/	Walter Quadrini (POLIMI)	Conference organised by AIOTI	Reference event for AIOTI community. Good opportunity to position the project.

Such an approach allowed the project partners to identify the main academic and practitioners' communities to be addressed, which have been divided into ICT Engineering, Cybersecurity (related to technical Work Packages), Manufacturing, Logistics, Computer Vision, Multi-Agent Networks (related to integration Work Packages and Application Areas).

This approach allowed the consortium to tackle these communities in a structured way. And a total of 11 articles has been published and presented at scientific conferences (to which a recently submitted item can be also added). Results are collected in Table 2 and highlight how the majority of publications are related to technical Work Packages (coherently with the overall project timeline, which forecasts technical advancements related to the software modules to be developed before their deployment into Application Areas). At the same time, however, the first results of implementation on related to WP5 have produced some results deemed valuable for scientific publishing.

Table 2: Realised scientific papers

Paper title	Authors	Journal/Conference proceeding	DOI	Partner involved	Status
Short Paper: Estimating Patch Propagation Times across Blockchain Forks.	Sebastien Andreina, Lorenzo Alluminio, Giorgia Azzurra Marson, Ghassan Karame	International Conference on Financial Cryptography and Data Security	doi	NEC	Published
The INCODE (INtelligent COllaborative DEployments) European project: logistics and transport quality value chain application area	Panagiotis Zikos, Stathis Vlachos, Despina Tomkou, George Tsironis	4th Symposium on Circular Economy and Sustainability	N/A	iLink	Published
Cross-Language Interoperability of Heterogeneous Code	Athanasios Stratikopoulos, Florin Blanaru, Juan Fumero, Maria Xekalaki, Orion Papadakis, Christos Kotselidis	In Companion Proceedings of the 7th International Conference on the Art, Science, and Engineering of Programming (Programming› '23)	doi	UMAN	Published
Scaling Up Performance of Managed Applications on NUMA Systems	Orion Papadakis, Andreas Andronikakis, Nikos Foutris, Michail Papadimitriou, Athanasios Stratikopoulos, Foivos Zakkak, Polychronis Xekalakis, Christos Kotselidis	The 2023 ACM SIGPLAN International Symposium on Memory Management (ISMM 2023)	doi	UMAN	Published
A Multifaceted Memory Analysis of Java Benchmarks	Orion Papadakis, Andreas Andronikakis, Nikos Foutris, Michail Papadimitriou, Athanasios Stratikopoulos, Foivos Zakkak, Polychronis Xekalakis, Christos Kotselidis	20th ACM SIGPLAN International Conference on Managed Programming Languages and Runtimes (MPLR '23)	doi	UMAN	Published
Unified Shared Memory: Friend or Foe? Understanding the Implications of Unified Memory on Managed Heaps	Juan Fumero, Florin Blanaru, Athanasios Stratikopoulos, Steve Dohrmann, Sandya Viswanathan, Christos Kotselidis	20th ACM SIGPLAN International Conference on Managed Programming Languages and Runtimes (MPLR '23)	doi	UMAN	Published
Beehive SPIR-V Toolkit: A Composable and Functional API for Runtime SPIR-V Code Generation	Juan Fumero, Gyorgy Rethy, Athanasios Stratikopoulos, Nikos Foutris, Christos Kotselidis	2023 Workshop on Virtual Machines and Language Implementations	doi	UMAN	Published

Efficient CNN-based low-resolution facial detection from UAVs	Julio Diez-Tomillo, Ignacio Martinez-Alpiste, Gelayol Golcarenarenji, Qi Wang & Jose M. Alcaraz-Calero	Neural Computing and Applications	doi	UWS	Published
Empirical Comparison of Face Verification Algorithms from UAVs	Julio Diez-Tomillo, Jose M. Alcaraz-Calero & Qi Wang	2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)	doi	UWS	Published
Approaching interoperability and data-related processing issues in a Human-centric industrial scenario	Danish Abbas Syed, Walter Quadrini, Nima Rahmani Choubeh, Marta Pinzone	Global IoT and Edge Computing Summit (GIECS 2024)	N/A	POLIMI	Submitted
Larger-scale Nakamoto-style blockchains don't necessarily offer better security	Jannik Albrecht, Sebastien Andreina, Frederik Armknecht, Ghassan Karame, Giorgia Marson, Julian Willingmann	IEEE Symposium on Security and Privacy (S&P)	doi	NEC	Published
Towards Intent-based Network Management for the 6G System adopting Multimodal Generative AI	Dimitrios Brodimas, Kostis Trantzas, Besiana Agko, Georgios Christos Tziavas, Christos Tranoris, Spyros Denazis, Alexios Birbas	European Conference on Networks and Communications &6G Summit (EuCNC&6G 2024)	doi	UoP	Published

3.2 Next actions (M19-M36)

The second reporting period of the project will complete the activities related to the Interest creation in the addressed communities, as per AIDA model. This step will be achieved through a replica of the behaviour that the consortium has adopted, in particular with respect to the production of scientific articles allowing the single results to be adequately exploited in the aforementioned communities.

For the last year of the project, the consortium is expected to be deal with the creation of Desire among the targeted audience. This will be reached through new scientific publications, devoted not only to the presentation of single modules or single features of the technical and integration Work Packages, but mainly pertaining to the integration of the technical solutions in the Application Areas (AAs). Throughout this approach, the consortium expects to be able to further raise the 'hype' in particular for what concerns the practitioners' community, with respect to effective benefits of the developed solution in a business perspective. For this reason, the production of scientific articles is supposed to reverse the trend, going from technical WPs-related subjects to AAs-related ones.

In order to promote open science and to further disclose the achieved results towards the communities, the publication of datasets coming from AAs is also expected take place, as well as contributions based on AAs' evidences are supposed to be able to gain visibility into Standard Development Organizations and Open source large communities.

3.3 Activities connected to standardisation bodies

As an activity deeply connected to innovation and research, the project has forecasted a dissemination campaign related to Standard Developing Organisations. These organisations are traditionally intended as National Standard Bodies members of the International Organization for Standardization (ISO) or as Non-Governmental Organizations (NGOs) devoted to the publication of reference documents aimed at norming business practices and guided by practitioners' communities (e.g., IEC, IEEE, and AES). Given, however, the time-related constraints of the project (against the long iterations often provided by these bodies), and the opportunity to provide visibility about the obtained results in the policy-making institutions, the consortium decided to target industrial associations characterised by the presence of working groups devoted to the establishment of de-facto standards or actively influencing public institutions towards the regulation of technology and its usage.

For this purpose, all the project partners of the consortium have been queried about their involvement into such institutions and in the related working groups/task forces related to policy making and standardisation. The results of this activity highlighted 6 associations potentially exploitable for disseminating the project's findings at a "political" level.

- The **6G Smart Networks and Services Industry Association (6G-IA)** is an industry association that represents the private sector in the development of 6G infrastructure. It aims to support and promote research and innovation in 6G technologies within Europe. 6G-IA works closely with the European Commission and other organizations to contribute to the European Union's policies and strategies for 6G. iLink and IPTO are members of the pre-standardization Working Group and can provide visibility into this body for the results of the project.

- **European Telecommunications Standards Institute (ETSI)** is a traditional SDO, instituted by the European Union, which develops and tests global technical standards related to the communication technologies. ETSI is divided into several committees, among which the consortium has shown interest in industry specification groups and has identified two potential audiences for the dissemination of the project results: the **Software Development Group for OpenSlice (OSL)**, which is led by UoP and is developing an open source service based Operations Support System (OSS) to deliver Network Slice as a Service (NSaaS); the **Industry Specification Group (ISG) cross cutting Context Information Management (CIM)**, which is overseen by FIWARE, with a vice chair and two members who contribute in the specification of the ETSI NGSI-LD API as well as in the corresponding Testing Task Force (TTF) to create the ETSI NGSI-LD Conformance Tests to contribute to the state-of-the-art of the IoT Controller and IoT Driver in the context of T3.2.

- **one6G**, which collaborates with various stakeholders to influence and contribute to the development of future communication standards, which counts as members iLink and MARTEL.

- **Alliance for IoT and Edge Computing Innovation (AIOTI)**, which promotes, bridges and cooperated in IoT and Edge Computing and other converging technologies research and innovation, standardisation and ecosystem building. POLIMI is academic member of the association and actively involved in the Standardization working group.

- **Big Data Value Association (BDVA)**, an industry-driven organisation aimed at developing and promoting data and AI-driven practices. POLIMI is again academic member of Standards and Benchmarking task force.

- The **Unified Acceleration (UXL) Foundation** is aimed at supporting the unified programming model across multi-architecture and multi-vendor software. Project's personnel affiliated to UMAN is actively contributing to its regulation activities.

- **The International Telecommunication Union (ITU)** is another traditional SDO. ITU-T Focus Group on Autonomous Networks was established by ITU-T Study Group 13 at its virtual meeting, 17 December 2020. The Focus Group is drafting technical reports and specifications for autonomous networks, including exploratory evolution in future networks, real-time responsive experimentation, dynamic adaptation to future environments, technologies, and use cases. The Focus Group will also identify relevant gaps in the standardization of autonomous networks. The primary objective of the Focus Group is to provide an open platform to perform pre-standards activities related to this topic and leverage the technologies of others where appropriate. UWS is member of this Focus Group, and the project was introduced in the ITU AI for Good Global Summit 2024 in the invited talk by Qi Wang, which started the activity related to the contribution to SDOs for the project itself.

Apart from SDOs and regulation-related organisations, the project partners also tried to provide evidence of the gained advancements in open-source communities. Towards this target, RedHat has notably contributed (benefiting of its well-ranked position), with two presentations in two consecutive annual events of DevConf.cz, a reference event for the community gravitating around the RedHat, Fedora Core and OpenShift environments.

Co-funded by
the European Union

4 Events

This section collects all events that project partners have attended or organised/co-organised, presented as a stand-alone section as both T6.1 and T6.2's efforts in this regard contributed to the results achieved – and were monitored by both.

4.1.1 Events organised

In the reporting period, consortium partners co-organised **2 webinars**, following the KPIs set for T6.1 and counted under those, although T6.2 was directly and organically involved. Here below, the details on both events.

OSL 2 TECH Day

OSL 2 TECH Day took place online on February 29, 2024; project partner UoP was co-organiser of the event, in which the ETSI OSL community deployed an OSL Demo. The event was widely promoted on the project website and social media channel - and within the UoP and OSL community networks – gathering 45 participants in total.

Figure 11: Promotional online material in support of OSL 2 TECH Day

"Tackling the ever-increasing complexities of developing efficient heterogeneous swarm systems" - an EUCloudEdgeIoT Webinar

In the context of the "EUCloudEdgeIoT.eu RIA Showcase" organised by the Open Continuum CSA to present cutting-edge results and advancements in the Cloud-Edge-IoT Computing Continuum, INCODE and the fellow Horizon Europe Framework-funded project TaRDIS co-organised a webinar to compare standpoints, achievements and recommendations among the swarm computing-focused projects operating under the EUCloudEdgeIoT umbrella. The webinar took place on May 28, 2024 and saw the participation of fellow Swarm Computing cluster projects TaRDIS, OASEES, OpenSwarm and SMARTEDGE.

Co-funded by the European Union

EUCloudEdgeIoT.eu
Hosted by
TaRDIS
WEBINAR
[Featuring OASEES, OpenSwarm and SMARTEDGE]
Tackling the ever-increasing complexities of developing efficient heterogeneous swarm systems
Hosted by TaRDIS and Programming Platform for Intelligent Collaborative Deployments over Heterogeneous Edge-IoTEnvironments (formerly INCODE)
28th May, 2024 | Online
10.00 - 11.30 CET

Figure 12: Promotional online material in support of "Tackling the ever-increasing complexities of developing efficient heterogeneous swarm systems" - an EUCloudEdgeIoT Webinar

The webinar attracted an audience of over 100 stakeholders, connecting from 17 countries, and provided an excellent opportunity to explore the current state and future directions of swarm computing. It highlighted the need for interoperability, scalability, and efficient resource management while showcasing practical applications and the critical role of collaboration in driving innovation. The discussions emphasised the potential of swarm computing to address complex real-world problems through coordinated, intelligent systems.

Promotion was conducted via our online outlets, as per usual, but the support of the other projects involved – and of the EUCloudEdgeIoT initiative – created an extended network that greatly extended reach, as demonstrated by the attendance numbers.

A report and a full-length video recording of the event will be made available to all registered participants and on the EUCloudEdgeIoT website between June and July 2024.

4.1.2 Events attended

Project partners have attended or participated to **19 events** so far (reported in Table 3), either giving presentations or promoting the projects goals and achievements. The table here below summarizes the events attended. These participations have been reported in the news section and the events calendar of the project's website and have been promoted through the social media channels and newsletters. In addition to what is being reported in the table below, project partner UBI also presented the concept of the project before its formal start, at a webinar entitled "IoT/Cloud/Edge Computing Continuum – From Research to Deployment", which took place on November 30, 2022, as deemed a valuable opportunity to kickstart communication and dissemination activities, in line with what stated in the Description of Action (Part B).

Table 3: Events attended M01-M18

Event	Date, location	Type of audience	Approx. audience size	Activities	Lead partner
REWIRE info Day - Greece	online, 6/02/2023	Researchers, policy makers, industry	50	Project presentation	iLink
TRANSFERRING - SYNERGETIC EVENT - Intelligent Aerial Cities - Innovation Opportunities for Sustainable Infrastructure and Innovation	Patras, 24/01/2023	Researchers, policy makers, industry	N/A	Project presentation	iLink
EUCloudEdgeIoT.eu initiative	online, 8/02/2023	EUCEI community, IoT community	70	Project overview	UNIS
Computing Continuum Cluster	Online, 21/09/2023, 27/03/2024, 28/06/2024	Computing Continuum Members	15-20	Project overview	FIWARE
Presentation to NTNU	Milan, 29/03/2023	Academic visitors	15	Project presentation	POLIMI
Concertation and Consultation on Computing Continuum Meeting: From Cloud to Edge to IoT	Brussels, 10-11 May 2023	EUCEI community, IoT community	>70 (over 25 other projects in attendance)	Project presentation	UNIS
DevConf.cz	Brno, 16-18 June 2023	Developers, researchers	100	Project presentation	REDHAT
ECESCON 14	Volos, 21-23/04/2023	Academic visitors	50	Project presentation	IPTO
IAFA EVENT SERIES #1 - Digital Innovation Hubs to strengthen knowledge exchange with SNS community and collaboration	online, 05/10/2023	DIH community	30	Project (Application Area 3) presentation	POLIMI
EBDVF 2023	Valencia, 25-27 October 2023	Researchers, policy makers, industry	>600	2 organised workshops (Martel and MADE with the participation of UNI) + 1 invited speaker (PoliMi)	MADE4.0, UNI, MARTEL, POLIMI
DISCOVER-US networking event	online, 12 January 2024	EUCEI community, Transatlantic collaboration	>50	Project presentation	UNIS
Data Spaces Symposium 2024	Darmstadt, Germany, 12-14 March 2024	Researchers, policy makers, industry	800/900	Keynote, presentation	FIWARE

Co-funded by the European Union

ITU AI for Good Global Summit 2024	Geneva, Switzerland, 29-31 May 2024	The AI for Good Global Summit is the leading action-oriented United Nations platform promoting AI to advance health, climate, gender, inclusive prosperity, sustainable infrastructure, and other global development priorities. AI for Good is organized by the International Telecommunication Union (ITU) – the UN specialized agency for information and communication technology – in partnership with 40 UN sister agencies and co-convened with the government of Switzerland.	10,000+ registered 4,500+ In-person visitors 100+ exhibitors 25,000+ YouTube livestream audience	Invited talk	UWS
ECESCON 15	Xanthi, 19-21/04/2024	Academic visitors	50	Project presentation	IPTO
2024 EuCNC/6G Summit	Antwerp, 3-6 June 2024	Researchers, policy makers, industry	30	Paper presentation	UoP
DevConf.cz	Brno, 13 June 2023	Developers, researchers	100	Project presentation	REDHAT
EUCEI's Open Continuum Final Conference	Brussels, Belgium, June 18, 2024	EUCEI community, industry, European Commission representatives	55	Participating, presenting project, networking	AHRS

4.1.3 Planned events participation

The table below presents a list of events for which participation in the second half of the project has been planned, or that will be in the project's radar for communication activities:

Table 4: Events targeted M19-M36

Event	Date, location	Type of audience	Approx. audience size	Activities	Lead partner
10th FIWARE Global Summit	Naples, 18-19 September 2024	Researchers, policy makers, industry	>400	Project partner co-organising, potential project presentation	FIWARE, POLIMI
European Big Data Value Forum (EBDVF)	Budapest, 2-4 October 2024	Researchers, policy makers, industry	>600	Potential booth+session with the swarm computing cluster	UNIS, POLIMI

Co-funded by the European Union

Computing Continuum Cluster	Brussels, 24-25/09/2024	Cluster members	15-20	Potential presentation about project together with the activities in AerOS and COGNETs projects	FIWARE

5 Exploitation

5.1 INCODE's Exploitation strategy

5.1.1 Commercialisation

To direct INCODE's outcomes towards viable commercial solutions and assets, a targeted commercialization strategy with measurable outcomes is integrated into the project lifecycle. The finalized commercialization and marketing plan will be detailed in the final version of D6.3, a preliminary version was produced at M18 in D6.1 Innovation and IPR Management. This plan overall includes individual plans for each beneficiary as well as joint exploitation solutions for up to three years post-project. A comprehensive socio-economic analysis and migration study of the project outcomes, detailed in the deliverable D5.3, will outline commercially viable solutions, assets, and use case applications, considering both a broad cross-consortium perspective and market trends and technology providers' views.

5.1.2 Further research work

The promotion of knowledge for educational purposes and the expansion of research activities is a shared goal among all academic partners. Specific plans include UWS enhancing its leadership in end-user service solutions, UOP establishing its unique IoT-5G system testbed as one of the top testbeds in Europe, POLIMI advancing its expertise in targeted Industry 4.0 solutions, and UMAN promoting its world-class TornadoVM solution in practical deployments.

5.1.3 Open source

INCODE adheres to technical standards and directives, contributing to them with blueprints and specific reference implementations where applicable. The project places emphasis on open initiatives and related contributions to definitions and visions to promote the INCODE vision. Technologically, the alignment with existing standards and active standardization efforts under development is a key focus as well as contributing towards open-source initiatives. FIWARE takes a relevant role here as an open source community where the Context Controller and Context Driver are open-license components. Additionally, the participation in the Smart Data Model program also guarantee the open and free to use of the data models defined in the project.

5.2 Partners' individual exploitation plans

UNIS

UNISYSTEMS has established itself as a leading ICT systems integration company in the European markets, serving diverse sectors such as banking and finance, telecom, government, cultural institutions, and health. Within the INCODE project, UNISYSTEMS, acting also as a cloud infrastructure provider, envisions leveraging the technological know-how gained to enhance its portfolio of services and products. The technological advancements from the overall INCODE platform, including the software components and architecture, will enable UNISYSTEMS to deliver secured edge and cross-cloud applications in areas such as data analytics, cloud and edge computing, Industry 4.0, and smart cities.

UNISYSTEMS investigates the possibility of enriching its offerings, both through the foreground of stand-alone assets produced within INCODE, but also in smaller, leaner sub-

Co-funded by the European Union

value chains with selected partners to seek market penetration opportunities through pilot platforms based on use-cases as "marketing teaser examples". This approach aims to showcase the practical applications and benefits of INCODE innovations to potential customers. In pursuit of this goal, UNISYSTEMS will examine multi-lateral collaborations with INCODE project partners, leveraging its extensive promotional network to form mutual agreements in the form of Value-Added Reseller (VAR) partnerships. Hopefully, such partnerships will follow commercial agreements and appropriate IPR licensing, ensuring mutual benefits and market expansion.

Additionally, UNISYSTEMS will try to identify appropriate contacts to be approached for demo showcases of INCODE's capabilities, having as ultimate goal to create a list of first adopters. In the case that such network will be established, then it will be promoted to other partners within the project to facilitate joint bi-lateral collaborations, enhancing the collective market reach and impact.

Moreover, UNISYSTEMS will introduce INCODE's services and solutions to its parent group of companies, ranging from courier services to IT and logistics companies. This internal introduction will be complemented by seeking accompanying consulting service offerings, creating opportunities for collaboration with other partners. These partners will be invited for deployment, integration, and consulting roles, ensuring a comprehensive and integrated approach to commercializing INCODE innovations.

Finally, the UNISYSTEMS commercialization opportunities conclusions will be presented at the deliverable D6.3 "Final Dissemination-Communication Exploitation report".

REDHAT

Red Hat is a leading American software company specializing in open-source software solutions. We are best known for Red Hat Enterprise Linux (RHEL) operating system. Founded in 1993, Red Hat provides a wide range of enterprise software products and services, including cloud computing, virtualization, and middleware. REDHAT exploitable assets are summarised in Table 5.

Table 5: REDHAT's exploitable asset

Exploitable Asset	
Name	Multi-cluster Scheduler
Short description	Add the necessary mechanisms to the Kubernetes scheduler to schedule different components of an application on clusters across the edge-cloud continuum.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Commercial
Related UCs	All
Related WPs	WP3
Ownership	REDHAT

Co-funded by the European Union

Constraints to Intellectual Property Rights (IPR)	TBD
Customer Target Group	Developers, Cluster Admins, End Users
Customer Target Problem	Geographical distribution of users, scalability needs, resilience requirements, resource optimization goals, cost considerations, regulatory compliance, and disaster recovery preparedness.
Customer Key Benefits	Resolves issues related to resource management, scalability, resilience, latency, cost efficiency, disaster recovery, and regulatory compliance, making it a valuable tool for organizations managing complex distributed applications.
Customer target geographical scale	Global
Competitors	N/A
Differentiation of exploitable asset	A multi-cluster scheduler serves as a strategic asset by efficiently distributing workloads across multiple Kubernetes clusters. It enhances scalability, resilience, and high availability by spreading tasks across different clusters, thereby improving performance and reducing latency for end-users. This approach optimizes resource utilization and cost management by leveraging diverse cluster environments, including edge and cloud resources. Additionally, it strengthens disaster recovery capabilities and facilitates compliance with regulatory requirements by enabling workload placement in appropriate geographic locations. Overall, the multi-cluster scheduler enhances operational efficiency and reliability, making it a valuable asset in modern IT infrastructures.
Marketing, communication and promotion	Project dissemination, communication, and internal promotion
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	6
Planned activities for exploitation	We intend to integrate the components developed during the project into the relevant Red Hat’s products, more specifically RedHat OpenShift (OCP), Red Hat Advanced Cluster Management (ACM) and RHEL for Edge.
Notes / Additional information	N/A

NEC

NEC Laboratories Europe (NLE), which was established in 1997, is a subsidiary of NEC Corp. With around one hundred researchers, NEC Laboratories Europe conducts fundamental and applied research, organized in different areas, including Security, 6G Networks, Data Ecosystems, and Intelligent Software Systems. The Lab's Security group has been involved in numerous other European projects such as 5G-ENSURE, TREDISEC, TeraFlow, SPIRS, and ACROSS. The group has over ten years' experience in blockchain and its applications (including Digital Identity Management and Self-Sovereign Identities). Research topics within the security group are trusted computing technologies and safe AI, focusing here on the robustness and privacy of ML-based approaches. The group's research results are regularly published and presented at top-tier security venues, such as ACM CCS, Usenix Security, and NDSS. NLE works in close collaboration with NEC´s business units (NEC BU), sharing with them its research results, i.e., NLE is in constant contact with NEC BUs that are eager to learn about and use results from research projects for future NEC products. More concretely, the developments and findings from the project will be presented to the business units that operate and develop network and digital services for smart cities and IoT platforms. Results from the project (Table 6) can leverage digital innovation for NEC's technologies, including new applications and business models beyond 5G networks. Furthermore, NEC's work within the project will enhance the company's own security portfolio and contribute to the development and deployment of trustworthy, scalable, and effective management of networks and its services.

Table 6: NEC's exploitable asset

Exploitable Asset	
Name	Blockchain-enhanced compute node attestation service
Short description	Compute node attestation service based on Keylime (Open-source client-server attestation solution). The results from the attestation are registered on NEC's blockchain and can be securely retrieved afterwards. This blockchain, based on Fabric, provides extended security even for wallets. This is done by means of a "chainproof" that guarantees the validity of the contents received from the Blockchain, achieving security levels for wallets that are similar to actually running a full Blockchain node.
Type of exploitable asset	Software services
High-level goal (commercial, research, policy-making)	Research
Related UCs	Logistics and transport quality value chain, Utilities inspection
Related WPs	WP3
Ownership	NEC
Constraints to Intellectual Property Rights (IPR)	To be studied

Co-funded by the European Union

Customer Target Group	NEC Corp. and Business Units
Customer Target Problem	Securing IoT deployments and network/digital service deployments
Customer Key Benefits	Enhanced security
Customer target geographical scale	World
Competitors	To be studied
Differentiation of exploitable asset	Enhanced security over traditional Fabric-based solutions
Marketing, communication and promotion	Internal corporate events, tech talks and BU pitches
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	5
Planned activities for exploitation	To be studied after the responses from NEC Corp. and Business Units
Notes / Additional information	N/A

FIWARE

FIWARE Foundation is the legal independent body providing shared resources to help achieve the FIWARE mission by promoting, augmenting, protecting, evolving and validating the FIWARE technologies as well as the activities of the FIWARE Community, empowering its members including end-users, developers and rest of stakeholders in the entire ecosystem.

FIWARE Foundation is open: anybody can join contributing to transparent governance of FIWARE activities and rising through the ranks, based on merit. FIWARE Foundation is a non-profit organisation that drives the definition and encourages the adoption of open standards (implemented using open-source technologies) that ease the development of smart solutions across domains such as Smart Cities, Smart Energy, Smart Water, Smart AgriFood and Smart Industry, based on FIWARE technology. Founded in 2016, the foundation has Atos, Engineering, Madinah city, NEC, RedHat, and Telefónica among its Platinum members. Only by truly eliminating the existing technical and commercial obstacles hindering the effective usage of meaningful data, smart digital solution providers will be able to move forward and drive the market up, based on FIWARE technology.

Using FIWARE technologies, organisations can capture the opportunities that are emerging with the new wave of digitalisation brought by combining the Internet of Things with Context Information Management and Big Data services on the Cloud. Using FIWARE technologies, developers can gather context information at large scale from many different sources. FIWARE also helps to easily process, analyse and visualise managed context information, easing the implementation of the smart behaviour and the enhanced user experience required by next-generation Smart Applications. FIWARE plans to be able to integrate its service portfolio and catalogue thanks to the project, as depicted in Table 7, Table 8, and Table 9.

Table 7: FIWARE's exploitable asset (ETSI NGSI-LD Broker)

Exploitable Asset	
Name	ETSI NGSI-LD Broker
Short description	Context broker offering ETSI's NGSI-LD subscribable API and Internet of Things Agent for a JSON based protocol (with AMQP, HTTP and MQTT transports). This IoT Agent is designed to be a bridge between JSON and the NGSI-LD interface of a context broker.
Type of exploitable asset	Software reference architectures based on the components mentioned and standardisation support.
High-level goal (commercial, research, policy-making)	Proven and working reference architectures and data models.
Related UCs	Secure IoT applications & platforms Industrial IoT applications & platforms Data Spaces with System of Systems Data and Service Exchange solutions and platforms Trusted Data Exchange services
Related WPs	WP2; WP3; WP5; WP6
Ownership	FIWARE
Constraints to Intellectual Property Rights (IPR)	N/A – Everything is open source and based on open standards. Aligned with EU standards and regulations.
Customer Target Group	Public Administrations / Private Companies / System Integrators.
Customer Target Problem	Acceleration in the development of Smart solutions. Overcome business barriers in phase of upstream and downstream.
Customer Key Benefits	Open-source technology with vibrant community and global contributors with use cases from around the world.
Customer target geographical scale	Global
Competitors	OGC SensorThings API
Differentiation of exploitable asset	• Global Community, from the public administration to businesses, corporations to research centers, Europe to Africa, to Africa, from the USA to Asia. • Technical services on a large scale from newbies to experts. • Support members to go-to-market.

	- Business unit to support the positioning of FIWARE solutions developed by Members.
Marketing, communication and promotion	- Online and offline events at international level. - Co-branding and co-marketing activities.
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	5
Planned activities for exploitation	- The INCODE project is aligned with future activities related to our organizational mission to empower the value of data. By participating in the project, we will have the opportunity to collaborate with like-minded partners to also spread strategic communications actions, like the participation at Global event empowered the engagement activities and these actions will be followed in future. - The INCODE project will serve as a platform for us to further enhance our expertise in IoT, Edge, and Cloud computing driving continuous innovation within our organization. - The outcomes of the project have the potential to improve the ETSI ISG CIM standard adding new use cases in the federation of Context Brokers which will be exploited.
Notes / Additional information	N/A

Table 8: FIWARE's exploitable asset (Decentralized Authentication, Authorization & Access Control)

Exploitable Asset	
Name	Decentralized Authentication, Authorization & Access Control
Short description	A set of components providing the Data Access for the context information offered by the ETSI's NGSI-LD API.
Type of exploitable asset	Software reference architectures based on the components mentioned and standardisation support.

Co-funded by the European Union

High-level goal (commercial, research, policy-making)	Proven and working reference architectures and data models.
Related UCs	Secure IoT applications & platforms Industrial IoT applications & platforms Data Spaces with System of Systems Data and Service Exchange solutions and platforms Trusted Data Exchange services
Related WPs	WP2; WP3; WP5; WP6
Ownership	FIWARE
Constraints to Intellectual Property Rights (IPR)	N/A – Everything is open source and based on open standards. Aligned with EU standards and regulations.
Customer Target Group	Public Administrations / Private Companies / System Integrators.
Customer Target Problem	Acceleration in the development of Smart solutions. Overcome business barriers in phase of upstream and downstream.
Customer Key Benefits	Open-source technology with vibrant community and global contributors with use cases from around the world.
Customer target geographical scale	Global
Competitors	Eclipse Foundation
Differentiation of exploitable asset	• Global Community, from the public administration to businesses, corporations to research centers, Europe to Africa, to Africa, from the USA to Asia. • Technical services on a large scale from newbies to experts. • Support members to go-to-market. • Business unit to support the positioning of FIWARE solutions developed by Members.
Marketing, communication and promotion	• Online and offline events at international level. • Co-branding and co-marketing activities.
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	5
Planned activities for exploitation	• The INCODE project is aligned with future activities related to our organizational mission to empower the

	value of data. By participating in the project, we will have the opportunity to collaborate with like-minded partners to also spread strategic communications actions, like the participation at Global event empowered the engagement activities and these actions will be followed in future. • The INCODE project will serve as a platform for us to further enhance our expertise in IoT, Edge, and Cloud computing driving continuous innovation within our organization. • The outcomes of the project have the potential to improve the ETSI ISG CIM standard adding new use cases in the federation of Context Brokers which will be exploited.
Notes / Additional information	N/A

Table 9: FIWARE's exploitable asset (Blockchain-based data provenance tool)

Exploitable Asset	
Name	Blockchain-based data provenance tool
Short description	Blockchain-based data provenance tool recording and tracking the origin process, movement, and changes to data throughout its lifecycle, provides a secure, transparent, and tamper-proof record of ETSI NGSI-LD data history.
Type of exploitable asset	Software reference architectures based on the components mentioned and standardisation support.
High-level goal (commercial, research, policy-making)	Proven and working reference architectures and data models.
Related UCs	Secure IoT applications & platforms Industrial IoT applications & platforms Data Spaces with System of Systems Data and Service Exchange solutions and platforms Trusted Data Exchange services
Related WPs	WP2; WP3; WP5; WP6

Co-funded by the European Union

Ownership	FIWARE
Constraints to Intellectual Property Rights (IPR)	N/A – Everything is open source and based on open standards. Aligned with EU standards and regulations.
Customer Target Group	Public Administrations / Private Companies / System Integrators.
Customer Target Problem	Acceleration in the development of Smart solutions. Overcome business barriers in phase of upstream and downstream.
Customer Key Benefits	Open-source technology with vibrant community and global contributors with use cases from around the world.
Customer target geographical scale	Global
Competitors	To be studied
Differentiation of exploitable asset	• Global Community, from the public administration to businesses, corporations to research centers, Europe to Africa, to Africa, from the USA to Asia. • Technical services on a large scale from newbies to experts. • Support members to go-to-market. • Business unit to support the positioning of FIWARE solutions developed by Members.
Marketing, communication and promotion	• Online and offline events at international level. • Co-branding and co-marketing activities.
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	5
Planned activities for exploitation	• The INCODE project is aligned with future activities related to our organizational mission to empower the value of data. By participating in the project, we will have the opportunity to collaborate with like-minded partners to also spread strategic communications actions, like the participation at Global event empowered the engagement activities and these actions will be followed in future. • The INCODE project will serve as a platform for us to further enhance our

	expertise in IoT, Edge, and Cloud computing driving continuous innovation within our organization. - The outcomes of the project have the potential to improve the ETSI ISG CIM standard adding new use cases in the federation of Context Brokers which will be exploited.
Notes / Additional information	N/A

SMNS

SIEMENS is a global powerhouse in electric and electronic industry, a world leader in complex infrastructures solutions and an active provider of technologies. Siemens exposes in digital industry a unique automation portfolio, ranging from integrated drives and smart controllers to innovative PLM software. As a front runner for Industry 4.0, Siemens aim for increased productivity, efficiency, speed, and quality. Siemens is the leader of European patent applications and more than a quarter of them are in the area of digitalization. Looking at large, innovation at Siemens is happening in close contact with customer needs and interaction. This way the innovation is done following a pragmatic pattern, seeking for the benefit of all stakeholders, and the particular advantages gained thanks to the project are reported in Table 10.

Table 10: SMNS's exploitable asset

Exploitable Asset	
Name	Telemetry Analytics Module
Short description	Analytics over aggregated service and infrastructure telemetry in order to expose complex behaviour.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Commercial
Related UCs	All
Related WPs	WP4
Ownership	Siemens
Constraints to Intellectual Property Rights (IPR)	TBD
Customer Target Group	Developers, Cluster Admins
Customer Target Problem	Resilience requirements, resource optimization goals and cost considerations.
Customer Key Benefits	Uncovers complex hidden behaviour based on data that is not normally correlated and might be stored distributed, allows debugging of

	distributed applications, allows deployment support for distributed applications.
Customer target geographical scale	Global
Competitors	N/A
Differentiation of exploitable asset	Usual monitoring dashboards are based on ephemeral telemetry data and generally shows distributed system health and state. In order to uncover more complex behaviour that affects either functionality or performance, it's required to process and correlate said telemetry data. Process mining and general machine learning will be employed for this purpose.
Marketing, communication and promotion	Project dissemination, communication, and internal promotion
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	6
Planned activities for exploitation	N/A
Notes / Additional information	N/A

IPTO

IPTO (Independent Power Transmission Operator) is the Greek TSO, responsible for the operation, maintenance and development of the electricity transmission grid in Greece with over 11,000 km of system covering the whole of mainland Greece and a great number of facility sites. IPTO participates at different research projects through its Department of Research, Technology and Development (DRTD), acting as the vertical user and participating at the integration, validation and field trials of novel Smart Factory solutions at its premises. In this project IPTO provides the testing facilities in the Application area 2: Utilities inspection, HV substation data for the development of novel power utility applications and functional requirements for the novel power utility applications. In this context, the expected stakeholders include power Transmission & Distribution System Operators (TSOs & DSOs), energy aggregators and energy providers, which could benefit from the asset reported in Table 11.

Table 11: IPTO's exploitable asset

Exploitable Asset	
Name	Smart Data Analytics App for Utilities Inspection
Short description	Application for collecting, processing and analysing real-time industrial data from power utility infrastructures and gaining valuable insights for predictive maintenance purposes
Type of exploitable asset	Software

Co-funded by the European Union

High-level goal (commercial, research, policy-making)	For research for now and may explore commercialisation opportunities
Related UCs	AA2-UC1
Related WPs	WP4
Ownership	IPTO
Constraints to Intellectual Property Rights (IPR)	TBA
Customer Target Group	Power utility infrastructure operators (TSOs, etc.)
Customer Target Problem	The legacy infrastructure of HV substations is not being monitored in real-time, and no smart data analytics are applied to recognize varied power utility events (over/under-voltage, etc.)
Customer Key Benefits	Gain valuable insight from integrating HV substation real-time power utility data, concluding on critical on-time decisions
Customer target geographical scale	Europe and beyond
Competitors	TBA
Differentiation of exploitable asset	We expect to differentiate by combining smart data analytics & real-time data for monitoring HV infrastructure and enabling predictive maintenance actions
Marketing, communication and promotion	N/A
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	4
Planned activities for exploitation	Plan to explore further funded R&D projects to continue the research in this direction
Notes / Additional information	N/A

MADE

MADE is a North-Italian competence centre serving as an aggregator of industries, institutions and academia whose focus is oriented on the technology transfer towards local manufacturing SMEs. As such, and given its role and the resources involved in the project, MADE does not forecast to materially or intellectually own any of the achieved results of the project for a business/research exploitation, but the competences gained throughout the project, and (mostly) the results obtained in the AA3 are supposed to benefit from MADE's ecosystem as a dissemination multiplier, as well as to position the competence centre itself as a reference entry point for the manufacturing SMEs' galaxy seeking for mentoring in embodying human-centric manufacturing practices.

UBI

UBITECH aims to leverage the technological expertise gained from its INCODE research activities to enhance its offerings and market presence. Specifically, UBITECH intends to exploit the advancements made in the MAESTRO multi-cloud orchestrator used in the H2020 RAINBOW project. As an SME software house, UBITECH plans to further test and validate the Service Orchestrator in-house (Table 12), eventually offering it as a market-ready solution. Moreover, UBITECH envisions utilizing these technological developments to enhance its research, training, and consultancy services, enriching its portfolio. Additionally, UBITECH seeks to participate in the broader exploitation framework created by INCODE, either by directly contributing to the INCODE service offerings or by extending the INCODE Service Orchestrator with INCODE technologies.

Furthermore, UBITECH sees several exploitation opportunities: expanding consultancy services to include IoT-to-Edge-to-Cloud continuum concepts, improving academic and training services related to continuum computing and security enforcement, and building on the INCODE developments to further enhance its expertise and involvement in future European and national research projects. This strategic exploitation plan will position UBITECH at the forefront of technological innovation in the IoT-to-Edge-to-Cloud continuum, driving growth and value creation across its service offerings.

Table 12: UBI's exploitable asset

Exploitable Asset	
Name	Service Orchestrator
Short description	The INCODE Service Orchestrator (SO) manages end-to-end services over 5G, IoT, and cloud environments, automating service onboarding, ordering, and lifecycle management. It integrates service management, real-time telemetry, and policy enforcement, ensuring seamless, secure, and high-performance operations.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	INCODE Service Orchestrator is currently a closed source project to be promoted by UBITECH as a paid solution to customers in Greece, Cyprus (where UBI has offices) and widely in the EU market. Therefore, UBI will protect the orchestrator services solely owning the copyrights and trade secrets.
Related UCs	AA1-AA4
Related WPs	WP4-5
Ownership	UBI (100%)
Constraints to Intellectual Property Rights (IPR)	Proprietary software, no public license
Customer Target Group	Telecom providers, IoT solution providers, and

Co-funded by the European Union

	large enterprises with complex IT infrastructures needing advanced service management across 5G, IoT, and cloud environments.
Customer Target Problem	Challenges in managing end-to-end services across diverse and distributed domains, requiring automated, secure, and efficient orchestration to reduce operational complexity and ensure seamless integration.
Customer Key Benefits	Enhanced operational efficiency through automation, real-time monitoring, and dynamic policy enforcement, ensuring high performance, robust security, and seamless integration of their services across heterogeneous environments.
Customer target geographical scale	Europe, Middle East, South America
Competitors	Kestra, Ericsson Service Orchestration, Blue Planet Orchestration, Apache Airflow, Argo, Dagster, Prefect, K8s & Kubespray
Differentiation of exploitable asset	Targeted support for 5G and IoT environments, advanced security features, and automation capabilities.
Marketing, communication and promotion	Promote the Service Orchestrator at industry-specific conferences and workshops by actively participating and showcasing demonstration activities. Engage in relevant research projects to enhance visibility and credibility. Create a webpage with up-to-date information and leverage social media channels for continuous promotion and audience engagement.
Initial Technological Readiness (TRL)	2
Final Technological Readiness (TRL)	5
Planned activities for exploitation	Create partnerships with key industry players to integrate and deploy the service orchestrator, targeted marketing campaigns to highlight the orchestrator's unique benefits and use cases, training sessions and webinars to demonstrate the product's capabilities and drive adoption.
Notes / Additional information	N/A

SUITE5

Co-funded by the European Union

Suite5 Data Intelligence Solutions Ltd (S5) expects to acquire further technological and innovation know-how related to smart IoT services and the orchestration of decentralized applications, to further expand its unique solution portfolio on analytics and smart scheduling solutions for the manufacturing and utilities sectors. S5 aims to experiment on and implement new data analytics and optimization techniques, which in turn shall further expand the capabilities of the S5 Enterprise Analytics software. The exploitation of the results and of the work performed inside the INCODE project shall help gain insights into emerging innovation areas around smart IoT and novel business models including IoT services in the domains of smart manufacturing, utilities, and energy sectors. S5 aspires to upgrade its services portfolio with smart IoT specific technological and innovation know-how.

ILINK

iLINK is a software development company established in Athens. Its main expertise revolves around logistics and supply chain operational management. More precisely, route optimization and overall fleet management services have been provided to numerous clients over the past 20 years, and are supposed to be further exploited throughout the project, as per Table 13. Additionally, iLINK participates in several research activities and Project on the Industrial Smart Safety. In this context, iLINK aims to create a strong network of stakeholders related to the logistics and Industry 4.0, such as research institutions, SMEs, Universities, large corporate bodies, and key industrial players.

Table 13: ILINK's exploitable asset

Exploitable Asset	
Name	Smart Industrial Safety / Fleet Management and Route Optimization utilizing AI.
Short description	Full Applications for Indoor positioning of moving entities and collision avoidance AND fleet management based on multiple factors. Computer Vision models and IoT sensors will be employed aiming to enhance the cargo monitoring processes in real time. On top of that, 5G technology will enable seamless and fast data transmission.
Type of exploitable asset	Software and Hardware
High-level goal (commercial, research, policy-making)	commercial
Related UCs	UC1 - UC2
Related WPs	WP4-WP5
Ownership	ILINK
Constraints to Intellectual Property Rights (IPR)	TBA
Customer Target Group	Large industrial facilities / Logistic and supply chain companies, governments, municipalities

Co-funded by the European Union

Customer Target Problem	Industrial Safety Standards / Insufficient fleet management operations
Customer Key Benefits	Reduction in resource consumption, improvement of time efficiency
Customer target geographical scale	EUROPE
Competitors	TBA
Differentiation of exploitable asset	N/A
Marketing, communication and promotion	Participation in workshops, webinars, expos, and
Initial Technological Readiness (TRL)	5
Final Technological Readiness (TRL)	6
Planned activities for exploitation	Participation in other EU funded Projects with high TRL.
Notes / Additional information	N/A

K3Y

K3Y is a dynamic Small and Medium Enterprise (SME) specialising in cybersecurity and Research and Development (R&D) activities. Founded in Sofia, Bulgaria, in 2018, K3Y primarily serves the European and Bulgarian markets while actively participating in national and European Union (EU)-funded projects. K3Y's core activities can be categorised into two primary areas: (a) Cybersecurity Services and (b) R&D Activities. In the realm of Cybersecurity Services, K3Y offers four main services: Vulnerability Assessment, Penetration Testing, Purple Teaming, and Cybersecurity Consulting. On the other hand, K3Y participates in several R&D projects and initiatives. In the context of INCODE, K3Y aims to fully leverage the project's expertise and technological advancements to enhance its cyber-AI solutions, strengthening its competitiveness in the public and private sectors, especially in the industry domain. This involves adapting and optimising K3Y's cybersecurity tools (K3CyberRadar, K3DecoyNet and K3NetOrchestra), delivering new cyber-AI models, and enhancing its technical know-how in cybersecurity services. More precisely, in INCODE, K3Y is developing the exploitable assets described in Table 14 and Table 15.

Table 14: K3Y’s exploitable asset (Malware Detection Component)

Exploitable Asset	
Name	Malware Detection Component (MDC)
Short description	The Malware Detection Component (MDC) serves as a tool for malware detection within the field of software security attestation. It is designed to determine whether a software container, such as Docker images, has been compromised before being on-boarded and deployed in a production environment. Specifically, the MDC transforms software

	containers into visual representations and utilizes pre-trained vision models to assess if the integrity of the software container has been compromised.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Research
Related UCs	All
Related WPs	WP4
Ownership	K3Y
Constraints to Intellectual Property Rights (IPR)	N/A
Customer Target Group	System Administrators, Developers, Technicians
Customer Target Problem	Organisations face significant risks when integrating containers that may have been compromised or tampered with, potentially leading to data breaches or system failures. This tool addresses the critical need to verify the integrity of these containers efficiently.
Customer Key Benefits	MDC offers multiple benefits, such as enhancing security by reducing the risk of deploying compromised software containers, thus protecting against potential breaches and malware. Furthermore, MDC integrates state-of-the-art technology to detect integrity issues that conventional mechanisms may miss. Finally, MDC can be easily integrated into existing workflows, thus offering scalability to accommodate enterprises of all sizes.
Customer target geographical scale	Worldwide
Competitors	The main competitors related to MDC are summarised below. • **Aqua Security**: Aqua Security security solutions for securing containerised applications at various scales. • **Tenable**: Tenable provides various vulnerability assessment solutions like Nessus Vulnerability Scanner that can assess containers for potential weaknesses and vulnerabilities. • **NeuVector**: NeuVector Full Lifecycle Container Security Platform delivers the only cloud-native security with uncompromising end-to-end protection

	from DevOps vulnerability protection to automated run-time security, and featuring a true Layer 7 container firewall.
Differentiation of exploitable asset	Compared to the previous competitor solutions, MDC offers a holistic approach, allowing the visual and AI-based detection of potential security issues. This method complements the conventional solutions of current competitors, which primarily rely on source-code vulnerability assessments or system vulnerability scans. The use of visual representations coupled with advanced AI models allows more completeness and effective detection of threats, offering a significant advantage in identifying and mitigating risks that traditional methods might overlook.
Marketing, communication and promotion	Project dissemination and communication via research publications and participation in industry events.
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	4
Planned activities for exploitation	Participation in R&D activities and projects to further evolve the architectural components mechanisms behind MDC, integrating beyond state-of-the-art mechanisms.
Notes / Additional information	N/A

Table 15: K3Y's exploitable asset (Attack Mitigation Component)

Exploitable Asset	
Name	Attack Mitigation Component (AMM)
Short description	AMM focuses on detecting potential cyberattacks and operational anomalies and identifying appropriate mitigation actions. For this purpose, AMM leverages network traffic data and AI. More details for this component are provided in D3.1.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Research
Related UCs	AA4

Related WPs	WP4
Ownership	K3Y
Constraints to Intellectual Property Rights (IPR)	N/A
Customer Target Group	System Administrators, Technicians
Customer Target Problem	The target problem for AMM is the detection and mitigation of potential cyberattacks and operational anomalies, thus ensuring network security and maintaining business continuity for organisations.
Customer Key Benefits	It ensures continuous network monitoring, offers real-time alerts, provides automatically potential mitigation actions, identifies the best mitigation action with the minimum operational cost.
Customer target geographical scale	Worldwide
Competitors	• **AT&T Cybersecurity**: AI-enabled Behavioural Analysis, Threat Intelligence Integration, Automated Threat Detection, Incident Investigation and Response • **Fortinet:** Fortinet is a leading provider of network security appliances and solutions. FortiGuard provides a range of security services and threat intelligence capabilities to help organizations protect their networks, endpoints, applications, and data from cyber threats • **Vectra AI**: Vectra AI is a cybersecurity company that specializes in network detection and response (NDR) solutions powered by artificial intelligence (AI) and machine learning (ML) technologies. • **CrowdStrike**: CrowdStrike is a leading cybersecurity company known for its cloud-native endpoint protection platform. • **Splunk**: Machine Learning Toolkit (MLTK), Natural Language Processing (NLP), AI-enabled Anomaly Detection, Predictive Analytics, Security Analytics
Differentiation of exploitable asset	Compared to existing solutions, AMM integrates application-layer traffic aggregators that feed AI and allow the detection of potential attacks at the application layer. On the other side, the current competitor solutions are limited to TCP/IP solutions. Finally, AMM automates the identification of mitigation actions and identifies the best of them with the

Co-funded by the European Union

	minimum operational cost.
Marketing, communication and promotion	Project dissemination and communication via research publications and participation in industry events.
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	4
Planned activities for exploitation	Participation in R&D activities and projects to further evolve the architectural components mechanisms behind AMM, integrating beyond state-of-the-art mechanisms.
Notes / Additional information	N/A

AGE

Agentscape AG (AGE) is a Berlin-based high-tech SME (Small and Medium Enterprise) that develops and markets basic technology and solutions for dynamic personalization and social-oriented intelligent software agents and operates managed cloud-native solutions for enterprise customers. The platforms include advanced information management solutions based on statistical machine learning technologies applied to high-dimensional unstructured and structured data and a knowledge-based Interaction Engine capable of implementing social-intelligent and business-oriented agent behaviours, where the knowledge gained in the project could benefit in terms of User Interaction (UI), as reported in Table 16.

Table 16: AGE's exploitable asset

Exploitable Asset	
Name	Application Operations and Business Portals
Short description	User interfaces (UIs) and dashboards for various stakeholders, enabling secure and regulated access to infrastructure resources. User-friendly UIs for application providers to onboard and manage application components, dependencies, and Service-Level Agreements (SLAs). Visualization of runtime information and telemetry data across the IoT-Edge-Cloud continuum for operational insights and reconfigurations.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Research
Related UCs	All
Related WPs	WP4

Ownership	AGE
Constraints to Intellectual Property Rights (IPR)	N/A
Customer Target Group	End Users, Developers, Administrators, Managers
Customer Target Problem	Complexity of managing and orchestrating services across diverse and distributed environments, leading to inefficiencies and limited visibility. Additionally, security and compliance challenges, coupled with slow development and deployment cycles, hinder operational efficiency and responsiveness.
Customer Key Benefits	Creating an efficient, scalable, and secure development ecosystem that enhances productivity, fosters innovation, and ensures seamless deployment and management of applications in IoT and edge environments.
Customer target geographical scale	Worldwide
Competitors	Tools and platforms that offer similar functionalities for managing and orchestrating applications and services across diverse environments.
Differentiation of exploitable asset	Intuitive and user-friendly interfaces designed for diverse stakeholders including end users, developers, administrators, and managers. Robust security features, including role-based access control (RBAC) and comprehensive compliance tools integrated throughout the service and resource management layers.
Marketing, communication and promotion	Project dissemination and communication
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	4
Planned activities for exploitation	Participate in joint research projects and publications to advance the state of the art. Partner with industry-specific organizations and consortia to tailor the platform to specific verticals.
Notes / Additional information	-

AXON

AXON, founded in 1989, is a research and innovation SME. It offers advanced research tools and consultancy in applied mathematics, computing, and engineering, targeting sectors like AI, cybersecurity, edge-cloud computing, and green communications. The expected stakeholders of the Intelligent task offloading algorithm, described in Table 17, may include academic researchers, technology developers, and businesses seeking cutting-edge solutions.

Table 17: AXON's exploitable asset

Exploitable Asset	
Name	Intelligent task offloading algorithm
Short description	The algorithm utilizes reinforcement learning for optimizing task offloading decisions across scheduling slots, resulting in lower computation loads and offloading switching costs compared to the centralized scheme.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Currently focused on research with potential for future exploration of commercialization opportunities.
Related UCs	AA2-UC2
Related WPs	WP4
Ownership	AXON
Constraints to Intellectual Property Rights (IPR)	N/A
Customer Target Group	Network infrastructure providers and application developers.
Customer Target Problem	Addressing privacy concerns and optimizing resource allocation in vehicular networks while minimizing computation loads and offloading switching costs.
Customer Key Benefits	Enhanced privacy protection, improved network efficiency and minimized offloading switching costs.
Customer target geographical scale	Europe and beyond
Competitors	Other algorithms or solutions focused on privacy preservation and resource optimization in vehicular networks
Differentiation of exploitable asset	This approach ensures better privacy protection, efficient resource allocation, and reduced computation loads compared to traditional centralized systems
Marketing, communication and promotion	N/A
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	4
Planned activities for exploitation	We intend to pursue additional funded R&D projects to further advance research in this direction.

Co-funded by the European Union

Notes / Additional information	N/A

ARHS

Arηs Group (pronounced "Aris") is a prominent IT consulting and services company that focuses on providing advanced and reliable information systems. Founded in 2003, the group has expanded to encompass 12 entities, each specializing in various aspects of IT, including software development, business intelligence, digital trust, infrastructure, and more. In the context of the project, the work carried out in AA1 will produce the exploitable asset depicted in Table 18.

Table 18: ARHS's exploitable asset

Exploitable Asset	
Name	Low-cost alert system
Short description	The solution will utilize various sensors to capture images and perform analysis to identify objects that meet specific standards, as well as obstacles that may pose collision risks. Primarily, the solution should address two key issues: a) identifying potential collision threats and providing a safety factor for personnel, whether they are on foot or operating vehicles like forklifts (as in the case of AA1).
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Currently focused on research with potential for future exploration of commercialization opportunities.
Related UCs	AA1-UC1
Related WPs	WP5
Ownership	ARHS
Constraints to Intellectual Property Rights (IPR)	It will be under MIT License
Customer Target Group	Automotive companies, Logistic Platforms, Automatic route planning platforms (for drones, vehicles)
Customer Target Problem	Provide solution for health and safety to industrial environments as well as provide extra features to vehicles
Customer Key Benefits	Improve performance of obstacle detection in matter of time and accuracy
Customer target geographical scale	Europe and beyond
Competitors	Other algorithms or solutions focused on AI detection, cameras with embedded algorithms, industrial computer

	vision systems
Differentiation of exploitable asset	This approach will be optimized for forklifts or other industrial vehicles and equipment. Having that as ground truth, it will be lightweight and capable to be used in several IoT devices.
Marketing, communication and promotion	N/A
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	4
Planned activities for exploitation	We intend to pursue additional funded R&D projects to further advance research in this direction.
Notes / Additional information	N/A

UoP

University of Patras, established in the city of Patras in 1964 and commenced operating in the academic year 1966-1967, boasts a rich history of research projects within its Electrical & Computer Engineering department. Notably, the Applied Electronics Laboratory (APEL) and the Patras5G team have been pivotal in driving forward these initiatives. Beyond their involvement in research projects, these teams have spearheaded various initiatives such as the establishment of the P-NET Competency Centre, Sense City, OpenSlice (Table 19), and more (i.e., the testbed described in Table 20).

Table 19: UoP's exploitable asset (OpenSlice)

Exploitable Asset	
Name	OpenSlice
Short description	OpenSlice is an open-source service based Operations Support System (OSS) to deliver Network Slice as a Service (NSaaS).
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Research
Related UCs	Applicable to all the UCs in the project
Related WPs	WP3
Ownership	UoP
Constraints to Intellectual Property Rights (IPR)	TBA
Customer Target Group	MNOs, integrators, researchers

Customer Target Problem	Addressing the issue of managing heterogeneous computational and network resources and services.
Customer Key Benefits	Offering a seamless, unified and standardized manner to manage the underlying computational and network resources.
Customer target geographical scale	Global
Competitors	OSM, ONAP, Contrail
Differentiation of exploitable asset	Following TMF standards makes this asset highly interoperable with different controllers and drivers from different domains and cooperates with any other OSS that supports those standards. This asset is also highly customizable and open source.
Marketing, communication and promotion	Through ETSI's SDG OSL
Initial Technological Readiness (TRL)	4
Final Technological Readiness (TRL)	5
Planned activities for exploitation	Plan to explore further funded R&D projects to continue the research in this direction
Notes / Additional information	This asset is the core of the resource orchestrator, and it includes also the policy engine.

Table 20: UoP's exploitable asset (IoT-5G system testbed)

Exploitable Asset	
Name	IoT-5G system testbed
Short description	Provision of an open IoT-5G testbed to experiment with, test or benchmark: 1) hardware including sensors, computational nodes, gNBs, antennas, etc., 2) services managing those kinds of hardware, 3) services enhancing hardware's operation 4) end-to-end services including both applications and the underlying hardware
Type of exploitable asset	hardware
High-level goal (commercial, research, policy-making)	Research
Related UCs	Applicable to UCs 1,2 and 4
Related WPs	WP5

Ownership	UoP
Constraints to Intellectual Property Rights (IPR)	TBA
Customer Target Group	MNOs, integrators, researchers
Customer Target Problem	Addressing the issue of lack of such open testbeds.
Customer Key Benefits	Offering an open and heterogenous testbed that consists of a plethora of IoT sensors and computational resources interconnected through 5G to form a unique testbed for edge-cloud applications.
Customer target geographical scale	Europe
Competitors	OpenIreland Testbed, Slices testbed
Differentiation of exploitable asset	Offering a 5G oriented IoT testbed open to experimentation and testing
Marketing, communication and promotion	N/A
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	4
Planned activities for exploitation	Plan to explore further funded R&D projects to continue the research in this direction
Notes / Additional information	N/A

POLIMI

Politecnico di Milano (POLIMI) is a North-Italian technical university, whose primary mission is the proper training of its pupils in engineering, design and architecture. In order to maintain high standards of education and to allow these students to be able to face the challenges of their future professional life, POLIMI has been actively worked on research projects since its foundation in 1863. With respect to the reported activity, in particular, POLIMI involved its Manufacturing Group, which is largely interested in the digital tools supporting operations in industrial sector. Given, indeed, the recent trend of human-centric manufacturing, POLIMI is aiming to develop software applications deployable at a shopfloor level which respect requirements of human-centricity, interoperability and high data bandwidth (see Table 21 and Table 22).

Table 21: POLIMI's exploitable asset (Fatigue detector)

Exploitable Asset	
Name	Fatigue detector
Short description	Machine Learning-based clustering of biometric live data coming from manual operators, in

	order to adapt the production output according to the physical stress the operator is currently subject to.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Multidisciplinary research (behavioural science, industrial engineering).
Related UCs	UC3
Related WPs	WP5
Ownership	POLIMI
Constraints to Intellectual Property Rights (IPR)	TBA
Customer Target Group	Research community, manufacturing community
Customer Target Problem	Chronical injuries derived by manual repetitive activities are considered one of the most impacting factors of human resources-related costs in manufacturing. Several companies have indeed invested in recent years on technological aid measures to prevent these effects on their labour force.
Customer Key Benefits	Research community will be given a new tool to estimate the fatigue derived from manual tasks. This could be exploited on the long term in safety studies comparing different approach to physical tasks.
Customer target geographical scale	Worldwide
Competitors	TBA
Differentiation of exploitable asset	TBA
Marketing, communication and promotion	Dissemination through scientific articles, joint actions with national initiatives.
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	5
Planned activities for exploitation	Further research projects are expected to continue the research with wider application cases.
Notes / Additional information	N/A

Table 22 : POLIMI's exploitable asset (Biosignal analysis library)

Exploitable Asset	

Name	Biosignal analysis library
Short description	Python library devoted to the analysis of biosignals
Type of exploitable asset	Software library
High-level goal (commercial, research, policy-making)	Research
Related UCs	UC3
Related WPs	WP5
Ownership	POLIMI
Constraints to Intellectual Property Rights (IPR)	TBA
Customer Target Group	Research community
Customer Target Problem	Current open-source libraries lack of integration components in case of multi-source data production.
Customer Key Benefits	Unique access point for several different classes of bio-sensors (i.e., ECGs, EMGs)
Customer target geographical scale	Worldwide
Competitors	TBA
Differentiation of exploitable asset	TBA
Marketing, communication and promotion	Dissemination through scientific articles, joint actions with national initiatives, software developers' conventions.
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	5
Planned activities for exploitation	Further research projects are expected to continue the research, adding new functions and supporting wider range of technologies (e.g., eye-tracking).
Notes / Additional information	N/A

MARTEL

Headquartered in Zurich, with offices in Amsterdam and Chiasso, Martel is an innovative and dynamic SME specialized in the management, innovation and promotion of international Research and Innovation projects with a focus on advanced Internet technologies, such as 5G, IoT and Cloud.

Co-funded by the European Union

Martel, with more than 20 years' experience in the European and Global ICT scene, includes three departments that work side by side to deliver the best quality to its customers.

In recent years, Martel has been strongly involved in several HORIZON EUROPE, Digital Europe, H2020 and FP7 projects whose scope and activities in the fields of Big Data, Cloud Computing, Smart Cities and IoT are directly impacted by the challenges that Martel tries to solve in INCODE i.e. enforce data privacy. Besides funded research, Martel is active also with private customers e.g. cities and utility companies which are leveraging Martel's IoT Open Source Platform Orchestra Cities, the main beneficiary of the innovation developed in the project.

Martel is producing the Self-Aware Data Privacy component to allow data owners to enforce protection of their data leveraging language-independent access policies for API and a recommender system to allow the specification of such policies.

Exploring and developing innovative features is extremely important to Martel to ensure advantages with respect to the wide competition on the market. The potential for enhancing Orchestra Cities with advanced privacy will be explored with key customers, such as the city of Wolfsburg and the EKZ (Elektrizitätswerke des Kantons Zürich), which are currently employing the Orchestra Cities platform.

The Self-Aware Data Privacy component is released as Open Source and can immediately be used by other partners, for example to combine access policies and algorithms of data encryptions (XLAB). The Self-Aware Data Privacy Component was employed by domain B (BOX2M) and C (RGB) to test the field-to-cloud data transmission with augmented data privacy and included in the Orchestra Cities platform offering of Martel.

UWS

UWS is a university working on research of next-generation platforms for application developers and is leading the R&D activities on Internal Developer Platform (IDP) in this project whilst focusing on the IDP Core component (Table 23). The expected stakeholders may include application developers, service providers and other interested parties that contribute to improving the efficiency of application developers' job in application development towards deployment.

Table 23: UWS's exploitable asset

Exploitable Asset	
Name	Internal Developer Platform (IDP) Core
Short description	The core part of the IDP to facilitate vertical application development, with a built-in pipeline and supporting features to trigger application deployment, and extensible to allow additional plug-ins.
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	For research for now and may explore commercialisation opportunities
Related UCs	Applicable to all the UCs in the project

Related WPs	WP4
Ownership	UWS
Constraints to Intellectual Property Rights (IPR)	TBA
Customer Target Group	Application developers
Customer Target Problem	Addressing the problem faced by application developers due to the lack of an integrated platform for streamlined application development towards deployment
Customer Key Benefits	Offering an integrated and extensible platform to help application developers to achieve streamlined application development towards deployment
Customer target geographical scale	Europe and beyond
Competitors	TBA
Differentiation of exploitable asset	Integrated and extensible platform to meet the essential requirements of application development and facilitate Infrastructure as Code deployment
Marketing, communication and promotion	N/A
Initial Technological Readiness (TRL)	3
Final Technological Readiness (TRL)	4
Planned activities for exploitation	Plan to explore further funded R&D projects to continue the research in this direction
Notes / Additional information	This asset is the core platform part of the IDP and it does not include IDE plugin (UBITECH), Code acceleration (UMAN)

UMAN

UMAN is one of the largest institutions in the UK and a proud member of the prestigious Russell Group. UMAN is providing the Software Acceleration component (Table 24), which will enable the transparent acceleration of suitable applications on heterogeneous hardware devices. Due to the unique advantages that the Software Acceleration component offers, i.e., its high-level Java APIs, transparent runtime optimizations and the ability to target heterogeneous devices from various vendors, it can be used in a wide range of sectors, including Fintech, NLP, Health Analytics and Retail.

Table 24: UMAN's exploitable asset

Exploitable Asset	
Name	Software Acceleration
Short description	The software Acceleration component will enable the transparent execution of suitable applications on heterogeneous hardware resources
Type of exploitable asset	Software
High-level goal (commercial, research, policy-making)	Research
Related UCs	Under discussion
Related WPs	WP4
Ownership	UMAN
Constraints to Intellectual Property Rights (IPR)	No, it is open-source
Customer Target Group	Fintech, NLP, Health Analytics, Retail
Customer Target Problem	High engineering costs for accessing heterogeneous resources
Customer Key Benefits	High-level Java APIs, transparent runtime optimizations, support for a wide range of hardware
Customer target geographical scale	Europe and beyond
Competitors	Aparapi, IBM OpenJ9
Differentiation of exploitable asset	High-level Java APIs, transparent runtime optimizations, support for a wide range of hardware
Marketing, communication and promotion	Blogs, industrial conferences, social media presence, YouTube videos
Initial Technological Readiness (TRL)	7
Final Technological Readiness (TRL)	8
Planned activities for exploitation	Plan to spin-out a company based on the core component of the software acceleration module
Notes / Additional information	-

Co-funded by the European Union

6 Monitoring of activities

Over the course of the project, WP6's activities will be regularly monitored to ensure the success of the project. To gauge the effects and make the most precise evaluation of such actions, a set of KPIs has been created. The table here below contains the key performance indicators (KPIs), their applicability to the tools and channels employed, and the expected goal value and the current status at M18.

The KPIs may be revised and updated, if needed, over the course of the project.

Table 25: Key Performance Indicators (KPIs)

	KPIs	Target at M36 (Dec 2025)	Current status (June 2024)
Communication activities	Website	> 6.000 visits	2,800
	Social media	>150 X/Twitter followers >300 LinkedIn followers	152 227
	Videos uploaded on YouTube channel	≥ 6 videos	2
	Newsletters	9	3
	Public appearances	6	1 (HiPEAC infomagazine n.71)
	Technical brochures Non-technical brochures	>3 >3	1 roll-up and 1 introductory flyer
	Press Releases	9	1 (for the KoM)
	Events (Organized & Participated)	>8 >100 visitors	19 >5,000 visitors
Dissemination activities	Scientific publications	>20	11 + 1 submitted
	Conference participation	>20	10
	Scientific workshops	>2 >100 participants	0

Co-funded by the European Union

	Webinars	>4	2
	Contributions to SDOs and open-source communities	>6	3
	Datasets for open access	>20	0
	Transfer of concept and established links to	>6 associations	6
	Liaisons with other projects	>5	4
	Co-organized workshops with other projects	2	2
	Co-organized webinars on common research areas	4	2

7 Conclusions

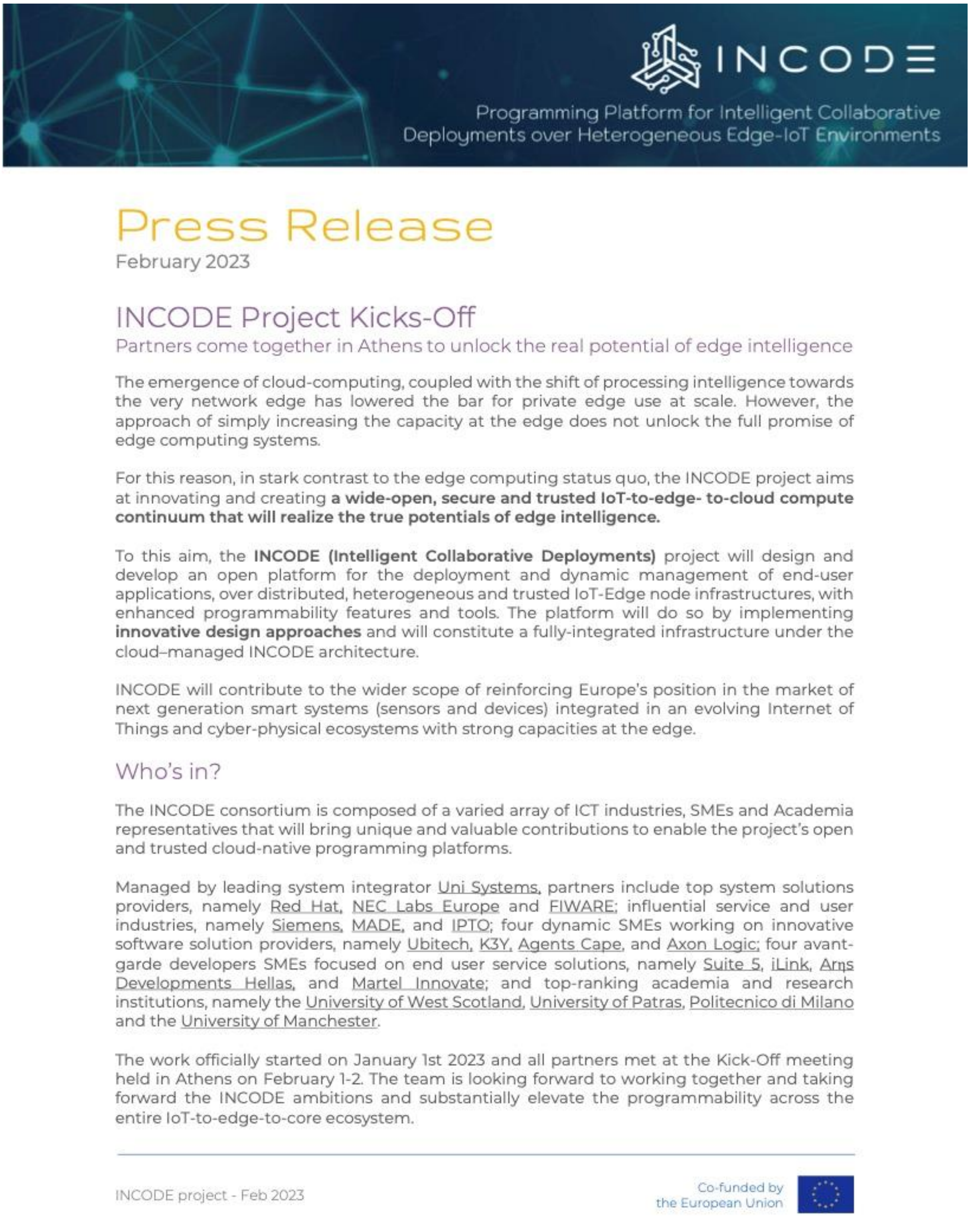
At M18 of the project, the overall activities appear to be aligned with the roadmap stated in the Description of Action (Part B). This is reflected from the KPIs reported in the document, whose numbers are aligned with the plans forecasted in the proposal preparation stage.

Some of these KPIs, related to Dissemination and Communication activities, are also overperforming with respect to what initially planned for the time being (e.g., scientific publications and conference attendances, which usually are expected to have their peak of performance in the last months of the activities, after the consolidation of results in pilots and testbeds, and for which the consortium, at month 18, has already achieved half of the target planned for month 48, as per Description of Action). One possible explanation for this phenomenon could sit in the interest of the scientific and practitioners' communities with respect to the topics researched in the technical Work Packages.

The KPIs which are still "far" from the target levels are anyway deemed under control (i.e., provision of datasets), given the fact that they are linked to activities related to integration in Application Areas, which is supposed to provide relevant results in the last stages of the project.

Concerning the Exploitation activities, the wide variety of tools supported by the partners are supporting the expectation for a duration of the project-related activities beyond its formal ending, relying on potential future research funding to increase the maturity level of the tools and switch to products and services, or to keep on the maintenance of these tools to allow their exploitation in the open-source community.

Annex A



INCODE

Programming Platform for Intelligent Collaborative Deployments over Heterogeneous Edge-IoT Environments

Press Release

February 2023

INCODE Project Kicks-Off

Partners come together in Athens to unlock the real potential of edge intelligence

The emergence of cloud-computing, coupled with the shift of processing intelligence towards the very network edge has lowered the bar for private edge use at scale. However, the approach of simply increasing the capacity at the edge does not unlock the full promise of edge computing systems.

For this reason, in stark contrast to the edge computing status quo, the INCODE project aims at innovating and creating **a wide-open, secure and trusted IoT-to-edge- to-cloud compute continuum that will realize the true potentials of edge intelligence.**

To this aim, the **INCODE (Intelligent Collaborative Deployments)** project will design and develop an open platform for the deployment and dynamic management of end-user applications, over distributed, heterogeneous and trusted IoT-Edge node infrastructures, with enhanced programmability features and tools. The platform will do so by implementing **innovative design approaches** and will constitute a fully-integrated infrastructure under the cloud–managed INCODE architecture.

INCODE will contribute to the wider scope of reinforcing Europe's position in the market of next generation smart systems (sensors and devices) integrated in an evolving Internet of Things and cyber-physical ecosystems with strong capacities at the edge.

Who's in?

The INCODE consortium is composed of a varied array of ICT industries, SMEs and Academia representatives that will bring unique and valuable contributions to enable the project's open and trusted cloud-native programming platforms.

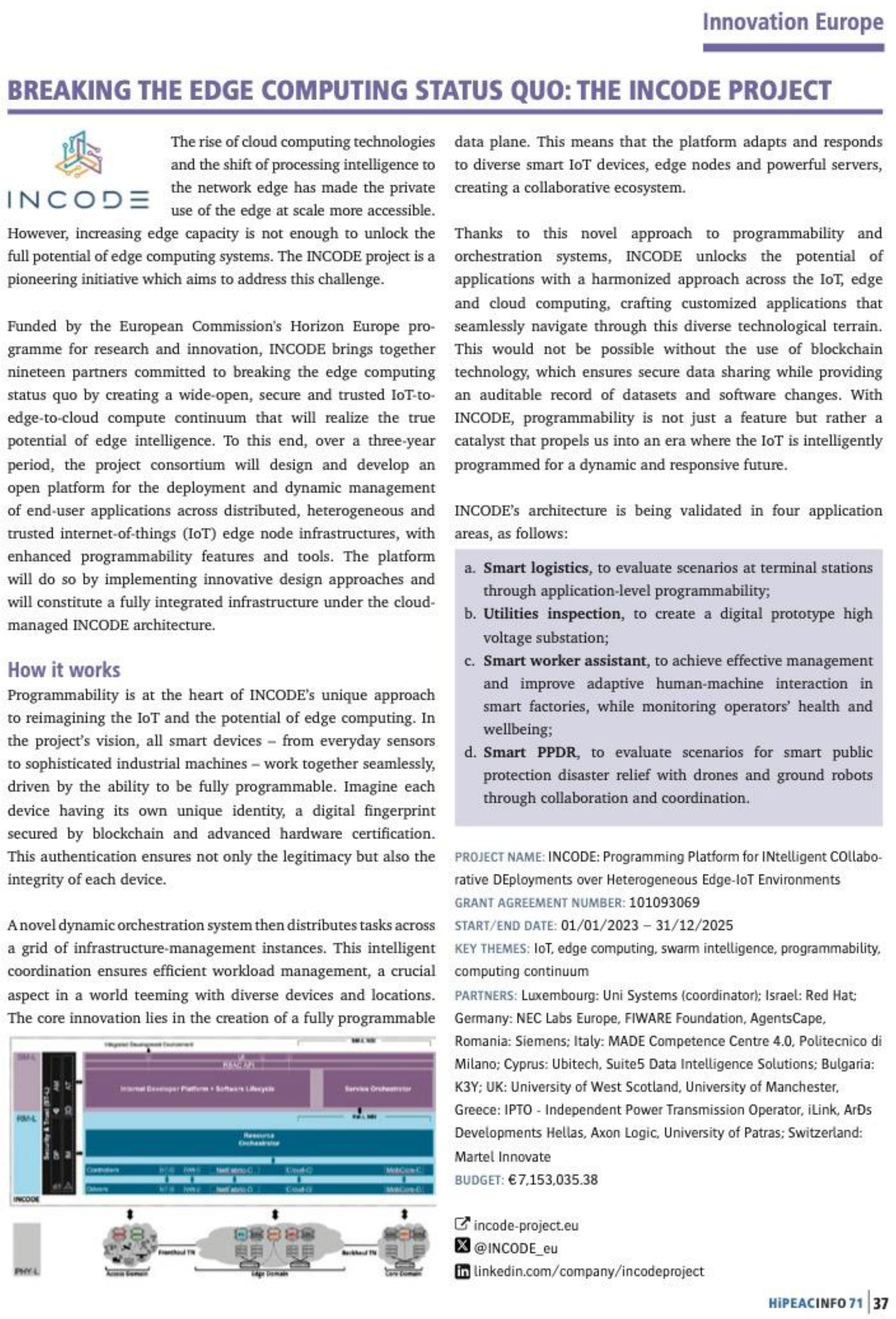
Managed by leading system integrator Uni Systems, partners include top system solutions providers, namely Red Hat, NEC Labs Europe and FIWARE; influential service and user industries, namely Siemens, MADE, and IPTO; four dynamic SMEs working on innovative software solution providers, namely Ubitech, K3Y, Agents Cape, and Axon Logic; four avant-garde developers SMEs focused on end user service solutions, namely Suite 5, iLink, Arηs Developments Hellas, and Martel Innovate; and top-ranking academia and research institutions, namely the University of West Scotland, University of Patras, Politecnico di Milano and the University of Manchester.

The work officially started on January 1st 2023 and all partners met at the Kick-Off meeting held in Athens on February 1-2. The team is looking forward to working together and taking forward the INCODE ambitions and substantially elevate the programmability across the entire IoT-to-edge-to-core ecosystem.

INCODE project - Feb 2023

Co-funded by the European Union

Figure 13: 1st project press release



Innovation Europe

BREAKING THE EDGE COMPUTING STATUS QUO: THE INCODE PROJECT

INCODE

The rise of cloud computing technologies and the shift of processing intelligence to the network edge has made the private use of the edge at scale more accessible. However, increasing edge capacity is not enough to unlock the full potential of edge computing systems. The INCODE project is a pioneering initiative which aims to address this challenge.

Funded by the European Commission's Horizon Europe programme for research and innovation, INCODE brings together nineteen partners committed to breaking the edge computing status quo by creating a wide-open, secure and trusted IoT-to-edge-to-cloud compute continuum that will realize the true potential of edge intelligence. To this end, over a three-year period, the project consortium will design and develop an open platform for the deployment and dynamic management of end-user applications across distributed, heterogeneous and trusted internet-of-things (IoT) edge node infrastructures, with enhanced programmability features and tools. The platform will do so by implementing innovative design approaches and will constitute a fully integrated infrastructure under the cloud-managed INCODE architecture.

How it works

Programmability is at the heart of INCODE's unique approach to reimagining the IoT and the potential of edge computing. In the project's vision, all smart devices – from everyday sensors to sophisticated industrial machines – work together seamlessly, driven by the ability to be fully programmable. Imagine each device having its own unique identity, a digital fingerprint secured by blockchain and advanced hardware certification. This authentication ensures not only the legitimacy but also the integrity of each device.

A novel dynamic orchestration system then distributes tasks across a grid of infrastructure-management instances. This intelligent coordination ensures efficient workload management, a crucial aspect in a world teeming with diverse devices and locations. The core innovation lies in the creation of a fully programmable data plane. This means that the platform adapts and responds to diverse smart IoT devices, edge nodes and powerful servers, creating a collaborative ecosystem.

Thanks to this novel approach to programmability and orchestration systems, INCODE unlocks the potential of applications with a harmonized approach across the IoT, edge and cloud computing, crafting customized applications that seamlessly navigate through this diverse technological terrain. This would not be possible without the use of blockchain technology, which ensures secure data sharing while providing an auditable record of datasets and software changes. With INCODE, programmability is not just a feature but rather a catalyst that propels us into an era where the IoT is intelligently programmed for a dynamic and responsive future.

INCODE's architecture is being validated in four application areas, as follows:

a. **Smart logistics**, to evaluate scenarios at terminal stations through application-level programmability;
b. **Utilities inspection**, to create a digital prototype high voltage substation;
c. **Smart worker assistant**, to achieve effective management and improve adaptive human-machine interaction in smart factories, while monitoring operators' health and wellbeing;
d. **Smart PPDR**, to evaluate scenarios for smart public protection disaster relief with drones and ground robots through collaboration and coordination.

PROJECT NAME: INCODE: Programming Platform for INtelligent COllaborative DEployments over Heterogeneous Edge-IoT Environments
GRANT AGREEMENT NUMBER: 101093069
START/END DATE: 01/01/2023 – 31/12/2025
KEY THEMES: IoT, edge computing, swarm intelligence, programmability, computing continuum
PARTNERS: Luxembourg: Uni Systems (coordinator); Israel: Red Hat; Germany: NEC Labs Europe, FIWARE Foundation, AgentsCape, Romania: Siemens; Italy: MADE Competence Centre 4.0, Politecnico di Milano; Cyprus: Ubitech, Suite5 Data Intelligence Solutions; Bulgaria: K3Y; UK: University of West Scotland, University of Manchester, Greece: IPTO - Independent Power Transmission Operator, iLink, ArDs Developments Hellas, Axon Logic, University of Patras; Switzerland: Martel Innovate
BUDGET: €7,153,035.38

incode-project.eu
@INCODE_eu
linkedin.com/company/incodeproject

HiPEACINFO 71 | 37

Figure 14: HIPEAC info Nr. 71 feature