D7.1 Kick-off Meeting Report

Revision: v.1.0

Work package	WP7: Project Management
Task	Task 7.1
Due date	31/10/2021
Submission date	31/10/2021
Deliverable lead	Technische Universiteit Delft (TU Delft)
Version	1.0
Authors	Aaron Ding (TU Delft)
Reviewers	n.a.

Grant Agreement No.: 101021808
Call: H2020-SU-DS-2020
Topic: SU-DS02-2020
Type of Action: RIA

Abstract	This report summarizes the kick-off meeting of SPATIAL project, which was held by TU Delft on 29 September 2021.
Keywords	KOM; Kick-off; Meeting; Project Management

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	31/10/2021	First version	Aaron Ding (TU Delft)

DISCLAIMER

COPYRIGHT NOTICE

© 2021 - 2024 SPATIAL

Project funded by the European Commission in the H2020 Programme under grant agreement No. 101021808		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g., web	✔
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to SPATIAL project and Commission Services	

* R: Document, report (excluding the periodic and final reports)
 DEM: Demonstrator, pilot, prototype, plan designs
 DEC: Websites, patents filing, press & media actions, videos, etc.
 OTHER: Software, technical diagram, etc

EXECUTIVE SUMMARY

SPATIAL builds the pathway toward a trustworthy European cybersecurity sector, developing trustworthy governance and regulatory framework for AI-driven security in Europe.

Achieving trustworthy AI is a top priority for Europe, often hindered by the opacity of algorithms in software and hardware operations. SPATIAL solves such uncertainty by enforcing data privacy, resilience engineering, and legal-ethical accountability.

On the day of the hybrid kick-off meeting (Delft, 29/09/2021), SPATIAL consortium members introduced themselves and learned from partner institutions background and expertise on which the project idea originated and how these are interconnected throughout the meeting sessions.

In the morning during the introductions, participants presented their organizations and learned about each other's contributions and expectations. Team members discussed planned synergies between different work packages and made concrete agreements regarding how to contribute to upcoming tasks and deliverables. Participants also met the European Commission Project Officer, Mr Georgios KAIAFAS who provided a detailed presentation about the varying regulatory aspects (e.g., issues related to financial reporting and administrative management of the project) for successful project execution.

In the afternoon, during an intensive WP leader review session all seven work package leaders presented their WP objectives, goals, and planning of their contribution to the overall workplan. After the coffee break, in a plenary session, the EMDESK project management tool was introduced by means of a live (GANTT) planning review. This was followed by a use case review where the four use cases were presented and discussed to collect inputs from all partners regarding the main data collection efforts envisioned.

In the late afternoon, participants received an online onboarding session provided by trainers of EMDESK. This ensured efficient kick-off and guaranteed use. In the plenary session participants also reflected on topics associated with dissemination efforts of interest for the public like for instance the website design and planned (social) media campaign. Ideas and questions around these topics were shared.

In the final session, 1st year deliverables and progress were highlighted and quality assurance responsibilities were distributed among partners. A finance check was performed and the data management and ethical considerations were discussed. The ethical advisor (Prof. Zimmer) joined the session and was introduced to the consortium. Future steps for upcoming meetings were coordinated.

For those who were physically present on-site (TUD and EUR delegates) the day ended with a lovely consortium dinner on campus, during which participants had the chance to further get to know each other and share personal and professional experiences.

TABLE OF CONTENTS

1 ATTENDANCE AND AGENDA

1.1 LIST OF PARTICIPANTS

All 12 consortium partners attended the kick-off meeting with a total of 40 participants who were present on-line (though a Zoom connection) or on-site in the Pulse Building on the TUD campus in Delft, the Netherlands.

Names and affiliations of all participants are listed in the table below.

First Name	Last Name	Organisation	note
Georgios	Kaiafas	EC	Online
Aaron	Ding	TU Delft	Onsite
Cornelis	van de Kamp	TU Delft	Onsite
Marijn	Janssen	TU Delft	Onsite
Martijn	Warnier	TU Delft	Onsite
Roel	Dobbe	TU Delft	Onsite
Catholijn	Jonker	TU Delft	Online
Alexey	Kirichenko	F-Secure	Online
Samuel	Marchal	F-Secure	Online
Edgardo	Montes de Oca	Montimage	Online
Ana	Cavalli	Montimage	Online
Wissam	Mallouli	Montimage	Online
Vinh-Hoa	La	Montimage	Online
Manh-Dung	Nguyen	Montimage	Online
Sasa	Klopanvic	Mainflux	Online
Drasko	DRASKOVIC	Mainflux	Online
Nicolas	Kourtellis	Telefónica	Online
Souneil	Park	Telefónica	Online
Nikolay	Tcholtchev	FOKUS	Online
Michell	Boerger	FOKUS	Online
Madhusanka	Liyanage	UCD	Online
Shen	Wang	UCD	Online
Bart	Siniarski	UCD	Online
Thulitha	Senevirathna	UCD	Online
Abeysinghe	Sandeepa	UCD	Online
Huber	Flores	Tartu	Online
Claudio	Soriente	NEC	Online
Jason	Pridmore	EUR	Onsite
Joao	Goncalves	EUR	Onsite
Jorge	Campos	EUR	Onsite
Anouk	Mols	EUR	Onsite
Tessa	Oomen	EUR	Onsite

Jose	Gonzalez	Australo	Online
Miguel	Garcia	Australo	Online
Giulia	Pastor	Australo	Online
Blanca	Aniel-Quiroga	Australo	Online
Iiris	Bisi	Reaktor	Online
Ville	Sinisalo	Reaktor	Online
Jon	Crowcroft	Cambridge (advisory board)	Online
Michael	Zimmer	Marquette (advisory board)	Online

1.2   KICK-OFF MEETING AGENDA

Hybrid Meeting
<u>on-site:</u> Pulse Building Hall-7, TUD campus, Delft, the Netherlands
<u>on-line:</u> Zoom

Morning Sessions

Time	Topic	note
10:00-11:00	Opening	Aaron Ding (TU Delft) Georgios Kaiafas (EC)
11:00-11:15	Coffee Break	
11:15-12:30	Partner introduction*	TU Delft, by Aaron F-Secure, by Alexey Montimage, by Edgardo Mainflux, by Sasa Telefónica, by Nicolas Fraunhofer FOKUS, by Niko UCD, by Madhusanka Tartu, by Huber NEC, by Claudio Erasmus, by Jason Australo, by Jose Reaktor, by Iiris

Afternoon Sessions

Time	Topic	note
14:00-15:15	WP leader session*	EMDESK overview by Cornelis WP7: Aaron WP1: Niko WP2: Shen WP3: Huber WP4: Jason WP5: Souneil WP6: Giulia
15:15-15:30	Coffee Break	
15:30-16:30	Plenary session 1*	EMDESK tutorial Use cases review by Telefonica, Montimage, Fraunhofer FOKUS, and F-Secure
16:30-16:45	Coffee break	
16:45-17:30	Plenary session 2*	1st year deliverables and progress Finance check Ethics advisor Task leaders' discussions

2 MEETING MINUTES AND IMPRESSIONS

2.1 ZOOM RECORDING

Given the hybrid form in which the kick-off meeting was hosted, organizers chose to record the sessions indicated in the program with an asterisk (*). This was performed with consent of all attendees and only intended as full fledge meeting minutes archive.

Morning Sessions:
https://tudelft.zoom.us/rec/share/4wOsAs-X76Yl62sMGdGdHwbyut1n55Vy5An_Y53wgKPnMQ1X-SleCukipIxpHFEu.H4tB3pGv_z1RMCr0

Passcode: upon request to SPATIAL coordinator

Afternoon Sessions:
https://tudelft.zoom.us/rec/share/GEwQlvLU-inZNRDKODa4fBZ16_HZnal512rfXQGx9I1DuSxc5phqTgPnLcS3bMhy.OuEh-GSsK6Ns5kb7

Passcode: upon request to SPATIAL coordinator

2.2 SUMMARY OF SESSIONS

Morning Session 10:00-11:00

The kick-off meeting started with a brief opening talk by the consortium coordinator Aaron Ding and the presentation by Geogios Kaifas as EC Project Officer. The talk by Geogios Kaiafas provided a detailed illustration about the varying regulatory aspects including issues related to financial reporting, administrative management of the project, technical review, potential connection with Security Research Event (SRE), Community of European research and Innovation for Security (CERIS). Important notices are also conveyed transparently such as PO approval requirement for traveling outside Europe, a crisis communications POC. The consortium partners also consulted with Project Officer on practical project arrangement.

Morning Session 11:15-12:30

In the partner introduction session, the PI from each consortium partner presented their organizations (details in Appendix). The presentations and discussions allowed participants to learn about each other's contributions and expectations.

Afternoon Session 14:00-15:15

In the WP leader session, leaders of every work package presented their vision, work planning, and concrete actions for each corresponding tasks (details in Appendix). Through presentations, team members discussed planned synergies between different work packages and made concrete agreements regarding how to contribute to upcoming tasks and deliverables. TU Delft also made a brief introduction on the digital tool EMDESK, which will be used by SPATIAL partners to communicate and monitor the progress.

Afternoon Session 15:30-16:30

In the first Plenary session, representative of EMDESK made a 20-minute presentation to walk through the core functionality of EMDESK. After the EMDESK tutorial, each use case leader, including Telefónica, Montimage, FOKUS and F-Secure, presented their latest planning and arrangement about four SPATIAL use cases. Team members exchanged with use case leaders to clarify the design, vision, and agreed on the general planning.

Afternoon Session 16:45-17:30

In the second Plenary session. The coordinator highlighted the 1st year deliverables, checked with partners on the financial status. All partner institutions confirmed that they have received the initial funding transaction. The coordinator also introduced Prof. Michael Zimmer to the consortium as SPATIAL Ethics Advisor. It's agreed that every use case about the possibility of using human participants shall contact Prof. Zimmer for advice.

The discussions with task leaders also resolved the D1.2 timeline concern. Based on discussions, all partners agreed that there will be internal review one month before the deliverable deadline. Work package leaders will coordinate with task leaders to prepare potential list of internal reviewers, contact internal reviewers and arrange the internal reviewing.

For technical tasks, coordinator discussed with work package and use case leaders to prepare the quality assessment plan (expected in M6), which will be used to assist the task leaders and internal reviewers to guard the quality of technical development.

2.3 ACTION POINTS

At the SPATIAL kick-off meeting, representatives of all partner institutions discussed upcoming challenges and made concrete decisions. First decisions concerning steps forward were made, specifically regarding upcoming deliverables, future meetings and communication and coordination.

Action Point	Who	Notes

Internal Technical Review Arrangement	All	Internal review will take place one month before deliverable deadline. Coordinator and WP leaders will jointly prepare and coordinate internal reviewers for each specific deliverable.
WP meeting arrangement	WP leaders	WP leaders agreed with work package members to start the first WP meeting in October. In the first WP meeting, future meeting frequency and general practice will be agreed upon.
Ethics advisor involvement	Use case leaders	Use case leaders will add necessary lines of description about ethics/human subjects involved in each use case, and consult with ethics advisor
SPATIAL website	All	WP6 leader will coordinate and collect information from all partners to set up the SPATIAL website, ready by the end of October 2021.
SPATIAL mailing list	All	WP7 leader will collect email addresses from all consortium partners to set up work package, management, and general mailing list to facilitate the project communication.

2.4   IMPRESSIONS

Photos taken by the organizers during the SPATIAL kick-off meeting:

FIGURE 1: PULSE BUILDING WHERE KICK-OFF MEETING WAS HOSTED (SOURCE: CVDK TUD)
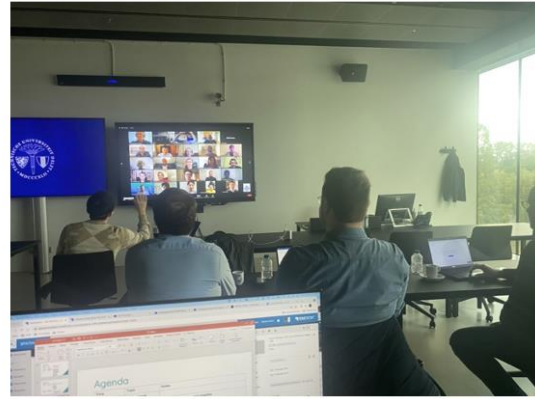
FIGURE 2: GROUP PHOTO OF KICK-OFF MEETING PARTICIPANTS (SOURCE: CVDK TUD)

FIGURE 3: GROUP PHOTO OF KICK-OFF MEETING PARTICIPANTS (SOURCE: CVDK TUD)

FIGURE 4: SOCIAL DINNER OF KICK-OFF MEETING PARTICIPANTS (SOURCE: CVDK TUD)

Online participants partial screenshot (Source: Australo)

2.5 CONCLUSIONS

To conclude, at the kick-off meeting, SPATIAL consortium partners have gained a better understanding of the aims and tasks within the project. Through this hybrid meeting, all participants were able to discuss and reflect on concrete tasks. The upcoming deliverables were clarified. Agreements on actions points were also made and reviewing plan for deliverables were agreed. Consortium partners will share files and drafts of deliverables in EMDESK. Corresponding work package leaders agreed to organize monthly meetings via the video conference tool Zoom, given the pandemic uncertainties. Most importantly, the SPATIAL partners got to know each other, learned about each other's expertise and agreed on how to make this project a success.

3   APPENDIX

3.1   SLIDES: WELCOME AND EC PO

Agenda

Time	Topic	Notes
10:00-11:00	Opening	Aaron Ding (TU Delft) Georgios Kaiafas (EC)
11:00-11:15	Coffee Break	
11:15-12:30	Partner introduction	TU Delft: Aaron Ding F-Secure: Alexey Montimage: Edgardo Mainflux: Sasa Telefonica: Nicolas Fraunhofer FOKUS: Niko UCD: Madhusanka Tartu: Huber NEC: Claudio Erasmus: Jason Australo: Jose Reaktor: Iiris

Agenda

Time	Topic	Notes
14:00-15:15	WP leader session	Cornelis: EMDESK overview, GANTT WP7: Aaron WP1: Niko WP2: Shen WP3: Huber WP4: Jason WP5: Souneil WP6: Giulia
15:15-15:30	Coffee Break	
15:30-16:30	Plenary session 1	EMDESK tutorial - 20 mins Use cases: Telefonica, Montimage, Fraunhofer FOKUS, F-Secure

Agenda

Time	Topic	Notes
16:30-16:45	Coffee break	
16:45-17:30	Plenary session 2	1st year deliverables and progress
		Finance check
		Ethics advisor
		Task leaders discussions

4

SPATIAL

Thank you

MORE INFO

@SPATIAL_H2020

the rest of these 130 slides are available for SPATIAL partners through the secure link:
https://spatial.emdesk.com/#!/documents/direct/d13235

3.2 SLIDES: PARTNER INTRODUCTION

Team TU Delft

- TU Delft
  - Staff: 5421
  - Students: 28,066
  - #1 Engineering in Netherlands

- SPATIAL Project
  - Coordinator: Aaron Ding
  - Duration: 2021-2024
  - SU-DS02-2020: Intelligent security and privacy management
  - Grant No. 101021808
  - Trustworthy AI vision

1
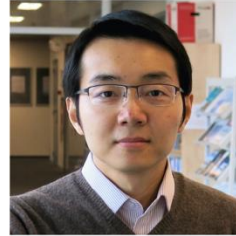
Team TU Delft

- Team
  - Cornelis van de Kamp (Manager)
  - Marijn Janssen
  - Catholijn Jonker
  - Martijn Warnier
  - Roel Dobbe
  - Postdoc + PhDs

- Research Expertise
  - Edge AI
  - Trustworthy AI, XAI
  - IoT Networking and Services
  - ICT Governance
  - Data-driven Control and Decision-making

2

SPATIAL Contributions

		1	2	3	4	5	6
TUD	WP1	Task 1.1	Task 1.2	Task 1.3			
	WP2	Task 2.1	Task 2.2	Task 2.3			
	WP3		Task 3.2	Task 3.3	Task 3.4		Task 3.6
	WP4	Task 4.1		Task 4.3	Task 4.4	Task 4.5	
	WP5	Task 5.1		Task 5.3			
	WP6	Task 6.1	Task 6.2	Task 6.3	Task 6.4		
	WP7	Task 7.1	Task 7.2	Task 7.3	Task 7.4		

3

F-SECURE
INTRO & SPATIAL FOCUS

SPATIAL Kick-off Meeting

Alexey Kirichenko

29/9/2021

F-Secure

1

F-SECURE IN BRIEF

- Founded in 1988, headquartered in Helsinki
- 2020 revenue €220.2M
- ~1700 employees and 29 locations worldwide
- Solutions and services for dynamic attack detection and response, malware protection, vulnerability management, Smart Home protection, Incident Response and digital forensics, red teaming, identity protection, VPN service, ...

We are the largest European single source of cybersecurity services and detection and response solutions for companies, and the leading provider of consumer security software through telecom operators.

GEO Mix

Other, 13%
US, 10%
Europe, 77%

Revenue Mix

Consulting; 21%
Consumer; 45%
Corp Products; 34%
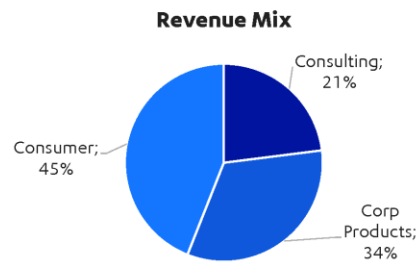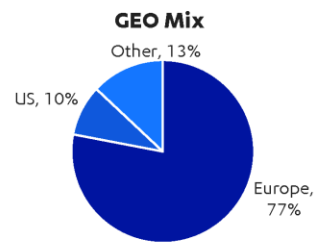
F-SECURE RESEARCH INTERESTS

- Use of machine learning for detecting, investigating and responding to cyber attacks, including advanced ones
- Utilization of machine learning for malicious entities detection
- Security of machine learning and AI-powered systems
- Distributed attack detection approaches
- Support of security personnel with data and machine learning
- Security of Smart Home and IoT devices

SPATIAL FOCUS

- **WP1: T1.1, T1.2 (lead), T1.5**
  Analysis of security requirements for and threats to ML-powered systems
  - Algorithmic attacks in focus
  - Weaknesses in architectures and implementations as parts of the ML system lifecycle
  - Relevant trade-offs

- **WP2: T2.1, T2.2, T2.3**
  Metrics for desirable properties of ML-powered systems, focusing on use cases in the pilot domains

- **WP5: T5.3**
  Pilot on resilient AI in cybersecurity applications

Presentation of montimage in SPATIAL
SPATIAL Kick-Off
29/09/2021

Edgardo Montes de Oca
edgardo.montesdeoca@montimage.com

Brief presentation of Montimage

- **Created in 2004; located in Paris (13ème)**
- **100% independent, research and business oriented SME**
- **Team expert in Cybersecurity and Cyberdefence**
- **Recognized in Europe for its implication in ICT security research:**

  H2020, ANR…, Systematic "Innovation Success Story", EU seal of excellence, CelticPlus/ITEA awards
  Strong collaborations with academia (IMT, UMU, U.of Saclay…)

➢ **Software solutions and tools:**

- **Prevention and detection of cyberthreats (high/low bandwidth, IoT, cloud, 4G/5G):** MMT-Framework, DPI, IDS/IPS, AI/ML, MMT-Cloud
- **Instant creation of 4G/5G networks:** EPC-in-a-Box
- **Cyber Threat Intelligence services**
- **Security audit and red team for enterprises**
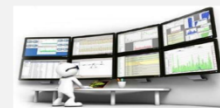
Other collaborative research projects

➢ **5G and beyond security enablers and architecture**
- H2020 INSPIRE-5Gplus (https://www.inspire-5gplus.eu/)
  - Probes, AI/ML, RCA, SSLAs, MTD
- H2020 SANCUS (https://www.sancus-project.eu/)
  - Detection, reaction and attack generation
- ANR MOSAICO (https://www.mosaico-project.org/)
  - Low latency applications, security

➢ **Use case provider of 5G/IoT security monitoring and management**
- H2020 SPATIAL (https://cordis.europa.eu/project/id/101021808)

➢ **Cascading effects in critical regional infrastructures and smart cities**
- H2020 PRECINCT (https://cordis.europa.eu/project/id/101021668)

3

Innovation and advantages

➢**Monitoring framework**
- Real-time protection and prevention based on behaviour analysis of Network, Application and System traces
- Easy to define Security and Service Level Agreements
- Scalability and adaptability in different environments and business activity
- Protocol analysis and DPI/DFI at all OSI levels
- AI for traffic classification and anomaly detection, evasion, encrypted traffic analysis, and Root Cause Analysis

➢**Cyber Threat Intelligence**

Open Source Intelligence · Darknet · Honeypot
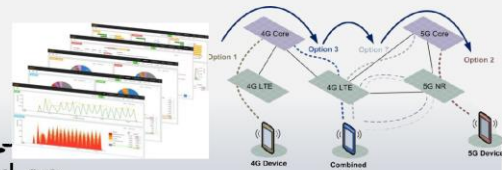
- Wide network of honeypots and darknets for detecting attack campaigns
- Aggregation of OSINT and commercial threat intelligence
- Real-time protection and prevention based on sharing

4

What we expect to achieve

➢ **Improving use, resiliency, explainability and assessment of AI/ML**
   • Use cases:
        Cybersecurity analysis and protection of 5G and IoT networks
        Analysis of encrypted traffic
        Root Cause Analysis
   • Metrics for the assessment of AI/ML
   • Optimization: distributed ML data and processing
   • Testing: cyber range, pentesting, explainable and adversarial AI/ML
   • Increase trust in the use of AI
   • Legal issues involved in: liability analysis, privacy

➢ **Improve the innovation/competitiveness of our security framework**
   • Integrate and fast exploitation of the techniques and algorithms

5

Involvement in WPs

➢ **WP1 (6 PMs) Requirement and threat modelling**
   • Requirements of our use case (F, NF, Perf)
   • Threats to AI
   • Explainable and resilient AI

➢ **WP2 (11 PMs) Requirement and threat modelling**
   • Analyse existing solutions
   • Define metrics

➢ **WP4 (2 PMs) User Engagement, Acceptance and Practice Transitions**
   • Validation of training modules
   • Link with TRUST network dedicated to trust enhancing techniques such as DLT

➢ **WP5 (10 PMs) Deployment and Demonstration**
   • Pilot on Cybersecurity AI analysis in 4G/5G/IoT networks
   • Testbed pilot to deploy, demonstrate and assess the improved techniques

➢ **WP6 (4 PMs) Impact, Outreach and Collaboration**
   • Dissemination activities
   • Exploitation planning
   • Links to other projects

6

SPATIAL project is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

Page 24 of 118

Mainflux Technology Adoption

Participation in projects funded by EU H2020 Research and Innovation program

Horizon 2020 – European Union Funding for Research & Innovation

EU H2020 – EUR 5mil Digital Building Twins

Member of the consortium funded by EU H2020 Research and Innovation program for development of assistants for Safe, and Productive Virtual Construction Design, Operation & Maintenance using a Digital Twin. Mainflux was invited by TU Berlin, other members include Erasmus Universiteit Rotterdam, German and Scandinavian construction structural engineering companies.

Horizon 2020 – European Union Funding for Research & Innovation

EU H2020 – EUR 5mil Trustworthy AI

Member of the consortium funded by EU H2020 Research and Innovation program for development developing resilient accountable metrics, privacy-preserving methods, verification tools and system framework that will serve as critical building blocks to achieve trustworthy AI in security solutions. Member of consortium Includes Fraunhofer, Delft University of Technoogy, Telefonica, NEC, among the others.

Participation in consortiums that competed for EU H2020 funding

Horizon 2020 – European Union Funding for Research & Innovation

Quality Control In Smart Manufacturing EUR 10 mil

Mainflux Labs was invited by Fraunhofer IAPT to participate on 10 million EUR Call which aims to address the challenge of data reliability, the sensors, actuators and instruments used at various levels of integration in the manufacturing process.

Horizon 2020 – European Union Funding for Research & Innovation

Cloud Computing: Towards A Smart Cloud Computing Continuum EUR 4 mill

Invited by Universidad Politecnica de Catalunya, Barcelona, to participate on a 4million EUR H2020 call for comprehensive cloud solutions and testbeds combining for ubiquitous and seamless execution computing environments.

Horizon 2020 – European Union Funding for Research & Innovation

Upgrading Smartness of existing Buildings EUR 5 mil

Mainflux Labs was invited by by TU Berlin to participate on a call which aims improve the smart readiness of buildings to allow for energy savings, more flexible operations, increased usability, and better maintainability.

Researches which used Mainflux IoT Platform

Publications	Authors	Description
Enabling the Orchestration of IoT Slices through Edge and Cloud Microservice Platforms	MDPI sensors / uc3m Universidad Carlos III de Madrid / ERICSSON	This article addresses one of the main challenges related to the practical deployment of Internet of Things (IoT) solutions: the coordinated operation of entities at different infrastructures to support the automated orchestration of end-to-end Internet of Things services. This idea is referred to as "Internet of Things slicing" and is based on the network slicing concept already defined for the Fifth Generation (5G) of mobile network.
A Multi-Site NFV Testbed for Experimentation With SUAV-Based 5G Vertical Services	IEEE Access / uc3m Universidad Carlos III de Madrid / UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH / i2dea networks / University of the Basque Country	The goal of this testbed is to explore synergies among NFV, SUAVs, and vertical services, following a practical approach primarily governed by experimentation. To verify our testbed design, we realized a reference use case where a number of SUAVs, cloud infrastructures, and communication protocols are used to provide a multi-site vertical service..
ETSI - TECHNICAL REPORT SmartM2M; Guidelines for using semantic interoperability in the industry	ETSI TECHNICAL REPORT	The main objective of the present document is to push semantic interoperability in IoT forward in raising awareness about its importance in industry in order to unlock the potential economic value of IoT. A major focus is on thedevelopment of guidelines on how to use semantic interoperability in the industry. 5.2.5 Open source - 5.2.5.1 Mainflux /

Organizations which are using Mainflux IoT Platform

ORGANIZATIONS AND COMPANIES WHICH ARE USING MAINFLUX AS AN OPEN-SOURCE SOLUTION

TARGET – USA
Implementation of Mainflux IoT Platform as Core IoT platform in Smart Retail Store project

XEROX PARC – USA
Predictive maintenance for manufacturing

OSIRIS SYSTEMS FOR INDIAN COAST GUARD - INDIA
Osiris system used Mainflux IoT platform to develop solution for the centralized monitoring and control of vital metrics of geographically spread multitude of data centers

TALOSLOGY – SRI LANKA
Taloslogy uses Mainflux to create IoT based Building Automation System for the mix-used facility in Sri Lanka that cost significantly less than the traditional BAS solutions

TECHOLUTION FOR MAURITIUS TELECOM – USA/INDIA
Techolution uses Mainflux to monitor hard-to-reach BST Towers and replaces expensive manual maintenance to prevent power outages

TOUCH PANEL CONTROL - AUSTRALIA
School Management System for Australian Universities

DIGITAL TWIN TECHNOLOGY- GERMANY
Mainflux is used for health monitoring solution deployed in 40 buildings in Berlin

Mainflux Labs Clients

CLIENTS

MULTINATIONAL COMPANY'S STARTUP - FRANCE
Development of blockchain powered data marketplace.

WORLDWIDE PROVIDER OF OILFIELD & GAS EQUIPMENT - USA
Implementation of Mainflux IoT Platform for gathering operational data from Oil & Gas equipment.

INDEPENDENT SOFTWARE VENDOR - RUSSIA
PoC - Monitoring of operational indicators of underlying IoT specific IT-infrastructure, remote control of the lifecycle of remote devices.

SYSTEM INTEGRATOR - GERMANY
PoC - Connecting pharma manufacturing machines via enterprise network to Mainflux.

SYSTEM INTEGRATOR - INDIA
PoC - IoT Platform connected with provisioning, monitoring & analysis with mongoDB with full UI. First phase: Oil & Gas use case demo kit.

SYSTEM INTEGRATOR - GEORGIA
Customization of IoT platform for NB-IoT devices for smart metering aimed for Eastern Europe Telecom.

LEADER IN RECYCLING AND WASTE MANAGEMENT VENTURES - EU
Mainflux IoT Platfrom deployment as company-wide general IoT platform Development of custom components and knowledge transfer and trainings.

Mainflux Labs Team for SPATIAL

DRASKO DRASKOVIC – Task Manager
MSc degree in Electrical Engineering
› 16 years of professional experience in hardware and embedded-systems development, semiconductor and telecommunication technologies
› 10 years experience in open-source community
› Working experience in NOKIA, PHILIPS, Alcatel-Lucent, Texas-Instruments
› Leadership and Innovation & Technical Contribution awards from Linux Foundation EdgeX Foundry community

IVAN MILOSEVIC – Team Member
MSc degree in Electrical Engineering
› 10 years experience in Serbian largest hosting companies
› Developed control panels integrated with various shared and cloud hosting platforms (cPanel, OnApp, AppLogic, Hyper-V)
› Experienced in Container Orchestration Tools such as Docker, Kubernetes, Helm

SASA KLOPANOVIC - PLEAR – Team Member
MSc degree in Philosophy
› 15 years experience in sales as an entrepreneur
› 10 years experience in marketing, including on the biggest real-estate project in East Europe master-planned by world renowned architects
› Coordinated successful crowdfunding campaign for IoT hardware - WeIO and its commercialization in 40 countries
› Proposal for Grant from the Government of Serbia Innovation Fund
› Digital marketing resulting with global awareness of Mainflux Labs

Mainflux Labs Team for SPATIAL

Team	Role and Tasks in SPATIAL	
DRASKO DRASKOVIC – Task Manager MSc degree in Electrical Engineering	WP 1 Requirement And Threat Modelling	T1.1 - Requirements analysis for AI introduction towards addressing security risks and threats to system architectures
		Task 1.3 - Requirements for explainable and resilient AI deployments and provisioning
		T1.4 - Methodology and tools for continuously updating the requirements and security risks for system architectures
	WP 2 Resilient accountability metrics and embedded algorithmic accountability	Task 2.1 - Analyse existing AI algorithms along with their accountabilities and resilience within the context of applications to IoT, 5G, and cyber security
IVAN MILOSEVIC – Team Member MSc degree in Electrical Engineering	WP 3 System architecture, consistency and accountability for AI, Validation and Testing	Task 3.1 - Distributed mechanisms to detect data biases in AI models
		Task 3.4 - Re-configuration mechanisms for tuning AI systems to be robust in a decentralized environment
		3.5 - Trusted Execution Environment for accountable and resilient AI
SASA KLOPANOVIC - PLEAR – Team Member MSc degree in Philosophy	WP 6 Impact, Outreach and Collaboration	Task 6.1 - Stakeholder Collaboration Framework
		Task 6.2 - Dissemination and Communication Plans
		Task 6.3 - Innovation Management, Exploitation and Sustainability Period
	WP 7 Project Management	Task 7.1 - Implementation of the management structure and data management plan

Our Expectations From SPATIAL

Three Directions

01
- ▸ Systematic investigation and evaluation of authentication, authorization, and accounting services requirements across IoT devices/ecosystems

  with

- ▸ Definition of appropriate system architectures and implementation approaches

02
- ▸ A set of accountable AI algorithm(s) designed specifically for cybersecurity

- ▸ Methods to enable model distillation for pre-trained ML models

- ▸ Certification methods for AI-based products and their security-related operations

03
- ▸ Design mechanisms for trusted executions of AI applications

- ▸ Security standards for AI-based decentralized deployments

- ▸ Set of solutions to aid the deployment of secure AI-based solutions
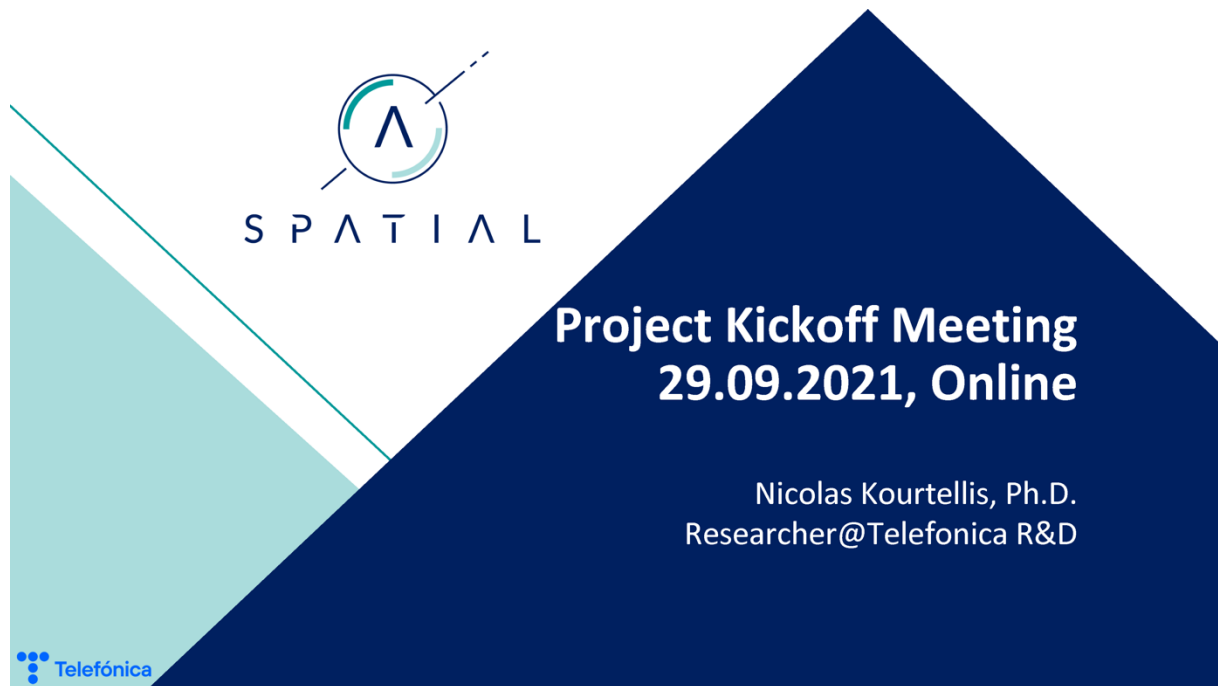
Thank you

MORE INFO
@SPATIAL_H2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

Project Kickoff Meeting
29.09.2021, Online

Nicolas Kourtellis, Ph.D.
Researcher@Telefonica R&D

Telefonica

- One of largest telco operators in the world
- 14 countries
- 300+ million end-user subscribers
- 5.5M+ B2B customers
- Primary focus: Spain, Germany, UK, Brazil
- 120k+ employees
- Headquarters: Madrid, Spain

Telefonica I+D (TID)

- Telefonica Research group created in 2006
- Located in Barcelona, Spain
- 12 PhDs + {PhD students, visiting professors, interns, etc.}
- Publishing to academic venues*
- Patents for IP of TEF
- Participating in EU and national projects
- Internal innovation projects of TEF

*https://www.telefonica.com/en/web/innovation/core-innovation/research

Telefónica

Telefonica I+D (TID)

- Telefonica Research group created in 2006
- Located in Barcelona, Spain
- 12 PhDs + {PhD students, visiting professors, interns, etc.}
- Publishing to academic venues*
- Patents for IP of TEF
- Participating in EU and national projects
- Internal innovation projects of TEF

*https://www.telefonica.com/en/web/innovation/core-innovation/research

Telefónica

Other Research EU Projects

- Concordia: Cyber Security Competence for Research and Innovation
- PimCity: Building the Next Generation Personal Data Platforms
- Accordion: Adaptive Edge-Cloud Compute and Network to support Next-Gen Application
- Charity: Cloud for Holography and Augmented Reality
- Deamon: Network Intelligence for Adaptive and Self-learning Mobile Networks
- NGI: Measuring Multi-Carrier Cellular Access International Roaming Performance

FOKUS @ SPATIAL

- 48 PMs

- Work Package Lead for WP1

- Deliverable Lead for D1.1, D1.3, D2.1, D3.4, (D5.2)

- Task Lead for T1.1, T1.5, T2.1, T3.6, T6.4

- Lead for MS4

- Use case 3: *EMYNOS - Accountable AI in Emergency eCall System*

11 29.09.21 | SPATIAL Kickoff

Fraunhofer
FOKUS

Thank you for your attention!
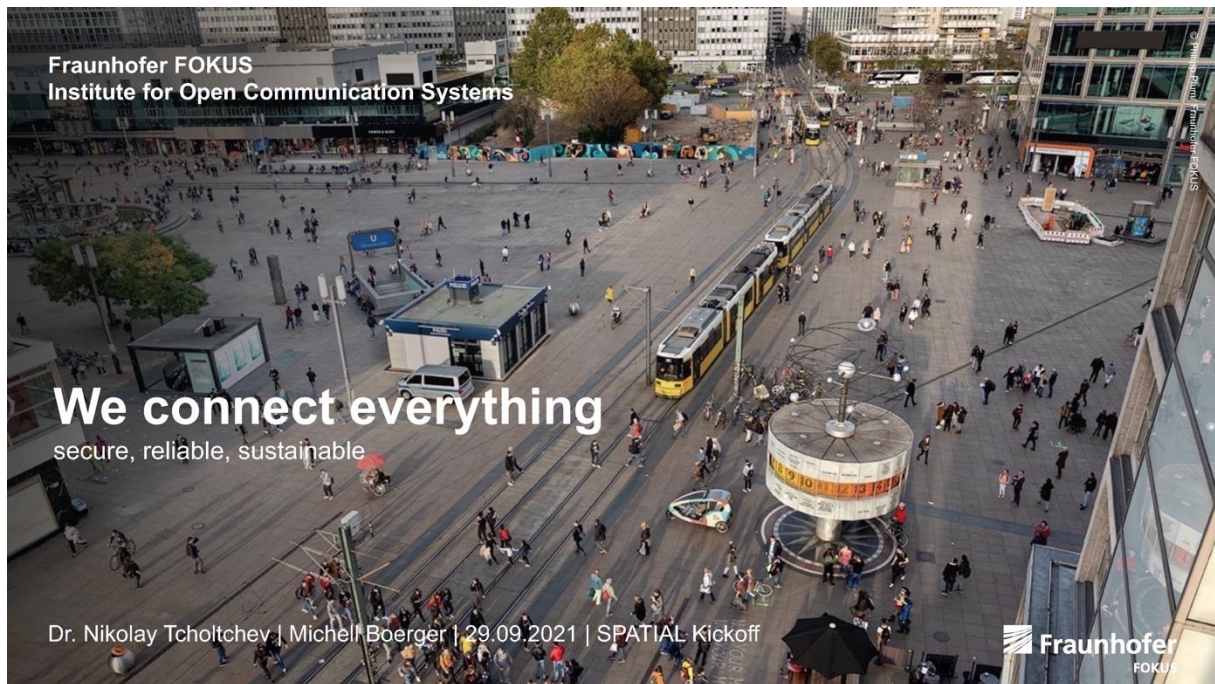
Fraunhofer FOKUS
Institute for Open Communication Systems

Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
www.fokus.fraunhofer.de

Dr.-Ing. Nikolay Tcholtchev

Senior Researcher
nikolay.tcholtchev@fokus.fraunhofer.de
+49 (30) 34 63 - 7175

Michell Boerger

Researcher
michell.boerger@fokus.fraunhofer.de
+49 (30) 34 63 - 7452

Fraunhofer
FOKUS

UCD School of Computer Science
www.ucd.ie/cs

UCD School of Computer Science
www.ucd.ie/cs/

- The largest computer science department in Ireland.
- Offer a 4-year BSc Honours degree in Computer Science, a range of Masters degrees for both computer science graduates and conversion students, plus a suite of 4-year Structured PhD programs.
- Leading and hosting various Research Centers
  - Insight - Centre for Data Analytics
  - UCD CCI - Centre for Cybersecurity & Cybercrime Investigation
  - CeADAR: National Centre for Applied AI
  - CONSUS
  - ML Labs: SFI Centre for Research Training in Machine Learning

University College Dublin
Ireland's Global University

SPATIAL project is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

Page 42 of 118

SPATIAL Project Collaborations
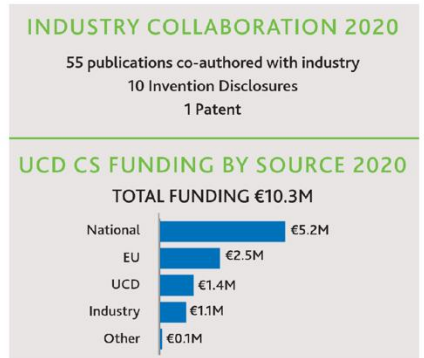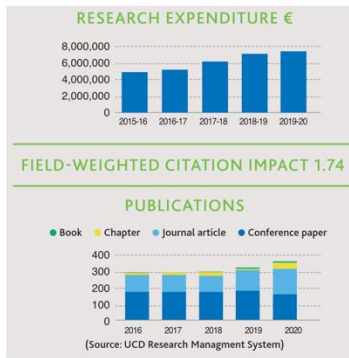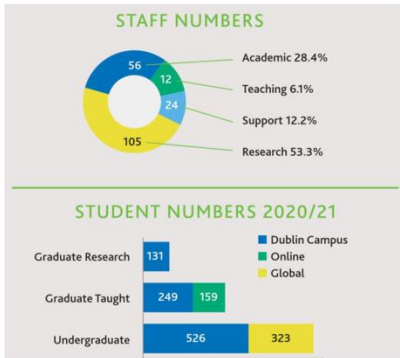
- CONNECT: Science Foundation Ireland Research Centre for Future Networks and Communications
https://connectcentre.ie/
- CeADAR: National Centre for Applied AI
https://www.ceadar.ie/
- ML-Labs: SFI Centre for Research Training in Machine Learning
https://www.ml-labs.ie/

UT team for SPATIAL

Distributed and Pervasive Systems Group

https://dps.cs.ut.ee

Huber Flores

ASSOCIATE PROFESSOR

Tartu, Estonia, Kick-off meeting, 29/09/2021   1

About us

Delta Centre (Tartu, Estonia)
Distributed and Pervasive Systems Group

https://dps.cs.ut.ee
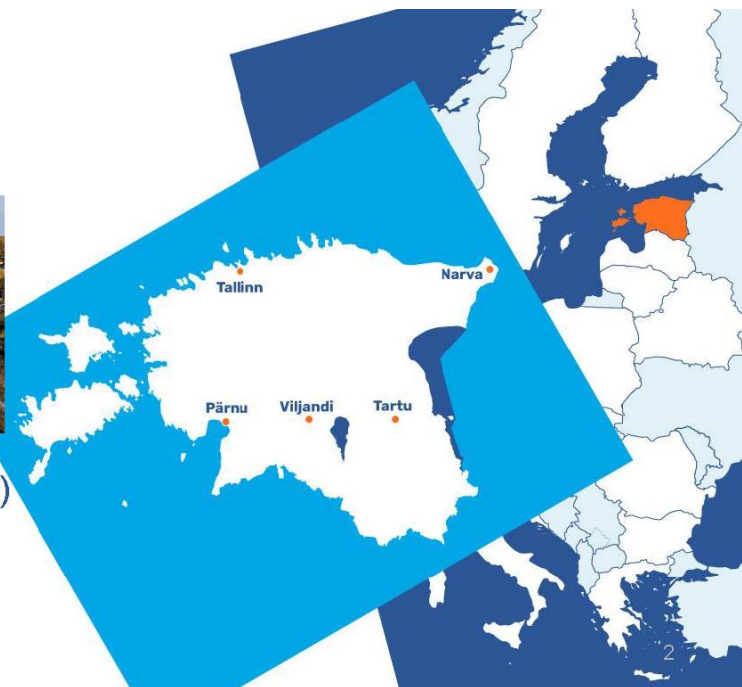
UT team

Research staff:

- PhD candidate, Abdul-Raheed Ottun
- PhD candidate, Souvik Paul
- PhD candidate, Farooq Dar
- PhD candidate, Zhigang Yin
- Lecturer, Mohan Liyanage, PhD
- Associate Professor, Huber Flores, PhD

3

UT team: SPATIAL development

Research staff:

- **Upcoming postdoc**
- **PhD candidate, Abdul-Raheed Ottun**

- PhD candidate, Souvik Paul
- PhD candidate, Farooq Dar
- PhD candidate, Zhigang Yin
- Lecturer, Mohan Liyanage, PhD

- **Associate Professor, Huber Flores, PhD**

4

Our research

Distributed Systems

Drones
Sensors
Smart devices
Networks (5G, LTE, Wireless)
Data science
Wearables
IoT

Mobile and Pervasive computing

Our expertise
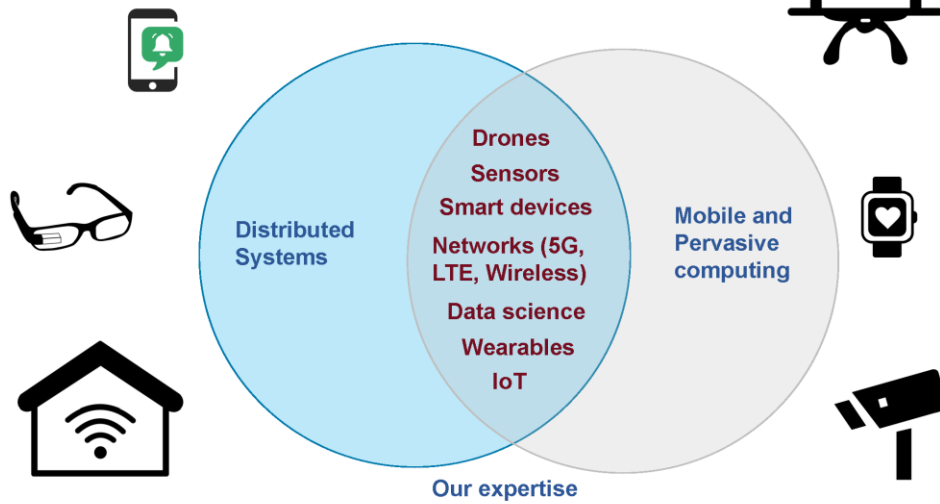
5

Our research

[IEEE-Pervasive] *Lagerspetz, E., Hamberg, J., Li, X., Flores, H., Nurmi, P., Davies, N., & Helal, S. (2019).* **Pervasive data science on the edge.** *IEEE Pervasive Computing, 18(3), 40-49.*

[IEEE-IoT] *Flores, H., Motlagh, N. H., Zuniga, A., Liyanage, M., Passananti, M., Tarkoma, S., ... & Nurmi, P. (2021).* **Toward large-scale autonomous marine pollution monitoring.** *IEEE Internet of Things Magazine, 4(1), 40-45.*
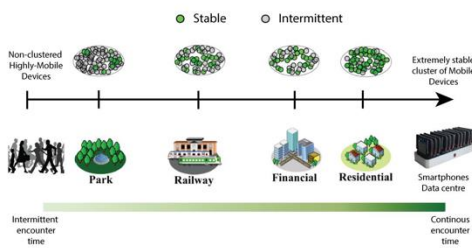
[IEEE-PeCom] *Flores, H., Zuniga, A., Faghihi, F., Li, X., Hemminki, S., Tarkoma, S., ... & Nurmi, P., March).* **Cosine: Collaborator selector for cooperative multi-device sensing and computing.** *In IEEE PerCom 2020.*

[IEEE-Computer] *Flores, H., Zuniga, A., Faghihi, F., Tonetto, L., Braud, T., & Nurmi, P., March).* **Collaboration Stability: Quantifying the Success and Failure of Opportunistic Collaboration,** *IEEE Computer.*

[IEEE-TMC] *Flores, H., Hui, P., Nurmi, P., Lagerspetz, E., Tarkoma, S., Manner, J., ... & Su, X. (2017).* **Evidence-aware mobile computational offloading.** *IEEE Transactions on Mobile Computing, 17(8), 1834-1850.*
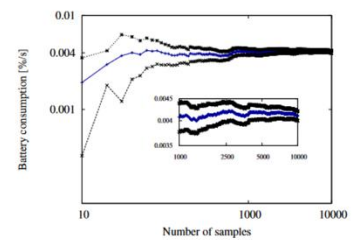
Our research (SPATIAL)

Key areas to build on further.

- Federated learning
- Distributed machine learning
- Collaborative processing
- Performance-based modelling
  - (expertise obtained from previous FP7)

Leading WP3, we will also have active participation in other WPs

7

UNIVERSITY OF TARTU
Institute of Computer Science

Thank you!

huber.flores@ut.ee
http://huberflores.com

unitartu

tartuuniversity

NEC Laboratories Europe GmbH

◆ Advanced research addressing societal needs, technology and business trends in Europe and world-wide

◆ Collaboration with academic and industrial research groups, public institutions

◆ Research areas:
  ■ Data Science
  ■ Security
  ■ 5G Networks
  ■ System Platforms for IoT and AI

◆ Located in Heidelberg since 1997

◆ https://www.neclab.eu/

People Involved

◆ Samira Briongos
- ■ Research Scientist
- ■ At NLE since 2020
- ■ Trusted Execution Environments, Anomaly detection, Side channels

◆ Claudio Soriente
- ■ Principal Researcher
- ■ At NLE since 2017
- ■ Applied crypto, Trusted Execution Environments

\Orchestrating a brighter world NEC

WP Involvement

◆ WP1 (4PM)
◆ WP2 (1PM)
◆ WP3 (36PM)
- ■ **Task 3.5** Trusted Execution Environment for accountable and resilient AI (M13-M28)
  - • With UT, MFX
  - • M13-M28
  - • Trusted Execution Environments, Multiparty-computation, Data privacy, Remote attestation, Scalability
- ■ **D3.3** [M25] Automated diagnosis and mechanisms for tuning AI-based systems and Trusted Execution Environments for accountable and resilient AI (UCD and NEC)
◆ WP6 (5PM)
◆ WP7 (1PM)

\Orchestrating a brighter world NEC

SPATIAL

Erasmus School of History, Culture and Communication

EUR SPATIAL Focus and Team

Department of Media and Communication

Erasmus University Rotterdam

EUR focus areas

- Technology development in context
  - o Practice based approach
  - o Technology Studies, Human-Computer Interaction (HCI), Computer supported cooperative work (CSCW)
- Social research on ICTs related to:
  - o Privacy
  - o AI and Ethics/Social Impact
  - o Security
  - o Digitalisation
  - o Surveillance
- EUR SPATIAL Work
  - o Leading WP4

Current EU projects

SPATIAL Team EUR

Jason Pridmore

Anouk Mols

João Gonçalves

Tessa Oomen

Jorge Campos

SPATIAL

MARKETING THE FUTURE

Jose Gonzalez
CEO and Founder | jose@australo.org

SCIENCE.
INNOVATION.
THRIVE.

R

Reaktor Education
Revolutionising online learning for society

Iiris Bisi
iiris.bisi@reaktor.com
tel. +358 44 058 8538

Ville Sinisalo
ville.sinisalo@reaktor.com
tel. +358 40 7622019

Design and technology

Reaktor

Reaktor Education is part of Reaktor, a hybrid consulting company combining world class expertise on **Design, UX and technology.**

#2 of most innovative companies in education (Fast company)

550 consultants and staff on **3 continents**.

See more at: www.reaktor.com

Mission

In Reaktor Education we partner with world-class organisations and education providers to develop online courses designed to empower people to participate in our rapidly-evolving society.

Reaktor Education

MOOCs for Modern Life

SPATIAL project is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

Page 59 of 118

Rethink Education

We don't compete with online courses, we compete with Netflix and Facebook.

Reaktor Education

Rethink Education
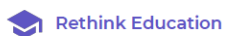
Understand WHY people learn.

What are their feelings on the subject you are about to teach?

Is it boring? Is it too confusing or elitist or overwhelming to know where to start? Is the current way of discussing the topic gender biased? Is there a fear about the effect your subject might have on the student's future, on society?

Why do they care?

Do they want to be like someone they know who has a job requiring these skills? Do they want to earn more money? Do they want to be able to work remotely? Do they want to seem aware and up-to-date at their next meeting/ dinner party /job interview?

Reaktor Education

Design with the user in the center

Have a clear target group. For Elements of AI it was a female highschool student.

Design for engagement. People could watch Netflix or use Facebook instead.
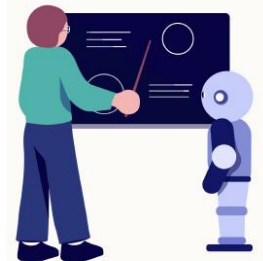
Agile ways of working

True innovation seldom happens in a strictly structured environment.

Ways of working should be agile and the product should be tested with real users as often as possible.

Multidisciplinary team

Nothing happens by just putting together same type of thinking.

Best content happens when it is well planned, budgeted and executed professionally.

Reaktor Education

• Elements of AI

Elements of AI ranked as the #1 Computer Science online course in the world, ahead of Stanford, Harvard, and MIT.

Class Central 2021
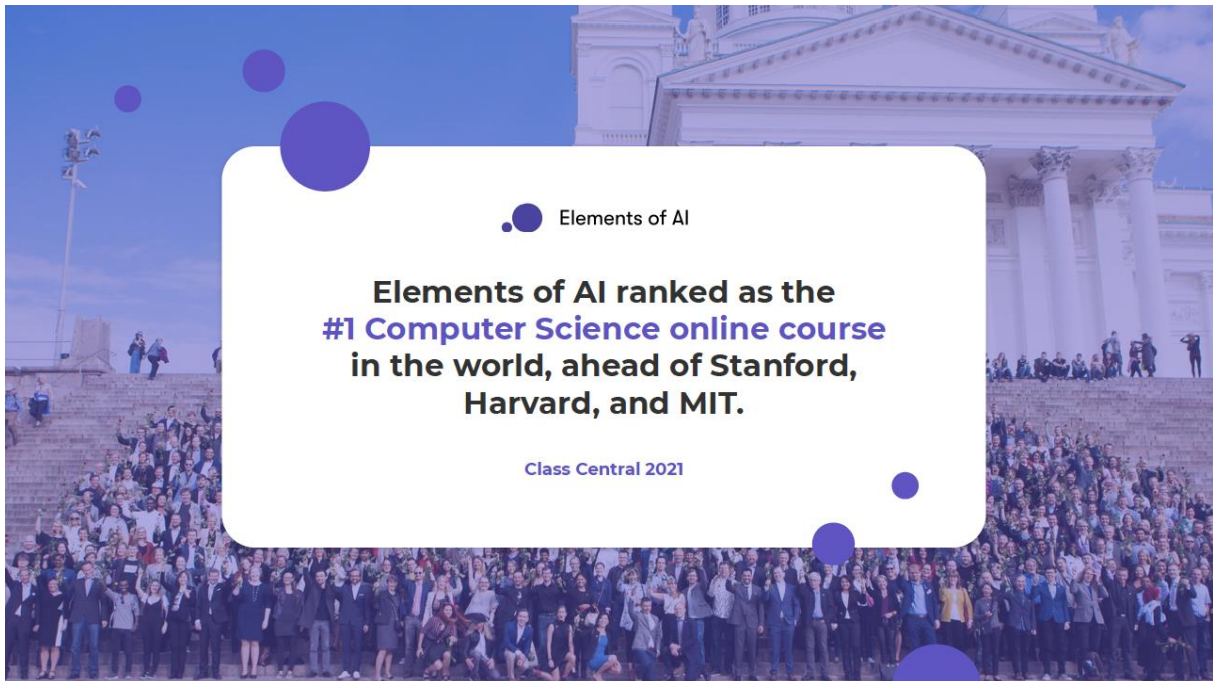
SPATIAL

We will lead the Task 4.5 Educational module development and implementation (M12-M36).

Following the baseline content work by the technical universities (TUD, UCD, UT), we will **design and develop**, in collaboration with EUR, the educational module to disseminate the Spatial findings and **educate future professionals** based on the knowledge gathered.

The course development will **leverage the existing technical solutions** provided by Reaktor Education platform and the **experience gained** from co-creating Elements of AI.

Reaktor Education

The people behind the courses

Iiris Bisi
Project director

Ville Sinisalo
Contracts / Legal

Concept designer

Designer

Copywriter

Developer

Reaktor Education

R

Thank you!
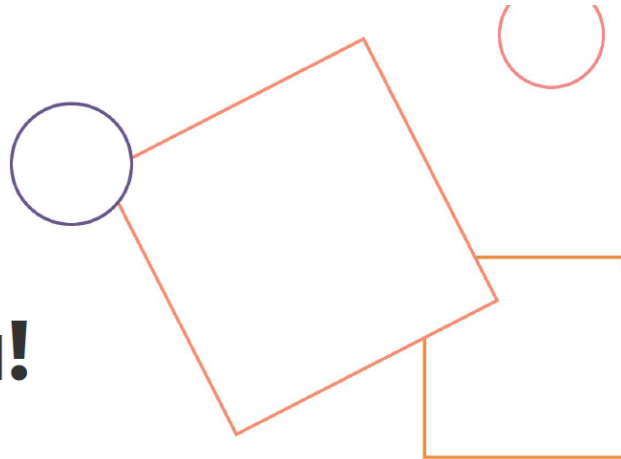
Iiris Bisi
iiris.bisi@reaktor.com
tel. +358 44 058 8538

Ville Sinisalo
ville.sinisalo@reaktor.com
tel. +358 40 7622019

3.3   SLIDES: WP REVIEW

Management Overview

Aaron Ding: SPATIAL coordinator & technical director

Cornelis van de Kamp: project manager
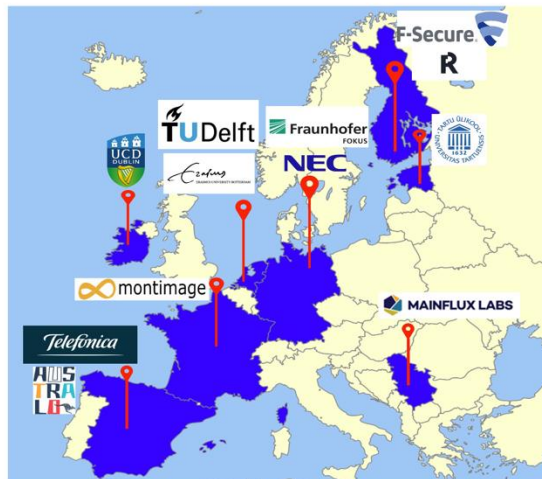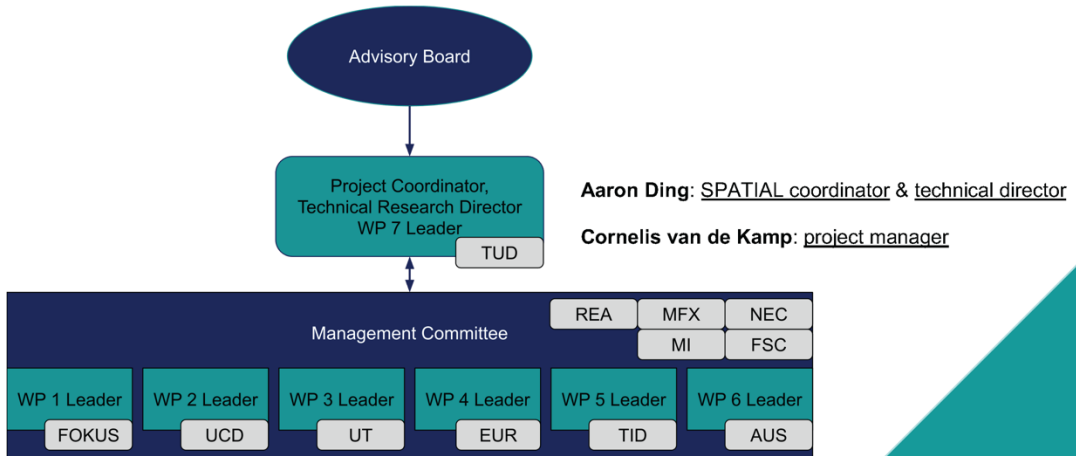
Advisory Board

Advisory Board Member	Position	Institution	Country
Eve Schooler	Director and Principal Engineer, Emerging IoT Networks	Intel Corporation	USA
Jon Crowcroft	Marconi Professor of Communications Systems	University of Cambridge	UK
Henning Schulzrinne	Julian Clarence Levi Professor of Computer Science	Columbia University	USA
Stefan Schmid	Professor of Faculty of Computer Science	University of Vienna	Austria
Ilias Leontiadis	Senior Researcher of AI Systems	Samsung AI Center	UK
Michael Zimmer (SPATIAL Ethics Advisor)	Associate Professor, Department of Computer Science	Marquette University	USA

WP Overview
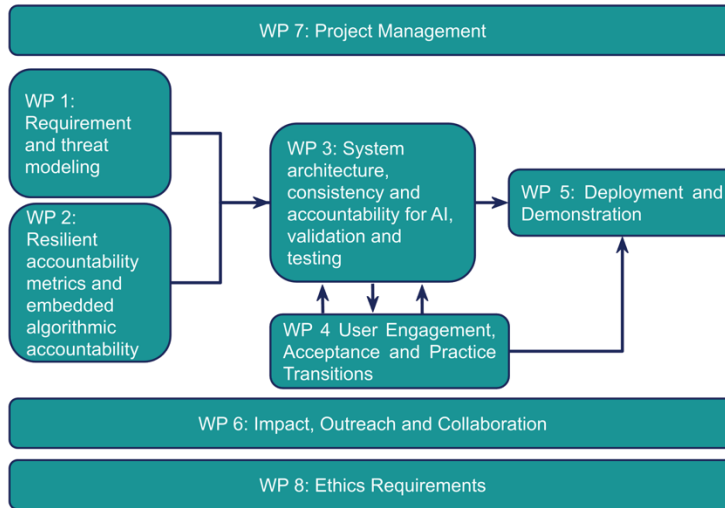
Important Events

Month	WPs involved	Meeting	Partners involved	Location	
1	7	Kick-off meeting	All consortium partners	Delft, NL	
9	2 ,3	Analysis and framing workshop*	All consortium partners, advisory board	Berlin, DE	
17	3, 4, 5	Pre-deployment workshop	All consortium partners	Barcelona, ES	
25	4, 5	Specifications, methodology and tools *	All consortium partners, advisory board	Dublin, IE	Technical Review
31	5, 6	Internal demonstrations and education module development	All consortium partners	Tartu, EE	
36	6, 7	Final Conference*	All consortium partners, advisory board	TBD**	

Good to Know

- EMDESK is our management platform
  - Task coordinating, communications, Deliverable co-editing

- Grant Agreement & CA are the 'absolute' reference

- WP leader is a key person
  - Coordinate with task leaders and participating partners
  - Synchronize with SPATIAL coordinator

Management Committee			REA	MFX	NEC
				MI	FSC

WP 1 Leader	WP 2 Leader	WP 3 Leader	WP 4 Leader	WP 5 Leader	WP 6 Leader
FOKUS	UCD	UT	EUR	TID	AUS
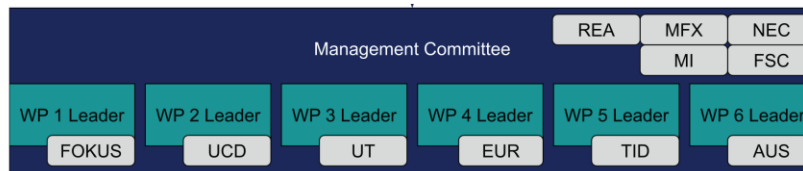
6

WP Leader

6.5 Work Package Leaders

Consortium Agreement Definition

The Work Package Leaders are responsible for the implementation and coordination of the work packages and tasks, primarily the timely completion of the associated deliverables. Work Package leadership includes the following responsibilities:

- Planning and organising the activities of the work plan as outlined for each Work Package (WP);
- Monitoring the completion of deliverables and milestones associated to their WP, within budget and allocated time frame;
- Progress reporting to the project coordinator and research director, timely submission of deliverable reports according to the templates incorporated in the Quality Assurance Plan;
- Interacting with consortium partners, including proactive information exchange among WPs;
- Solving issues in case of difference of opinions within a WP or between WPs. If needed, WP leaders should involve the Coordinator.

7

Visibility & Publications

- Acknowledgement in Open Access publications
  - The authors gratefully acknowledge the funding from European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 101021808

- Keep track of publications for your team

8

Keep Pace

	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8	Total Person/Months per Participant
1 - TU Delft	3	5	26	4	4	7	27	✓	76
2 - FSC	14	15	0	0	6	2	1		38
3 - MI	6	11	0	2	10	4	1		34
4 - MAINFLUX LABS	7	4	19	0	0	9	1		40
5 - TID	7	10	15	0	10	4	1		47
6 - Fraunhofer	16	7	14	4	4	2	1		48
7 - NUID UCD	12	16	16	2	7	2	1		56
8 - Tartu	3	3	41	2	8	0	1		58
9 - NEC	4	1	36	0	0	5	1		47
10 - EUR	2	0	1	32	0	3	1		39
11 - AUS	2	0	0	3	0	32	1		38
12 - Reaktor	0	0	0	10	0	0	1		11
Total Person/Months	76	72	168	59	49	70	38		532

9

Thank you

MORE INFO
@SPATIAL_H2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

- https://spatial.emdesk.com/#!/documents/direct/f4434

Work Package 1

Requirement and threat modelling

Dr.-Ing. Nikolay Tcholtchev | Michell Boerger | 29.09.2021 | SPATIAL Kickoff

Work Package 1

*REQUIREMENT AND THREAT MODELLING
(M01–M30, 76 PMS, LEAD: FOKUS)*

- Aims to capture the requirements and general design principles for modern system architectures based on AI
- Goal is to:
  - design and apply algorithms in an explainable manner
  - support the accountability of the overall AI based system
- Work package 1 defines:
  - 5 tasks
  - 4 deliverables

Partners

Partner	Acronym	PMs
Fraunhofer FOKUS *(LEAD)*	FOKUS	16
F-Secure OYJ	FSC	14
University College Dublin	UCD	12
Mainflux Labs	MFX	7
Telefonica	TID	7
Montimage	MI	6
NEC Laboratories	NEC	4
TU Delft	TUD	3
Tartu Ulikool	UT	3
ERASMUS Universiteit Rotterdam	EUR	2
Australo Interinnov Marketing Lab	AUS	2

Tasks

		Lead	Scheduled	Deliverables
T1.1	Requirements analysis for AI introduction towards addressing security risks and threats to system architectures	FOKUS	M01 - M30	D1.1 - D.1.4
T1.2	Analysis of potential threats to AI-based systems	FSC	M04 - M15	D1.2
T1.3	Requirements for explainable and resilient AI deployments and provisioning	UCD	M11 - M28	D1.4
T1.4	Methodology and tools for continuously updating the requirements and security risks for system architectures	UT	M10 - M24	X
T1.5	Non-functional aspects: scalability, usability, performance implications and hardware implications	FOKUS	M06 - M24	D1.1, D1.3, D.1.4

Task 1.1

REQUIREMENTS ANALYSIS FOR AI INTRODUCTION TOWARDS ADDRESSING SECURITY RISKS AND THREATS TO SYSTEM ARCHITECTURES.
(M01–M30, LEAD: FOKUS)

- Capture and continuously refine requirements for AI towards addressing security risks and threats to system architectures, originating from...
  - different use cases and industrial experiences of involved partners
  - desktop research, literature review, survey methods, etc.
- Comprehensive catalogue of aspects to be considered, when integrating and utilizing AI algorithms and frameworks for addressing security risks and threats for system (and network) architectures
- Contributes to Deliverable D1.1, D1.2, D1.3, D.1.4 and influences WP2 and WP3

Task 1.2

ANALYSIS OF POTENTIAL THREATS TO AI–BASED SYSTEMS
(M04–M15, LEAD: FSC)

- Identify potential threats which are specific to AI based systems
- Focus on attacks, which aim to manipulate or make AI algorithms, their implementations, or ways of their utilisation functioning incorrectly or even leading to security breaches or overall system unavailability
  - *Quality of training data (poisoning attacks)*
  - *Malicious inputs (evasion and model stealing attacks)*
  - *Privacy and confidentiality of data (inference attacks and data leakage)*
  - *DoS attacks on the AI infrastructure*
- Attack vector analysis for decentralized environments to tackle multiple stakeholders in AI-based operations
- Contributes to D1.2 and influences WP3

Task 1.3

REQUIREMENTS FOR EXPLAINABLE AND RESILIENT AI DEPLOYMENTS AND PROVISIONING
(M11–M28, LEAD: UCD)

- Defining the requirements for the deployments and architectures of the proposed accountability supporting AI type of systems
    - Security risks and threats requirements from Task 1.1
    - Threat analysis from Task 1.2
- SPATIAL AI architecture and deployment concept will be addressing the intrinsic accountability requirements for security and privacy by extending the concepts for existing AI systems.
    - Deep examination of existing infrastructures and an extensive study of present accountability supporting AI technologies
- Addresses the compromising of computational resources and packet switching resources in an infrastructure running an AI system
- Contributes to D1.4 and relevant for WP2, WP3, WP5

Task 1.4

METHODOLOGY AND TOOLS FOR CONTINUOUSLY UPDATING THE REQUIREMENTS AND SECURITY RISKS FOR SYSTEM ARCHITECTURES
(M10–M24, LEAD: UT)

- Identifying a set of tools (i.e. toolchain) and establishing the verification process to be used to capture the different functional and non-functional requirements from the experimental and use cases applications
    - Used to verify the continuous tuning of requirements
- Evaluate, identify, and put in place existing tools for supporting the activities of the other WP1 tasks
- Tools should be:
    - Cloud based
    - Utilize open interfaces
    - Easily and non-discriminatory accessible
    - Preferably Open Source

Task 1.5

NON-FUNCTIONAL ASPECTS: SCALABILITY, USABILITY, PERFORMANCE
IMPLICATIONS AND HARDWARE IMPLICATIONS
(M06-M24, LEAD: FOKUS)

- Investigate and capture a catalogue of non-functional requirements for accountability supporting AI systems
  - Performance and implications on the hardware architectures
  - Usability
  - (theoretical) scalability
  - Security by design
- Envisioned AI algorithms and architectures should be
  - Explainable
  - Privacy preserving
  - Ethical
- Contributes to D1.1, D1.3, D1.4 and influences WP2 and WP3

Deliverables

			Lead	Due
WP1	D1.1	Requirements Analysis for AI towards Addressing Security Risks and Threats to System and Network Architectures	FOKUS	M08
	D1.2	Security Threats modeling for AI based System Architectures	FSC	M10
	D1.3	Final Requirements Analysis for AI towards Addressing Security Risks and Threats to System and Network Architectures	FOKUS	M24
	D1.4	Design Principles for Accountable and Resilient AI Architectures	UCD	M28

Resulting Time Schedule

D1.1: Requirements Analysis for AI towards Addressing Security Risks and Threats to System and Network Architectures

D1.2: Security Threats modeling for AI based System Architectures

D1.3: Final Requirements Analysis for AI towards Addressing Security Risks and Threats to System and Network Architectures

D1.4: Design Principles for Accountable and Resilient AI Architectures

	Year	Year 1												Year 2												Year 3											
	Month	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
WP1 Requirement and threat modeling	Overall												MS4												MS6												
	T1.1								D1.1																D1.4												
	T1.2										D1.2																										
	T1.3																												D1.3								
	T1.4																																				
	T1.5																																				

SPATIAL

Thank you

Dr.-Ing. Nikolay Tcholtchev
Senior Researcher
nikolay.tcholtchev@fokus.fraunhofer.de
+49 (30) 34 63 - 7175

Michell Boerger
Researcher
michell.boerger@fokus.fraunhofer.de
+49 (30) 34 63 - 7452

WORK PACKAGE 2
(DR SHEN WANG, UCD)

Resilient accountability metrics and embedded algorithmic accountability

Outline

01 **Objectives**

02 **Outcomes**

03 **Tasks**

04 **Deliverables**

OBJECTIVES

- O2.1: To analyse existing AI algorithms accountability in the applications of IoT, 5G, and cybersecurity

- O2.2: To define parameters for constructing accountability and resilience metrics

- O2.3: To propose a process to integrate accountability with existing AI algorithms

OUTCOMES

- Provide a concrete framework to properly interpret the term AI accountability/explainability in both qualitative and quantitative perspectives.

- Concretely, the outcome of this WP will be reported in **3 deliverables** and contribute to SPATIAL's 2 milestones: **MS5 [M16]** and **MS7 [M24].**
    - MS5: Proposed metrics are accountable and resilient (TID, D2.2)
    - MS7: Proposed process enables resilience and accountability features of existing AI systems (UCD, D2.3)

TASK 2.1 (FOKUS, M1–M10)

- Analyse existing AI algorithms along with their accountabilities and resilience within the context of applications to IoT, 5G, and cyber security

- Contributors: FSC, UCD, TUD, MFX, MI

- **Deliverable 2.1 [M10, June 2022]** Existing AI Algorithms and their Accountability and Resilience Features within the Context of Applications to IoT, 5G, and Cyber Security (**FOKUS**)

TASK 2.2 (TID, M8–M16)

- Define parameters and elements to construct accountability, resilience and privacy metrics

- Contributors: NEC, FSC, UT, MI, TUD

- **Deliverable 2.2 [M16, Dec 2022]** Robust Accountability Metrics for AI Algorithms (**TID**)

TASK 2.3 (UCD, M13-M24)

- Propose a process with assessing metrics into existing AI algorithms for addressing accountability and enhancing resilience

- Contributors: FOKUS, FSC, UT, TID, MI, TUD

- **Deliverable 2.3 [M24, Aug 2023]** Process to Integrate Accountability and Resilience Features into AI Algorithms (**UCD**)

PERSON MONTHS DISTRIBUTION

Partner	TUD	FSC	MI	MFX	TID	FOKUS	UCD	UT	NEC	EUR	AUS	REA
Person months	5	15	11	4	10	7	**16**	3	1	0	0	0

SPATIAL project is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

Page 80 of 118

Objectives [WP starts in M10]

- O3.1 Investigate the different data trade-offs and data biases that influence the training process and execution behavior of AI models

- O3.2 Develop the fundamental principles for accounting AI-based system architectures

- O3.3 Create the explanatory mapping between technical knowledge and users interfaces to explain AI systems to any type of users

- O3.4 Develop actionable feedback to improve trust, usability and transparency in AI-based systems

- O3.5 Develop mechanism to leverage Trusted Execution Environments for making AI accountable

- O3.6 Build, test and deploy that can explain the behavior of AI using accountable metrics.

Outcomes

- Controlled evaluation of proposed solutions in rigorous testbeds located in different partners (FOKUS, UT, Delft), and guidelines and lesson learned for designing pilots in real testbeds (Telefonica, FOKUS)

- Four (4) deliverables are the outcome of this WP, and those contribute to SPATIAL's milestones MS10[M25] and MS11 [M28]
    - D3.1 -> Task 3.1 and Task 3.2
    - D3.2 -> Task 3.3 and Task 3.4
    - D3.3 -> Task 3.5
    - D3.4 -> Task 3.6

    - MS10: Explanatory platform can be used to explain basic functionalities of AI-based applications
    - MS11: Final release of algorithmic metrics and methods

Task 3.1 (UT, M10-M18)

- Develop the distributed mechanisms to detect data biases in AI models

- Contributors: TID, MFX, FOKUS

- Deliverable 3.1 [M18]: This task contributes to the deliverable – Detection mechanism to identify data biases and exploratory studies about different data quality trade-offs for AI-based systems (UT)

Task 3.2 (UT, M12-M25)

- Federated learning for distribution of accountable and resilient AI

- Contributors: TID, FOKUS, TUD

- Deliverable 3.1 [M18]: This task contributes to the deliverable – Detection mechanism to identify data biases and exploratory studies about different data quality trade-offs for AI-based systems (UT)

Task 3.3 (TUD, M12-M27)

- Explanatory AI platform

- Contributors: FOKUS, UCD, UT

- Deliverable 3.2 [M22]: This task contributes to the deliverable – An explainatory platform that accounts AI systems based on its quantified quality (TUD)

Task 3.4 (UCD, M14-M27)

- Re-configuration mechanisms for tuning AI systems to be robust in a decentralized enviroment

- Contributors: MFX, TUD, FOKUS

- Deliverable 3.2 [M22]: This task contributes to the deliverable – An explainatory platform that accounts AI systems based on its quantified quality (TUD)

Task 3.5 (NEC, M13-M28)

- Trusted execution environments for accountable and relisient AI

- Contributors: UT, MFX

- Deliverable 3.3 [M25]: This task contributes to the deliverable – Automated diagnosis and mechanisms for tuning AI-based systems and trusted execution enviroments for accountable and reslieint AI (UCD and NEC)

Task 3.6 (FOKUS, M13-M28)

- Evaluation and testing in controlled testbeds

- Contributors: TID, UCD, NEC, UT, TUD

- Deliverable 3.4 [M28]: This task contributes to the deliverable – Performance evaluation in controlled enviroments and guidelines touild the pilot studies in real testeds (FOKUS)
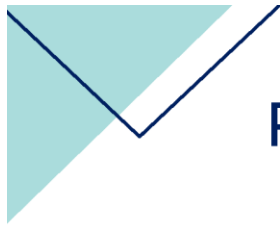
Person months distribution

Partner	TUD	FSC	MI	MFX	TID	FOKUS	UCD	UT	NEC	EUR	AUS	REA
Person months	26	0	0	19	15	14	16	41	36	1	0	0
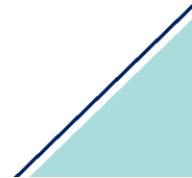
SPATIAL

Thank you

MORE INFO

huber.flores@ut.ee

http://spatial-h2020.eu
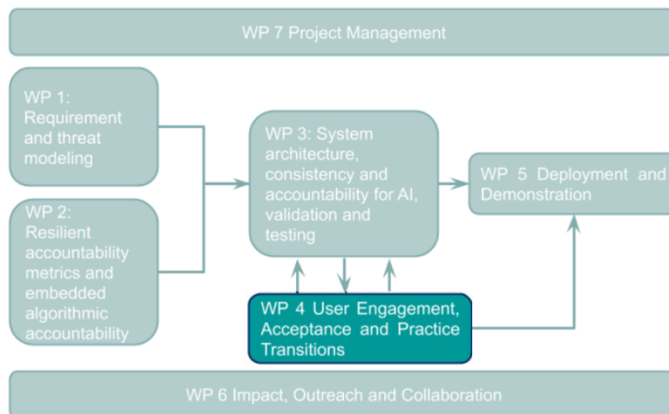
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

User Engagement, Acceptance and Practice transitions

Work Package 4

Work Package 4

Table of contents

WP4 Role and relevance

- Understanding situational contexts for development and deployment of SPATIAL tools

- Evaluating social, legal and technical limitations, including gender and diversity considerations

- Changing practices in relation to accountability of AI

- Educating current and future AI designers and engineers

WP4 Objectives

O4.1
Develop a framework for a full sociotechnical analysis of SPATIAL tool development

O4.2
Engage in an embedded social science analysis of developing technical processes and practices from a sociotechnical perspective

O4.3
Determine the limitations and concerns of SPATIAL tool development in relation to social, legal and ethical concerns in order to provide validation feedback for full deployment and demonstration
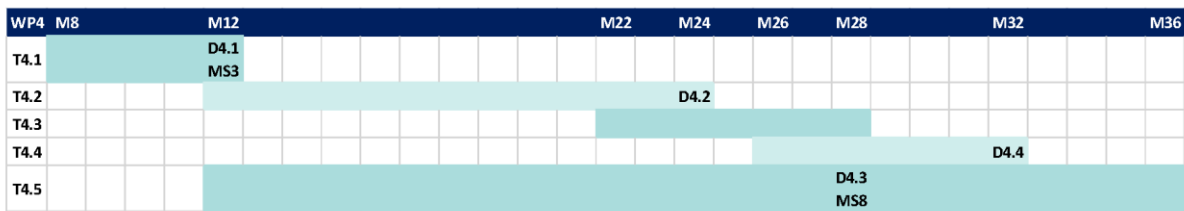
O4.4
Develop and deploy education modules to transition current AI practices in line with increasing accountability within AI

WP4 Overview and timeline

■ M8: April 2022	■ M36: August 2024	■ 5 tasks, 4 deliverables 2
Start	End	Milestones

WP4	M8		M12								M22	M24	M26	M28			M32			M36
T4.1			D4.1 MS3																	
T4.2												D4.2								
T4.3																				
T4.4																	D4.4			
T4.5														D4.3 MS8						

Task list and descriptions

Task	Task title	Lead	Runtime
T4.1	Framework development for sociotechnical analysis	EUR	M8-M12
T4.2	Embedded field analysis	EUR	M12-M24
T4.3	Social, regulatory and ethical implications of algorithmic accountability tools	EUR	M22-M28
T4.4	Sociotechnical Assessment and Validation of SPATIAL tools	EUR	M26-M32
T4.5	Educational Module development and implementation	REA	M12-M36

Deliverables and milestones

D|MS	Title	Lead	Deadline
D4.1	Socio Technical analysis Framework	EUR	M12
D4.2	Field research based academic article	EUR	M24
D4.3	Education module full launch	REA	M28
D4.4	Sociotechnical, regulatory and ethical implications and integration guidelines report	EUR	M32
MS3	Completion of Analysis Framework	EUR	M12
MS8	Soft launch of education module	REA	M24

SPATIAL

Thank you

MORE INFO
@SPATIAL_H2020
SPATIAL home page

WP5: Deployment & Demonstration (TID)

Contributors: FOKUS, FSC, MI, UCD, TUD, UT
Souneil Park, Ph.D.
Researcher@Telefonica R&D

Overarching goal

- Integrate & verify methodological contributions via use cases
  - Building infrastructure for the pilots
  - Deployment of the use cases
  - Evaluation on real user traffic or endpoint data

- 4 use cases / tasks:
  1. Privacy-preserving AI on the Edge and beyond
  2. Improving explainability, resilience and performance of cybersecurity analysis of 4G/5G/IoT networks
  3. Accountable AI in Emergency eCall System
  4. Resilient Cybersecurity Analytics

WP5 Tasks

- T1: Edge computing platform for running privacy-preserving AI methods
  - Leader / Contributors**: TID** / TUD, UT
  - Summary: Explore performance – privacy trade-off of privacy preserving ML methods in a telco environment

- T2: Pilot on e-health emergency case
  - Leader / Contributors**: FOKUS** / UCD, UT
  - Summary: emergency communication triggered based on sensor data from IoT networks and eHealth sensors communicating with various end user devices

WP5 Tasks

- T3: Pilot on resilient AI in cybersecurity applications
  - Leader / Contributors**: FSC** / TUD
  - Summary: environment, prototypes, and a methodology for experimenting with poisining attacks and evaluating proposed solutions

- T4: Pilot on Cybersecurity AI analysis in 4G/5G/IoT networks
  - Leader / Contributors**: MI** / UCD
  - Summary: Integrate and evaluate the results for explainability and resiliency from WP2 and WP4 with respect to the requirement of WP1 based on the 4G/5G/IoT testbed provided by MI

Timetable of Deliverables

	Year	Year 1												Year 2												Year 3											
	Month	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
WP5 Deployment and Demonstration	Overall																								MS9									MS12			
	T5.1																		D5.1						D5.2									D5.3			D5.4
	T5.2																		D5.1						D5.2									D5.3			D5.4
	T5.3																		D5.1						D5.2									D5.3			D5.4
	T5.4																		D5.1						D5.2									D5.3			D5.4

D5.1 Initial description of use-case, design, testbed, experimentation for all pilots

D5.2 Initial technology transfer and recommendations derived from each pilot

D5.3 Final description of use-case, experimentation and results for the pilots

D5.4 Final technology transfer and recommendations derived from each pilot

SPATIAL KoM
WP6 Impact, Outreach and Collaboration

Giulia Pastor, Jose Gonzalez, Blanca Aregui,
AUSTRALO

T6.1

Stakeholders collaboration framework

TU Delft   MAINFLUX LABS

Fraunhofer FOKUS

TARGET GROUPS

AI Developers/ Engineers	System Integrators Service/App Providers Academia & RTOs	Data brokers/ aggregators AI Communities Digital Skills Networks
Cybersecurity Providers	Security & Privacy Providers Legal & Ethical Providers H2020-SU-ICT-03	H2020-SU-DS02 Standardisation & Open Source ECSO & Cybersecurity PPP
End Use sectors	Telecom sector E-Health sector	IoT/Smart city sector Education Platform
Policy makers	European Commission Regulators	ENISA Member States
Society as a whole	General Public	Non-specialised media

DISSEMINATION ACTIVITIES

Drive awareness, use and uptake of the project RESULTS to specific target audiences

Measure	KPIs
Publications	10 Peer-reviewed scientific research publications in journals
	30 Peer-reviewed publications and presentations in conferences
	50 Scientific and Technical Publications (e.g. articles, blog posts)
Events	Participation in +20 scientific events
	Participation in +30 nonscientific events
Workshops/webinars	10+ organised

@ALL To propose opportunities
@TUDelft To validate proposals

Contact AUSTRALO to organise the promotional activities/campaigns

DIGITAL CHANNELS

WEBSITE

- Homepage online www.spatial-h2020.eu
- Full website up and running on October 30, 2021, as per the GA
- Content Informative website, linking to main activities, resources and channels
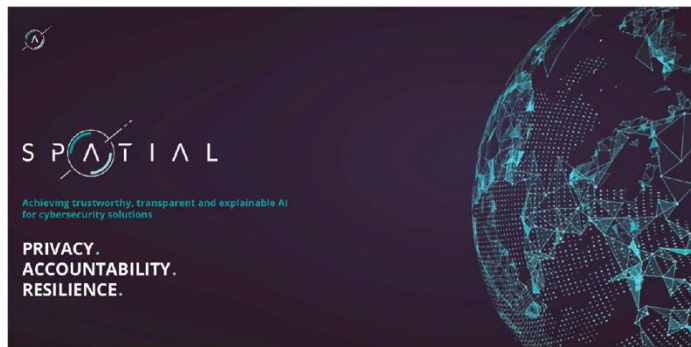
SPATIAL builds the pathway toward a **trustworthy European cybersecurity sector**, developing trustworthy governance and regulatory framework for AI-driven security in Europe.

THE MISSION.

Achieving trustworthy AI is a top priority for Europe, often hindered by the opacity of algorithms in software and hardware operations. SPATIAL solves such uncertainty by enforcing data privacy, resilience engineering, and legal-ethical accountability.

OUR AMBITION.

Transparency and Explainability

Develop verification and validation mechanisms for software + hardware that ensure AI transparency and explainability in the development of security solutions

Resilience and Privacy

Enhance resilience and preserve privacy during the training and deployment of AI services in decentralised, uncontrolled environments.

Societal Impact for Uptake

Create practical guidelines on regulation, governance and standardisation procedures for AI in cybersecurity.

Education and Skills Building

Offer an online educational module to build appropriate skills to strike a balance among technical, human and legal complexity.

New Business Models

Foster and streamline novel business opportunities for the ecosystem of data platforms, certification bodies, AI providers and users.

OUR TEAM.

Funded by the European Union, **SPATIAL** is a consortium led by **TU Delft**, consisting of **12 partners from 8 EU member states**.

DIGITAL CHANNELS

SOCIAL MEDIA

LinkedIn: https://www.linkedin.com/company/spatial-h2020

Twitter: https://twitter.com/SPATIAL_H2020

MENTION THE PROJECT @SPATIAL_H2020
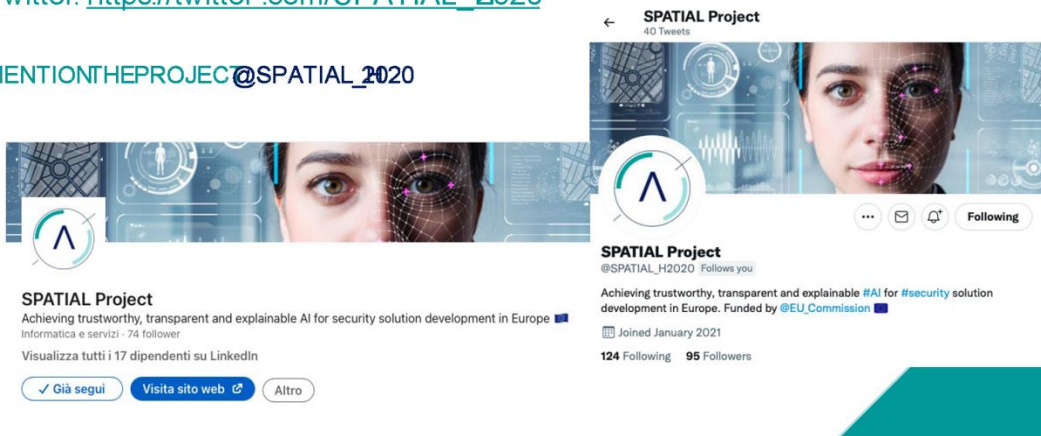
DIGITAL CHANNELS

PRESS RELEASE

First joint press release out

https://rebrand.ly/SPATIAL_PR_September2021

ZENODO
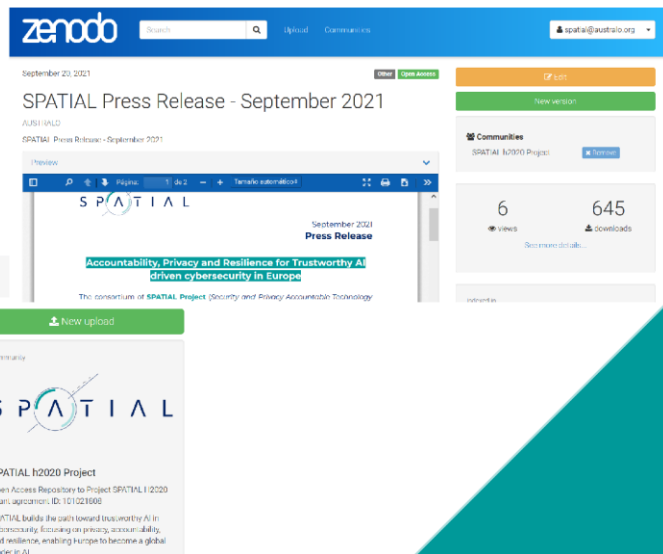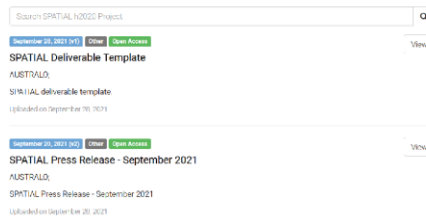
https://zenodo.org/communities/spatial

DIGITAL CHANNELS & TEMPLATES

NEWSLETTERS
- KPI 10 (end of project)
- Approach: rather than creating our own newsletters (poor ROI), we will aim at participating in relevant ones → @ALL: provide suggestions to blanca@australo.org

TEMPLATES
Slides deck: https://rebrand.ly/SPATIAL_PitchDeck_Template
Deliverable template: https://rebrand.ly/SPATIAL_Deliverable_Template

SPATIAL

Branding guidelines

Elements & rules 2021
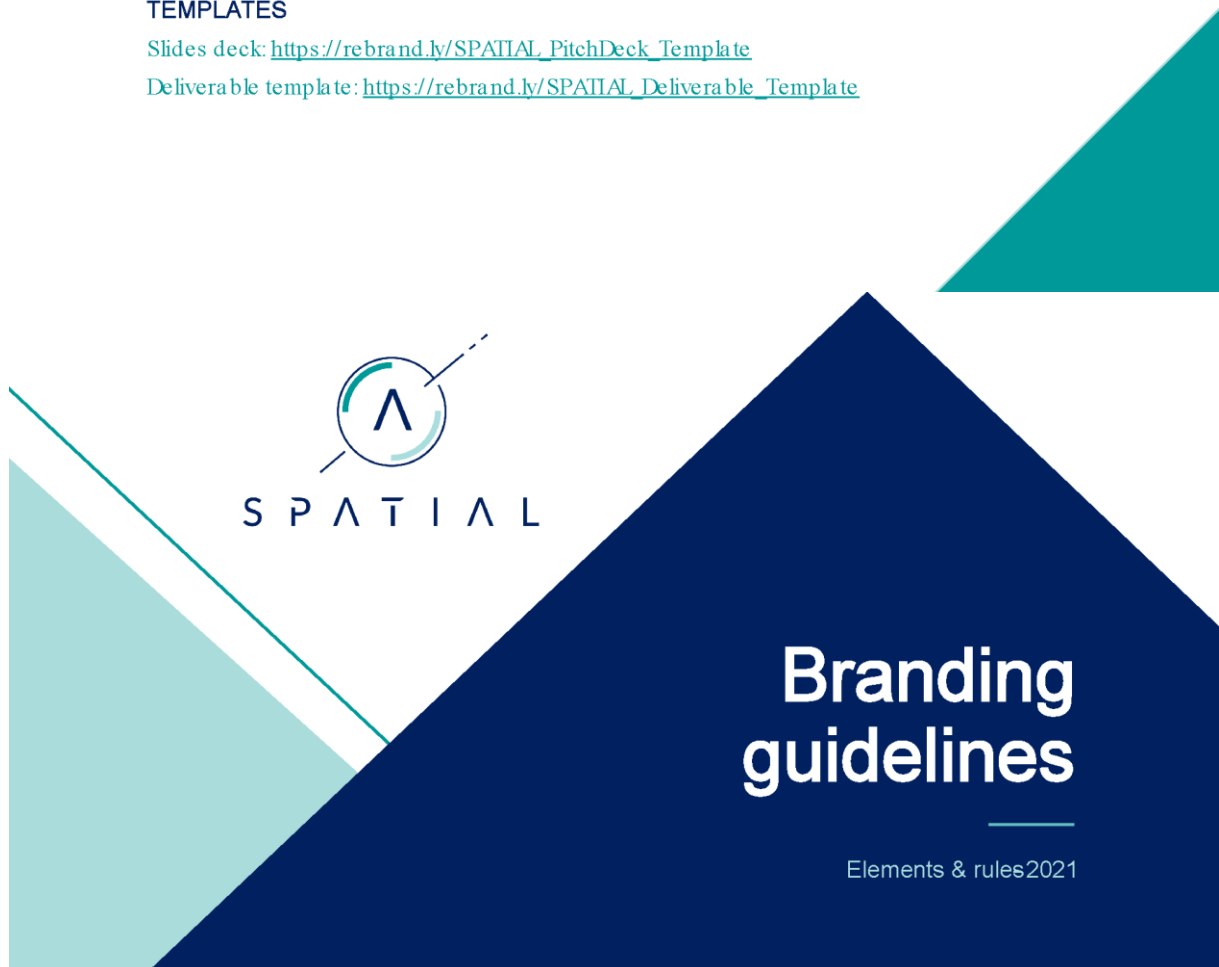
Logo onwhite background

This logo is to be used on white and lightly colored backgrounds.
It must not be used on blue or green backgrounds.
Pick the format based on your needs.

https://rebrand.ly/SPATIAL_Logos_and_Icons

Logo on blue background

This logo is to be used on blue and dark colored backgrounds.
It must not be used on white or green backgrounds.
Pick the format based on your needs.
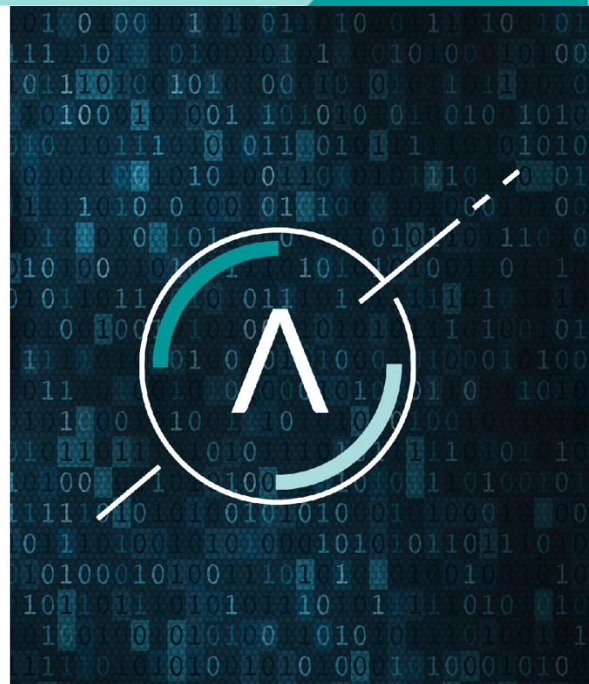
FONTS

Titles

Open Sans Bold/Extrabold

Abcdefghijklmn
opqrstuvwxyz
1234567890

Download here

Main Texts

Lato Light/Regular

Abcdefghijklmn
opqrstuvwxyz
1234567890

Download here

T6.3

Innovation management,
Exploitation and
Sustainability

MAINFLUX LABS

TU Delft   F-Secure
Telefónica   NEC   \Orchestrating a brighter world   montimage   AUS TRA LO

ACTIVITIES

Exploitation→ Managing the overall exploitation strategy of SPATIAL to ensure the successful use, adoption and sustainability of its results

Innovation management→ Design sustainable business models, aiming to develop a strategy that can drive long-term leadership, based on the technical excellence of the project

Key Exploitable assets→ Describe the services and use cases provided within the scope of the project that will improve performances and create new business roles

T6.4

Standardisation and Open Source

Fraunhofer
FOKUS

TUDelft   Telefónica   Erasmus University Rotterdam

ACTIVITIES

Identifying and enforcing synergies with standardization bodies and open source communities, at European and international level
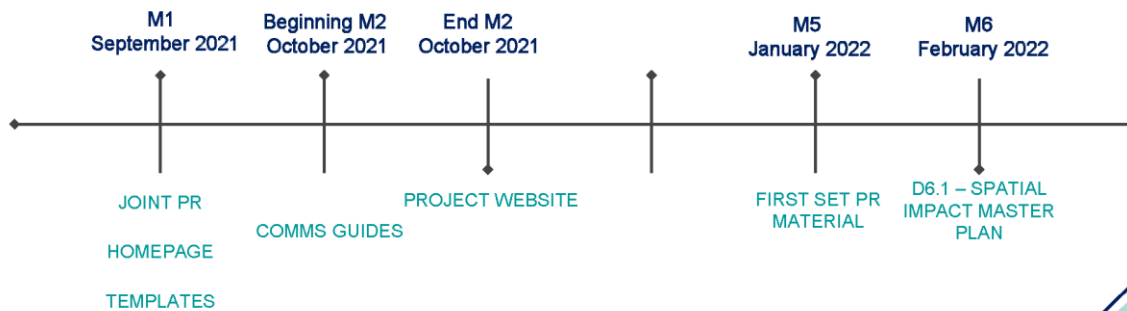
Collaboration plan → i) Evaluate state-of-art advances in transparency, explainability and end use validation of AI to the activities of the project; ii) Propose relevant contributions to these bodies:

- STANDARDISATION: 6GPPP, ETSI, IRTF, IETF, DIN, 5GPPP
- OPEN SOURCE: EdgeX Foundry, Mainflux IoT Platform, Hyperledger Project

Synergies with StandIct.eu project → Collaboration to be discussed together with D6.1

MAIN ACHIEVEMENTS M1-M6

M1 September 2021	Beginning M2 October 2021	End M2 October 2021		M5 January 2022	M6 February 2022
JOINT PR HOMEPAGE TEMPLATES	COMMS GUIDES	PROJECT WEBSITE		FIRST SET PR MATERIAL	D6.1 – SPATIAL IMPACT MASTER PLAN

3.4 SLIDES: USE CASE REVIEW

Pilot on edge computing platform for running privacy-preserving AI methods (TID)

(M13-M36)
Contributors: TUD, UT

Objectives

- Assess performance of Privacy-Preserving Machine Learning (PPML)
  - Classical & Deep Learning methods
  - Deployed on edge / other hierarchical nodes
  - Collaborative ML training across 3rd-parties
- Assess tradeoff between FL/HFL methods
  - Convergence, accuracy, privacy

Telefónica

SPATIAL

SPATIAL

Interaction with other WPs

- Privacy metrics & AI methods (from T2.2, T2.3)
- Results from ML training & testing (from T3.1, T3.2)
- Evaluation & testing aligned with effort in T3.6

Telefónica

SPATIAL

Evaluation

- Leverage already existing edge computing infra
    - Local, in-house
    - 5TONIC Lab
- Results communicated/disseminated
    - Technical conferences
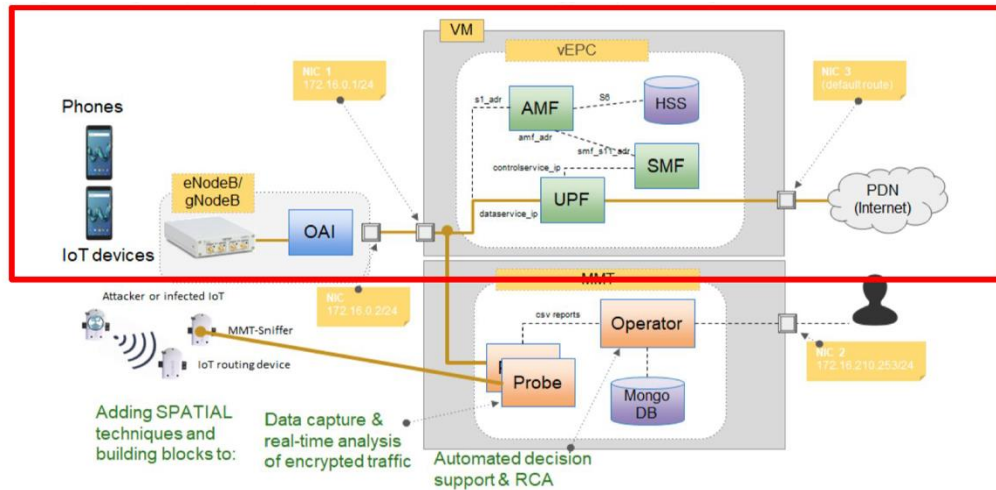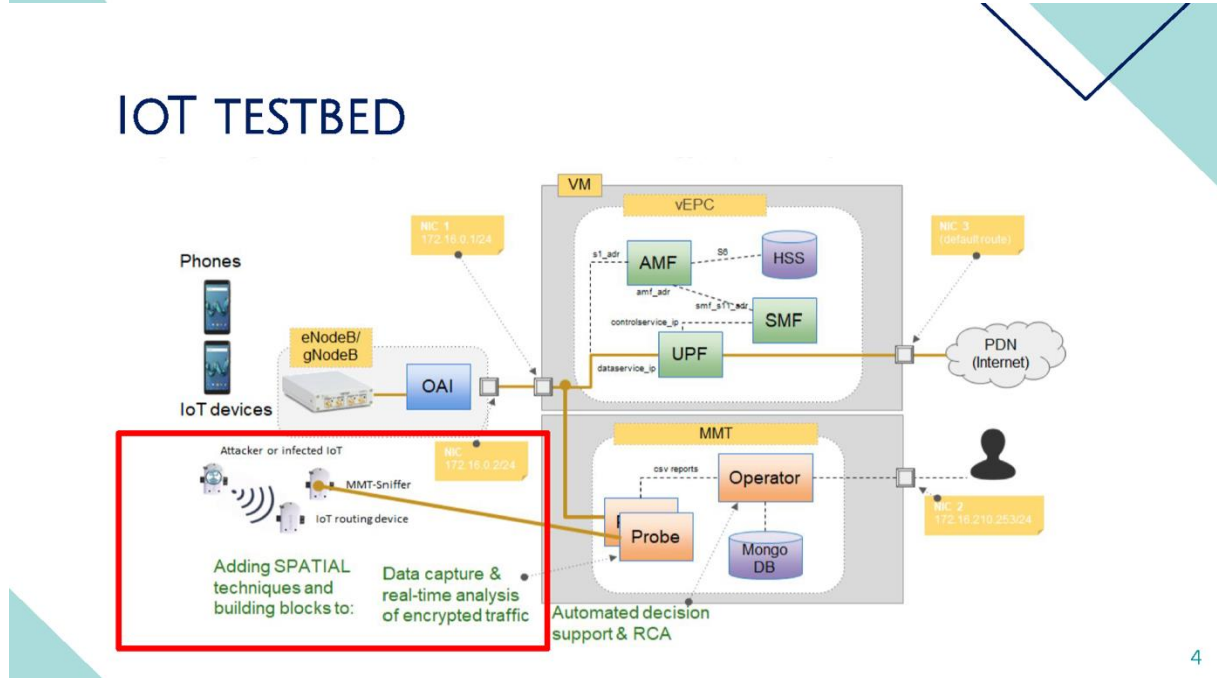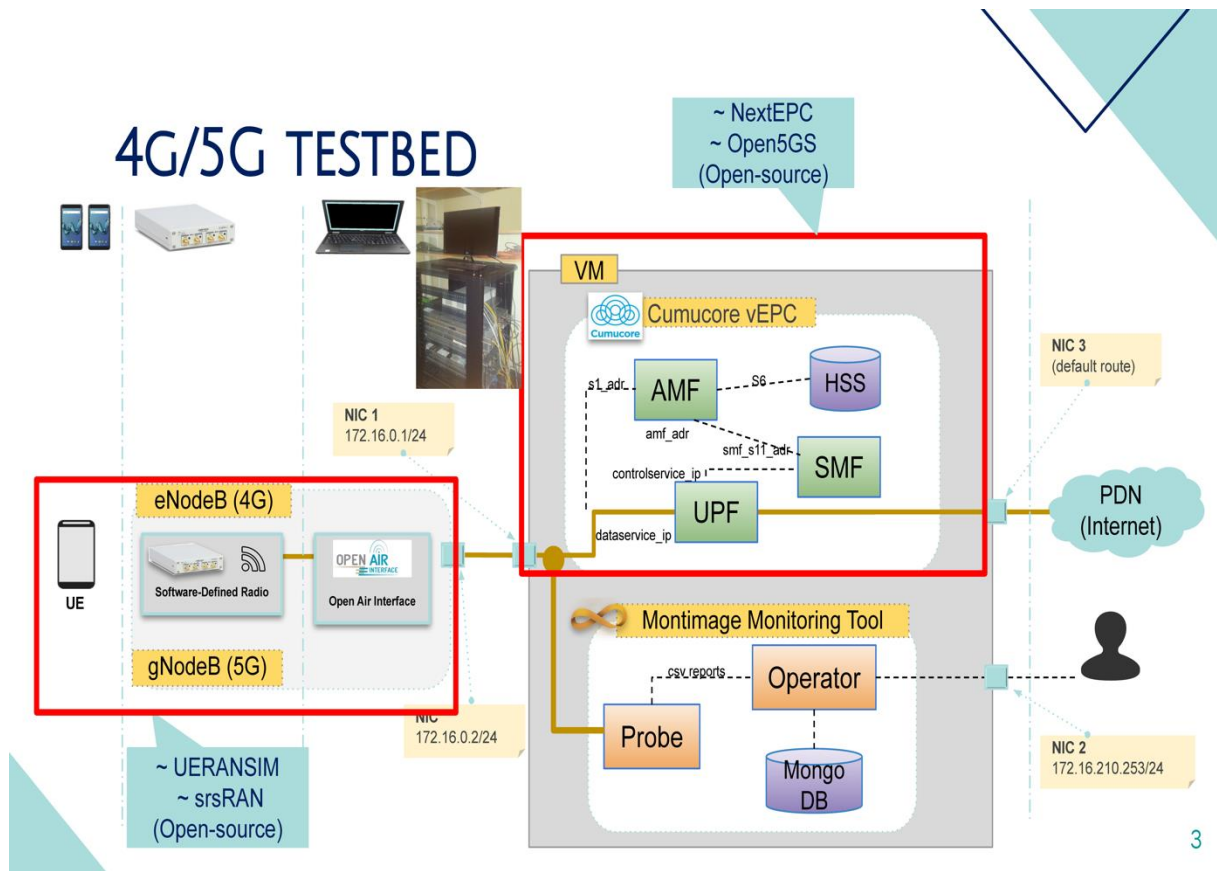   - Specialized industry events
    - Patents

Telefónica

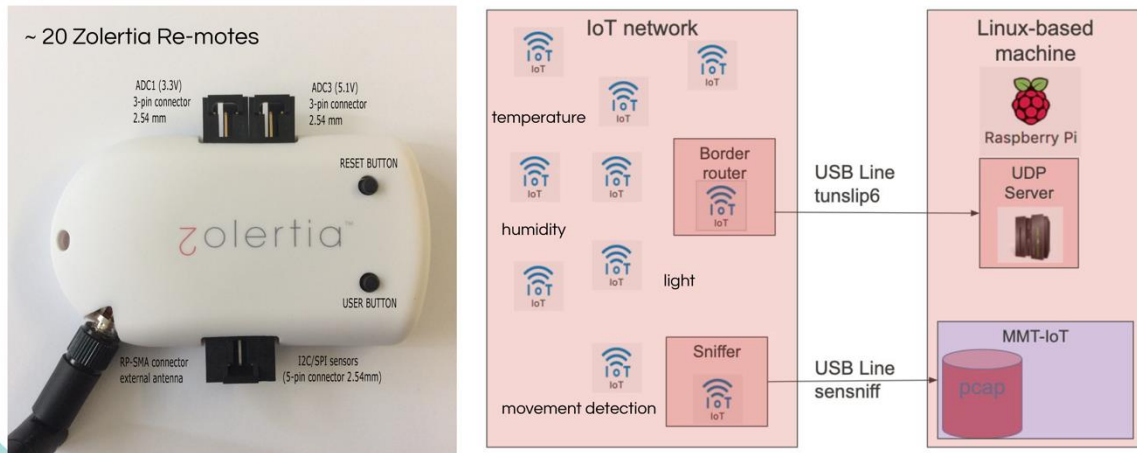Pilot on Cybersecurity AI analysis in 4G/5G/IoT networks

Montimage
SPATIAL Kick-off Meeting, September 29th 2021

4G/5G TESTBED

IOT TESTBED

~ 20 Zolertia Re-motes

~ 10 Raspberry Pi

5

SPATIAL – USE CASE 2

"Improving explainability, resilience and performance of cybersecurity analysis of 4G/5G/IoT networks"

- Objectives:
  - Integration of improved AI/ML techniques (e.g., for Anomaly Detection/ RCA) as well as to make the pilot resilient against adversarial AI attacks.
  - Measuring the improvements made in terms of explainability, resilience, and performance.

6

SPATIAL – USE CASE 2

"Improving explainability, resilience and performance of cybersecurity analysis of 4G/5G/IoT networks"

- Users:
  - As a monitoring framework, the solution provided here could be interested by the 5G Providers/ Network Operators or IoT Manufacturers.
  - The framework will collect data (network traffic) from IoT/ 5G users via their IoT devices / 5G phones.

7

Thank you

MORE INFO

Vinh La (vinh_hoa.la@montimage.com)
Edgardo Montes de Oca (edgardo.montesdeoca@montimage.com)
Manh-Dung Nguyen (manhdung.nguyen@montimage.com)
Ana Cavalli (ana.cavalli@it-sudparis.eu)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

SPATIAL project is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.

Page 111 of 118

Use Case 3

EMYNOS - Accountable AI in Emergency eCall System

Dr.-Ing. Nikolay Tcholtchev | Michell Boerger | 29.09.2021 | SPATIAL Kickoff

H2020 EMYNOS

- IP-based telecom platform for "eCall and VoIP NG 112" emergency communications that overcomes limitations in
  - transmission of caller location
  - forwarding of emergency calls
  - integration of sensor data and IoT architectures
- Integrates rich-media emergency calls with a combination of voice, text, IoT sensors, social network information and video
- Monitoring using eHealth sensors and resulting automated emergency calls

Potential SPATIAL Extensions

- Extend architecture and embed accountable and transparent AI procedures for automated eHealth sensor based eCalls

  1) processing relevant data (e.g. IoT data like heart beats measurement)

  2) automatically initiate a connection to the call center

  3) support Backend to distinguish between serious, false, and hoax calls

- Accountable, explainable and transparent ML procedures are required towards a later product certification

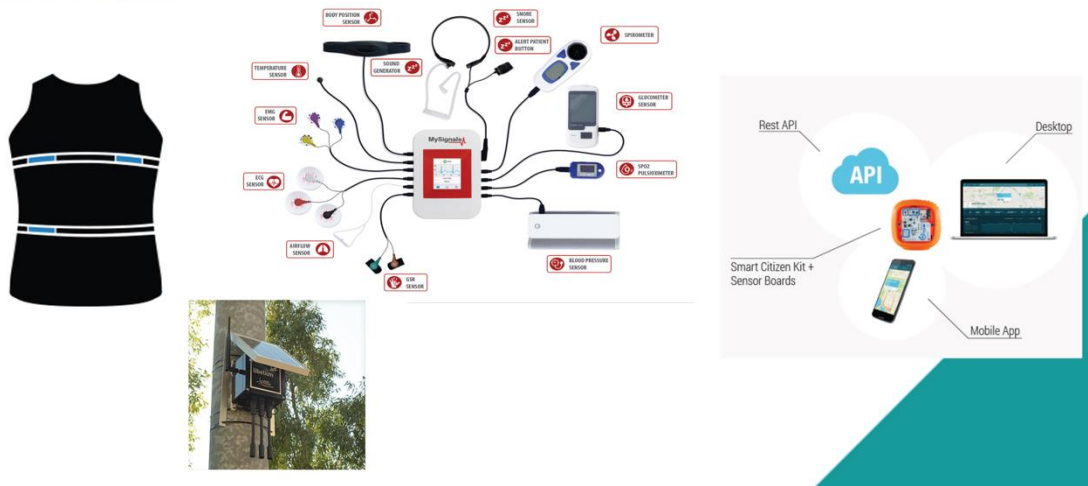# EMYtest Architecture
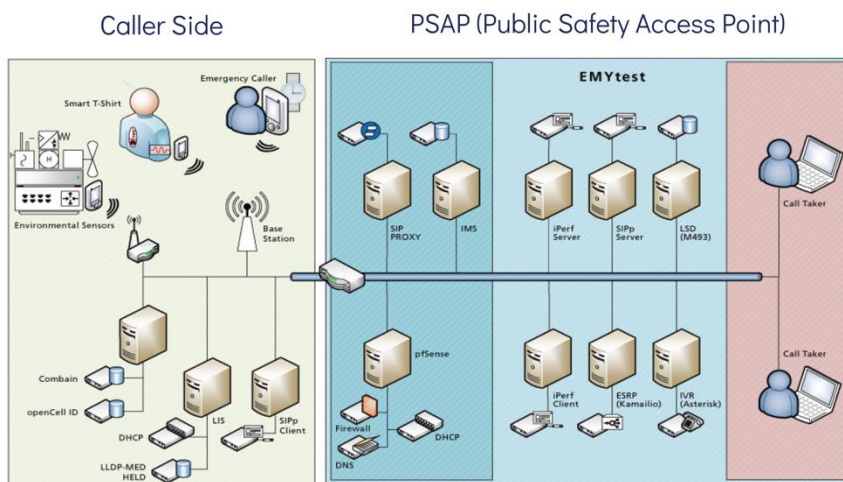
Experimental Infrastructure
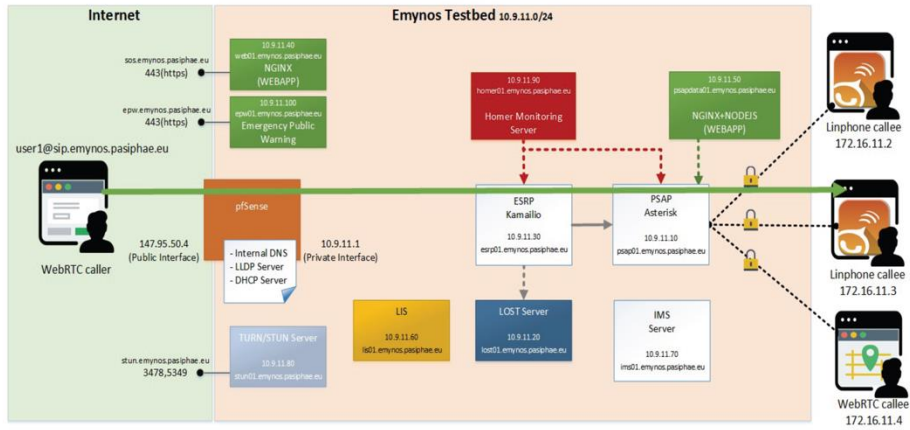
Future Work: Emynos Sensors

The Hexoskin Smart Shirts are a comfortable new way to monitor precise cardiac, respiratory, sleep and activity data.

Malicious Document Detection

Objective: Predict whether an MS Office document is malicious or not

Input data: ~150 features extracted from each document, incl. document meta features and counts for keywords in document macros

Model: Random Forest classifier

Host Profiler

Objective: Predict the "type" of a (Windows) host (to be used in attack detection logic)
- technical
- non-technical
- server

Input data: 1000s of event counts for each host to profile
- processes
- domains (network connections)
- file types

Model: XGBoost classifier

Attack Scenarios

Malicious document model

Attacker wants a malicious document to be predicted as benign → evade detection

Host profiler

Attacker wants the host profiler to predict an incorrect type for a host (e.g., *non-technical → technical*). If an incorrect set of detection rules is chosen:

- Attacker can carry out malicious activities on the host and remain undetected → evade detection
- Benign behavior is detected as anomalous → Denial of Service

Attack Vectors

Evasion attack: Modify features representing hosts / documents at the inference time

- Preserve malicious functionality of a host / document
- Modify the prediction of the detector / profiler

Poisoning attack: Inject malicious data in the detector / profiler training dataset at the training time

- Compromise the trained detector / profiler to force incorrect predictions at the inference time

Work Plan

Study vulnerabilities of ML models to adversarial ML attacks
- Threat modeling for the use-cases
- Design and test attacks (evasion / poisoning) against the models
- Quantify vulnerabilities to these attacks

Defend against adversarial ML attacks
- Design methods to detect ML attacks
- Deploy and test the defenses in the proposed use-cases

SPATIAL

Thank you

MORE INFO

samuel.marchal@f-secure.com
alexey.kirichenko@f-secure.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101021808.