OpenSwarm

www.openswarm.eu

Call: HORIZON-CL4-2022-DATA-01

Type of action: Horizon Research & Innovation Actions

Grant agreement: 101093046

Start date: 01/01/2023

Duration: 40 months

D1.3 Collection of ethics, safety & regulation guidelines to be reviewed yearly

Work Package 1 (WP 1): Requirements and System Architecture

Task Lead: Inria, France

WP Lead: Inria, France

This project has received funding from the European Union's Horizon Europe Framework Programme under Grant Agreement No. 101093046.

Funded by the European Union

Document information	
Deliverable number	D1.3
Deliverable title	D1.3 Collection of ethics, safety & regulation guidelines to be reviewed yearly
Description	This report is dedicated to addressing the ethics, safety, and regulatory considerations integral to the project's development.
Issued by	INRIA
Lead authors	Clotilde MONNET, Thomas WATTEYNE
Contributors	Sylvain PETITJEAN (OCELER INRIA) Anne COMBE (Data Protection Officer INRIA) Michele BARBIER, (European project Manager INRIA & Independant Ethics expert for the EC) Micael COUCEIRO (ING), Franz ZEILINGER (SIA), Jochen NICKLES (SIG)
Submission date	30-Sept-2023
Due date	30-Sept-2023
Work package leader	INRIA
Type	ETHICS
Dissemination level	PU

Document history			
Date	Version	Author(s)	Comments
06/09/2023	1	Clotilde MONNET (INRIA)	First draft
03/10/2023	2	Sylvain PETITJEAN (OCELER INRIA)	Corrections and Comments
04/10/2023	3	Anne COMBE (Data Protection Officer INRIA)	Corrections and Comments
04/10/2023	4	Clotilde MONNET (INRIA)	Updated draft
06/10/2023	5	Michele BARBIER, (European project Manager INRIA & Independant Ethics expert for the EC)	Corrections and Comments
09/10/2023	6	Clotilde MONNET (INRIA)	Updated draft
11/10/2023	7	Micael COUCEIRO (ING), Franz ZEILINGER (SIA), Jochen NICKLES (SIG)	Integration of reviewers feedback

DISCLAIMER

This technical report is an official deliverable of the OpenSwarm project that has received funding from the European Union's Horizon Europe Framework Programme under Grant Agreement No.101093046. Contents in this document reflects the views of the authors (i.e., researchers) of the project and not necessarily of the funding source the European Commission. The report is marked as PUBLIC. Reproduction and distribution is limited to OpenSwarm Consortium members and the European Commission.

Table of contents

Executive Summary

This report focuses on the ethics, safety and regulatory aspects of the OpenSwarm project. There are four goals for this report. First, provide all partners with accessible, clear and appropriate legislative documentation and European Commission (EC) guidelines on the ethics, safety and regulation aspects of the project development. Second, on ethics, follow European guidelines on Artificial Intelligence (AI) and other guidelines and legislations, and be able to reach out to the institutional review board of each academic partner if an ethical issue is raised. This includes the research ethics committees of the project partners, Operational Committee for the Evaluation of Legal and Ethical Risks (OCELER) for INRIA, but also IMEC's ethics code of conduct, the Social and Societal Ethics Committee (SMEC) at Katholieke Universiteit Leuven and the University Research Ethics Committee (UREC) at University of Sheffield. Third, concerning safety aspects, and in compliance with regulatory frameworks and each partner's national safety laws, the OpenSwarm project envisages the establishment of a safety plan to address any security issues. If a risk is detected, a contingency plan, decided upon collaboratively and transparently with all consortium partners, will be implemented. Fourth, regulatory monitoring on applicable standards (robotics, AI, drones, data sharing), evolution of the regulatory framework on each technical and scientific core activities of the project.

The Project Coordinator (PC) promotes the sharing of good practices between partners, management of this aspect is carried out by the scientific committee with the help of the Project Management Office and the support of expert external bodies, if relevant during the project lifespan.

Objectives

The purpose of this document is to provide a consistent set of ethics, safety and regulatory guidelines to ensure the quality of the project and its outcomes.

The OpenSwarm project aims to trigger the next revolution in data-driven systems by developing true collaborative and distributed smart nodes, through groundbreaking R&I in three technological pillars: efficient networking and management of smart nodes, collaborative energy-aware Artificial Intelligence (AI), and energy-aware swarm programming. Results are implemented in an open software package called “OpenSwarm”, which is verified in our labs on two 1,000 node testbeds. OpenSwarm is then validated in five real-world proof-of-concept use cases, covering four application domains: Renewable Energy Community (Cities & Community), Supporting Human Workers in Harvesting (Environmental), Ocean Noise Pollution Monitoring (Environmental), Health and Safety in Industrial Production Sites (Industrial/Health), Moving Networks in Trains (Mobility). A comprehensive dissemination, exploitation, and communication plan (including a diverse range of activities related to standardization, educational and outreach, open science, and startup formations) amplifies the expected impacts of OpenSwarm, achieving a step change enabling novel, future energy-aware swarms of collaborative smart nodes with wide range benefits for the environment, industries, and society.

The Grant Agreement (GA) and the Consortium Agreement (CA) of the project describe the actions and regulate the legal aspects of the project in detail.

This deliverable is provided as a tool for all involved in the project, a convenient means for finding the information needed on ethics, safety and regulatory aspects of the project OpenSwarm. This is a living document that tracks the legal and regulatory developments of the European Union and the member countries within the consortium.

This deliverable can be found on the project’s collaborative platform (SharePoint), allowing all involved in the OpenSwarm project to add comments to the document. Suggestions for improvements and changes should be communicated to the Project Manager.

List of acronyms/abbreviations

Abbreviation	Explanation
AB	Advisory Board
ADI	Analog Devices Ireland, Ltd

AI	Artificial intelligence
AI&R	Artificial intelligence and robotics
CA	Consortium Agreement
D	Deliverable
DMP	Data Management Plan
DoA	Description Of the Action
DPO	Data Protection Officer
EC	European Commission
EDPS	European Data Protection Supervisor
EHS	Environment, Health, and Safety
ESAB	Ethics and Safety Advisory Board
EU	European Union
ExCom	Executive Committee
GA	Grant Agreement
GB	Governing Board
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IMEC	Interuniversitair micro-electronica Centrum
ING	Ingeniarius LDA
INRIA	Institut national de recherche en informatique et automatique
IoT	Internet of Things

IP	Intellectual property
IPRs	Intellectual property rights
IR	Intermediate Report
KPI	Key Performance Indicator
KUL	Katholieke universiteit leuven
LED	Law Enforcement Directive
OCELER	Operational Committee for the Evaluation of Legal and Ethical Risks at INRIA
PMO	Project Management Office
PoC	Proof of Concept
SMEs	Small and Medium-Sized Enterprises
SMEC	Social and Societal Ethics Committee at KUL
SIG	Siemens aktiengesellschaft
SIA	Siemens aktiengesellschaft oesterreich
SO	Scientific Objective
UOS	The University of Sheffield
UREC	University Research Ethics Committee at UOS
WE	Wattson elements
WP	Work Package

Glossary of terms

Term	Explanation

Artificial intelligence	The science and engineering of machines with capabilities that are considered intelligent (i.e., intelligent by the standard of human intelligence). Major applications of AI technology are in transportation, education, finance, industry, healthcare, marketing, management, telecommunications, entertainment and defense, amongst other fields. Important sub-fields of AI include: knowledge representation and automated reasoning, artificial neural networks, machine learning, computer vision, computer audition, natural language processing, expert systems, data mining, intelligent agent systems and automated planning, evolutionary computation.
Automated decision-making	Decision based solely on automated processing, including profiling, which produces legal effects concerning a data subject or similarly significantly affects him or her (GDPR, Article 22[1]). It refers to individual decision-making made by automated means without any human involvement. Examples include: an online decision to award a loan; and a recruitment aptitude test which uses pre-programmed algorithms and criteria[2] (Information Commissioner's Office)
Machine learning	A set of approaches within AI where statistical techniques and data are used to "teach" computer systems how to perform tasks, without these systems being explicitly programmed to do so.
Open-Source software	Open-source software is software which users are authorized to use, study, modify or duplicate with a view towards distribution, without any technical or legal impediments. Unlike proprietary software, its source code is accessible, allowing anyone to consult, copy, redistribute or even modify the software, for whatever purpose.
Regulation	The intentional use of authority to affect the behavior of a different party according to set standards. Law is one of the institutions for purposively attempting to shape behavior and social outcomes, but

[1] https://gdpr-info.eu/art-22-gdpr/

[2] Information Commissioner's Office (ICO), "Rights related to automated decision-making including profiling". https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

	there may be other means, including the market, social norms, and technology itself. Examples of regulation: a type of EU legal act with a direct effect defined by Article 288 of the Treaty on the Functioning of the European Union[3] or, in some instances, a legal act adopted at the national level.
Regulatory bodies	Bodies that exercise regulatory or supervisory powers. E.g., regulatory agencies, watchdogs, Commission
Robotics	The field of science and engineering that deals with the design, construction, operation, and application of robots. Major applications of robots are in transportation, industry, healthcare, education, entertainment, space exploration, defense, retail, companionship, housekeeping and other areas. Important subfields of robotics were found to include: robot mechanics, robot sensing, robot control (including many subareas, such as robot learning, adaptive control, developmental robotics, evolutionary robotics, cognitive robotics, behavior-based robotics, robotic mapping and planning), robot locomotion, bio-inspired and soft robotics, humanoid robotics, microrobotics, nanorobotics, beam robotics, cloud robotics, swarm robotics, telerobotics, social robotics and human-robot interaction.
Swarm Robotics	Swarm robotics is concerned with the interplay and coordination of a swarm of simple homogeneous robotic units cooperating together to accomplish a task through local communication in a distributed and decentralized way.

[3] According to this provision, “To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions. A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods. A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them. Recommendations and opinions shall have no binding force.” 9 Goncales, Maria Eduarda, Maria Ines Gameiro, “Hard Law, Soft Law and Self-regulation: Seeking Better Governance for Science and Technology in the EU”, Working paper, 2011.

https://www.researchgate.net/publication/272351073_Hard_Law_Soft_Law_and_Self-regulation_Seeking_Better_Governance_for_Science_and_Technology_in_the_EU

Introduction

In the pursuit of its ambitious goals, the OpenSwarm project places a strong emphasis on ethics, safety, and regulatory compliance throughout its development journey. The project's commitment to ensuring the highest ethical standards and safety measures is not only a fundamental principle but also a critical aspect of its success. This report serves as a comprehensive guide on how the project effectively addresses these crucial dimensions.

One of the primary objectives of this report is to provide all project partners with accessible, clear, and pertinent legislative documentation and guidelines from the European Commission (EC) pertaining to the ethics, safety, and regulatory aspects of the project's development. This not only establishes a common understanding but also ensure that ethical and safety considerations are at the forefront of every project phase.

Moreover, the report serves as a dynamic resource that can be regularly updated throughout the project's lifespan. The responsibility for keeping the report up-to-date lies with the Project Coordinator and Work Package (WP) leaders, who collaborate to ensure that it remains a current and relevant source of information. It is made available to all project stakeholders through the project's SharePoint platform, facilitating easy access and dissemination of critical guidelines.

Importantly, having these guidelines in advance, prior to the implementation of the technology in the various use cases planned throughout the project, is of paramount importance. It enables the project to integrate ethical and safety considerations seamlessly into the development process, ensuring that the technology aligns with the highest ethical standards and safety protocols.

1. Compliance with European guidelines on AI and other guidelines and legislations

The OpenSwarm project is committed to implementing its activities and scientific results in strict compliance with current technical standards and regulations governing robotics and drones, ongoing guidelines for AI[4] and design principles identified and drafted early on the project so that the robotic swarm poses no risk to the personnel involved in the evaluation processes or during the PoC-based validation. Furthermore, the use of artificial intelligence in the EU is regulated by the Regulation of the European Parliament and of the Council on harmonized rules for Artificial Intelligence, amending certain Union Legislative Acts. The consortium/partners regularly stay informed about the current legislation.

Research activities of the project are conducted in accordance with the principles of the applicable country-specific national data protection legislation. OpenSwarm commits to the highest standards of the charter for fundamental rights[5], of the European Union, the European code of conduct for research integrity (https://allea.org/code-of-conduct/), the data security and protection in order to preserve the personal rights and interests of each potential participant.

All partners bodies are aware and committed to the European Code of Conduct for Research Integrity, the General Data Protection Regulation (EU 2016/679) and its application domains, and strictly follow those regulations, with the support of the Project Management Officer (PMO) and an external Ethics and Safety Advisory Board (ESAB), if necessary, for the potential AI issues. All public partners are supported by an internal ethical advisory board to be seized when relevant and the securement of data management of their research activities is guarantee with a dedicated Data Protection Officer (DPO) who ensures the compliance with the General Data Protection Regulation (GDPR) principles.

All personal data (including registration data collected by participants in project events, data included in stakeholders' database/contact lists, etc.) collected or generated during the

[4] Ethics guidelines for trustworthy AI, The European Commission,16 November 2021

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

project are processed in line with the GDPR by each DPO, in terms of informed consent procedures, security measures to prevent unauthorized access, data minimization and anonymization and data transfer procedures.

All scientific research and development activities, as well as communication, dissemination and exploitation of project results activities carried out by the British partner (UOS) are designed and implemented in rigorous compliance with the British general regime of protection of personal data and thus European standards, in accordance with the Law Enforcement Directive (LED) of the EU GDPR voted in June 2021 and effective until the 27th June 2025. The OpenSwarm project relies on the Data Protection Officer (DPO) to monitor the evolution of these agreements between the EU and the UK and make any modifications necessary, in constant collaboration with Project Coordinator (PC).

The devices augmented with intelligence are designed in overall transparency, under human control and do not affect human self-governance. Aspects related to AI misuses or AI interaction with human are subject to particular attention in the general oversight of ethics, safety and regulation aspects handled by INRIA with the support of all partners of the project, and more generally on the implementation of the management rules and procedures of the project all along its lifespan.

To ensure the project’s systems are ethically suitable for human participation with swarm intelligence and AI in general, R&D is conducted in accordance with the guide to the ethical design and application of robots and robotic systems (updated in 2022) and IEEE’s P7000 Model Process for Addressing Ethical Concerns During System Design (2021). The impact of the appropriation of PoC3 technology development for military application is to be taken into consideration in our risk management plan. Misuse of research is another risk that needs to be foreseen in the project management plan throughout its progress. To help identify and address properly this risk, we follow advice given by the European Commission in its Guidance note on potential misuse of research[6]. With the support of the ESAB, the consortium focuses on identifying and preventing those risks by taking all required appropriate action.

[6] Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, 25 November 2021, The European Commission

2. Ethical and safety management

The OpenSwarm project demonstrates its commitment to ethical and safety compliance by taking into account the Charter of Fundamental Rights and legal regulations of the European Union in the field of swarm robotics, artificial intelligence (AI), and machine safety and.

Safety of OpenSwarm Robots

OpenSwarm considers previous legal and regulatory contributions regarding machine safety, including the European Union's Machinery Directive 2006/42/EC. This directive established essential safety requirements for machines, ensuring that they do not pose risks to users. OpenSwarm ensures that its robots comply with these requirements to guarantee their safety during use.

Use of Artificial Intelligence in OpenSwarm Robots

Previous directives, such as the Directive 2014/30/EU on electromagnetic compatibility and Directive 2014/35/EU on pressure equipment, laid the groundwork for regulating the integration of AI into machines and electronic equipment. OpenSwarm draws inspiration from these regulations to ensure that the artificial intelligence used in its robots complies with safety and ethical standards.

Documentation and Transparency

Previous directives, such as the Machinery Directive 2006/42/EC, emphasized the importance of technical documentation to ensure compliance with safety standards. OpenSwarm follows these legal precedents by carefully documenting the design and operation of its robots, promoting transparency and compliance with relevant regulations.

Cost Reduction and Alignment with SME Needs

Previous directives also addressed the need to reduce administrative burdens and costs for manufacturers, particularly for small and medium-sized enterprises (SMEs). OpenSwarm draws from these legal precedents to incorporate simplified solutions, thereby reducing conformity assessment costs and promoting competitiveness in the swarm robotics sector, including SMEs.

3. Real-world proof-of-concept applications (PoC)

OpenSwarm incorporates ethical and safety compliance into its two 1,000 robot testbeds, on the UOS and ADI premises and its five real-world proof-of-concept applications (PoC). OpenSwarm project is placing a strong emphasis on the design and execution of PoC2, PoC3, and PoC4. We are committed to implementing an Ethics and Safety Framework (ESAB), which is overseen by the Project Coordinator and the Executive Committee. We actively engage with the research ethics committees of all academic partners within the consortium, with a special focus on INRIA's own committee. These consultations ensure that ethical principles are upheld and honored throughout the project.

PoC1. “Cities & Community: Renewable Energy Community”

- ***Concept***

This PoC focuses on the implementation of renewable energy communities (RECs) to achieve climate neutrality and decarbonize the energy system. OpenSwarm develops a system of smart sensors (the devices) that orchestrate and interact in a collaborative manner with the customer gateway (the edge) using distributed swarm intelligence and low-latency communication. The devices monitor raw data (e.g. instantaneous energy consumption), forward that to the edge device which generates a summary of the data (e.g. using a Exponential Moving Average) to the OpenSwarm cloud. The cloud, which runs on a server on the Internet, dynamically orchestrates the local electricity demand (the consumption of the homes) with the supply (the production of their solar panels). This use case verifies the OpenSwarm network's ability to operate renewable energy communities with a hierarchical network organization as well as to analyze the current consumption pattern using distributed AI.

- ***Ethical and Safety compliance***

OpenSwarm's approach to addressing cybersecurity threats in smart grids is underpinned by a robust and comprehensive strategy. As the implementation of renewable energy communities (RECs) gains momentum to achieve climate neutrality and decarbonize the energy system, the protection of these critical infrastructure components becomes paramount. OpenSwarm's system of smart sensors, which form an integral part of this initiative, are equipped with state-of-the-art cybersecurity features.

Firstly, OpenSwarm prioritizes secure communication within its network, utilizing encryption protocols and authentication mechanisms to safeguard data transmission. This ensures that sensitive information related to energy consumption, production, and distribution remains protected from potential cyberattacks.

Furthermore, OpenSwarm collaborates with cybersecurity experts and authorities to align its practices with national and international standards for protecting critical infrastructure. This includes compliance with regulations such as the European Union's NIS Directive (Network and Information Systems Directive) to bolster the resilience of the smart grid against cyber threats.

In summary, OpenSwarm is fully committed to ensuring the cybersecurity of smart grids in Austria, implementing a multi-faceted approach that encompasses encryption, monitoring, collaboration, and compliance with established cybersecurity standards to protect renewable energy communities and their associated smart grid infrastructure.

PoC2 “Environmental: Supporting Human Workers in Harvesting”

- ***Concept***

This PoC aims to develop a swarm robotic solution using Unmanned Aerial Vehicles (UAVs). Each UAV (the device) is a quadcopter approx. 50 cm in diameter, equipped with a LiDAR or depth camera, a wireless radio, and enough processing power to run motion control and simultaneous localization and mapping (SLAM) routines on-board. Each UAV runs the OpenSwarm networking technology, allowing it to communicate with a leader UAV (the edge). This swarm approach is developed in forest conditions to map the environment. Each UAV flies under the canopy and runs AI routines locally to detect features for odometry estimation, which is needed to subsequently map the environment. The UAV forwards that information to the edge which serves as the expedition leader and coordinates with the cloud. The cloud builds a map of the forest based on data collected by all UAVs. We acknowledge the potential recording of unexpected and sensitive information that could pose harm to individuals or the environment. Instances, such as incidents of assault, acts of arson, and other harmful activities, may inadvertently be captured, emphasizing the importance of responsible data management and ethical considerations in the use of recording technologies.

- ***Ethical and Safety compliance***

PoC2 “Environmental: Supporting Human Workers in Harvesting” involves swarms of UAVs flying in the forest to ease the work on harvesting personnel by acquiring data using advanced sensors and on-board AI to generate forestry maps. ING has close ties with regional and local authorities, such as the Civil Protection of Valongo, to whom authorization to deploy UAVs are sought.

While not intended, it is possible that someone is present in these forests and appears in the footage. Although the project never records any sensitive data, some basic personal biographical data may be required, e.g., age range, gender, nationality, job role, etc. However, the anonymity of participants is maintained throughout the project, and data is anonymized at the point of collection. If participants are required for repeated trials, their datasets can be linked using a coding technique and any identification is kept secure and disposed of as soon as the datasets have been processed. No names are included in the reporting and dissemination of results and data is only be reported at an aggregated level, unless an individual presents a remarkable unique finding that should be reported; if this occurs, anonymity is observed. Drone images are scanned and processed to remove any identifiable data, if any.

The OpenSwarm project has recognized the critical importance of implementing a robust and comprehensive policy for managing incidental findings. This policy, aimed at addressing unforeseen situations, includes a well-defined process for reporting such findings to the ESAB members for advice and guidance. Additionally, it outlines procedures for alerting the appropriate authorities, such as law enforcement agencies, when necessary. By establishing an Incidental Findings Policy, OpenSwarm underscores its commitment to responsible and ethical research practices, ensuring the safeguarding of both project participants and the broader community.

PoC3 “Environmental: Ocean Noise Pollution Monitoring

- ***Concept***

The goal is to develop an automated system that monitors and counts boats in a protected marine area (PMA), and tracks their speed to help manage underwater noise pollution. The proposed system uses smart buoys (the devices): we insert electronics inside each buoy and attach hydrophones to listen to the underwater sounds. The electronics feature a wireless radio and a microcontroller that implements the OpenSwarm networking solution. This allows the buoys to form a 6TiSCH network with a gateway buoy (the edge), which is itself connected to the OpenSwarm cloud running on the Internet. The devices run an AI routine locally to detect boats from the sounds recorded by their hydrophones. They send the timestamped sound signature to the edge, which compares them, computes the location and speed of the boats, before forwarding that information to the OpenSwarm cloud running on a server on the Internet. The cloud monitors the performance of the embedded AI routine on the buoys, and continuously and remotely fine-tunes it. The project demonstrates swarm communication, constrained AI framework and energy-aware swarm operation. It also takes advantage of the OpenSwarm swarm compiler, which allows a user to efficiently program and control the behavior of the devices.

- ***Ethical and Safety compliance***

PoC3 “Environmental: Ocean Noise Pollution Monitoring” involves deploying hydrophones in marine environments to identify the noise of boats, thereby counting them and potentially verifying they do not enter certain areas or exceed certain speed limits. The hydrophones operate AI recognition routines onboard, potentially sending raw sound snippets to a central server for training the AI model. Never is there an attempt at identifying the boat and/or its owner or occupants.

The PoC3 use case "Environmental: Ocean Noise Pollution Monitoring" falls within the scope of environmental protection, particularly concerning European and national regulations regarding protected natural areas, such as Natura 2000 sites, as well as specific prefectural orders for coastal protection and boat traffic. WE have inquired about the legislation concerning scientific research activities in Marine Protected Areas, and will submit an application to the prefecture to obtain the necessary authorizations in accordance with Decree No. 2017-956 of May 10, 2017,[7] setting out the conditions for the implementation of Articles L. 251-1 and following of the Research Code related to marine scientific research. The compliance of PoC3 with the European legislative framework can be demonstrated in several ways:

- European Legislation: Natura 2000 and European Union Law:

Natura 2000 sites are protected natural areas within the European Union, established under the EU Habitats Directive (Directive 92/43/EEC) and the Birds Directive (Directive 79/409/EEC). These sites aim to preserve biodiversity and natural habitats. The introduction of hydrophones to monitor marine noise pollution aligns with the goal of protecting these areas.

PoC3 for marine noise pollution monitoring does not intend to identify boats, their owners, or occupants. It focuses on collecting environmental data, specifically quantifying boat noises in the area. This means that PoC3 respects Natura 2000 legislation by avoiding any harm to marine fauna and their habitats.

- National Legislation: Prefectural Orders for Coastal Protection:

Specific prefectural orders in France can establish strict rules for maritime navigation in sensitive areas, including speed limits for boats and restrictions on access to certain zones. PoC3 aims to monitor compliance with these regulations by quantifying boat noises and verifying whether they enter restricted areas or exceed speed limits.

[7] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034675364

The emphasis is on collecting environmental data without attempting to identify boats, their owners, or occupants. Thus, PoC3 does not violate individuals' privacy or engage in intrusive surveillance, aligning with laws protecting personal privacy.

In our pursuit of developing an automated system to monitor and count boats in protected marine areas (PMAs) while tracking their speed to mitigate underwater noise pollution, the OpenSwarm project places a paramount emphasis on security and responsible research practices. We understand that the implementation of such a system can potentially yield incidental findings, including the capture of sounds originating from human activity. To address these unforeseen situations, OpenSwarm establishes an incidental findings policy. This policy outlines a structured approach for handling unexpected discoveries and sensitive information. In cases where unanticipated data is collected, such as sounds related to human or animal activities within PMAs, the OpenSwarm team can ask follows a well-defined process for reporting such findings to the ESAB members for advice and guidance. Furthermore, we recognize the importance of compliance with legal and regulatory requirements, and we are committed to seeking the necessary permissions and ensuring full compliance with all relevant authorities.

PoC4 “Industrial/Health: EHS in Industrial Production Sites”

- ***Concept***

This use case focuses on the importance of Environment, Health, and Safety (EHS) measures in industrial sites, and the challenge of managing them in the context of increasing automation and collaboration between workers and machines. We equip mobile operators with smart OpenSwarm wearables, and attach smart tags to static and mobile machines/robots in the factory (the devices). These devices form a highly reliable low-power wireless network around a gateway device (the edge). The devices monitor the distance between one another, send those measurements to the edge, which summarizes the information (e.g., removing duplicate information) and forwards that to the OpenSwarm cloud running on a server on the factory’s computer network. This allows the cloud service to closely monitor the distance between workers and machines/robots, and it ready to stop robots to avoid injuries

- ***Ethical and Safety compliance***

PoC4, titled "Industrial/Health: EHS in Industrial Production Sites," is centered on the implementation of innovative safety measures to enhance the well-being of factory workers in industrial production sites. This use-case involves equipping a select group of factory workers with intelligent tags capable of warning them when they are in proximity to robotic actuators, ultimately preventing accidents and improving workplace safety.

To ensure ethical and voluntary participation in PoC4, SIG is actively seeking 12 factory workers who volunteer to participate in the project. Participation is strictly voluntary, and each worker receives an information sheet outlining the project's objectives, operational procedures, potential risks, and their rights. Additionally, participants are required to sign an informed consent form. Templates for these informed consent forms including the objectives of the research activities, risks and benefits, right to withdraw (see annex), addressing relevant issues related to voluntary participation and data protection, are provided by the Data Protection Officer of INRIA in English. To ensure clarity for all parties involved, these templates are translated into German by SIG, as PoC4 is set to take place at a Siemens factory in Germany. This comprehensive procedure is designed to ensure that all participants provide informed and uncoerced consent based on a detailed project information sheet.

It is essential to emphasize that PoC4 does not introduce any additional risk to individuals in industrial environments. All existing and approved safety measures remain in place and cannot be replaced or bypassed during the PoC. The primary objective is to increase the efficiency, reliability, and transparency of existing safety measures, making them more accessible and acceptable to individuals while potentially reducing costs.

Regarding data privacy and security, the project team has no plans to record or request any personal data. The maximum extent of data collection currently considered involves (anonymous) movement trajectories of mobile consumer devices. This data is indistinguishable from the movements of other machines or sensor nodes. In alignment with data protection regulations, Siemens does not record or store personal data. However, in the unlikely event that such data collection becomes necessary, appropriate data protection declarations will be obtained from individuals involved. The project is fully committed to adhering to all applicable data protection regulations.

In conclusion, PoC4 is intended as an enhancement to existing safety measures in industrial environments, with a paramount focus on safety, ethics, and data privacy. There is no inherent danger to individuals in industrial settings, as the project aims to introduce innovations that streamline and improve safety measures. Our objective is to ensure the well-being and safety of factory workers, minimize risks, and create an environment that is both secure and respectful of privacy and data protection regulations. We are dedicated to transparent and ethical practices throughout the project, guided by a commitment to safeguarding individuals and upholding the highest standards of safety and privacy.

The OpenSwarm project hence wants to be extremely attentive to PoC2, PoC3 and PoC4 design and implementation. We implement an ethics and safety framework (ESAB), driven by the Project Coordinator and Executive Committee. We interact with the research ethics committees of each consortium academic partner involved, in particular INRIA’s own committee. These are consulted to ensure ethical principles are followed and respected.

PoC5. “Mobility: Moving Network in Trains”

- ***Concept***

The shift of passengers from air, and goods from road to rail, significantly reduces CO2 emissions. Existing sensor systems for monitoring train components are not suitable for brownfield, and do not adapt to changing operating conditions (e.g. changing the wagons in a train). OpenSwarm creates a reconfigurable network of sensor nodes (devices), which we install and test on an Intercity Express passenger train. These devices monitor the state of key elements of the train, for example the vibration of moving elements. They are synchronized to static or mobile rail infrastructure (edge), which can be present on the train, along a track, or in a train station. The devices monitor the raw data, the edge summarizes the data and sends that to the OpenSwarm cloud, which determines whether any element on the train needs maintenance. This use case validates the concepts of low-power constrained AI, synchronized operation and an easy-to-use high-level programming environment for complex interactions.

- ***Ethical and Safety compliance***

PoC5. “Mobility: Moving Network in Trains” focuses on improving rail transportation sustainability and addressing data privacy and GDPR compliance within this PoC is a critical aspect of our approach. As we gather and process data from the reconfigurable network of sensor nodes installed on Intercity Express trains, ensuring the protection of individuals' privacy and adhering to GDPR regulations is of utmost importance.

To secure GDPR compliance within this PoC, OpenSwarm follows a stringent set of data protection measures:

- Data Minimization: OpenSwarm ensures that only essential data necessary for the specific purposes of the PoC is collected. This minimizes the risk of handling excessive or sensitive personal information.
- Anonymization: Any data that could potentially identify individuals is anonymized or pseudonymized, rendering it impossible to trace back to specific individuals.
- Encryption: All data transmitted between the sensor nodes, edge devices, and the OpenSwarm cloud is encrypted using robust security protocols, ensuring that data remains confidential and secure during transit.
- Access Control: Strict access controls are implemented to limit data access to authorized personnel only. Role-based access control ensures that only individuals with a legitimate need can access and handle sensitive information. Consent and Transparency: OpenSwarm is committed to transparency in data handling. Individuals whose data is collected are informed about the purposes and processing of their data, and their consent is obtained when necessary.
- Data Retention Policy: OpenSwarm establishes a clear data retention policy that specifies the duration for which data is stored. Once data is no longer required for the PoC's purposes, it is promptly deleted.
- Privacy by Design: The OpenSwarm project incorporates privacy principles into its system design from the outset. Data protection is an integral part of the development process.

- Data Protection Officer (DPO): INRIA's Data Protection Officer oversees and ensures GDPR compliance within the project, providing expertise on data privacy matters.

4. Monitoring applicable standards

Our commitment to regulatory monitoring and compliance with applicable standards in the fields of robotics, AI, drones, and data sharing is a critical aspect of OpenSwarm project's success. The approach involves a dynamic and proactive strategy to integrate the evolving regulatory framework into the core activities of the project.

The Project Coordinator (PC) plays a central role in this endeavor by fostering a culture of collaboration and the sharing of best practices among project partners. However, the management of regulatory aspects is primarily overseen by the Scientific Committee, supported by the Project Management Office (PMO) team. When necessary, we also engage expert external bodies to ensure comprehensive compliance during the entire project lifespan.

In the context of hardware security, which is closely tied to the OpenSwarm project's exploitation strategy, we are vigilant in monitoring and complying with relevant European legislative acts. These acts guide OpenSwarm activities not only from a safety perspective but also in terms of industrial standardization and commercialization, such as ISO standards.

Monitoring Legislative Acts

OpenSwarm continuously tracks and adapts to legislative acts at the European level that pertain to its project's activities. This includes acts related to safety, data protection, AI (AI Act) and industry-specific standards.

Designing and implementing an incidental findings policy

Some PoCs might arise the unintentional collection, observation, recording of incidental findings, with ethical, safety and security issues. A policy /process will be designed to discuss how to process the information.

Standardization and Commercialization

Products created as part of the project adhere to industrial and commercial standards, such as the IETF, to ensure that our technological developments align with established norms and best practices.

Internal Ethics consultation & Collaboration

The OpenSwarm project regularly leverages internal expertise on ethical and security issues. This includes OCELER for INRIA, but also IMEC's ethics code of conduct, the KUL's Social and Societal Ethics Committee (SMEC) and the UOS' University Research Ethics Committee (UREC).

Engaging External Expertise

When needed, OpenSwarm project members collaborate with external experts – as part of SAB members and ESAB members for instance – in regulatory compliance and European and national organizations to mitigate risks and ensure that our project remains compliant with evolving standards.

Relying on competent European and national organizations

The OpenSwarm project relies on specific European organizations to stay updated on ethical, security, data protection, and management risks aspects in the fields of AI and robotics. Here are some relevant European organizations for each domain:

Artificial Intelligence (AI) and Robotics

- European Union Agency for Cybersecurity (ENISA): ENISA offers expertise in cybersecurity and can assist in addressing security concerns related to AI and robotics.

- European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG): This group provides guidance on AI ethics and policy at the European level.
- European Robotics Forum (ERF): ERF serves as a platform for discussing and addressing robotics-related challenges, including ethical and safety issues.

Data Protection:

- European Data Protection Board (EDPB): EDPB provides guidance on data protection and privacy matters within the European Union.
- National Data Protection Authorities (DPAs): Each EU member state has its own DPA responsible for enforcing data protection laws at the national level.
- ethical, security, data protection, and drone management risks in the fields of AI and robotics

Drone Management

- European Union Aviation Safety Agency (EASA): EASA establishes regulatory standards and guidelines for the safe operation of drones in European airspace.
- European Union Agency for the Cooperation of Energy Regulators (ACER): ACER focuses on energy-related drone regulations and safety within the energy sector.

The OpenSwarm project relies on national organizations to stay updated on ethical and risk management aspects:

- National Data Protection Authorities: In each European Union country, there exists a National Data Protection Authority (DPA). These bodies are responsible for enforcing national data protection laws and ensuring compliance with the European General Data Protection Regulation (GDPR). They can provide guidance, direction, and information on data management, legal obligations, and best practices in data protection.
- National Civil Aviation Authorities: National civil aviation authorities in each country are responsible for regulating and overseeing civil

aviation, including drone management. They can offer information on national rules regarding drone operations, safety requirements, and necessary permits.

- Maritime authorities: Key entities such as the Maritime Prefectures, Customs authorities, and the French Coast Guard ensure safety, security, and regulatory compliance.
- Information Technology and Cybersecurity Regulatory Authorities: Some countries have specific regulatory authorities for information technology and cybersecurity. These organizations can be consulted for matters related to IT security, cybersecurity, and best security practices in the fields of AI and robotics.
- National Defense Ministries and Organizations: National defense ministries and security organizations may have responsibilities in managing risks associated with AI, robotics, and drones, especially concerning national security. They can provide advice on security requirements and regulations specific to sensitive technologies.
- National Standardization Bodies: National standardization bodies, such as the National Institute for Standardization and Metrology (INM) in France, develop national standards that may be relevant to the fields of AI, robotics, and drone management. They can be consulted to ensure that projects comply with applicable national standards.

When operating in a specific country such as in Portugal, Germany or France, it is essential to become familiar with the relevant national organizations, as they are often the primary authorities responsible for regulating and overseeing activities related to AI, robotics, data protection, and drone management at the national level.

Conclusion

This deliverable presents the OpenSwarm project’s commitment to uphold ethical standards, ensuring safety, and comply with regulations at every stage of development. These principles are not only foundational but also instrumental in achieving our project's objectives. This report represents a comprehensive and vital guide of how we address these critical dimensions effectively.

The primary objective of this report is to provide all project partners with accessible, clear, and pertinent legislative documentation and guidelines from the European Commission (EC) related to ethics, safety, and regulatory aspects. This effort establishes a common understanding and ensures that ethical and safety considerations remain central throughout the project's phases.

Furthermore, this report serves as a dynamic resource continuously updated throughout the project's duration. Responsibility for its maintenance rests with the Project Coordinator and Work Package (WP) leaders, who collaborate to ensure its ongoing relevance. It is readily accessible to all project stakeholders through our SharePoint platform, facilitating easy access and the dissemination of critical guidelines.

Crucially, having these guidelines in advance, prior to implementing the technology across the project's various use cases, is of paramount importance. This proactive approach enables the seamless integration of ethical and safety considerations into our development process, ensuring that our technology aligns with the highest ethical standards and safety protocols. It underscores our unwavering commitment to ethics, safety, and regulatory compliance as we work toward realizing our project's ambitious goals.

References

- Horizon Europe, Work Programme 2023-2024, Digital, Industry and Space, European Commission Decision C(2023) 2178 of 31 March 2023
- The EU Artificial Intelligence Act, June 14, 2023
- Regulations on drones in Europe https://www.easa.europa.eu/en/domains/civil-drones and https://drone-laws.com/drone-laws-in-finland/#Are_drones_allowed_in_Finland
- The Data Act : https://digital-strategy.ec.europa.eu/en/policies/data-act
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- Smart Grid Threat Landscape and Good Practice Guide, ENISA, December 17, 2013
- Environment, Health and Security conditions (EU): European Agency for Safety and Health at work https://osha.europa.eu/en/about-eu-osha/national-focal-points/germany
- Regulations on clean data https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3052