
D8.1

# Management and Quality Plan

## WP8 – Project Management

**SIFIS-HOME**

*Secure Interoperable Full-Stack Internet of Things for Smart Home*

Due date of deliverable: 31/1/2021

Actual submission date: 27/1/2021

*Responsible partner: Intelligentsia Consultants (IC)*

*Editor: Giles Brandon*

Version 1.2

*E-mail address: giles.brandon@intelligentsia-consultants.com*

| Project co-funded by the European Commission within the Horizon 2020 Framework Programme | | |
|---|---|---|
| **DisseminationLevel** | | |
| **PU** | Public | **X** |
| **PP** | Restricted to other programme participants (including the Commission Services) | |
| **RE** | Restricted to a group specified by the consortium (including the Commission Services) | |
| **CO** | Confidential, only for members of the consortium (including the Commission Services) | |


*The SIFIS-HOME Project is supported by funding under the Horizon 2020 Framework Program of the European Commission SU-ICT-2-2020#952652*

**Authors:** Giles Brandon (IC)

**Approved by:** Andrea Saracino (CNR), Marco Tiloca (RISE)

**Reviewed by:** Andrea Saracino (CNR), Marco Tiloca (RISE)

## Revision History

| Version | Date | Name | Partner | Section Affected Comments |
|---|---|---|---|---|
| 0.1 | 10/12/2020 | Initial Structure | IC | All |
| 1.0 | 7/1/2021 | First version | IC | All |
| 1.1 | 14/1/2021 | Ready for review | IC | All |
| 1.2 | 18/1/2021 | Final version | IC | All |

SIFIS-Home aims at providing a secure-by-design and consistent software framework for improving resilience of Interconnected Smart Home Systems at all stack levels. To this end, the framework enables the development of security, privacy aware and accountable applications, algorithms and services, and makes it possible to detect and dynamically react to cyber-attacks and intrusion attempts or violation of user-defined policies, thus increasing control and trust of Smart Home end users.

Smart Home is an emerging application paradigm which has been gaining increasing popularity. Most recently, the Internet of Things (IoT) has been fostering a vision of Smart Home systems, where users can install connectable (smart) devices and appliances that cooperate to automatically manage home services and functionalities. This emerging market is rapidly attracting software developers to produce novel applications and services, to provide additional Smart Home functionalities. However, noticeable barriers and concerns are still present, mainly related to cyber-security and safety within Smart Home systems, as well as to the privacy and integrity of produced and consumed data, most of which are personal and sensitive. Also, many Smart Home devices use custom and proprietary security solutions that do not account for interactions with other devices in the Smart Home system. Plus, developers have to develop applications adaptable to different systems and architectures, where security aspects are often neglected or poorly addressed.

The consortium combines leading industry players in the IoT, telecommunication and cyber-security markets with research and academic institutions, also involved as key contributors to premier international standardisation bodies (e.g. IETF), and having leading roles in the SPARTA, CONCORDIA and CyberSec4Europe projects of the European Cyber Competence Network. SMEs active in the Smart Home and IoT markets and Open Source community complete the consortium.

**LEGAL NOTICE**

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use, which might be made, of the following information.

The views expressed in this report are those of the authors and do not necessarily reflect those of the European Commission.

**© SIFIS-HOME Project 2021**

Reproduction is authorised provided the source is acknowledged

## Executive Summary

This document reports the management and quality plan agreed between the partners of the SIFIS-Home consortium. The presented guidelines leverage on a set of best practices to ensure smooth coordination and collaborations among the partners, clear assignment of tasks and responsibilities, high quality and timely production of the project deliverables.

# Table of Contents

# 1. General Provision

## 1.1. Aim of the Management and Quality Plan

The present Management and Quality Plan is elaborated within the context of the SIFIS-HOME project, a Research and Innovation action funded by the EC's Horizon 2020 Programme (H2020) under SU-ICT-02-2020 Building blocks for resilience in evolving ICT systems.

The main objectives of the Management and Quality Plan (MQP) are to ensure:

- smooth implementation of the project;
- on time completion of the project's tasks, and
- high quality of the project's activities and deliverables.

To this end, and in line with the contractual obligations that the Project Coordinator, CNR, has undertaken with the EC, the MQP provides:

1. an overview of the management structure, roles and responsibilities of the project participants and
2. procedures for the monitoring of progress, quality assurance and overall for the project management, including risk assessment/monitoring and suggestions of fallback solutions.

Compliance with the MQP is essential for the project leader CNR and its consortium partners. The MQP complements but does not replace the Contract with the EC or the Consortium Agreement between project participants.

## 1.2. Structure of the Management and Quality Plan

The MQP is divided into five main chapters plus annexes.

- ***First chapter*:** includes the objectives, a short description of its structure, as well as the control procedures (preparation, approval, amendments, distribution, etc.).
- ***Second chapter*:** the management structure is presented together with the roles and responsibilities of the participants.
- ***Third chapter*:** the control of documents – deliverables of the project is analysed (quality control, monitor changes, management of records / files, etc.).
- ***Fourth chapter*:** internal communication (between project partners) issues are presented in short; issues regarding external communication (formal communication with the EC, communication with coordinators / contractors of similar projects or Research and Innovation Action projects under the targeted areas, other communication with EC services, etc.) are addressed.
- ***Fifth chapter*:** describes the way that project planning and monitoring is performed (tasks, sub-tasks, checks, etc.).

### 1.3. Control of the Management and Quality Plan

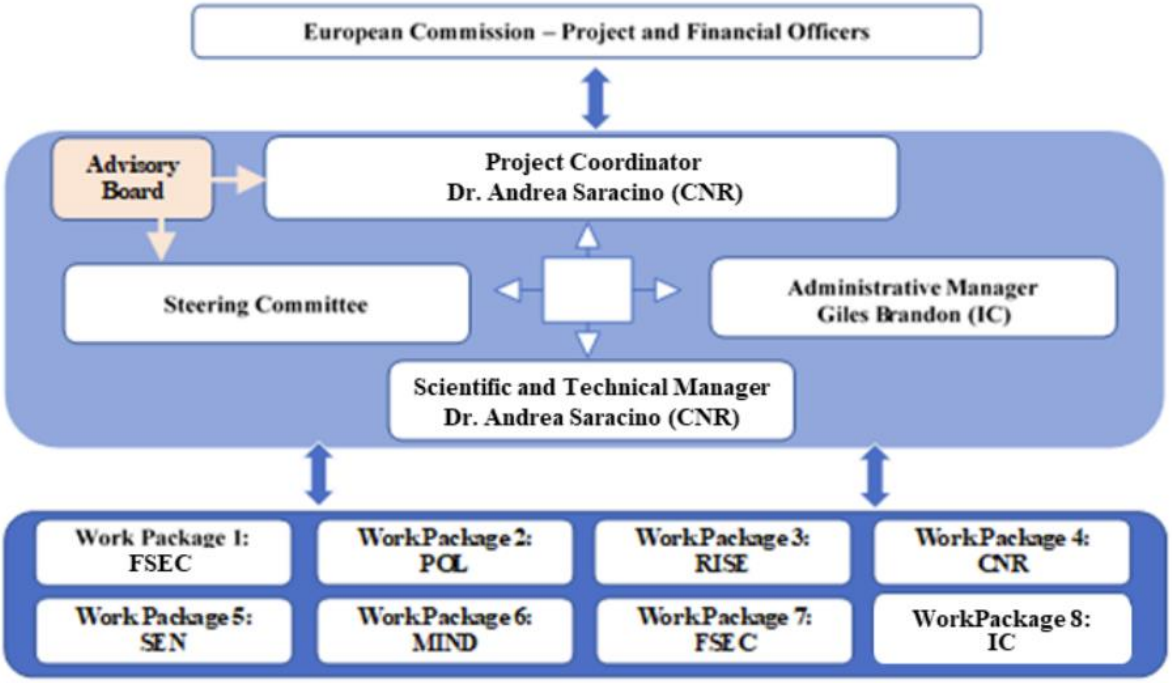
The MQP is produced by the partner Intelligentsia Consultants (IC) under the supervision of the Project Coordinator, CNR, and approved by the Steering Committee. The partner IC and Project Coordinator, CNR,are responsible for updating or changing the MQP, when necessary. The two partners are also responsible for reviewing periodically the MQP and recommending relevant changes. Any changes are marked appropriately (briefly on the cover page of the MQP and the new or modified text will also be highlighted accordingly). After each change, a new version of the MQP will be distributed to all project participants.

Before the new version is put into force, it will be sent for comments by the Project Coordinator to the Steering Committee. The Project Coordinator will take into account the comments of the Steering Committee, finalise the new version of the MQP, and send it to all project members in electronic form.

# 2. Organisational Issues

## 2.1. Management Structure

The project management structure is presented in the following diagram:




## 2.2. Roles and Responsibilities

The selected structure consists of a Project Coordinator, Steering Committee, Administrative Manager, Scientific and Technical Manager, and Advisory Board. The Steering Committee will ensure that activities are properly monitored, coordinated and kept on budget with Work Package leaders having scientific and technical responsibility with project milestones being used as review checkpoints. The Steering Committee will hold management meetings online every month using Teams and face-to-face every six months. The above structure is appropriate for the consortium size, budget, timescale and complexity of this project.

The Steering Committee will be comprised of one representative from each member of the Consortium and will oversee the risk management programme (via the Scientific and Technical Manager) and have ultimate authority in resolving any issues (scientific, technical, contractual, commercial or otherwise) that may arise.

We have established that the six-monthly face-to-face management and technical meetings will require the participation of all consortium partners. If this is not possible, the Project Coordinator reserves the right to postpone the meeting.

At Steering Committee meetings, an assessment will be made of progress against scientific and technical objectives and all consortium members are expected to make a contribution in project management, decision-making and validation of results as the project progresses. Regular communication will be positively encouraged, whether formal or informal. The Steering Committee will review milestones and agree scientific, technical and management actions for the next period. These meetings will also be used to raise exploitation and IPR issues for discussion by the partners and the Scientific and Technical Manager.

All meetings will have well prepared agendas and will be accurately documented. WP leaders will communicate regularly with the Project Coordinator with regard to resource planning and the timely delivery of reports and results. Each WP leader will communicate regularly with the consortium members involved in their work package activities and the use of telephone, email and video-conferencing will be encouraged.

WP leaders will be responsible for their technical activities and will inform the Scientific and Technical Manager and Project Coordinator, if an unforeseen event occurs which has the potential to delay or prevent an objective being achieved. The WP leader, Scientific and Technical Manager and Project Coordinator will jointly review the issue. The issue will be recorded in the risk log, together with risk mitigation measures, which will be maintained to monitor developments. If the issue cannot be resolved, then the Work Package may need to be modified and new technical objectives set. The Scientific and Technical Manager will make recommendations to the Steering Committee, and changes to the work plans will require approval by the Steering Committee. Contingency plans will be implemented by the relevant technical WP leader and significant changes to the work plan will be relayed to the EC. At management and technical meetings, evaluation of achievements will be reviewed, enabling assessment of the cumulative effect of failures upon the final set of project objectives. This overview will form a key basis for effective project control.

## Table: Roles & Responsibilities per Partner

| Partners | Country | Responsibilities in SIFIS-HOME |
|---|---|---|
| **CNR** | Italy | **Overall Project Co-ordinator, Scientific and Technical Manager, and Leader of WP4 Privacy-Aware Analytics for Security and Services**<br>**a) Overall responsibility for Security and Privacy Goals (Task 1.2).**<br>**b)** Support to other tasks in WP1 Distributed System Architecture.<br>**c) Overall responsibility for Policy-based Software Security Compliance (Task 2.3).**<br>d) Support to other tasks in WP2 Guidelines and Procedures for System and Software Security and Legacy Compliance.<br>**e) Overall responsibility for Dynamic Multi-Domain Security and Safety Policy Handling (Task 3.3).**<br>**f)** Support to other tasks in WP3 Network and System Security.<br>**g) Overall responsibility for Multi-level Anomaly and Misbehaviour Detection and Prevention (Task 4.1).**<br>**h) Overall responsibility for Privacy Aware Speech Recognition and Smart Service Analytics (Task 4.4).**<br>**i)** Support to other tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>**j)** Support to tasks in WP5 Integration, Testing and Demonstration.<br>**k)** Support to tasks in WP6 Smart Home Use Case.<br>**l) Overall responsibility for Dissemination (Task 7.1).**<br>**m)** Support to other tasks in WP7 Dissemination, Standardization and Exploitation.<br>**n) Overall responsibility to collate deliverables, milestones and reports (Task 8.1).**<br>**o) Overall responsibility to ensure communication between partners (Task 8.3).**<br>**p) Overall responsibility to manage scientific and technical activities (Task 8.4).**<br>**q)** Support to other tasks in WP8 Project Management. |
| **ERI** | Sweden | a) Support to tasks in WP1 Distributed System Architecture.<br>b) Support to tasks in WP3 Network and System Security.<br>c) Support to tasks in WP5 Integration, Testing and Demonstration.<br>d) Support to tasks in WP6 Smart Home Use Case.<br>e) Support to tasks in WP7 Dissemination, Standardization and Exploitation.<br>f) Support to tasks in WP8 Project Management. |
| **FSEC** | Finland | **Leader of WP1 Distributed System Architecture and WP7 Dissemination, Standardization and Exploitation.** |

| Partners | Country | Responsibilities in SIFIS-HOME |
|---|---|---|
| | | **a) Overall responsibility for System Requirements Elicitation (Task 1.1).**<br>**b) Overall responsibility for Definition of Secure Component Design, System Architecture, and Intercommunication (Task 1.3).**<br>c) Support to other tasks in WP1 Distributed System Architecture.<br>d) Support to tasks in WP2 Guidelines and Procedures for System and Software Security and Legacy Compliance.<br>e) Support to tasks in WP3 Network and System Security.<br>f) Support to tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>g) Support to tasks in WP5 Integration, Testing and Demonstration.<br>h) Support to tasks in WP6 Smart Home Use Case.<br>**i) Overall responsibility for Business Planning and Commercial Exploitation (Task 7.3).**<br>j) Support to other tasks in WP7 Dissemination, Standardization and Exploitation.<br>k) Support to tasks in WP8 Project Management. |
| **INT** | Germany | a) Support to tasks in WP1 Distributed System Architecture.<br>b) Support to tasks in WP2 Guidelines and Procedures for System and Software Security and Legacy Compliance.<br>c) Support to tasks in WP3 Network and System Security.<br>d) Support to tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>e) **Overall responsibility for Testbed Design (Task 5.1).**<br>f) Support to other tasks in WP5 Integration, Testing and Demonstration.<br>g) Support to tasks in WP6 Smart Home Use Case.<br>h) Support to tasks in WP7 Dissemination, Standardization and Exploitation.<br>i) Support to tasks in WP8 Project Management. |
| **IC** | Luxembourg | **Administrative Manager, Leader of WP8 Project Management.**<br>**a) Overall responsibility tomanage legal, contractual, financial, ethical and administrative matters (Task 8.2).**<br>**b) Overall responsibility to organise project steering committee meetings (Task 8.5).**<br>c) Support to other tasks in WP8 Project Management. |
| **LUM** | Italy | a) Support to tasks in WP1 Distributed System Architecture.<br>**b) Overall responsibility for Dynamic Code Quality/Security Evaluation (Task 2.2).**<br>c) Support to other tasks in WP2 Guidelines and Procedures for System and Software Security and Legacy Compliance.<br>d) Support to tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>**e) Overall responsibility for Evaluation and Validation (Task 5.3).**<br>**f) Support to other tasks in WP5 Integration, Testing and Demonstration.**<br>**g) Overall responsibility for Experimental Evaluation and Validation (Task 6.4).**<br>h) Support to other tasks in WP6 Smart Home Use Case.<br>i) Support to tasks in WP7 Dissemination, Standardization and Exploitation.<br>j) Support to tasks in WP8 Project Management. |
| **MIND** | Italy | **Leader of WP6 Smart Home Use Case.**<br>a) Support to tasks in WP1 Distributed System Architecture.<br>b) Support to tasks in WP2 Guidelines and Procedures for System and Software Security and Legacy Compliance.<br>c) Support to tasks in WP3 Network and System Security.<br>d) Support to tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>e) Support to tasks in WP5 Integration, Testing and Demonstration.<br>f) **Overall responsibility for Use Case Requirements Elicitation (Task 6.1).**<br>g) **Overall responsibility for Use Case Design and Implementation (Task 6.3).**<br>h) Support to other tasks in WP6 Smart Home Use Case.<br>i) Support to tasks in WP7 Dissemination, Standardization and Exploitation. |

| Partners | Country | Responsibilities in SIFIS-HOME |
|---|---|---|
| | | j) Support to tasks in WP8 Project Management. |
| **RIO** | Finland | a) Support to tasks in WP1 Distributed System Architecture.<br>b) Support to tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>c) Support to tasks in WP5 Integration, Testing and Demonstration.<br>**d) Overall responsibility for Use Case Security and Privacy Goal Refinement (Task 6.2).**<br>e) Support to other tasks in WP6 Smart Home Use Case.<br>f) Support to tasks in WP7 Dissemination, Standardization and Exploitation.<br>g) Support to tasks in WP8 Project Management. |
| **SEN** | Sweden | **Leader of WP5 Integration, Testing and Demonstration.**<br><br>a) Support to tasks in WP1 Distributed System Architecture.<br>b) Support to tasks in WP3 Network and System Security.<br>c) Support to tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>d) **Overall responsibility for Component Implementation, Integration and Deployment (Task 5.2).**<br>e) Support to other tasks in WP5 Integration, Testing and Demonstration.<br>f) Support to tasks in WP6 Smart Home Use Case.<br>g) Support to tasks in WP7 Dissemination, Standardization and Exploitation.<br>h) Support to tasks in WP8 Project Management. |
| **RISE** | Sweden | **Leader of WP3 Network and System Security.**<br><br>a) Support to tasks in WP1 Distributed System Architecture.<br>b) Support to tasks in WP2 Guidelines and Procedures for System and Software Security and Legacy Compliance.<br>c) **Overall responsibility for Secure, Interoperable and Robust Communication (Task 3.1).**<br>d) **Overall responsibility for Security Lifecycle Management (Task 3.2).**<br>e) Support to other tasks in WP3 Network and System Security.<br>f) Support to tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>g) Support to tasks in WP5 Integration, Testing and Demonstration.<br>h) Support to tasks in WP6 Smart Home Use Case.<br>i) **Overall responsibility for Standardisation (Task 7.2).**<br>j) Support to other tasks in WP7 Dissemination, Standardization and Exploitation.<br>k) Support to tasks in WP8 Project Management. |
| **CEN** | Finland | a) Support to tasks in WP1 Distributed System Architecture.<br>b) Support to tasks in WP3 Network and System Security.<br>c) **Overall responsibility for Network Intrusion Detection (Task 4.2).**<br>d) Support to other tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>e) Support to tasks in WP5 Integration, Testing and Demonstration.<br>f) Support to tasks in WP6 Smart Home Use Case.<br>g) Support to tasks in WP7 Dissemination, Standardization and Exploitation.<br>h) Support to tasks in WP8 Project Management. |
| **POL** | Italy | **Leader of WP2 Guidelines and Procedures for System and Software Security and Legacy Compliance.**<br><br>a) **Overall responsibility for Definition of Secure Development APIs (Task 1.4).**<br>b) Support to other tasks in WP1 Distributed System Architecture.<br>c) **Overall responsibility for Guidelines for IoT Software Development and definition of Security and Privacy Metrics (Task 2.1).**<br>d) **Overall responsibility for Legal Aspects and GDPR Compliance (Task 2.4).**<br>e) Support to other tasks in WP2 Guidelines and Procedures for System and Software Security and Legacy Compliance.<br>f) **Overall responsibility for Analytics for policy enforcement (Task 4.3).**<br>g) Support to other tasks in WP4 Privacy-Aware Analytics for Security and Services.<br>h) Support to tasks in WP5 Integration, Testing and Demonstration. |

| Partners | Country | Responsibilities in SIFIS-HOME |
|---|---|---|
| | | i) Support to tasks in WP6 Smart Home Use Case.<br>j) Support to tasks in WP7 Dissemination, Standardization and Exploitation.<br>k) Support to tasks in WP8 Project Management. |

### 2.3. Key members of the SIFIS-HOME team

The Steering Committee is presented in the table below:

| Partner Number | Partner | Key Person | Additional Responsibility |
|---|---|---|---|
| 1 | CNR | Andrea Saracino | Project Coordinator, Scientific and Technical Manager |
| | | Paolo Mori | WP4 leader |
| 2 | ERI | Göran Selander | |
| 3 | FSEC | Marko Komssi | WP1 leader |
| | | Sini Olkanen | WP7 leader |
| 4 | INT | Max Dmitrichenko | |
| 5 | IC | Giles Brandon | Administrative Manager, WP8 leader |
| 6 | LUM | Luca Barbato | |
| 7 | MIND | Domenico De Guglielmo | WP6 leader |
| 8 | RIO | Samuli Stenudd | |
| 9 | SEN | Håkan Lundström | WP5 leader |
| 10 | RISE | Marco Tiloca | WP3 leader |
| 11 | CEN | Joni Jämsä | |
| 12 | POL | Luca Ardito | WP2 leader |

### 2.4. Advisory Board

An Advisory Board will provide additional expert industrial advice to the Project Coordinator and the Steering Committee to help increase the relevance and exploitation of the project results. The meetings of the Advisory Board will be held in conjunction with the consortium meetings (probably on M9, M18 and M30). It is anticipated the Advisory Board will include the following members:

- Dr. Francesco Di Cerbo, Research, SAP Labs, France
- Prof. Olaf Maennel, Taltech (Partner in the ECHO European cybersecurity competence network)
- Dr. Massimo Valla, TIM, Italy

# 3. Records – Control of Deliverables

## 3.1. Records

Throughout the project duration the Project Coordinator and the project participants should maintain records in electronic and / or paper form. The Project Coordinator has the responsibility of maintaining the central records of the Project.

These records include:

- Contractual documents and correspondence with the EC;
- Correspondence with the project participants;
- Deliverables (including the MQP (all versions));
- Meeting presentations, minutes and other related material;
- Project reports (internal and external);
- Other important documents.

**Important remarks**

- Each project participant should maintain records of all documents that concern them or for which they are responsible for.
- Both the Project Coordinator and the participants are responsible for storing and maintaining in such a way that they are protected against damage, deterioration or loss.
- Especially with respect to the electronic records (files), all partners should perform back-ups regularly.

## 3.2. Control of Deliverables

Each participant should deliver on time the project deliverables which they are responsible for, to the Project Coordinator, according to the required specifications and format.

The (internal) approval of the deliverables is considered done after the successful completion of the quality control. The quality control is performed by the respective Reviewers.

If there are remarks (comments) then the deliverable is returned to the responsible partner for improvement. The deliverable is then re-examined to ensure that all remarks (comments) have been incorporated. **The Project Coordinator submits to the EC the deliverable after its internal approval.**

Each deliverable is examined with respect to its:

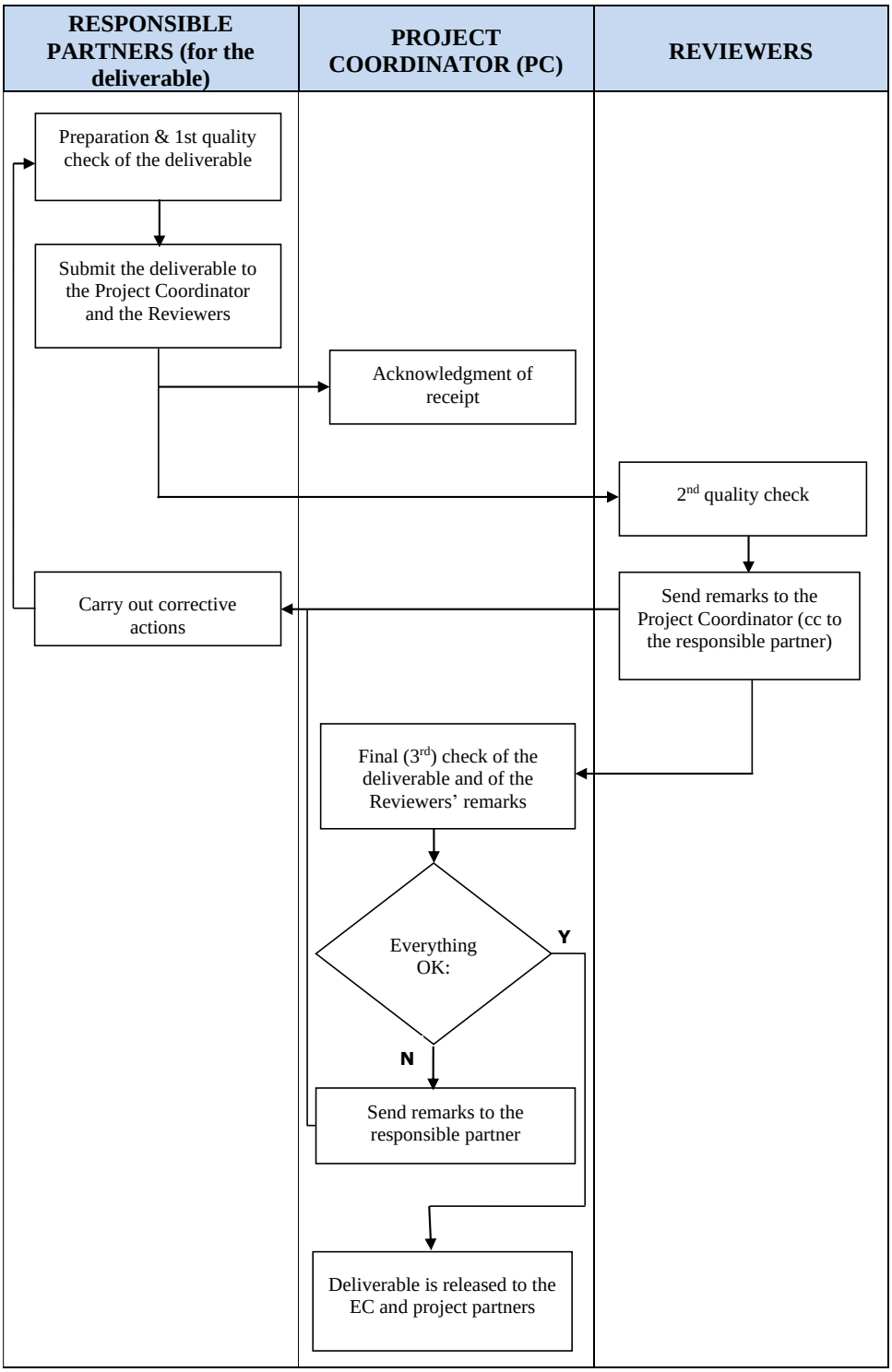
- *Quality* (acceptable level that meets the specifications – standards that have been set (where relevant) and based on the judgment of the WP leader / Project Coordinator),
- *Content* (to what extent the deliverable includes all the required information),
- *Data – information* (cross-check where necessary to ensure that no contradictions or overlaps between deliverables exist),
- *Accordance with the timetable* (delivery date has to be in line with the one agreed),
- *Attached documentation* (check if all necessary accompanied documents are attached),
- «*Structure, format and appearance*» (where necessary and especially with respect to the deliverables' model / template – to achieve uniformity of all project documents).

As a rule, to ensure that there is enough time for the quality control of each deliverable the respective **deadlines should be set well before the contractual deadline**. To this end a deliverable production and review calendar has been agreed among partners and is reported here as Annex II.

Each partner is responsible for the quality of its deliverables. The Project Coordinator is overall responsible for the quality of the whole project.

Where possible, all deliverables are prepared in a standard format based on the template of the present document.

The following diagram presents schematically the procedure of control and approval for deliverables.



# 4. Project Communication

## 4.1. Internal communication

Communication between the Project Coordinator and the project participants takes place with any convenient and available means (e-mail, telephone, Teams, meetings, etc.). Internal communication can be divided into formal and informal communication. The Project Coordinator has the main responsibility of ensuring smooth and effective internal communication.

The contact details of the partners are kept in separate Google Docs tables (see Annex III). In the event of any change in the contact details or in the project team, partners should notify the Project Coordinator, who will then inform the rest of the partners (and if necessary the EC).

Communication of important issues (e.g. sending deliverables, planning meetings, etc.), as well as any formal communication (e.g. project meetings, etc.) should be documented – written (e.g. preparing meeting minutes, maintain an electronic (e.g. emails) or paper copy record, etc.).

Informal communication taking place between the Project Coordinator, the WP leaders and the partners (through telephone, informal emails, etc.) need to be documented as well in case they have a significant impact on the project execution. The Project Coordinator and the WP Leaders are expected to communicate regularly with the project participants so as to follow closely the project and WP progress and identify on time potential deviations.

Close collaboration - communication between project partners is necessary especially in the cases where they have to collaborate to perform specific tasks.

## 4.2. External communication

### Communication with the EC

The Project Coordinator is solely responsible for the communication with the EC responsible Project Officer with respect to the project. The project participants should not contact the EC Project Officer without informing prior and in written the Project Coordinator. In such a case, the Project Coordinator is kept fully informed about the content of the communication and should be given explicit means to actively follow it, e.g. as CC-included when emails are used.

The Project Coordinator has the responsibility of submitting to the EC all the project reports and deliverables. He also provides the EC with any additional information and / or clarification (that have been requested by the EC). The Project Coordinator keeps all partners informed about any important communication with the EC.

### Communication with Third Parties

Contractors may and should communicate with third parties (e.g. national authorities, research organizations, National Contact Points, other EU-funded projects, EC services, etc.) within the context of the project. In all external communications a reference to the project should be made (e.g. acronym, EU programme / Theme, contract No).

**Complaints - Disputes**

The Steering Committee members and the WP Leaders will notify immediately the Project Coordinator for any events or circumstances that may significantly affect the performance of the work executed in their WP (e.g. suggestions for considerable improvements and modifications – changes in the methodology, timetable and task allocation, potential delays, disputes between partners, etc.).

WP Leaders will try to resolve any such event – circumstance that occurs under their work packages, and keep the Project Coordinator informed. In case they cannot find a solution or reach a consensus, the Project Coordinator will be responsible to resolve the issue by consulting all partners involved - affected. Where necessary (e.g. requirement of the Contract with the EC) the Project Coordinator will inform the EC and requests its feedback.

# 5. Work Plan, Monitoring and Control

## 5.1. Work Plan

The project work-plan is divided into Work Packages (WP) and each WP into Tasks, which may be divided in sub-tasks. The work plan includes:

- the WP and respective Tasks and sub-tasks,
- the duration, start and end dates for each Task and WP as whole,
- the responsible partner and the partners involved,
- the respective deliverables [external (that means the deliverables mentioned in Annex I of the Contract with the EC) and internal].

Any modification (with does not affect the overall course of the project) in the work plan is approved by the Project Coordinator. Any significant change should be in line with the contractual obligations and the rules of the EC.

The Project Coordinator is overall responsible for the successful implementation of the project work plan.

**Important notice**
In case the project partners fail to send a deliverable on time to the EC, the Project Coordinator should inform the EC before the deadline, justify the delay and suggest a new deadline. For this reason all participants should provide early warnings (about delays) to the respective WP leaders and the WP leaders to the Project Coordinator.

## 5.2. Project Meetings

Seven face-to-face project meetings are anticipated. For more details see Annex I of the Contract (WP1 description):

- One (1) kick-off meeting
- Five (5) interim project meetings
- One (1) final meeting
- Two (2) periodic review meetings with the EC (M18, M36), in conjunction with project meetings when possible

The Project Coordinator is responsible for the preparation of minutes for all project meetings. The meeting minutes are sent to all partners for approval.

## 5.3. Progress Monitoring

**9-month Progress Reports:** Every 9 months a short progress report will be prepared by each project participant to summarise the work progress in the WPs/Tasks for which they are responsible as well as the costs incurred in the reporting period (see model report in Annexes). All participants are expected to contribute to the scientific and technical targets as reported in the Impact section of Annex 1, including the exploitation and dissemination targets (please refer to indicators at the end of Section 2.2).

Based on the individual progress reports the Project Coordinator will elaborate the respective ‘aggregate 9-month Progress Report’ for the whole project. The aggregate 9-month Progress Report will be

incorporated into the major reports to the EC when the time of their elaboration coincides (in month 18, the mid-term progress report).

**Quarterly progress reports** will be communicated orally or through informal email exchange from each WP leader to the Project Coordinator. Quarterly reports will provide the Project Coordinator with a summarised unofficial picture of project's progress.

All project internal reports should be sent to the Project Coordinator no later than 15 days after the end of the respective reporting period. The Project Coordinator should provide comments within 15 days from the date of submission. If no comment is sent within this period, the submitted report is considered accepted.

### 5.4. Reports to the EC

The Project Coordinator is overall responsible for the preparation and on time submission of the project periodic reports to the EC. All partners provide the necessary input for the preparation of the reports.

Three such reports are required: the intermediate reports (period 1: M1-M18, period 2: M19-M36) and the final project report, combining the two intermediate reports.

### 5.5. Risk Management

The table below summarises the main internal & external risks and related mitigation measures. For each risk, the table also indicates: the probability (likelihood of occurrence); the impact (severity upon risk materialisation), with values: L=Low, M=Medium, H=High; and the related WP(s).

| Description of risk | Prob. | Imp. | WP | Proposed risk-mitigation measures |
|---|---|---|---|---|
| Technology replacement during the project runtime | L | L | WP1<br>WP3<br>WP4<br>WP5 | The consortium will constantly and closely observe the evolution of technologies related and relevant to the project during its whole runtime.<br>Also, the project will itself develop concepts, mechanisms and solutions built on current standards and recommendations. |
| Missing competences in the consortium when facing technical challenges | L | M | WP2<br>WP3<br>WP4 | The competences and complementary skills of all the successfully experienced partners make it possible to overcome many unforeseeable potential problems. |
| Implementation of analysis mechanisms needed to address project requirement takes longer than expected. | L | H | WP4 | The consortium will select algorithms and mechanisms whose implementation time can be easily and accurately estimated, also defining or exploiting alternative simpler mechanisms as safe fall-back. |
| Datasets needed for training and testing cannot be retrieved in a sufficient amount. | M | M | WP4 | Techniques for data oversampling, based mainly on interpolation, will be used to increase the knowledge base. Moreover, public available dataset accessible through public knowledge bases such as Kaggle or UCI ML-repository will be used to supply missing data. |
| The physical testbed may not provide a complete environment to fully run all defined test cases to verify all security aspects of the developed components. | H | M | WP5 | Carefully define reasonable test cases.<br>Close collaboration between WP5 and WP 2-4<br>When applicable, emulate IoT devices, threats etc.<br>Accept that some aspects cannot be validated in the physical test bed, but instead validated by other methods like SWOT. |

| | | | | |
|---|---|---|---|---|
| It is not possible to retrieve the needed hardware due to supplier ceasing activity. | L | M | WP5, WP6 | Hardware components needed for deployment of WP6 are provided by major international companies which are unlikely to stop selling the needed products before the end of the project. If it happens, the hardware will be replaced with the one of competitors of current supplier. |
| Users are not willing to participate to the validation phase. | M | M | WP6 | Prospective users will be contacted from the early stages of the pilot use case design involving them in the whole process, to motivate them in the participation of all phases, including validation. |
| Standardization work is delayed | H | L | WP7 | Once the project has developed a concept or approach we wish to contribute to standardization, partners with a long-term commitment and successful track record in standardization work will be able to drive these approaches beyond the scope and runtime of the project. |
| Project results does not create enthusiasm in consumers, partners, and IoT industry. | M | H | WP7 | Project hypotheses are iteratively validated and pivoted to match the market needs. The Industrial Partners will also spend special effort in marketing the project results in the selected media. |
| Conflicts among partners. | L | H | WP8 | Solve conflicts amicably and according to legal framework in place (consortium agreement and grant agreement). |
| Change/removal of key persons in the project team. | M | M | WP8 | Ensure smooth handover to successors by efficient debriefing and transfer of project documentation. |

In case of major deviations appearing in the project's work plan, targets or objectives, the Project Coordinator will examine corrective actions. In case of non-conformities, the Project Coordinator will implement mitigation measures.

The Project Coordinator (supported by the Steering Committee) will elaborate mitigation measures for the major risks and uncertainties of the project.

Each WP leader should communicate early to the Project Coordinator any identified problems and risks arising for each Task. In this way, the consortium will be able to develop appropriate counter-actions at an early stage.

# Annex I: List of Relevant / Complementary Documents

| Title of Document | Remark |
|---|---|
| **Official Documents** | |
| Contract with the EC and relevant Annexes | Signed by the Project Coordinator. |
| Consortium Agreement | Signed by all partners at the beginning of the project |
| H2020 Online Manual | https://ec.europa.eu/research/participants/docs/h2020-funding-guide/index_en.htm |
| **Internal Documents** | |
| Deliverables list and quality control review of deliverables | See Annex II and SIFIS-Home_Deliverable_Review_Calendar.docx |
| Project Team Contact List | See Annex III and SIFIS-Home_Contact_Persons.docx |
| Management progress reports | See SIFIS-Home_Mgt_Progress.docx (to be completed by each partner every 9-months) |
| Person-months table | See SIFIS-Home_PMs.xlsx (to be completed by each partner every 9-months) |
| Costs table | See SIFIS-Home_Costs.xlsx (to be completed by each partner every 9-months) |
| List of publications | See SIFIS-Home_List_of_Publications.xlsx<br>(to be completed by each partner on a regular basis) |
| Deliverables template | See SIFIS_DelivTemp.docx<br>(to be used for elaborating project deliverables) |

# Annex II: Deliverable Review Calendar

| Deliv. No. | Deliverable name | WP No. | Lead Beneficiary | Type | Diss. level | EC Due date | Deliv. Production deadline | Partner Deliv. Reviewers | Deliv. Review deadline |
|---|---|---|---|---|---|---|---|---|---|
| D7.7 | SIFIS-Home Website | 7 | CEN | Websites, patents filling, etc. | PU | M4 | 15/01/2021 | POL, RIO | 22/01/2021 |
| D8.1 | Management & Quality Plan. | 8 | IC | ORDP | PU | M4 | 15/01/2021 | CNR, RISE | 22/01/2021 |
| D1.1 | Initial Architecture Requirements Report | 1 | FSEC | Report | PU | M6 | 01/03/2021 | SEN, INT | 15/03/2021 |
| D2.1 | Report on Security and Privacy Metrics. | 2 | POL | Report | PU | M6 | 01/03/2021 | RISE, MIND | 15/03/2021 |
| D3.1 | Analyses and feedback on architecture requirements and goals | 3 | RISE | Report | PU | M8 | 30/04/2021 | POL, CEN | 15/05/2021 |
| D4.1 | Analyses and feedback on architecture requirements and goals | 4 | CNR | Report | PU | M8 | 30/04/2021 | FSEC, ERI | 15/05/2021 |
| D1.2 | Final Architecture Requirements Report | 1 | FSEC | Report | PU | M12 | 01/09/2021 | RIO, RISE | 15/09/2021 |
| D1.3 | Initial Component, Architecture, and Intercommunication Design | 1 | FSEC | Report | PU | M12 | 18/08/2021 | POL, ERI | 08/09/2021 |
| D2.2 | Preliminary Developer guidelines. | 2 | POL | Report | PU | M12 | 18/08/2021 | CEN, FSEC | 08/09/2021 |
| D2.6 | Initial Report on Legal and Ethical Aspects. | 2 | POL | Report | PU | M18 | 01/03/2022 | CEN, RIO | 15/03/2022 |
| D3.2 | Preliminary report on Network and System Security Solutions | 3 | RISE | Report | PU | M18 | 15/02/2022 | CNR, MIND | 08/03/2022 |
| D4.2 | Initial Design and Development of Privacy Aware Analytics for Secure Services | 4 | CNR | Report | PU | M18 | 15/02/2022 | RISE, ERI | 08/03/2022 |
| D7.1 | Preliminary Dissemination Report. | 7 | CNR | Report | PU | M18 | 01/03/2022 | INT, MIND | 15/03/2022 |
| D7.2 | Preliminary Standardization Report | 7 | RISE | Report | PU | M18 | 01/03/2022 | CNR, FSEC | 15/03/2022 |
| D7.3 | Preliminary Business and Exploitation Plan | 7 | F-SEC | Report | PU | M18 | 01/03/2022 | ERI, CEN | 15/03/2022 |
| D8.2 | Period 1 Management Reports | 8 | CNR | Report | PU | M18 | 01/03/2022 | IC, RISE | 15/03/2022 |
| D5.1 | First version of SIFIS-Home testbed | 5 | INT | Dem. | PU | M20 | 15/04/2022 | MIND, CEN | 08/05/2022 |
| D6.1 | Pilot Use Case requirements | 6 | MIND | Report | PU | M20 | 30/04/2022 | CNR, FSEC | 15/05/2022 |
| D1.4 | Final Component, Architecture, and Intercommunication Design | 1 | FSEC | Report | PU | M24 | 18/08/2022 | SEN, POL | 08/09/2022 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| D2.3 | First Version of Developer tools. | 2 | POL | Dem. | PU | M24 | 18/08/2022 | CNR, INT | 08/09/2022 |
| D5.2 | First version of SIFIS-Home Security Architecture Implementation | 5 | SEN | Dem. | PU | M24 | 18/08/2022 | MIND, RIO | 15/09/2022 |
| D6.2 | First version of Pilot Use Case implementation | 6 | MIND | Dem. | PU | M28 | 15/12/2022 | POL, ERI | 15/01/2023 |
| D2.4 | Final Developer guidelines | 2 | POL | Report | PU | M30 | 01/03/2023 | RISE, FSEC | 15/03/2023 |
| D2.5 | Final Version of Developer tools | 2 | POL | Dem. | PU | M30 | 01/03/2023 | RIO, INT | 15/03/2023 |
| D2.7 | Final Report on Legal and Ethical Aspects | 2 | POL | Report | PU | M30 | 01/03/2023 | IC, ERI | 15/03/2023 |
| D5.3 | Final version of SIFIS-Home testbed | 5 | SEN | Dem. | PU | M30 | 01/03/2023 | CEN,SEN | 15/03/2023 |
| D6.3 | Refined Pilot Use Case requirements | 6 | MIND | Report | PU | M30 | 01/03/2023 | CNR, FSEC | 15/03/2023 |
| D3.3 | Final report on Network and System Security Solutions | 3 | RISE | Report | PU | M33 | 18/05/2023 | INT, MIND | 08/06/2023 |
| D4.3 | Final Development of Privacy Aware Analytics for Secure Services | 4 | CNR | Report | PU | M33 | 18/05/2023 | POL, RIO | 08/06/2023 |
| D5.4 | Final version of SIFIS-Home Security Architecture Implementation | 5 | SEN | Dem. | PU | M33 | 01/06/2023 | ERI, RISE | 15/06/2023 |
| D6.4 | Final version of Pilot Use Case implementation | 6 | MIND | Dem. | PU | M36 | 01/09/2023 | CEN, INT | 15/09/2023 |
| D7.4 | Final Dissemination Report. | 7 | CNR | Report | PU | M36 | 10/09/2023 | SEN, MIND | 17/09/2023 |
| D7.5 | Final Standardization Report | 7 | RISE | Report | PU | M36 | 10/09/2023 | CNR, FSEC | 17/09/2023 |
| D7.6 | Final Business and Exploitation Plan | 7 | F-SEC | Report | PU | M36 | 01/09/2023 | RISE, INT | 15/09/2023 |
| D8.3 | Period 2 Management Reports | 8 | CNR | Report | PU | M36 | 01/09/2023 | IC, POL | 15/09/2023 |

# Annex III: Project Team Contact List

| Partner | Contact Person(s) | Email |
|---|---|---|
| CNR | Andrea Saracino (Coordinator) | andrea.saracino@iit.cnr.it |
| | Paolo Mori (WP4 leader) | paolo.mori@iit.cnr.it |
| | Giacomo Giorgi | giacomo.giorgi@iit.cnr.it |
| | Lucia Ghelardi (financial and reporting) | lucia.ghelardi@iit.cnr.it |
| ERI | Göran Selander | goran.selander@ericsson.com |
| | Francesca Palombini | francesca.palombini@ericsson.com |
| FSEC | Marko Komssi (WP1 leader) | marko.komssi@f-secure.com |
| | Sini Olkanen (WP7 leader) | Sini.Olkanen@f-secure.com |
| | Mika Lehtinen | mika.lehtinen@f-secure.com |
| | Sean Robinson | sean.robinson@f-secure.com |
| INT | Max Dmitrichenko | max.dmitrichenko@intel.com |
| | Fredrick Odhiambo | fredrick.odhiambo@intel.com |
| IC | Giles Brandon (WP8 leader) | giles.brandon@intelligentsia-consultants.com |
| LUM | Luca Barbato | luca.barbato@luminem.it |
| MIND | Domenico De Guglielmo (WP6 leader) | dome@mind.cc |
| | Luigi Rodorigo | luiss@mind.cc |
| | Lorenza Carà | lori@mind.cc |
| RIO | Samuli Stenudd | samuli.stenudd@riots.fi |
| | Saila Kakko | saila.kakko@riots.fi |
| SEN | Håkan Lundström (WP5 leader) | hakan.lundstrom@sensative.com |
| | Mats Petterson | Mats.Pettersson@sensative.com |
| RISE | Marco Tiloca (WP3 leader) | marco.tiloca@ri.se |

| | | |
|---|---|---|
| | Rikard Höglund | rikard.hoglund@ri.se |
| CEN | Joni Jämsä | Joni.Jamsa@centria.fi |
| | Laura Palovuori | laura.palovuori@centria.fi |
| | Katja Koutonen-Hautala | katja.koutonen-hautala@centria.fi |
| | Tom Tuunainen | tom.tuunainen@centria.fi |
| | Olli Isohanni | olli.isohanni@centria.fi |
| POL | Luca Ardito (WP2 leader) | luca.ardito@polito.it |
| | Michele Valsesia | michele.valsesia@polito.it |
| | Luigi De Russis | luigi.derussis@polito.it |
| | Alberto Monge Roffarello | alberto.monge@polito.it |
| | Marco Ciurcina | marco.ciurcina@polito.it |
| | Riccardo Coppola | riccardo.coppola@polito.it |