SECURIT

TOWARDS RESILIENT SMART CITIES & TERRITORIES

Project Deliverable

D4.2 Follow Up Report (Final Review) Open Call 2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Deliverable information	
Grant Agreement	N°101005292
Project Acronym	SecurIT
Project Title	New industrial value chain for Safe, sECure and Resilient cIties and Territories. Call: H2020-INNOSUP-2020-01-two-stage - Cluster facilitated projects for new industrial value chains
Type of action	IA Innovation action
Revision	V1.1
Due date	31 July 2024
Submission date	12 July 2024

Dissemination level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission)	
RE	Restricted to a group defined by the consortium (including the Commission)	
CO	Confidential, only for members of the consortium (including the Commission)	

Version	Date	Document history	Stage	Distribution
V0	29-04-2024	Document Creation	Draft	CenSec
V1	08-07-2024	Document review	Draft	FBA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table of content

Abstract 4
Deliverable D4.2: Follow Up Report (Final Review) Open Call 2 5
Introductions and project methodology 5
Overview of supported projects in Open Call 2 13
Prototype projects 14
Demonstration projects 19
Quantitative outcomes and lessons learned 34
Annexes 41
Follow Up Plans 42
Midterm Reports 64
Final Reports 79
KPI progress report 105
Demonstration questionnaire 106

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Abstract

The SecurIT project aims at supporting innovative technological solutions in the field of security, developed by consortia of European SMEs, that are granted with a prototype or demonstrator project, through a top-notch selective process of two Open Calls. In fine, the project will support collaborative projects that will create a new industrial value chain.

This document will firstly give an introduction to the methodology that the SecurIT consortium has developed in order to monitor project development on each of the 21 funded project both on an ad hoc and more formal basis. Secondly, the document will provide an overview of the funded Open Call 2 projects including information about the consortium partners, scope and objective of the projects and TRL levels at the start and end. In addition, for the demonstration projects, the overview will show if the demonstrations took place in a real or near-real environment. Lastly, some quantitative data will be displayed about the satisfaction of the FSTP projects to enter the SecurIT projects. At the end of this deliverable is an annex section, where all the different templates used to track and monitor project progress can be found.

Authors (organisation)

CenSec

Reviewers (organisation)

FBA

Keywords

Final review, project progress methodology, open call 2, security, cascade funding, FSTP.

Legal notice

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Deliverable D4.2: Follow Up Report (Final Review) Open Call 2

The following section will describe the mechanisms developed by the SecurIT consortium in order to ensure project progress and development among the funded projects during the entire project duration from the final selection to the closing of the projects.

The procedures described in this report are more or less the same, or with minor adjustments, compared with what was described in the public deliverable “D4.1 Follow Up Report (Final Review) Open call 1”, which was submitted on 15 December 2023. The adjustments described are optimizations based on lessons learned from the Open Call 1 (OC1) projects and procedures.

Introductions and project methodology

As for the OC1, a total of 21 projects were also funded during the Open Call 2 (OC2), based on the two instruments, in total 7 prototyping projects with a maximum budget of 74.000 euro and 14 demonstrations projects with a maximum budget of 88.000 euro. The projects were selected based on a rigorous screening and selection process described in deliverable D3.6 “Open Call Outcome report and Open Call Evaluation report 2”. In addition, for the OC2 projects, it turned out during the economic eligibility screening process, that two SMEs in two different projects consortia were not eligible to obtain financial funding. Despite not received cascade funding, the afflicted companies decided to stay in the project consortium and remained actively involved during the project period.

Because of this, some funding remained unspent as per budgeted, and the SecurIT consortium decided to create some prize awards allocated during the Final event and award show taking place 21 May 2024 in Paris. More information on the final event and award show is described later on in this deliverable and in depth in the public deliverable D5.5 “Report on final event: report on event and major outcomes”.

Monitoring and evaluation procedures

As mentioned, the same procedures have been followed for the OC2 projects, as was introduced for the OC1 projects, also when it comes to establishing formal and ad hoc monitoring and evaluation procedures to assess the effectiveness and impact of the SME projects initiated in the project. These tools are further described below. As for the OC1 projects, the OC2 projects were allocated a dedicated Follow Up Manager (FUM), from one of the consortium partners (all clusters, except FBA), and all partners have overseen three projects (and allocated about 0,25 PM per project per call). The dedicated FUM oversaw the regular dialogue with and support to the projects and was responsible for the first review and validation of the various project reports. The regular dialogue between the projects and the

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

dedicated FUM consisted for most of the projects of 30 minutes online monthly meetings. During the meetings, the FUM were briefed by the projects on the latest progress and upcoming achievements. The meetings also offered a chance for the projects to inform the FUM about difficulties and further insights into how the project partners expected to mitigate these issues. This information was documented in a joint project dashboard where each FUM would insert the latest update on the project, and this would be discussed in the bimonthly WP4 meetings on monitoring and progress in order to share knowledge and best practices with the other FUMs.

Regarding the project allocation procedure, the projects were allocated to the SecurIT consortium partners based on parameters such as membership with one of the cluster partners, relations with the lead project partner, geography, and technical insights into a specific technology area. For the OC1 projects, a “co-manager” was selected for those partners with an interest in the specific project (due to membership or other relations), but as this function was not as functional and not used as it was intended to, no co-managers were assigned to any of the OC2 projects.

Kick-off meeting

One of the lessons learned from the OC1 projects (and as mentioned in the D4.5), was to give the OC2 projects a proper introduction to the dedicated FUM (and preferably a face-to-face meeting), the various reports to be submitted during the support period and project requirements to know about during the support period. Therefore, for the OC2 projects the SecurIT consortium held a physical kick-off meeting taking place 5 July 2023 in Vilnius, Lithuania. The meeting was held at the premises of consortium partner L3CE, and all the 21 funded projects were represented. The agenda also set aside some time specifically for the FUMs to have meetings with each allocated project, and this offered a good chance to familiarize with each other. The conclusion from the SecurIT consortium partners is that this physical kick-off meeting indeed had a positive effect on the initial establishing of trust between the FUM and the project partners, and it has laid the foundation for a good collaboration throughout the project duration.

Best-practices sharing

During the OC2 support period, the SecurIT consortium has had bimonthly meetings in the work package “WP4 Monitoring and Impact”, and these meetings have been utilized to share best practices among the consortium partners, share news and progress made by the projects, but also to discuss about projects who encountered difficulties and supporting each other in how to best overcome these in order for the project to be successful. The regular WP4 meetings have furthermore been helpful in order to gain further insights into each project, and also to discuss new approaches for innovation uptake among end-users for which consortium partner L3CE has developed a new concept for called **project clustering approach**. This approach offers a novel and more efficient method to engage a broader community of users, providing them with a wider range of functionalities to address the specific problem or challenge. Piloted during the SecurIT project, this approach was deemed successful and has been chosen to continue with selected innovations. This approach is further explanted in the D2.5 ““Synergy

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

Analysis with the European Structural and Investment Funds. A Review of Other Innovation Support Practices".

Regular reporting

In order to measure progress in the SME projects, formal mechanisms were also imposed on the projects as they had to hand in three reports during the project duration; at project start, a Follow Up Plan (in M1) outlined the project plan, deliverables, milestones, KPIs, ethics and risks, and formed the baseline for the project during the support period. Based on the Follow Up Plan, a Midterm Report was handed in halfway in the support period. While most of the projects chose a 12-month support period, others chose a shorter period.

Towards the end of the project period, some projects went through some challenging stages for various reasons (difficulties internally, delay in response from demonstration sites etc.), and requested to extend the support period with a few months. At the end of the project period, all projects handed in a Final Report describing all the developments within the project period, based on the expected progress described in the initial Follow Up Plan. This procedure was valid for all projects regardless of which instrument they belonged to.

Specially for the OC2 projects, adhering to deadlines have been crucial, in particular for the Final Report as the SecurIT project itself is coming to an end at the end of August 2024. This means that all deliverables must be submitted prior to this deadline, which puts some pressure on the finalizing of all reports.

In order to validate the content of the three reports, the SecurIT consortium established several control mechanisms in order to ensure that all projects delivered what they were expected to. Based on the lessons learned from the OC1, for the OC2 projects, the consortium established an extra loop in order to support each FUM and ensuring that all projects were more or less aligned regarding the structure of the content. This mechanism was called "mini-committee meetings" and meant that after the FUM had had the initial review of the reports and considered them clear and consistent, the FUM would share the reports with two other consortium partners, and the three partners would go through the reports and evaluating if the project partners had described the various sections in the reports sufficiently compared to the expectations (in the Follow Up Plan at project start). It was deemed by the SecurIT consortium to be an extra layer and support internally for each partner, as the first report would trigger the 20% payment of the project budget.

In addition to this structure, for the Midterm and Final Reports, the consortium scheduled Follow Up Committee meetings, and this committee consisted of one partner from each of the SecurIT consortium partners. During the Committee meetings, each FUM would go through the reports and the Committee would discuss more in-depth about projects experiencing some difficulties and validating others. Together with the Midterm and Final Reports, a specific KPI progress report was developed and filled in by the FUM based on each report and the categories – technical performance indicators (progress

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

achievements), deliverables (content, clarity, quality, consistency) and deadline compliance - were considered and a score was given. The KPI progress report template can be found in the annex at the end of the deliverable.

A threshold of 7 points (out of 10) was decided to be the level that projects had to pass. Projects under 7 points would be discussed further by the Committee and measures would be taken to ensure that the project would recover when the difficulties toward the project end. The overview of the evaluation criteria can be seen below and was shared with the funded projects during the physical kick-off in Vilnius at project start so they were completely aware of the processes:

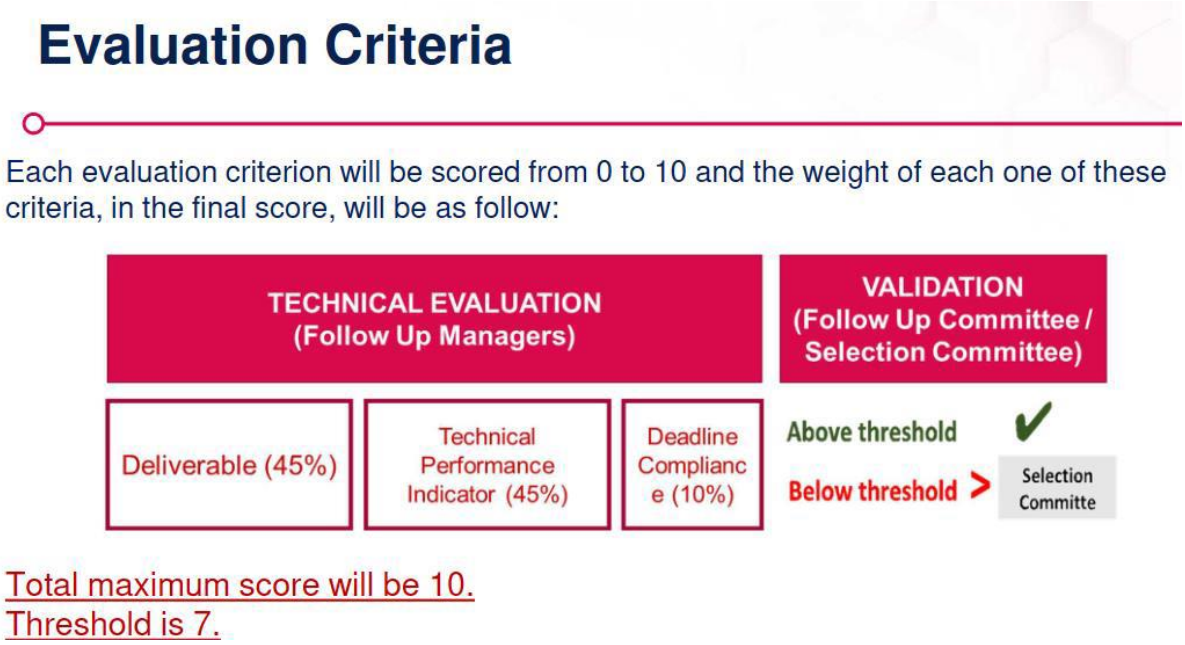


Figure 1: Evaluation Criteria

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

The validation process for the Follow Up Plan, the Midterm and Final reports can be seen as below overview:

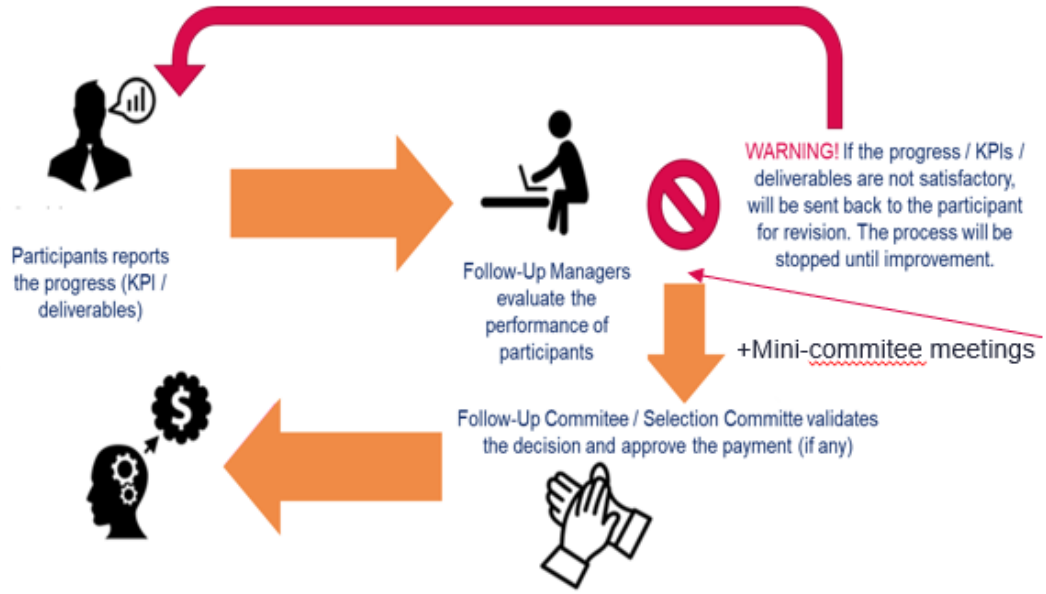


Figure 2: Validation process

As mentioned above, the validation process starts by the projects sending the report to the FUM, who then reviews it, and sent it back to the project in case of unclarities. When the FUM considers the report to be in order, it is shared with the mini-committee members. For the Follow Up report this process was initiated in order to help and support each FUM in validating the reports, and for the Midterm and Final Reports to efficiently and in a good manner speed up the discussions in the Follow Up Committee meetings. The process has shown to be working well.

Regarding the payment for the SME projects, the first 20 % was (for most projects) paid after the Follow Up Plan at project start, and the remaining (up to) 80 % at the project end after a validated Final Report. However, for two SMEs involved in two different project consortia, the process was slightly different as they did not receive any payment due to financial instability discovering during the eligibility check.

Overall, the budget distribution model was chosen to minimize the risk of the consortium partners (as the SecurIT consortium partners would have to cover the costs of eventual failing projects out of their own budgets), and to keep the incentives strong of finishing the projects in good time and manner for the project partners. Please see below an overview of the timeline for the support program that sums up the various steps:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Support program timeline:

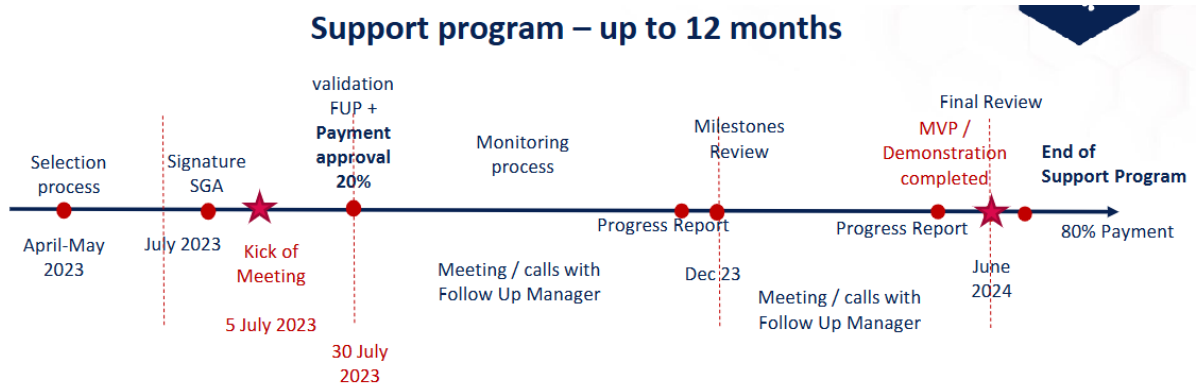
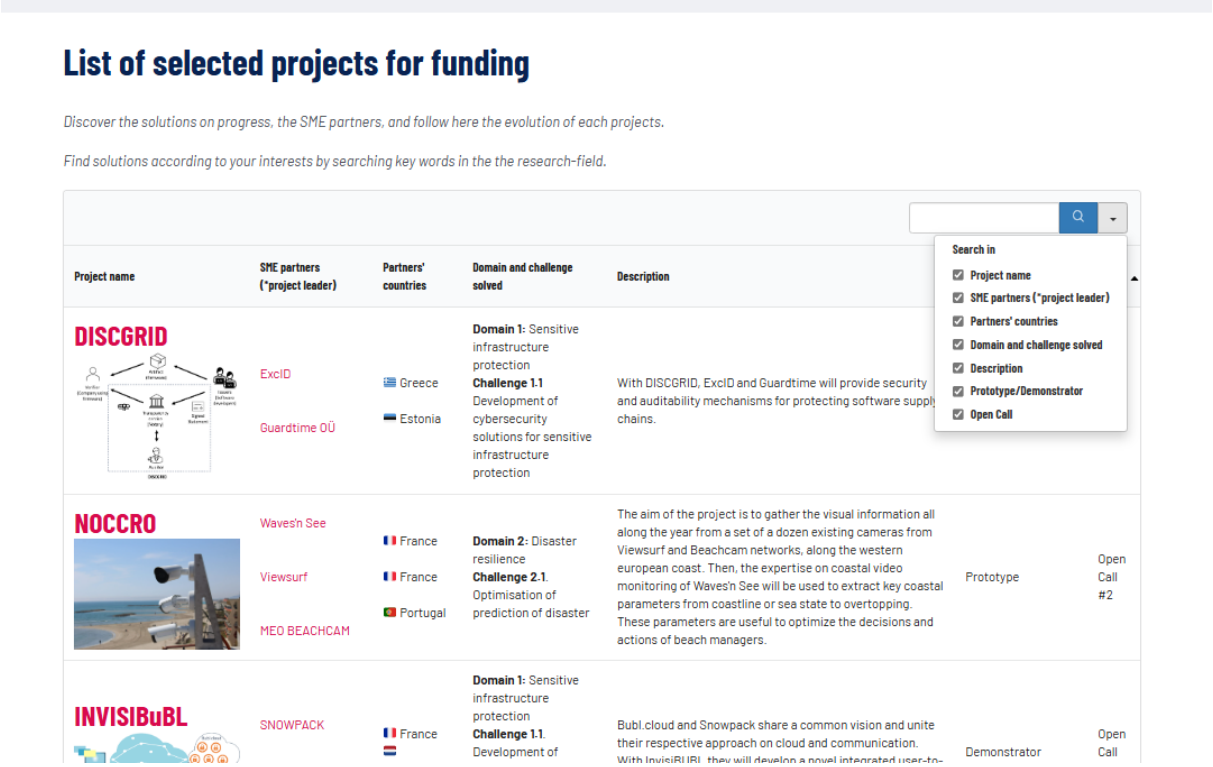


Figure 3: Support program timeline

As seen in the above overview, it is clear when the various steps are taking place, and this is the process that has been followed throughout the support period and what the projects were introduced to during the physical kick-off meeting in Vilnius.

Lastly, in order to share public available information about the funded projects and the progress made during the support period, all OC2 funded projects can be seen on the SecurIT website: [Open Call #2 Funded Projects – SecurIT (securit-project.eu)]

On the website (under the tab called “project results”), all projects from the OC2 are described in detail. See below screen shot of how the projects are presented in the overview list:



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

In addition, each project has a dedicated page where the information for public dissemination is mentioned -the project name icon should be pushed to enter the project specific information, and it is possible to scroll the page and see updated information about each project. See screen shot example below of the CMD project:

Information about the projects can be found by scrolling each project page, that is information about the project partners, project description, status and results from the Midterm and Final report and eventual a few project pictures (when relevant).

Lastly, regarding the final event and award show, in the frame of task 3.7, a contest was organised for the SecurIT Awards. It was only open to projects, which received funding from SecurIT OC1 or OC2 with the aim of selecting the three best collaborative projects of each funding batch.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

In total six prizes were awarded:

- Four financial prizes of €10.000 for demonstration projects (two per Open Call)
- Two financial prizes of €7.500 for prototype projects (one per Open Call)

The participants were asked to fill in a short application form with specific questions about their project and to produce a short video presenting their solution and its interest, highlighting its added value, impact and innovative aspect.

A Guide for Applicants was made available to all potential participants, detailing the rules and participation conditions of the contest. This guide also included requirements and guidelines for the video and the list of the evaluation criteria.

N°	CRITERIA	SCORE
1	The solidity of the project in terms of market fit, commercialization, or development strategy	1 - 5
2	The degree of innovation, from a security perspective, that should be generated by the participation in the SecurIT project	1 - 5
3	Involvement of end-users during and after the project	1 - 5
4	Quality of the video: time management, clarity, convincing, visual, originality	1 - 5

Each criterion has received a score from 1 to 5, 1 being the lowest and 5 the highest as follows:

1 VERY POOR	2 POOR	3 SUFFICIENT	4 GOOD	5 VERY GOOD

The evaluation of the applications was performed by the SecurIT consortium partners and one member of the Advisory Board. The SecurIT consortium received a total of 27 valid applications.

For the OC2, the awarded projects are:

Category OC2 – Demonstration:

- OPTIMIZ-NETWORK
- EV-SAFE

Category OC2 – Prototype:

- ERMINE

More details on the Awards can be found in the D5.5 “Report on final event: report on event and major outcomes”.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

Overview of supported projects in Open Call 2

The following section is providing an overview of the 21 funded projects when it comes to information about the project partners geography, project information and TRL level. The projects are divided between prototyping and demonstration projects, and the demonstration projects has an extra column inserted for information about their demonstrations (real or near-real environment).

As this deliverable is for public dissemination, the below information about the projects derive from their Final Report and this section is for public dissemination. For the sake of confidentiality about their newly developed products and solutions, we are not sharing further details about the projects.

The information in the “final project update” section differs both in length and structure due to the fact that different people have written it with their own understanding of how the section should be and how much they want to share.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

Prototype projects

The information below is on the funded prototyping projects and gives an overview of the project name, project period, partners geography, the final project update for public dissemination (from their Final Report) and the TRL level at project start and end. Overall, for the prototyping projects, they could apply for project funding starting at TRL 5 and was expected to reach TRL 6/7 at project end:

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start – end:
2 AI Disaster Emergency Com	01/07/2023-15/04/2024	• France • Greece	HighWind and GAGDPR developed a prototype as innovative AI-powered module for EU-ALERT text messages toward the population. Encapsulated within the smartphone broadcasted messages through a web link (URL), the module is opened on the web browser of any smartphone and allow citizen within the broadcasting area to report if they are safe, if they can see a danger from a safe place or if they are in an emergency situation. The artificial intelligence “computer vision” is used to pre-diagnose the nature and critical level of emergency signals, adding information to the auto-assessment of the population. Framed in an advanced GDPR compliant framework emphasizing the empowerment of the population to inform first respond during a crisis where lives are at stake, the solution is designed for quick and easy deployment on already existing EU standards of crisis communication.	6 - 8
7 ERMINE	01/07/2023-15/04/2024	• Estonia • Turkey	Over the past year, the ERMINE project has achieved progress in improving how we predict and respond to natural disasters. By using advanced drone technology and smart data analysis, we've created a powerful system that helps us better understand and manage events like wildfires and floods. Our work has been closely connected with disaster management teams in Tallinn, Sofia, and Istanbul. Together, we've made sure that ERMINE's tools are practical and effective in real-world situations, making a real difference on the ground. Throughout the project, we've engaged with local communities, response teams, and international partners to share our discoveries and gather valuable feedback. We've hosted workshops, attended conferences, and published our findings, spreading the benefits of ERMINE far and wide. Looking ahead, the future of ERMINE is very promising. Our technology is already being integrated into disaster management plans in Turkey, with plans to expand even further. With strong interest and pre-orders from Turkish authorities, we're set to boost disaster resilience across the region. Stay tuned for more updates as ERMINE continues to revolutionize disaster preparedness and response. Follow our journey on our website and social media for the latest news and developments!	5 - 7

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start – end:
12 NOCCRO	01/07/2023-30/06/2024	• France • France • Portugal	The aim of the NOCCRO project is to use the hundreds of existing beach cameras to help preserve the coastline. Beachcam and Viewsurf, partners in this project, operates a network of more than 150 tourist or surf cameras along the European coastline. Waves'n See has expertise in image processing and analysis to produce oceanographic data crucial for managing coastal erosion and marine submersion. The technical challenges involved acquiring, stabilizing and Processing images from non-scientific cameras so that oceanographic analysis algorithms could be used. The second key point was to georeference all the camera views so that each pixel corresponds to a GPS point. Finally, each camera selected as part of the project will have been able to acquire at high frequency at least one of these parameters: height, period, wave direction, coastline, beach slope. The final result of the project: an initial network of 12 beach cameras used as coastal scientific cameras, stretching from the north of France to the south of Portugal, and the drafting of technical specifications to enable the experiment to be replicated on a large scale.	5 - 6
14 ReBriNet, Rescilience Bridge Net	01/07/2023-30/06/2024	• Denmark • Spain	During the last half of the project period Social Tech Projects has developed advanced features leveraging machine learning and AI to enhance situational awareness and emergency response capabilities. The key innovations include APIs that organize data from impacted communities by topics, using AI Topic Modeling to categorize information and AI Summarization to provide quick insights. A map-based visualization tool integrates data from digital surveys with real-time updates. It displays incident locations and provides detailed, location-specific information critical for coordinating emergency responses. These features facilitate emergency responders in swiftly understanding and addressing situations. In parallel, ConnectingBrains conducted three workshops to test the ReBriNet emergency management application. These workshops simulated emergency scenarios such as flooding, earthquakes, and fires, involving 52 participants, including citizens and emergency responders. Held in Palo Alto, Barcelona, the workshops demonstrated the application's utility and gathered valuable feedback for improvement. Participants engaged in discussions, generating ideas for enhancing navigation and functionality. This comprehensive validation process highlights the potential of ReBriNet solution to improve urban resilience and emergency response efficiency, paving the way for wider deployment and adoption across Europe.	6 - 8

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start – end:
19 Smart Diri	01/07/2023-30/06/2024	• Norway • Norway	The SmartDiri project, a collaborative effort involving Diri AS and Homesourcing AS, aimed to redefine Cyber Risk Management through automated decision support. Upon completion, the SecurIT project detailed and produced a working AI-prototype for cyber security risk management called SmartDiri. This innovation targets efficiency gains, elevated quality standards, and essential insights crucial for fortifying cyber resilience in the digital landscape. The AI prototype embodies a 'hybrid wisdom of the crowds human-in-the-loop recommender system,' seamlessly integrating user opinions, diverse data sources, machine learning capabilities, and human input for advanced recommendations. The application includes a bilingual smart chatbot, offering tailored guidance and help to users needing assistance. Throughout the project, extensive evaluation of AI models tailored for the Norwegian language was conducted, initially focusing on NorBert 2 and NorBert 3. Later, the project transitioned to Azure OpenAI's GPT-4 turbo models, which provided superior language proficiency and performance. A robust testing environment was established by integrating essential libraries and creating a simulated database for controlled testing purposes. The SmartDiri prototype GUI has been developed and integrated into the Diri platform for user testing. The bot's conversational structures were crafted and refined, focusing on item generation in the Diri application. Iterative testing with real and simulated interactions was conducted to fine-tune the bot's responses and conversational flow. Contextual comprehension and subject recognition were thoroughly tested with promising outcomes, ensuring the bot accurately understood and responded to user inputs. The project was recognized in the national newspaper 'Shifter,' highlighting Norwegian innovation and underlining the relevance of these advancements. At the project's conclusion, we successfully developed a sophisticated AI chatbot capable of enhancing Cyber Risk Management for midsize businesses defined as essential services by the upcoming NIS2 directive, including suppliers of critical infrastructure. The prototype demonstrated the potential to offer significant efficiency gains, improved quality standards, and critical insights for cyber resilience.	5- 7
20 Sylviacare	01/07/2023-17/05/2024	• France • Belgium	The SYLVIACARE project aims to put on the market a very efficient wildfire detection solution, easy to set up and easy to interface with existing web platforms. The key performances are: • Very quick detection (<5min) • Precise geolocation (<50m) • Real Time in situ image transmission for false alarm rejection. This solution relies on: • A communicating sensor equipped with infrared cameras (microbolometer matrix). The sensor is to	5 – 6/7

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start – end:
			be installed at 3m height in the trees to watch-out a 10ha area. • A public low power wide area network (LPWAN) • A primary platform to monitor all the sensors and to share data with other platforms. • A secondary platform (Timbrack) to demonstrate the ability to easily communicate with the primary platform and get access to all the sensor information. The solution also permanently monitors local parameters at the sensor level such as temperature and hygrometry. The SYLVIACARE project mainly involves specific and consequent software development concerning sensors, communication network, edge computing and web platforms. At the beginning of the project, the two members of the consortium, SYLVIACARE and TIMBTRACK, worked hard to build detailed specifications that have been key success materials. They allowed an efficient software development process while mitigating the risks of failure during the integration part of the project: make all the equipment to perfectly communicate with each other. The software development process has been launched in December by each team. The modularity of the design associated to well documented specifications has allowed an efficient work inside each team. Regular points have been made between the teams that led to small specifications adjustments without impact on the schedule. Final integration tests performed in May 2024 demonstrated that the prototype solution is operational from the sensor toward the primary and secondary platforms through the communication network. We are proud to have achieved this ambitious challenge within a tight schedule. We are now on the road to build a demonstrator to be installed in the forest in real situation.	
21 WUI-Secure	01/07/2023-30/06/2024	• France • Spain	As the SecurIT funded project draws to a close, the WUI-Secure project has finalized the creation of its prototype tool that combines the project's two main modules: (1) Wildfire Modelling and (2) Vulnerability Assessment. The WUI-Secure tool is a fully functional tool that allows users to visualize the vulnerability of urban structures at the Wildland-Urban Interface using the building vulnerability index and identifying their susceptibility and risk with regards to different possible wildfire scenarios. The second half of the project allowed our team to create a desktop version of the platform to include innovative wildfire modelling technology and the Building Structural Vulnerability Index (BSVI)—created to assess the vulnerability of individual structures in terms of their structural characteristics and surroundings. The tool was successfully tested and validated using two case	5 - 7

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start – end:
			study scenarios in Catalonia, Spain, and Pyrenees-Orientales, France. It was presented to several key actors including researchers, local fire service, local and regional government members, among many others. The WUI-Secure modelling tool in its prototype stage and in its future iterations will be a valuable tool that has proven its potential use in various applications and at different scales.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Demonstration projects

The information below is on the funded demonstration projects and gives an overview of the project name, project period, partners geography, the final project update for public dissemination (from their Final Report) and the TRL level at project start and end. Overall, for the demonstration projects, they could apply for project funding starting at TRL 5 and was expected to reach TRL 8/9 at project end.

Specifically for the demonstration projects, an extra column has been added to share information about the environment in which the demonstration(s) were conducted. The demonstrations were targeted to be organized in real environments when possible and alternatively when it was not possible due to contextual barriers, the demo would be implemented in near to real environment infrastructure by simulating end-user operations in as close to real scenario as possible:

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
1 AIA Guard	01/07/2023-30/06/2024	• Italy • Denmark	Our goal with AIA Guard has from the start been to develop an end-to-end cybersecurity solution specifically designed against Artificial Intelligence Attacks. Designed to be GDPR compliant and capable of monitoring, detecting and mitigating AI models vulnerabilities. During this 12 month period we have been working toward that goal by: ● Enhanced Interpretability module: ○ Incorporated image analysis alongside text input analysis. ○ Added capabilities to process and analyse uploaded text files. ● Improved user experience (UX): ○ Continued enhancements based on user feedback. ● Expanded Data Anonymization module: ○ Detects more personally identifiable information (PII). ○ Introduced options for downloading anonymization results and selecting ● Adversarial Attack module:	6 - 9	Near-real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			○ Added four more datasets, achieving the project goal of eight datasets. During the project period we have created awareness to AIA Guard by several dissemination activities: ● Maintained an active LinkedIn page and project website with regular updates. ● Participated in seven relevant events and conferences, enhancing visibility and creating new collaboration opportunities. ● Launched a Google advertising campaign targeting IT leaders, CTOs, and security officers across Europe. We have conducted 4 demonstrations to various stakeholders, including hospitals, digital consulting firms, and government technology organisations. Feedback highlighted strong interest in anonymization features, custom solutions, and the critical importance of GDPR compliance. Where will we go from here? ● We will continue enhancing the platform by integrating new features based on emerging market needs and technological advancements.		
3 AIR-T4S	01/07/2023-30/06/2024	• Greece • United Kingdom	During AIR-T4S project, significant progress has been achieved, particularly in the domains of system design and integration. Challenges encountered have been effectively addressed through proactive strategies, including the utilization of end-user feedback and thoughtful planning. The main tasks accomplished so far include: Identification and Assessment of User Needs: Conducted comprehensive interviews and distributed questionnaires to successfully identify and assess specific user needs and challenges. System Integration: Successfully integrated the on-the-ground capabilities of T4S with the aerial support provided	6 - 8	Real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			by the AIROUS platform, creating a unified system that delivers comprehensive crowd safety and threat detection solutions. Demonstration Video Creation: Created a comprehensive demonstration video showcasing the platform's features and benefits, including testimonials from users. Testimonials: Peace and Friendship Stadium: "The demonstration of the AIR-T4S platform at our stadium was impressive, proven to be a vital tool in enhancing our public safety operations."		
4 AIRA	01/07/2023-30/04/2024	• Poland • Estonia	AIRA – an innovative solution for automated, evidence-based security risk assessments. Developed by ISSP, a cybersecurity service provider, in collaboration with Estonian ENKI Consulting, AIRA is a cutting-edge Software as a Service (SaaS) platform designed to enhance investigation accuracy, reduce time, and increase productivity in proactive risk discovery and breach response. AIRA concentrates on discovering attack surface, identifying vulnerabilities, and evaluating security setups, with a special focus on small businesses. The project has achieved significant milestones, completing Research & Development phases for MacOS and Linux. Building on this foundation, we've implemented new configuration and vulnerability assessment models using a new architectural approach, ensuring a robust cybersecurity framework. Expanding our web-platform capabilities, AIRA now supports not only Windows but also Linux and MacOS. This inclusivity extends to easy integration of new models directly on the AIRA platform, enhancing its adaptability to evolving cyber threats. **What are the main advantages of AIRA?** 1. High efficiency: By automating artifact collection, data enrichment, and analysis, AIRA expedites investigations, reducing the time required for	5/6 - 8/9	Real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			comprehensive assessments from months to hours. 2. Comprehensive Insights: AIRA offers a clear picture of an organization's cyber posture, shedding light on previously undetected vulnerabilities. Modern risk assessment tools, like the AIRA platform, mark a significant leap forward in cybersecurity. By receiving automation and data-driven insights, businesses can proactively mitigate cyber risks, fortify defenses, and safeguard their digital assets against evolving threats. In perspective, it helps them to be more profitable and avoid financial and reputational losses.		
5 CMD	01/07/2023-01/01/2024	• France • France	With safety concerns rising worldwide and the number of security cameras growing exponentially, the human ability to monitor that footage is rapidly decreasing. Since its inception, Neuroo's video analytics platform keeps heavily evolving in order to offer the best–in–class real–time data intelligence solution in its kind. From spotting suspicious and unattended luggage, to identifying hostile acts, Neuroo's AI powered features got you covered. The CMD project team made of Neuroo and MA2 members is proud today, to release one of the most advanced, production–ready video–based public panic detection feature, completing our set of events' detection and alerting functionalities. Panic can lead to stampedes, trampling, or crushes as people attempt to flee or find safety, resulting in injuries or fatalities. This new feature can detect panic within a crowd in real time and enable security personnel to take proactive responses within seconds. The challenge was intense, and the scientific literature was not easy neither to digest nor to ease a production–ready system with tons of field constraints associated with relevant results. But at the end, we were able to come up with a new and completely different approach to reach our target by building one of the first light, yet high accuracy AI public panic detection model.	6 - 8	Real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			Talk, being cheap, we decided to meet reality by testing our new feature on the field! Of course, no real public panic has been identified in the public space, but a simulation of an army of young rugby players from Vernon SPN Rugby Club in Normandy. 115+ players simulating a public panic in the stadium was as impressive as Neuroo's detection feature ability to highlight it within seconds. With these results in mind, we are ready now to start offering our new features to not only our current customers, but also in all locations. Stay tuned.		
6 DISCGRID	01/07/2023-30/06/2024	• Greece • Estonia	DISCGRID produced a solution that enhances the security of the smart grid firmware supply chain. The main building block of DISCGRID's approach is an append-only, immutable, Transparency Registry, where information about software artifacts, related to the released firmware, is recorded. This information can then be used to verify the validity of those artifacts. An important property of the Transparency Service is that it is auditable, hence at any time a third-party auditor can verify that information has not been removed or modified. Additionally, an auditor can notify firmware vendors or DSOs about new entries in the registry; these entries may correspond to legitimate activities, or to an ongoing attack. DISCGRID produced tools that hide the complexity of the transparency registry and enable integration with the CI/CD processes of firmware vendors. Additionally, DISCGRID eliminates the risk of security key breaches. This is achieved by supporting single-user signing keys included in short-lived certificates. DISGRID signature verification mechanisms allow DSOs to verify that a key was valid at the time a signature was generated. Finally, DISCGRID facilitates auditability and access control by bounding issued certificates to the identities of the firmware provider's users. This is achieved by integrating OpenID Connect and by including the information provided	5 - 9	Near-real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			in the corresponding “identity tokens” into the issued certificates. The DISCGRID toolchain can be easily integrated with any ID provider.		
8 ERRATA	01/07/2023-30/06/2024	• Greece • Greece • Italy	ERRATA introduces an innovative technological solution which aims at empowering operational teams deployed in hard-to-reach hazardous environments, with the right tools to detect or recover from a possible danger quicker and safer.The solution is co-developed by 2 deep tech startups from Greece (INSIGHIO & VERTLINER) excelling in the robotics and IoT fields respectively, who are assisted by a technology company from Italy (APOGEO SPACE), excelling in space-based connectivity. Imagine a hostile and harsh area, such as an underground tunnel, a mining environment at construction stage or a storage facility used to deposit sensitive chemicals. Such a site may have no pre-existing communications infrastructure, limited or no human access, and possible physical threats to safety and security. Remote teams need a special tool able to autonomously scan the area from a safe distance, detect possible dangers (e.g. gas leaks, breaches) and help on making informed decisions on-site. During the project duration the team has significantly matured its technical and business proposition. On the technical side the team has advanced the TRL of the solution from 5 to 8. To accomplish this: VERTLINER enhanced its generic aerial robotic platform (UAV), incorporating new high-end sensors and advanced software (SLAM algorithms) that allows to autonomously scan challenging confined indoor spaces and detect certain items and gases concentrations. INSIGHIO customized its flexible IoT device in two ways: incorporating oxygen/carbon dioxide sensors to offer gas detection capabilities, as well added long-range low-frequency connectivity capabilities to access sensing information and control the UAV from a safe distance.	5 - 8	Real environment

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			• APOGEO SPACE evolved the concept of providing a hybrid communications technology leveraging its proprietary long-range protocol applied in the exact same way over terrestrial gateways or its nano-satellite constellation. • Following the individual technical developments, VERTLINER and INSIGHIO integrated the technologies to a TRL8 IoT-empowered UAV system prototype which is able to autonomously perform complex operations in challenging indoor spaces. • Finally, the team validated the solution under real-world conditions, i.e. performed several missions in the Ancient Indoor Mining Sites of Lavrion Technology Park, located in Attica, Greece. The site is currently used for R&D purposes but also as a storage facility for securing sensitive materials (captured gas piles). The team presented the concept to 2 stakeholders, the Site Manager and the company who is responsible for storing the chemicals. On the business exploitation side, the team made progress in 2 key directions: • Identified 2 new target markets for commercially exploiting the developed system: i) Safety and Security in confined / hazardous areas like special storage facilities, mines, or tunnels, using tailor-made sensors, UAVs and connectivity. Of particular interest is ensuring safe conditions for workers. ii) Critical infrastructures monitoring in remote areas integrating hybrid terrestrial and satellite communications. These could include road networks, energy grids, oil and gas extraction facilities, etc. •Leveraging the acquired experience, the team has started investigating the next steps for productization and commercialization, including extensive system testing for further product verification and improvement, acquiring mandatory certifications, competition analysis, engagement of early adopters, promotion activities and financing needs.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
9 EV Safe	01/07/2023-30/06/2024	• Greece • Croatia • Greece	EV Safe proposal aims to deploy interoperable software tools and services aimed at Electric Vehicle Charge Point Operators (CPOs) to help them detect and remediate attacks against Electric Vehicle Charging Station (EVCS) infrastructure. EVSC Infrastructure is exposed to significant cyber risks that can affect the functioning of essential parts of the economy and transportation sector. For the past 12 months R&D projects team in EV Loader,Technomat and,Gridone worked in the following stages: Stage 1: Research cyber security practices for EV Charging stations and review actual cyber threat cases. Stage 2: 11 Charging Locations were added under monitoring of EV Safe tool and initial testing of the tool took place Stage 3. Simulation of cyber-attacks to EV Charging Stations and deployment of mitigation tools. At the end of SecurIT project key findings will be made available to the public via a whitepaper report. The end goal of the project is to deliver and implement a security provision framework for EVCS infrastructure addressing key threats against EV Charging Stations. Stage 4: Replication of tools in more than 50 charging stations of EV Loader. Inclusion of EV Loader and EV Safe within the offerings of Technomat. Replication with Croatian partners. Research team was successful in implementing improved cyber security measures aiming to prevent or quickly remediate malicious attacks against EV Charging stations. Project partners also set out a commercialization and distribution plan. Under this plan Parity Platform owns the software IP for EV Loader and EV Safe and continues to improve EV Safe tools, while Technomat and Gridone can distribute EV Loader and EV Safe under defined distribution agreements through their channels and relay feedback collected from clients to Parity Platform software team to continuously improve the tools.	6 - 9	Real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
10 FLOWGUARD	01/07/2023-30/06/2024	• Spain • Spain	FLOWGUARD has developed an advanced, real-time cybersecurity solution for water distribution networks, leveraging cutting-edge Graph Neural Networks and ETL processes. Our system detects and addresses anomalies indicative of cyber threats, ensuring the integrity of water infrastructures. Collaborations with key industry players and integration with leading commercial products position FLOWGUARD as a seamless, plug-and-play solution. Through targeted digital marketing strategies, we are driving lead generation and enhancing our market presence. Discover more at flowguardsolutions.com and watch our explainer video https://www.youtube.com/watch?v=iCZYOBqsbdc	6 - 9	Real environment
11 INVISIBuBL	01/07/2023-30/06/2024	• France • Netherlands	Thanks to SecurIT, Bubl and Snowpack have jointly developed Invisibubl, a first demonstrator of zero knowledge storage cloud service. Invisibubl is a cloud storage service that does not require to trust any of the infrastructure provider (i.e. server, host, cloud service provider, service provider (Bubl and Snowpack), …). Because such service prevents any data access from the hosting and service operators, it guarantees that even if the data is actually store on US or Chinese hyperscaler, the data will not be provided because of Cloud Act, Patriot Act or FISA section 702. Moreover, users keep a full control on the data they chose to share or revoke with third parties. As a result, this storage cloud service targets sensitive data, in particular those from critical infrastructure operators and public services. During the first half of the project, Snowpack has developed its Invisible Service connector and released it in production in November 2023 together with its 2.0 version. Bubl has industrialized its Bubl service and put it in production with a first client. The second half of the project has been focused on the integration of the Invisibubl demonstrator. In parallel, a first version of its business and pricing models was jointly defined, common marketing material was designed and a	5 – 7/8	Near-real enviroment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			draft threat model of their joint cloud service was produced.		
13 OPTIMIZ NETWORK	01/07/2023-30/06/2024	• France • Ireland	The OPTIMIZ NETWORK - ZARIOT project aims to deploy a solution for securing, monitoring and optimizing telecom infrastructures. During this 12 month project, we had the opportunity to implement not 1 but 3 demonstrators with telecommunications players (SIEL-TE and SOON THD) on fiber optic networks in operation as well as on the French electricity transmission network for verticality and shock measurements on the pylons. Our project was able to mature thanks to numerous exchanges with end users and by confronting operational realities and constraints. Through this, we have identified the strengths and weaknesses of our project in order to guide future developments. Our project went beyond our expectations and we even had the chance to win the Award for the most promising projects by the SECUR IT organizing teams. Throughout the project, we explored cutting-edge software technologies, with a focus on artificial intelligence applied to data lakes and blockchain. This approach allows us to envisage new uses and innovative applications. Our team has successfully completed several critical activities, improving the robustness and functionality of our solution. To ensure effective collaboration and integration of the demonstrators, OPTIMIZ-NETWORK used its best skills and experience in project management to carry out several steps: • Using our business knowledge, rapid studies were built and delivered with in-depth information on user management rights, instrumented use cases, monitoring points, hardware validation, network validations, and supply orders. • Workshops: Facilitation of several workshops to promote collective intelligence and stimulate innovation. • Software Platform Design: Development of the basic design of our software platform.	6 - 8	Real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			• Management of sensor installations in the field where we have successfully installed our solutions in the field for telecom operators. • Remote deployment team for sensor installations once everything has been tested and configured in our lab. • Development of subcontractor management solutions: We have launched a very innovative solution to manage, control and monitor the activities of technical subcontractors. Our solutions are built with NFC technology coupled with a web and mobile application. To date, the status is in the beta phase and is currently demonstrated with SOON THD. • Point-of-care sticker printing: Stickers produced to mark point-of-care and facilitate identification. • In the vision of having a solution ready to meet cybersecurity requirements, we conducted a risk analysis. • EBIOS RM Analysis: Conducting an in-depth risk analysis using the RM EBIOS methodology, a tool developed by the French National Agency for Information Systems Security (ANSSI) to assess and address digital risks. This ensures that our solutions are secure and compliant with NIS2 requirements. Our multi-faceted communication strategy ensures a strong presence in person and online. The main points are as follows: • UTHD Exhibition in Bourges, France: This exclusive event for telecom industry professionals serves as the main physical platform. It was an opportunity to showcase our advancements alongside leading infrastructure network companies by highlighting our contributions and innovations on a national scale. • Strategic digital presence: On platforms such as LinkedIn, we have built a vibrant digital community. This presence allows us to engage with industry leaders, share valuable information, and document our project journey. Through regular updates and interactions, we foster connections and awareness within the professional ecosystem. Finally, the OPTIMIZ-NETWORK initiative places the user at the heart of our project.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			To improve the user experience and usability , we commissioned an expert UX/UI consultant. This expert is focused on redesigning our platform interface and improving control and monitoring features, to ensure that our solutions are intuitive and efficient. • Use Case Validation: Testing multiple scenarios and alerts to validate the effectiveness of our solutions. • The three workshops we have organized are at the heart of our progress. Each workshop has an average of 14 participants, bringing together a diverse group of network operators, installation experts, security specialists, electronic designers, and product suppliers. This collective intelligence process is essential to develop innovative solutions. By combining different perspectives and expertise, we not only advance technology, but also strengthen the interconnected fabric of our professional communities.		
15 RESPO-C	01/07/2023-30/06/2024	• Sweden • United Kingdom	During the RESPO-C project period, our team has focused on creating a user-friendly and effective solution that empowers citizens to contribute to fire prevention and management efforts. We successfully developed a holistic fire management application that allows users to learn about different regulations and policies based on their geographical locations, receive real-time updates as well as access educational resources on fire safety. Various users participated in successful pilot testing of the application. The pilot testing phase received positive feedback from users, highlighting the app's ease of use and effectiveness in improving fire management practices. We conducted several social media campaigns to raise awareness about the application, using platforms like Facebook, LinkedIn, and Instagram. These campaigns reached a high number of individuals, resulting in a growing user base and enhanced community involvement (as we capture it from the analytics report in google play and apple stores). Through our collaboration with MHK, we received cybersecurity consultation services, ensuring that the application met high standards of security and privacy. This	5 - 8	Real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			collaboration made the application ready for distribution on Google Play and iOS channels, achieving a level of readiness that guarantees user data security and privacy, thus enhancing trust and adoption among users. Moving forward, we plan to continue promoting the app to reach more communities, particularly in fire-prone regions. We aim to incorporate additional features based on user feedback, such as advanced predictive analytics and integration with geospatial alert services. We will also try to establish new collaborations with environmental agencies (such as COPERNICUS), fire departments, and community organizations to further the app's reach and effectiveness.		
16 RS2DG	01/07/2023-30/06/2024	• Germany • Italy	The implementation of the energy transition poses strong challenges on the electricity distribution grid. New digital tools for identification and prediction of grid bottlenecks, for grid resilience and for grid extension planning are required. Due to the high dynamics over time and due to the high variability of consumption and generation behavior over different parts of the distribution grid, monitoring and planning of the grids must be able to use the true grid behavior and cannot rely on assumptions and standard load profiles any more. The Digital Twin of the electricity grid instead uses a combination of semi-static structural information about the grid topology together with electrical measurements from different grid locations and from different types of measurement devices and IT systems in order to automatically build up an model of the grid that accurately represents the time-series behavior of the true physical distribution infrastructure for planning. The trustworthiness of the result from the digital twin relies on the ability to detect anomalies in input measurement data fast. The project RS2DG has integrated and demonstrated a software solution, called Security & Resilience (S&R) component, that was successfully demonstrated to detect cybersecurity threats as well as anomalies in the electrical	5 - 8	Real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			measurements. Immediate alarms increase the resilience and the security of the digital twin of the electricity grid that is the basis for operations and planning of current and future the low and medium voltage grids. Two project demonstrations have demonstrated the viability of the automated anomaly detection for input data, despite the challenging scenario of heterogeneous data sources for the Digital Twin. The assessment showed the benefit of the S&R component through three technical KPIs: accuracy of the detection was shown to be high and significant reductions of recovery times from data faults and attacks as well as significant reductions of operational efforts due to the novel S&R component were shown.		
17 SAFE-FESTIVALS	01/07/2023-30/06/2024	• Italy • Netherlands • Netherlands	The SAFE-FESTIVALS project developed and experimented with an integrated, multiplayer, immersive platform that caters for scenario building and dynamic simulations of festivals and crowded events for the purpose of conducting trainings to better counter or reduce the impact of security threat scenarios. We initially worked closely with end-users and security stakeholders to collect their needs and expectations and derive the requirements for the SAFE-FESTIVALS platform, delivering a baseline architecture. Then we worked on integrating the D-GEM tool with the Crowd Simulator, while developing new functionalities to simulate threat scenarios at large festivals, in an Agile approach. Therefore, we worked with the festival organizers first to commonly define a demonstration plan and then to set up the virtual environment and demonstrate the threat scenarios in a multi-player serious gaming immersive environment at the Paaspop festival. A post-festival evaluation was finally conducted to measure the effectiveness of the platform. Next to development and experiments in the context of the Paaspop festival, with dissemination at other festivals, we discussed potential business models to exploit the SAFE-FESTIVALS results.	6 - 8	Real environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Project name:	Support period:	Partners geography:	Final project update:	TRL Level start - end	Real or near-real environment
			Testimonials have been part of the SAFE-FESTIVALS video, prepared for the SecurIT award. The key testimonials include: • Festival organizer: 'The usage of collected data at previous and current events can underpin the decision-making regarding future events". • Police: "SAFE-FESTIVALS can help during the preparation of big events. By simulating all kinds of scenarios we will get a better understanding on crowd behaviour and make better decision planning of resources, including security staff"		
18 ServAI Management	01/07/2023-15/05/2024	• France • France • Italy	ServAI Management achieved key milestones in enhancing emergency response and environmental safety by optimizing measurement strategies. Our innovative 'Little Alert Boxes' are now fully integrated on Kalisio's platform Kalisio Krisis, providing advanced monitoring and rapid alerting capabilities. These devices, equipped with radioactivity sensors and secured through a Prendoquota's Blockchain Logbook, have undergone extensive pre-testing to ensure reliability and accuracy in real-world conditions. Collaboration with authorities has enabled us to demonstrate the whole systems adaptability and impact in live operational scenarios, setting a new standard for emergency measurement strategies. We are proud to share the positive outcomes and transformative potential of our project, paving the way for a safer and faster operational interventions.	7 - 9	Real environment

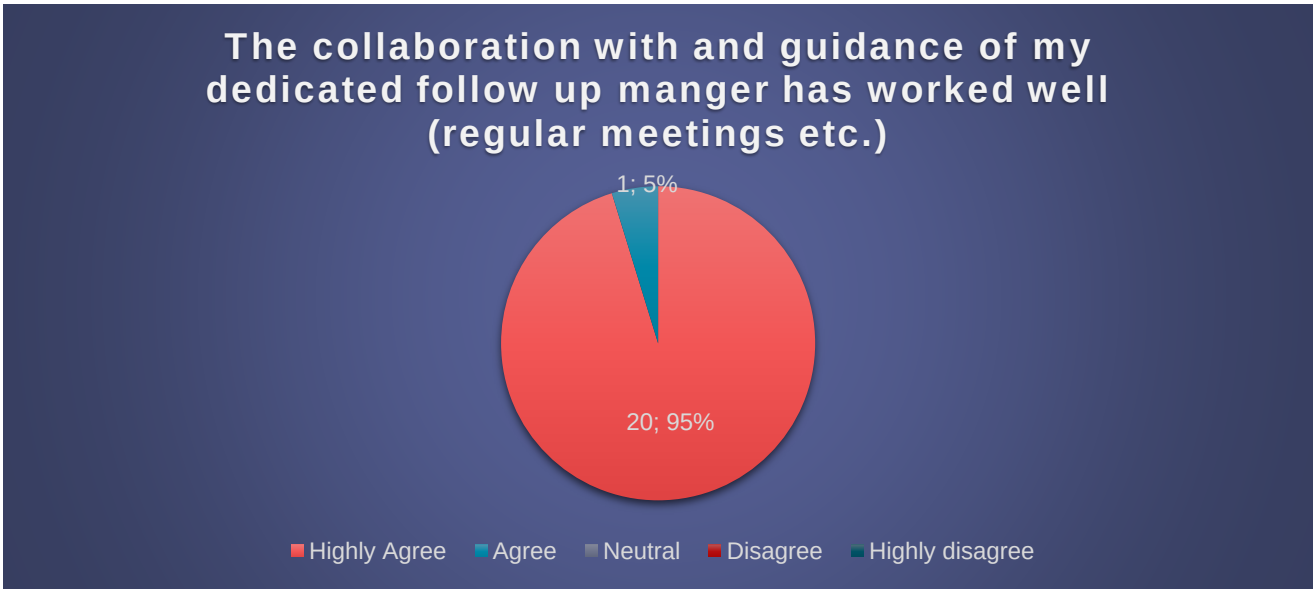
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Quantitative outcomes and lessons learned

As part of the Final Report, all projects were asked to answer four questions regarding their assessment and evaluation of the (up to) 12-month support period. All questions could be rated 1-5 where 1 was “highly disagree” and 5 was “highly agree”.

The questions and results were as follows:

For the first question:

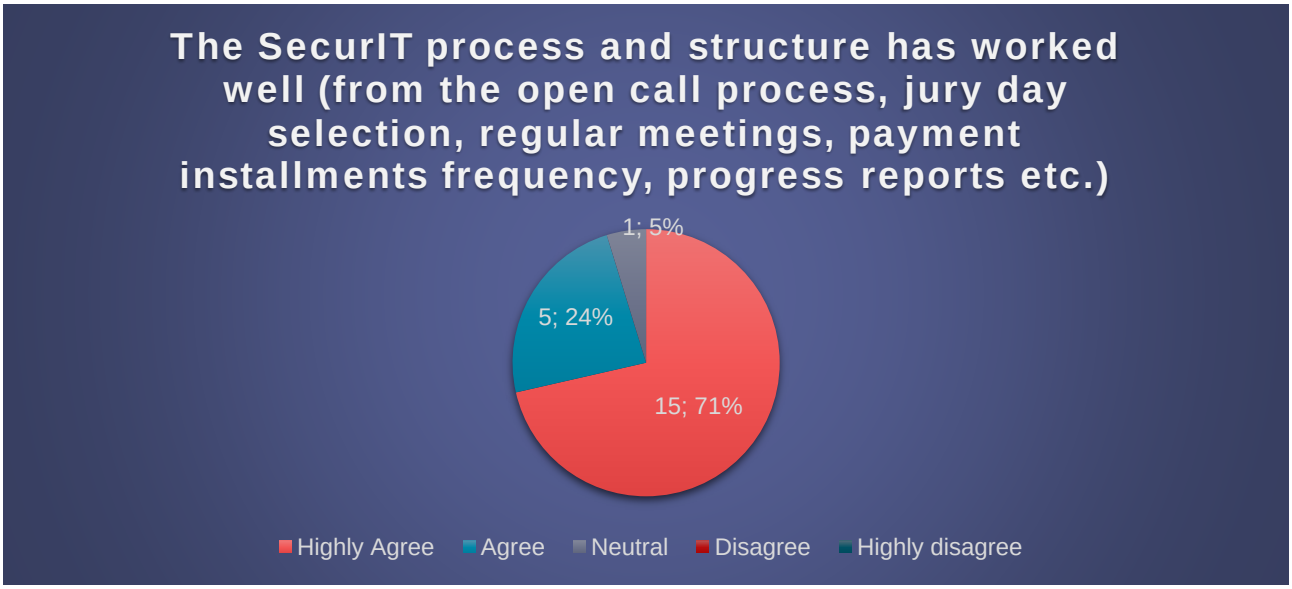


Out of the 21 projects, 20 gave the highest score of 5 meaning that they “highly agree” with the question concerning the collaboration with and guidance of the dedicated follow up manager. Only 1 project has given a 4 meaning “agree” with the statement. No projects have given a lower score, making it clear that the overall satisfaction with the follow up manager is very high.

Compared to the results based on the OC1 projects that were asked the same question in their final report, 19 replied “highly agree” and 2 “agree”. The conclusion for this question is that for both the OC1 and OC2 projects that the vast majority of projects have been very satisfied with the collaboration. The SecurIT consortium partners are very satisfied with this feedback, as we each have tried our best to support the projects in different ways and the feedback is a clear indication of that it worked well.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

For the second question:

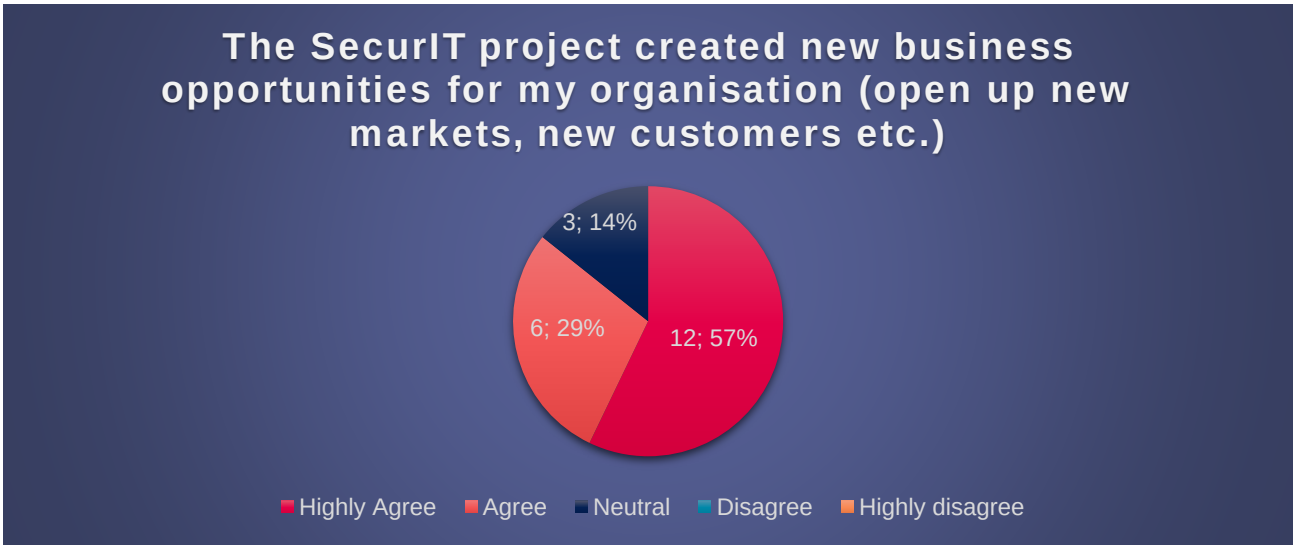


From the diagram we can see that out of the 21 projects, 15 have given the highest score of "highly agree", 5 projects "agree" and 1 project has given a neural score. Again, the majority of projects are highly satisfied with the SecurIT process and structure.

Compared with the OC1 projects, the distribution was different as 13 said they highly agree, 4 that they agree, 2 gave a neutral score and 2 disagree. Some of the reason behind the OC2 projects being overall more satisfied can be because the SecurIT consortium were more experienced in running the process and structure having had the experience from the OC1. Part of the reasons for the OC1 projects to be dissatisfied was partly due to the payment instalments frequency as some projects said to be unhappy with the majority of the budget being paid after the Final Report (and not at the beginning or Midterm). This aspect was emphasized for the OC2 projects, and in addition to this, the SecurIT consortium also changed the jury day structure from being a physical pitch session for the OC1 applicants to an online pitch session for the OC2 applicants. These changes can have had a positive influence on the satisfaction of the OC2 projects.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

For the third question:



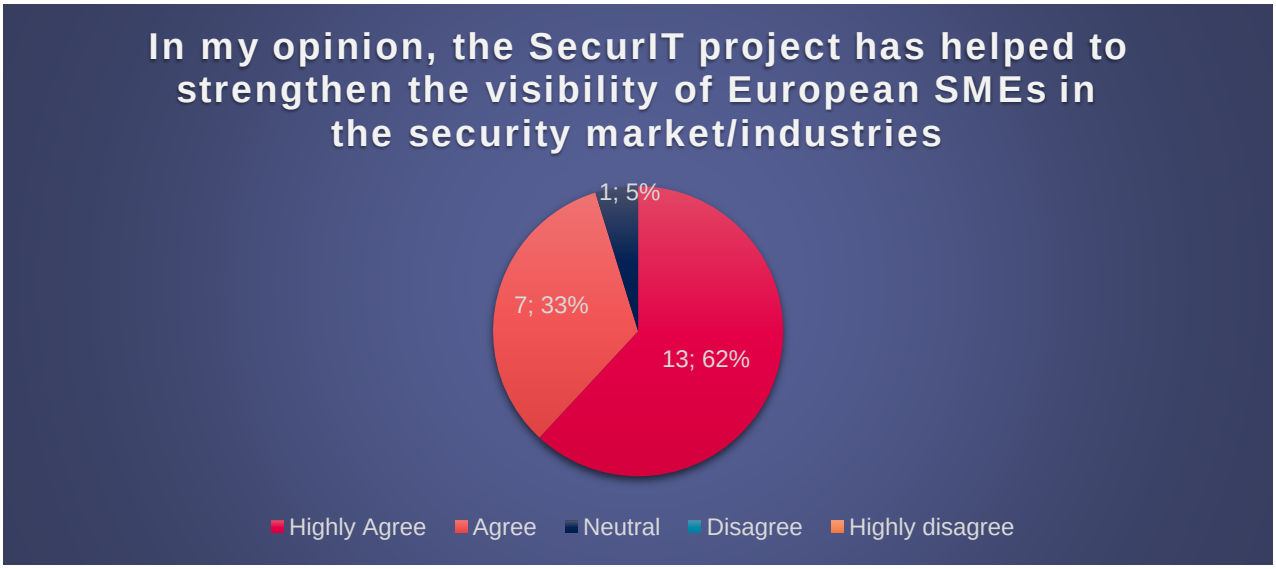
Regarding the question if the SecurIT project created new business opportunities for the involved organizations, there is a wider distribution among the answers as 12 has replied highly agree, 6 agree and 3 gave a neutral score.

For the OC1 projects, there is a slightly higher number of projects that agree as 14 projects stated that they highly agree, 4 projects agree and 3 have given a neutral score.

Some of the reasons behind the scores can be that the SecurIT project funded both demonstration and prototyping projects, and for the latter, the market and opportunities are still a bit further away. In addition, the SecurIT consortium partners can only do so much and connect the projects with potential end-users and partners, but the projects themselves need to be ready for these steps and be able to utilize these connections. Most of the companies involved in the funded projects are micro-SMEs with less than 10 employees, and to commercialise the funded solutions is a different process and requires other skills than development. Many of the projects also state in their final reports that they intend to employ new people with sales skills in order to grasp the opportunities based on the funded project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

For the fourth and last question:



The abovementioned and last question shows an overall large satisfaction with the participation in the OC2 as 13 projects have stated that they highly agree in the statement that the SecurIT project has helped to strengthen the visibility of European SMEs in the security market/industries. 7 projects mention that they agree and only 1 has given a neutral response.

Compared with the OC1 projects, the picture is very similar as 13 projects also stated that they highly agree in the statement, 5 projects mentioned that they agree and 3 were neutral.

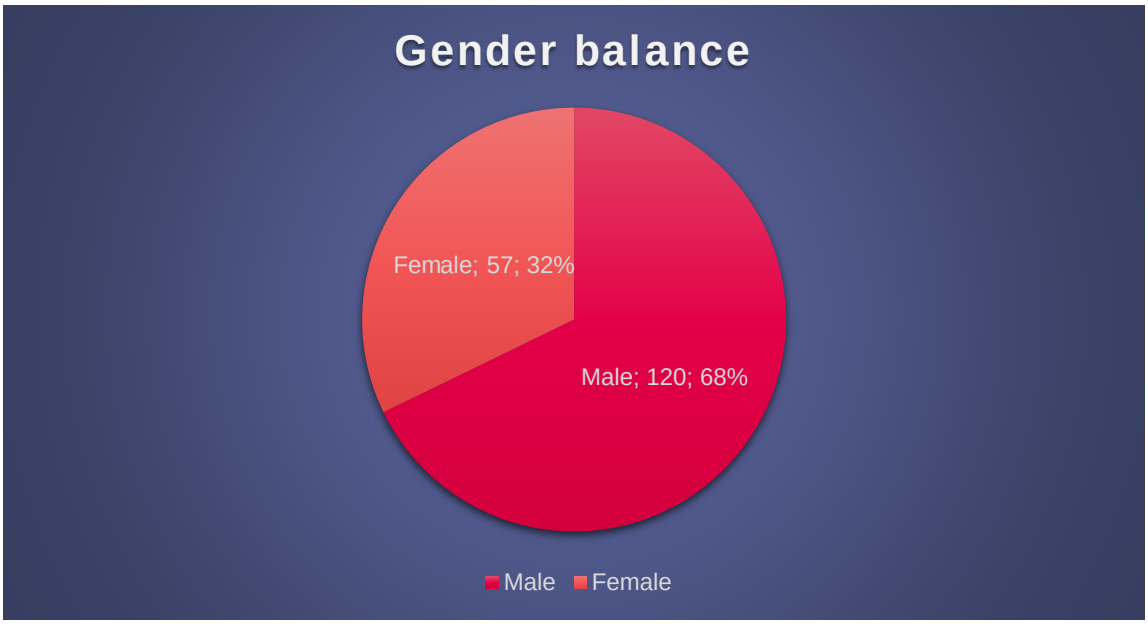
The overall conclusion on the abovementioned questions is that the OC2 projects have experienced a benefit and further strengthening of their position in the European security market by participating in the SecurIT project and are overall very satisfied with the support they have experienced through their support period.

The final aspect we want to mention is the gender balance and involvement for the OC2 projects.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Gender balance

In total, 177 people were involved in the 21 funded projects, and of this number 57 were women, giving a percentage of 32 % of women involved.



Compared with the OC1, the overall number of people being involved in the OC2 projects is higher as 166 people were involved in the OC1 projects. For the OC2 projects, the amount and percentage of women involved is also higher, compared with OC1 where 49 women were involved, giving a percentage of 29,5 % in total. The lower number of women involved in the projects were often mentioned by the projects to be of structural reasons as a lower number of women (currently) are involved in the security industry in Europe. This reason is also used by the OC2 projects when asked about the gender involvement in the project and in case there is a misbalance. However, with a slightly higher number of women involved in the OC2 projects, it is a positive sign of more focus on the issue.

To sum up on the OC2 and the involved projects, there has been an overall high satisfaction of being involved in the program and of the project support that the projects have experienced throughout the support period. From the SecurIT consortium's perspective, we have learned a lot by the OC1 projects and procedures and have tried our outmost to apply these experiences and lessons learned into improving the experience for the benefit of the OC2 projects. Based on the abovementioned results, our efforts and optimizations have worked.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Conclusion and lessons learned from the OC1 and OC2

Throughout the 36 months of the SecurIT project, the constant objectives for the consortium partners have been threefold when it comes to the funded projects; 1) how to disseminate and reach a wide range of stakeholder about the funding opportunities for the OC1 and OC2 in order to include as many and diverse security solutions as possible within the project's scope, 2) to support the SecurIT funded projects in the best possible way, and lastly 3) to share the information and disseminate on the security solutions developed and further matured during the support program period.

From the beginning of the SecurIT project, the consortium partners been focused on the development and implementation of a structure that worked well when it came to supporting, reporting and follow up structures that would work well for both the funded projects (ensuring a "light" reporting as was promised in the grant agreement) and for the SecurIT consortium partners, in order to have sufficient amount of information to be able to obtain both qualitative and quantitative information about the projects, their progress and outcomes.

When preparing for the OC1, formal follow up mechanisms as the three reports (Follow up Report at project start, Midterm report halfway through and the Final Report at the end) were developed keeping in mind, that the different sections in the Follow Up Plan should be useful in terms of the level of information, ask for measurable project progress milestones etc. The Midterm and Final Reports were based on the content of the Follow Up Plan. However, for the OC2 projects, minor corrections were made to the reports such as the introduction of an executive summary in the Final Report (in order to get a quick overview and insights into the project, especially for the mini-committee members). In addition, a section on intellectual property rights (IPR) were introduced in order to get better insights into how the projects each intended to handle this important aspect.

In addition, as the initial Follow Up Plan laid out the foundation for each project, an extra mini-committee meeting was introduced for the OC2 projects, in other to have more people reading the reports and validating them in addition to the FUM. This in order to support each FUM and avoid blind spots, that later on would be an issue in the Midterm and Report, that is not spotting unmeasurable KPIs, unclearly written milestones and deliverables, and clarify highly technical aspects. This process worked well and furthermore gave the mini-committee members a better understanding of and insights into the projects.

A final aspect that gave further positive implications for both the OC1 and OC2 projects, were the change of the jury day format for the OC2 projects, as this paved the way for prize awards to be offered during the Final Event for all funded projects. For the OC1 applications, the projects selected to attend the jury day had to fly into Paris and pitch their project idea. For this, they would be compensated with 1000 euro for each project. However, after the jury day, the SecurIT consortium evaluated this format and concluded that this approach was not sustainable neither regarding CO2 emissions nor regarding the time the participants spent in Paris for the short project pitch. Therefore, the SecurIT consortium decided to optimize the format and for the OC2 projects, this meant online pitch sessions for the jury day, and in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

addition to have a physical kick-off meeting only for the 21 selected projects at the start of their support period in order to get to know the project participants. This was deemed more useful for the project participants, and the feedback from the projects was also that they appreciated the physical kick-off meeting being organized. Because of this change, an extra amount of the budget dedicated to the SMEs was left to be allocated, giving the SecurIT consortium the opportunity to further increase the attention towards the project's final event by offering prize awards for the selected SecurIT funded projects. The result was a dynamic and well visited final event with many opportunities for all the funded projects to connect.

To sum up, based on the OC1 and OC2, the SecurIT consortium has gained valuable experience with cascade funding and functional follow up mechanisms and processes and will draw on this experience going forward.

The last part of this deliverable contains an annex section in which the various project templates are included for the sake of transparency and inspiration.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Annexes

In the annex section, the following project templates can be found:

- Follow up Plans
  - Prototyping
  - Demonstration
- Midterm Report
  - Prototyping
  - Demonstration
- Final Report
  - Prototyping
  - Demonstration
- KPI progress report
- Demonstration questionnaire

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Follow Up Plans

Prototyping template

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Follow Up Plan

For prototyping projects

Deadline: M1 (tbc date)

1. Basic information about the Follow Up Plan

Congratulations on receiving project funding for your prototyping project.

The following information will set the frame and clarify expectations on what you need to adhere to during the project period.

As soon as possible after you have received the confirmation that your project has been granted, you need to fill in this Follow Up Plan and it should be sent to your allocated Follow Up Manager **no later than one month after acceptance and signature of the sub-grant agreement**. This plan contains all the details about your project and specific measures that you will need to address and adhere to during the project period, and it will serve as the baseline for which your progress is measured against. In total, there are 3 report to fill in – the first Follow Up Plan (handed in during the first month), the Midterm Report halfway in your support period and the Final Report at the end of your project. The two latter reports are based on the information you have inserted in the initial Follow Up Plan in M1. **Please adhere to the deadlines and please be aware that all project activities must be finalized before 30 June 2024**.

The SecurIT consortium intends to make the reporting as light and smooth as possible. That being said, the SecurIT consortium will of course be held accountable by the European Commission that we develop mechanism to follow and track progress and development, ensuring that the funded projects will develop new and innovative solutions and services. During the project period, each project is allocated a dedicated Follow Up Manager who is responsible for having a regular dialogue with you, and to whom you can address any questions and challenges. In addition, please notice, that when you receive EU funding, you are required to inform about this on your own website and display the necessary logos, and the SecurIT consortium will supply you with the necessary logos. Lastly, we would like to inform you that you will receive a survey after finalizing your project in order to evaluate the project period and experience.

The SecurIT consortium looks forward to supporting you and your project consortium in the project period.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Follow Up Plan [M1] ***Annex to Sub Grant Agreement***

Contact information on consortium:	
Name of project:	
Project start date (DD/MM/YEAR):	
Project end date (DD/MM/YEAR):	
Midterm report due (halfway) (DD/MM/YEAR):	
Final report due (end of project, latest 30 June 2024) (DD/MM/YEAR):	
Contact information of lead partner:	Name:
	Email:
	Organisation:
	Title and function:
	Country:
	Website:
Contact information on 2nd consortium partner:	Name:
	Email:
	Organisation:
	Function:
	Country:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Website:
Contact information on 3rd consortium partner (if any):	Name:
	Email:
	Organisation:
	Function:
	Country:
	Website:
Project information:	
Project description for ***internal use only*** for the project consortium to get a better understanding of the project. This information will **not** be shared with external stakeholders.	
Project information for ***public dissemination***. The information will be published on the project website, social media sites and used for other public communication activities by the SecurIT project consortium. ***Please follow this format:*** • 10 lines of description of the key scope of the project • include logos for all partners (high res.) • 1-2 pictures to visualize your project. *Please send the logos and pictures to your Follow Up Manager in a separate email.*	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Please confirm that we are allowed to publish the abovementioned public information on the various public sites	
Domain (please mention the domain you are targeting with your project) (Domain 1: Sensitive infrastructure protection, Domain 2: Disaster Resilience, Domain 3: Public Spaces protection).	
Challenge(s) (please insert the challenge(s) you are targeting here with number and name).	
Project Plan:	
Please outline your project plan for the entire project period including the work packages (WP), tasks, expected deliverables and milestones, you intent to achieving during the project period, and please include the timings for these. Please build on what you already mentioned in your initial application. **Please be specific in your description.** **Deliverables** are additional outputs (e.g., information, special report, a technical diagram brochure, list, a software milestone, or other building block of the project) that must be produced at a given moment during the action.). *For software projects, it is crucial to deliver some tangible proof of the project progress (e.g., video etc.)*	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Milestones are control points in the project that help to chart progress, and they may correspond to the completion of a key deliverable, allowing the next phase of the work to begin or be needed at intermediary points.	
Dissemination activities:	
Please describe the dissemination activities that you expect/plan to execute during the project period (e.g. informing about the project in national medias, newsletters, during national events etc.). Please be specific in your description.	
TRL level:	
TRL level at project start (incl. a short description)	
TRL level at project end (incl. a short description)	
Key performance indicators: project specific	
Describe up to 4 project specific KPIs (*with a value for easier measurement*). You can use the description from the proposal. Please be specific in the description of the KPI and include an expected time for when they are expected to be achieved e.g., for the Midterm or Final report. This will be used to evaluate your progress in the Midterm and Final Reports respectively.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Midterm	Final
1.		
2.		
3.		
4.		

Key performance indicators: generic

The following section consists of 8 generic KPIs (*insert a value for easier measurement*). Please indicate a baseline (of the current status) and describe your expectations for the development of each parameter at the end of the project to be included in the Final Report:

	Baseline (current status)	Final
1. Employment created / safeguarded due to the Project (also stating the number of employees before the project		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

(baseline) as well as forecasts for Final/2024)		
2. Impact on turnover due to the project (baseline and forecasts for 2024)		
3. Market share acquired due to the project (baseline and forecasts for 2024)		
4. Environmental impact (if applicable), (water consumption, energy…) generated by the project (baseline and forecasts for 2024)		
5. Contribution of the project to new or significantly improved products launched (baseline and forecasts for 2024)		
6. Contribution of the project to new or significantly improved methods and processes (baseline and forecasts for 2024)		
7. Advancement of TRL due to the Project (baseline and forecasts for 2024)		
8. Other forms of finance, such as risk capital or public funds, raised by the Project (if applicable)		
Exploitation:		
Describe how you expect to exploit the knowledge and progress developed in the project (and how it will be used after the project is finished)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Please be specific in your description.	
Total budget distribution:	
Lead partner budget	Staff costs: Travel costs: Other costs (purchase of goods or services, please specify): Subcontracting costs:
2nd partner budget	Staff costs: Travel costs: Other costs (purchase of goods or services, please specify): Subcontracting costs:
3rd partner budget	Staff costs: Travel costs: Other costs (purchase of goods or services, please specify): Subcontracting costs:
(*only if applicable*) Demonstrate compliance with regulatory issues + timings for demonstrations (conditions):	
Please describe the timings, physical places and in which environments the demonstrations will be conducted over the project duration. Please be as precise as possible (and please indicate if	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

consortium members will be allowed to join the demonstrations). In addition, please address how you will ensure to remain GDPR compliant. Please be specific in your description.	
Ethics self-assessment:	
Please address any ethical issues that have been identified in the self-assessment evaluation and describe how counter measures will be put in place to mitigate any potential issues. Please explain in detail to avoid any misunderstandings. (If applicable) Also please address the ethical concerns that the ethical expert identified prior to the Jury Day.	
Risks:	
Please describe the risks you have identified (for instance technological, collaboration or external factors) and explain which mitigating practices you intend to put in place to keep the project on track for the project period.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Collaboration agreement		
Did you sign a collaboration agreement among the project partners?	Yes	
	If yes, please explain which kind of agreement (LoI, MoU etc.)	
	No	
	Follow Up Manager:	
Assigned Follow Up Manager (name, cluster, email)		

Signatures:

_____ _____

1st partner, name and date **2nd partner, name and date**

_____ _____

3rd partner, name and date **Follow Up Manager, name and date**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Demonstration template

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Follow Up Plan

For demonstration projects

Deadline: M1 (tbc date)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

2. Basic information about the Follow Up Plan

Congratulations on receiving project funding for your demonstration project.

The following information will set the frame and clarify expectations on what you need to adhere to during the project period.

As soon as possible after you have received the confirmation that your project has been granted, you need to fill in this Follow Up Plan and it should be sent to your allocated Follow Up Manager **no later than one month after acceptance and signature of the sub-grant agreement**. This plan contains all the details about your project and specific measures that you will need to address and adhere to during the project period, and it will serve as the baseline for which your progress is measured against. In total, there are 3 report to fill in – the first Follow Up Plan (handed in during the first month), the Midterm Report halfway in your support period and the Final Report at the end of your project. The two latter reports are based on the information you have inserted in the initial Follow Up Plan in M1. **Please adhere to the deadlines and please be aware that all project activities must be finalized before 30 June 2024**.

The SecurIT consortium intends to make the reporting as light and smooth as possible. That being said, the SecurIT consortium will of course be held accountable by the European Commission that we develop mechanism to follow and track progress and development, ensuring that the funded projects will develop new and innovative solutions and services. During the project period, each project is allocated a dedicated Follow Up Manager who is responsible for having a regular dialogue with you, and to whom you can address any questions and challenges. In addition, please notice, that when you receive EU funding, you are required to inform about this on your own website and display the necessary logos, and the SecurIT consortium will supply you with the necessary logos. Lastly, we would like to inform you that you will receive a survey after finalizing your project in order to evaluate the project period and experience.

The SecurIT consortium looks forward to supporting you and your project consortium in the project period.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Follow Up Plan [M1] ***Annex to Sub Grant Agreement***

Contact information on consortium:	
Name of project:	
Project start date (DD/MM/YEAR):	
Project end date (DD/MM/YEAR):	
Midterm report due (halfway) (DD/MM/YEAR):	
Final report due (end of project, latest 30 June 2024) (DD/MM/YEAR):	
Contact information of lead partner:	Name:
	Email:
	Organisation:
	Title and function:
	Country:
	Website:
Contact information on 2nd consortium partner:	Name:
	Email:
	Organisation:
	Function:
	Country:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Website:
Contact information on 3rd consortium partner (if any):	Name:
	Email:
	Organisation:
	Function:
	Country:
	Website:
Project information:	
Project description for ***internal use only*** for the project consortium to get a better understanding of the project. This information will **not** be shared with external stakeholders.	
Project information for ***public dissemination***. The information will be published on the project website, social media sites and used for other public communication activities by the SecurIT project consortium. ***Please follow this format:*** • 10 lines of description of the key scope of the project • include logos for all partners (high res.) • 1-2 pictures to visualize your project. *Please send the logos and pictures to your Follow Up Manager in a separate email.*	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Please confirm that we are allowed to publish the abovementioned public information on the various public sites	
Domain (please mention the domain you are targeting with your project) (Domain 1: Sensitive infrastructure protection, Domain 2: Disaster Resilience, Domain 3: Public Spaces protection).	
Challenge(s) (please insert the challenge(s) you are targeting here with number and name).	
Project Plan:	
Please outline your project plan for the entire project period including the work packages (WP), tasks, expected deliverables and milestones, you intent to achieving during the project period, and please include the timings for these. Please build on what you already mentioned in your initial application. **Please be specific in your description.** **Deliverables** are additional outputs (e.g., information, special report, a technical diagram brochure, list, a software milestone, or other building block of the project) that must be produced at a given moment during the action.). *For software projects, it is crucial to deliver some tangible proof of the project progress (e.g., video etc.)*	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Milestones are control points in the project that help to chart progress, and they may correspond to the completion of a key deliverable, allowing the next phase of the work to begin or be needed at intermediary points.	
Dissemination activities:	
Please describe the dissemination activities that you expect/plan to execute during the project period (e.g. informing about the project in national medias, newsletters, during national events etc.). Please be specific in your description.	
TRL level:	
TRL level at project start (incl. a short description)	
TRL level at project end (incl. a short description)	
Key performance indicators: project specific	
Describe up to 4 project specific KPIs (*with a value for easier measurement*). You can use the description from the proposal. Please be specific in the description of the KPI and include an expected time for when they are expected to be achieved e.g., for the Midterm or Final report. This will be used to evaluate your progress in the Midterm and Final Reports respectively.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Midterm	Final
1.		
2.		
3.		
4.		

Key performance indicators: generic

The following section consists of 8 generic KPIs (*insert a value for easier measurement*). Please indicate a baseline (of the current status) and describe your expectations for the development of each parameter at the end of the project to be included in the Final Report:

	Baseline (current status)	Final
9. Employment created / safeguarded due to the Project (also stating the number of employees before the project		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

(baseline) as well as forecasts for Final/2024)		
10. Impact on turnover due to the project (baseline and forecasts for 2024)		
11. Market share acquired due to the project (baseline and forecasts for 2024)		
12. Environmental impact (if applicable), (water consumption, energy…) generated by the project (baseline and forecasts for 2024)		
13. Contribution of the project to new or significantly improved products launched (baseline and forecasts for 2024)		
14. Contribution of the project to new or significantly improved methods and processes (baseline and forecasts for 2024)		
15. Advancement of TRL due to the Project (baseline and forecasts for 2024)		
16. Other forms of finance, such as risk capital or public funds, raised by the Project (if applicable)		
Exploitation:		
Describe how you expect to exploit the knowledge and progress developed in the project (and how it will be used after the project is finished)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Please be specific in your description.	
Total budget distribution:	
Lead partner budget	Staff costs: Travel costs: Other costs (purchase of goods or services, please specify): Subcontracting costs:
2nd partner budget	Staff costs: Travel costs: Other costs (purchase of goods or services, please specify): Subcontracting costs:
3rd partner budget	Staff costs: Travel costs: Other costs (purchase of goods or services, please specify): Subcontracting costs:
Demonstrate compliance with regulatory issues + timings for demonstrations (conditions):	
Please describe the timings, physical places and in which environments the demonstrations will be conducted over the project duration. Please be as precise as possible (and please indicate if	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

consortium members will be allowed to join the demonstrations). In addition, please address how you will ensure to remain GDPR compliant. Please be specific in your description.	

Ethics self-assessment:

Please address any ethical issues that have been identified in the self-assessment evaluation and describe how counter measures will be put in place to mitigate any potential issues. Please explain in detail to avoid any misunderstandings. (If applicable) Also please address the ethical concerns that the ethical expert identified prior to the Jury Day.	

Risks:

Please describe the risks you have identified (for instance technological, collaboration or external factors) and explain which mitigating practices you intend to put in place to keep the project on track for the project period.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Collaboration agreement		
Did you sign a collaboration agreement among the project partners?	Yes	
	If yes, please explain which kind of agreement (LoI, MoU etc.)	
	No	
	Follow Up Manager:	
Assigned Follow Up Manager (name, cluster, email)		

Signatures:

_____ _____

1st partner, name and date **2nd partner, name and date**

_____ _____

3rd partner, name and date **Follow Up Manager, name and date**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Midterm Reports

Prototyping template

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Midterm Report

For prototyping projects OC2

Deadline: Halfway

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

1. Information about the Midterm Report

The Midterm Report is based on the initial Follow Up Plan filled in and signed at the beginning of the project period.

The Midterm Report is intended to evaluate and measure your project progress halfway in your project period, in order for the SecurIT consortium to get further insights into your project development, outcomes and impacts.

The SecurIT consortium intends to make the reporting as light and smooth as possible. That being said, the SecurIT consortium will of course be held accountable by the European Commission that we develop mechanism to follow and track progress and development, ensuring that the funded projects will develop new and innovative solutions and services in line with the SecurIT objectives.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Contact information on consortium:	
Name of project:	
Project start date (DD/MM/YEAR):	
Project end date (DD/MM/YEAR):	
Midterm report due (halfway) (DD/MM/YEAR):	
Final report due (end of project) (DD/MM/YEAR):	
Contact information of lead partner:	Name:
	Email:
	Organisation:
	Title and function:
	Country:
	Website:
Contact information on 2nd consortium partner:	Name:
	Email:
	Organisation:
	Function:
	Country:
	Website:
Contact information on 3rd consortium partner (if any):	Name:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Email:
	Organisation:
	Function:
	Country:
	Website:

Project plan and progress:

With a point of departure in the project plan you outlined in the Follow Up Plan (M1), please describe the project achievements you have accomplished halfway in your project period, also including the achieved deliverables and milestones. Please be explicit in your explanation. If there are any deviations, please explain why this is the case and which corrective measures you have used or will use in order to get your project back on track.	

Dissemination activities:

Please describe the dissemination activities that you have participated in in the first half of your project period (both in terms of those activities mentioned in the first Follow Up Plan and additional ones).	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

If there are any deviations, please explain why this is the case and which corrective measures you have used or will use in order to get your project back on track.	

Information on your project progress for public dissemination:

Please describe your project progress halfway in your project, and please notice that this will be for ***public dissemination***. The information will be published on the project website, social media sites and used for other public communication activities by the SecurIT project consortium. Please follow this format: -10 lines of description of the key progress within the first half of the project. In addition, send pictures, videos, or other material to your dedicated Follow Up Manager in a separate email.	
Please confirm in the text that we are allowed to share the information.	

Key performance indicators: project specific

Please evaluate your project progress based on the KPIs you mentioned in the first Follow Up Plan and status halfway in your project period. If there are any deviations, please explain why this is the case and which corrective measures you have used or will use in order to get your project back on track:

	Halfway
1.	
2.	
3.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

4.	
Exploitation:	
Please describe how you have exploited the knowledge and progress developed and obtained in the project period so far (including business and market perspectives). Please be specific in your description.	
Demonstrate compliance with regulatory issues + timings for demonstrations (conditions) (*only if applicable):*	
Please describe the demonstrations executed in the first half of your project period (timings, physical places and in which environments the demonstrations have been conducted the first period). In addition, please address how you will ensure to remain compliant with GDPR and with other regulatory aspects. Please be specific in your description.	
Ethics self-assessment:	
Please address any ethical issues that you have identified (if any) during this project period and describe how counter measures have been or will be put in place to mitigate any potential issues. Please explain in detail to avoid any misunderstandings.	
Risks:	
Please describe the risks you have identified during the first half of your project period (for instance technological, collaboration or external factors) and explain which mitigating practices	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

you intend to put in place to keep the project on track for the remaining project period.	
Other identified issues:	
Please describe if you have encountered any issues e.g. technological gaps, technical components (supply), system integrations, market immaturity, lack of market, funding etc.	
Overall assessment and evaluation halfway in your project period:	
Please elaborate and sum up on the development and experience you have made halfway in the project period, and explain what has worked well, what has been challenging and what corrective measures you have taken to keep your project on track the remaining project period. You are also welcome to include a comment on your relations and collaboration with the SecurIT consortium, and let us know if we can improve in some aspects.	
	Follow Up Manager:
Assigned Follow Up Manager (name, cluster, email)	

Signatures:

_____ _____

1st partner, name and date **2nd partner, name and date**

_____ _____

3rd partner, name and date **Follow Up Manager, name and date**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Demonstration template

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Midterm Report

For demonstration projects OC2

Deadline: Halfway

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

1. Information about the Midterm Report

The Midterm Report is based on the initial Follow Up Plan filled in and signed at the beginning of the project period.

The Midterm Report is intended to evaluate and measure your project progress halfway in your project period, in order for the SecurIT consortium to get further insights into your project development, outcomes and impacts.

The SecurIT consortium intends to make the reporting as light and smooth as possible. That being said, the SecurIT consortium will of course be held accountable by the European Commission that we develop mechanism to follow and track progress and development, ensuring that the funded projects will develop new and innovative solutions and services in line with the SecurIT objectives.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Contact information on consortium:	
Name of project:	
Project start date (DD/MM/YEAR):	
Project end date (DD/MM/YEAR):	
Midterm report due (halfway) (DD/MM/YEAR):	
Final report due (end of project) (DD/MM/YEAR):	
Contact information of lead partner:	Name:
	Email:
	Organisation:
	Title and function:
	Country:
	Website:
Contact information on 2nd consortium partner:	Name:
	Email:
	Organisation:
	Function:
	Country:
	Website:
Contact information on 3rd consortium partner (if any):	Name:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Email:
	Organisation:
	Function:
	Country:
	Website:

Project plan and progress:

With a point of departure in the project plan you outlined in the Follow Up Plan (M1), please describe the project achievements you have accomplished halfway in your project period, also including the achieved deliverables and milestones. Please be explicit in your explanation. If there are any deviations, please explain why this is the case and which corrective measures you have used or will use in order to get your project back on track.	

Dissemination activities:

Please describe the dissemination activities that you have participated in in the first half of your project period (both in terms of those activities mentioned in the first Follow Up Plan and additional ones). If there are any deviations, please explain why this is the case and which corrective measures you have used or will use in order to get your project back on track.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Information on your project progress for public dissemination:	
Please describe your project progress halfway in your project, and please notice that this will be for ***public dissemination***. The information will be published on the project website, social media sites and used for other public communication activities by the SecurIT project consortium. Please follow this format: -10 lines of description of the key progress within the first half of the project. In addition, send pictures, videos, or other material to your dedicated Follow Up Manager in a separate email.	
Please confirm in the text that we are allowed to share the information.	

Key performance indicators: project specific	
Please evaluate your project progress based on the KPIs you mentioned in the first Follow Up Plan and status at mid-term. If there are any deviations, please explain why this is the case and which corrective measures you have used or will use in order to get your project back on track:	
	Halfway
1.	
2.	
3.	
4.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Exploitation:	
Please describe how you have exploited the knowledge and progress developed and obtained in the project period so far (including business and market perspectives). Please be specific in your description.	
Demonstrate compliance with regulatory issues + timings for demonstrations (conditions):	
Please describe the demonstrations executed in the first half of your project period (timings, physical places and in which environments the demonstrations have been conducted the first period). In addition, please address how you will ensure to remain compliant with GDPR and with other regulatory aspects. Please be specific in your description.	
Ethics self-assessment:	
Please address any ethical issues that you have identified (if any) in the first half of your project and describe how counter measures have been or will be put in place to mitigate any potential issues. Please explain in detail to avoid any misunderstandings.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Risks:	
Please describe the risks you have identified during the first half of your project (for instance technological, collaboration or external factors) and explain which mitigating practices you have, or you intend to put in place to keep the project on track for the remaining project period.	
Other identified issues:	
Please describe if you have encountered any issues e.g. technological gaps, technical components (supply), system integrations, market immaturity, lack of market, funding etc.	
Overall assessment and evaluation of the first half of your project period:	
Please elaborate and sum up on the first half of the project period, and explain what has worked well, what has been challenging and what corrective measures you have taken to keep your project on track the remaining project period. You are also welcome to include a comment on your relations and collaboration with the SecurIT consortium, and let us know if we can improve in some aspects.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Follow Up Manager:
Assigned Follow Up Manager (name, cluster, email)	

Signatures:

_____ _____

1st partner, name and date **2nd partner, name and date**

_____ _____

3rd partner, name and date **Follow Up Manager, name and date**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Final Reports

Prototyping template

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Final Report

For prototyping projects OC2

Deadline: (date of project ending)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

1. Information about the Final Report

The information in the Final Report is based on the information in the initial Follow Up Plan signed at the beginning of the project period, and the progress described in the Midterm Report.

The Final Report is intended to evaluate and measure your project progress during your (up to) 12-month project support program period and to give the SecurIT consortium insights into your project developments, outcomes and impacts. When the Final Report is validated by the consortium (firstly the Follow Up Committee and then the Selection Committee), it will trigger the 2nd and last payment to you and your project partners (up to 80 %).

The SecurIT consortium intends to make the reporting as light and smooth as possible. That being said, the SecurIT consortium will of course be held accountable by the European Commission that we develop mechanism to follow and track progress and development, ensuring that the funded projects will develop new and innovative solutions and services in line with the SecurIT objectives.

Testimonials

As part of the communication activities of SecurIT, testimonials and success stories of some of the funded collaborative projects, will be published by the SecurIT consortium on the dedicated SecurIT website, social media accounts and other platforms. Therefore, in addition to this Final Report, you might be contacted by the SecurIT consortium in order to elaborate these testimonials/success stories after your project has ended.

Final event of the SecurIT project

As part of the final event for the SecurIT project, an award ceremony and contest will be organised during Spring 2024. The contest will be open to all projects which got funding from SecurIT (1st and 2nd calls). The goal will be to select the “best” SecurIT collaborative projects. The rules and criteria for selection will be established into details in 2024. Participants to this contest will likely have to provide short videos describing their project and results. Specific guidelines will be established by the SecurIT consortium in 2024. All projects funded by SecurIT will be encouraged to participate, and therefore we encourage the funded projects to well document their prototyping or demonstration phase with pictures, videos, since such material could be useful for them for the contest.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

Contact information on consortium:	
Name of project:	
Project start date (DD/MM/YEAR):	
Project end date (DD/MM/YEAR):	
Final report due (DD/MM/YEAR):	
Contact information of lead partner:	Name:
	Email:
	Organisation:
	Title and function:
	Country:
	Website:
Contact information on 2nd consortium partner:	Name:
	Email:
	Organisation:
	Function:
	Country:
	Website:
Contact information on 3rd consortium partner (if any):	Name:
	Email:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Organisation:
	Function:
	Country:
	Website:

Executive summary:

Please provide an overview of the main developments and achievements during the project duration. *This summary will **not** be made public and is only intended for internal understanding of the project between the SecurIT consortium partners and the European Commission.*	

Project plan and progress:

With a point of departure in the project plan you outlined in the Follow Up Plan (M1), please describe all the project achievements you have accomplished during your project period, also including the achieved deliverables and milestones. ***Please be specific and exhaustive in your description and include all the information.*** If there are any deviations, please explain why this is the case.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Dissemination activities:	
Please describe the dissemination activities that you have participated in during the entire project period (both in terms of those activities mentioned in the first Follow Up Plan M1 and additional ones not initially anticipated). These activities include both physical and/or online activities, where you have informed about your SecurIT funded project to a larger group of stakeholders. If there are any deviations from the activities you planned at the beginning of the project, please explain why this is the case.	
Information on your project progress for public dissemination:	
Please describe your project progress within the entire project period, and please notice that this will be for ***public dissemination***. The information will be published on the project website, social media sites and used for other public communication activities by the SecurIT project consortium. *This is an opportunity for you to share information about your project that shows the impact of your solution developed in the program period.* *You can find examples of this at the SecurIT website, under each project (scroll to see all the information).* Please follow this format:	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

-description of the key progress within the entire project duration. *In addition,* ***send pictures, videos, or other material to your dedicated Follow Up Manager in a separate email.*** **Testimonials** In addition, you might be contacted by the SecurIT consortium in order to elaborate these testimonials/success stories after your project has ended.	
Please confirm in the text that we are allowed to share the information.	

TRL level:

Please insert your **project TRL level at the project start**, and a few lines of description to document this point of departure TRL level:	
Please insert your **project TRL level at the project end**, and a few lines of description to document this increase in the TRL level:	

Key performance indicators: project specific

Please evaluate your project progress based on the KPIs you mentioned in the first Follow Up Plan and status at the project end. If there are any deviations, please explain why this is the case. *It is important that you are clear and extensive in your description, so it is completely clear what you have accomplished at the project end. In the below, you will have an opportunity to differentiate between the expected KPI result as foreseen in the initial Follow Up Plan at the project start, and the actual results and achievements (if there is no difference between the expected and actual results, please add the same information in both columns):*

	Expectations (as foreseen in the Follow Up Plan M1)	**Project end** (actual achievements)
1)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

2)		
3)		
4)		

Key performance indicators: generic

Please insert the information from your Follow Up Plan M1 in both the baseline column and expectations at the project end and add the actual achievements in the column to the right. Please describe and comment on each of the KPIs (only in the right column of the actual achievements).

Example: E.g. *under "1) Employment created – if you at the baseline have inserted 4 and expected at the project end to increase to 20, but in reality you have only hired 2 new persons, please explain the reasons behind the deviations under the actual achievements.). If there are any deviations between your expectations and the realized KPIs at the project end, please explain why this is the case.*

	Baseline *(at project start, and as mentioned in the Follow Up Plan M1)*	**Expectations** *(at project end, and as mentioned in the Follow Up Plan M1)*	**Actual achievements** (at project end)
1) Employment created / safeguarded due to the project (number of employees at project start			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

(baseline), expectations and actual achievements)			
2) Impact on turnover due to the project (baseline, expectations and actual achievements)			
3) Market share acquired due to the project (baseline, expectations and actual achievements)			
4) Environmental impact (if applicable), (water consumption, energy…) generated by the project (baseline, expectations and actual achievements)			
5) Contribution of the project to new or significantly improved products launched (baseline, expectations and actual achievements)			
6) Contribution of the project to new or significantly improved methods and processes (baseline, expectations and actual achievements)			
7) Advancement of TRL due to the Project (baseline, expectations and actual achievements)			
8) Other forms of finance, such as risk capital or public funds, raised by the project (if applicable)			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Exploitation:	
Please describe how you have exploited the knowledge and progress developed and obtained in the project period so far. *This can be internal (within one of your companies) or external.*	
What was most successful in your exploitation activities? Briefly expand on the action and success	
Please indicate what your plans are for future exploitation beyond the SecurIT support program. *Please be specific in your description.* *Please remember that the Final event organized in the Spring 2024 (as mentioned in the introduction to this report), also is an opportunity for you to exploit the knowledge obtained in the project period and to develop your project further.*	
Demonstrations (*only if applicable*):	
Please describe the demonstrations executed during the entire project period (timings, end-users, physical places and in which environments the demonstrations have been conducted during the project period). In addition, please elaborate on the lessons learnt from the demonstrations. Lastly, please address how you ensured to remain GDPR compliant, and please be specific in your description.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Ethics self-assessment:	
Please address any ethical issues that you have identified (if any) in the project period and describe how counter measures have been put in place to mitigate any potential issues. ***Please explain in detail to avoid any misunderstandings.***	
Risks:	
Please describe the risks you have identified during the project period (for instance technological, collaboration or external factors) and explain how you have overcome these challenges.	
Gender balance:	
What was the gender balance in your project team? Please indicate the number of male and female members involved in your project execution (provide aggregated numbers for all partners).	- Number of female team members: - Number of male team members:
If there was a gender misbalance in your project, please explain the reasons behind this.	
Other identified issues:	
Please describe if you have encountered any issues during the project period e.g. technological gaps, technical components (supply), system integrations, market immaturity, lack of market, funding etc.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Sustainability of the Project:	
What are the challenges you need to overcome to ensure a successful future of the project? *Please describe 3-5 challenges and how you plan to overcome these challenges.*	
Do you need any further collaboration partner(s) or new partnerships for a successful commercialisation of your solution. And if yes, which types of collaboration/partnerships do you need? *Please be as concrete as possible, so, if possible, the SecurIT consortium can assist in the facilitation of a collaboration/partnership.*	
Commercialization strategy: please elaborate on your long-term vision of the marketing strategy incl. how do you propose to attract more potential clients, get into the right networks, and create your own brand. What will be the focus of your marketing strategy? *Max. 300 words.*	• **Market approach** • **Marketing strategy** • **Targets (in 1, 3 and 5 year(s))**
Outcomes regarding IPR management: please elaborate how you are planning to handle the Intellectual Property Rights (IPR) deriving from the project activities, and how you in the project consortium	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

expect to collaboration going forward (did you sign a collaboration agreement for future collaboration after the project end, how did you manage IPR based on the project results, and eventually any patents).	

Overall assessment and evaluation of the (up to) 12 months project period:

Please elaborate and sum up on the entire project period, and identify what has worked well, what has been challenging and what corrective measures you have taken to keep your project on track.	
You are also welcome to include a comment on your relations and collaboration with the SecurIT consortium and let us know if we can improve in some aspects.	
Based on the above provided assessment and evaluation, please provide a rating on a scale of 5-1 for the following aspects:	Please insert an x in the category that fits to your experience:

Categories:	**5 Highly agree**	**4 Agree**	**3 Neutral**	**2 Disagree**	**1 Highly disagree**
The collaboration with and guidance of my dedicated follow up manager has worked well (regular meetings etc.)					
The SecurIT process and structure has worked well (from the open call process, jury day selection, regular meetings, payment installments frequency, progress reports etc.)					

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

The SecurIT project created new business opportunities for my organisation (open up new markets, new customers etc.)					
In my opinion, the SecurIT project has helped to strengthen the visibility of European SMEs in the security market/industries					
In case you want to comment on your abovementioned scores, please elaborate here:					
Follow Up Manager:					
Assigned Follow Up Manager (name, cluster, email)					

Signatures:

1st partner, name and date

2nd partner, name and date

3rd partner, name and date

Follow Up Manager, name and date

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Demonstration template

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Final Report

For demonstration projects OC2

Deadline: (date of project ending)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

1. Information about the Final Report

The information in the Final Report is based on the information in the initial Follow Up Plan signed at the beginning of the project period, and the progress described in the Midterm Report.

The Final Report is intended to evaluate and measure your project progress during your (up to) 12-month project support program period and to give the SecurIT consortium insights into your project developments, outcomes and impacts. When the Final Report is validated by the consortium (firstly the Follow Up Committee and then the Selection Committee), it will trigger the 2nd and last payment to you and your project partners (up to 80 %).

The SecurIT consortium intends to make the reporting as light and smooth as possible. That being said, the SecurIT consortium will of course be held accountable by the European Commission that we develop mechanism to follow and track progress and development, ensuring that the funded projects will develop new and innovative solutions and services in line with the SecurIT objectives.

Testimonials

As part of the communication activities of SecurIT, testimonials and success stories of some of the funded collaborative projects, will be published by the SecurIT consortium on the dedicated SecurIT website, social media accounts and other platforms. Therefore, in addition to this Final Report, you might be contacted by the SecurIT consortium in order to elaborate these testimonials/success stories after your project has ended.

Final event of the SecurIT project

As part of the final event for the SecurIT project, an award ceremony and contest will be organised during Spring 2024. The contest will be open to all projects which got funding from SecurIT (1st and 2nd calls). The goal will be to select the “best” SecurIT collaborative projects. The rules and criteria for selection will be established into details in 2024. Participants to this contest will likely have to provide short videos describing their project and results. Specific guidelines will be established by the SecurIT consortium in 2024. All projects funded by SecurIT will be encouraged to participate, and therefore we encourage the funded projects to well document their prototyping or demonstration phase with pictures, videos, since such material could be useful for them for the contest.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

Contact information on consortium:	
Name of project:	
Project start date (DD/MM/YEAR):	
Project end date (DD/MM/YEAR):	
Final report due (DD/MM/YEAR):	
Contact information of lead partner:	Name:
	Email:
	Organisation:
	Title and function:
	Country:
	Website:
Contact information on 2nd consortium partner:	Name:
	Email:
	Organisation:
	Function:
	Country:
	Website:
Contact information on 3rd consortium partner (if any):	Name:
	Email:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Organisation:
	Function:
	Country:
	Website:

Executive summary:

Please provide an overview of the main developments and achievements during the project duration. *This summary will **not** be made public and is only intended for internal understanding of the project between the SecurIT consortium partners and the European Commission.*	

Project plan and progress:

With a point of departure in the project plan you outlined in the Follow Up Plan (M1), please describe all the project achievements you have accomplished during your project period, also including the achieved deliverables and milestones. ***Please be specific and exhaustive in your description and include all the information.*** If there are any deviations, please explain why this is the case.	

Dissemination activities:

Please describe the dissemination activities that you have participated in during the entire project period (both in terms of those activities mentioned in the first Follow Up	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Plan M1 and additional ones not initially anticipated). These activities include both physical and/or online activities, where you have informed about your SecurIT funded project to a larger group of stakeholders. If there are any deviations from the activities you planned at the beginning of the project, please explain why this is the case.	

Information on your project progress for public dissemination:

Please describe your project progress within the entire project period, and please notice that this will be for ***public dissemination***. The information will be published on the project website, social media sites and used for other public communication activities by the SecurIT project consortium. *This is an opportunity for you to share information about your project that shows the impact of your solution developed in the program period.* *You can find examples of this at the SecurIT website, under each project (scroll to see all the information).* Please follow this format: -description of the key progress within the entire project duration. *In addition,* ***send pictures, videos, or other material to your dedicated Follow Up Manager in a separate email.*** **Testimonials** In addition, you might be contacted by the SecurIT consortium in order to elaborate	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

these testimonials/success stories after your project has ended.	
Please confirm in the text that we are allowed to share the information.	

TRL level:

Please insert your **project TRL level at the project start**, and a few lines of description to document this point of departure TRL level:	
Please insert your **project TRL level at the project end**, and a few lines of description to document this increase in the TRL level:	

Key performance indicators: project specific

Please evaluate your project progress based on the KPIs you mentioned in the first Follow Up Plan and status at the project end. If there are any deviations, please explain why this is the case. *It is important that you are clear and extensive in your description, so it is completely clear what you have accomplished at the project end. In the below, you will have an opportunity to differentiate between the expected KPI result as foreseen in the initial Follow Up Plan at the project start, and the actual results and achievements (if there is no difference between the expected and actual results, please add the same information in both columns):*

	Expectations (as foreseen in the Follow Up Plan M1)	**Project end** (actual achievements)
1)		
2)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

3)		
4)		

Key performance indicators: generic

Please insert the information from your Follow Up Plan M1 in both the baseline column and expectations at the project end and add the actual achievements in the column to the right. Please describe and comment on each of the KPIs (only in the right column of the actual achievements).

Example: E.g. *under "1) Employment created – if you at the baseline have inserted 4 and expected at the project end to increase to 20, but in reality you have only hired 2 new persons, please explain the reasons behind the deviations under the actual achievements.). If there are any deviations between your expectations and the realized KPIs at the project end, please explain why this is the case.*

	Baseline *(at project start, and as mentioned in the Follow Up Plan M1)*	**Expectations** *(at project end, and as mentioned in the Follow Up Plan M1)*	**Actual achievements** (at project end)
1) Employment created / safeguarded due to the project (number of employees at project start (baseline), expectations and actual achievements)			
2) Impact on turnover due to the project (baseline,			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

expectations and actual achievements)			
3) Market share acquired due to the project (baseline, expectations and actual achievements)			
4) Environmental impact (if applicable), (water consumption, energy…) generated by the project (baseline, expectations and actual achievements)			
5) Contribution of the project to new or significantly improved products launched (baseline, expectations and actual achievements)			
6) Contribution of the project to new or significantly improved methods and processes (baseline, expectations and actual achievements)			
7) Advancement of TRL due to the Project (baseline, expectations and actual achievements)			
8) Other forms of finance, such as risk capital or public funds, raised by the project (if applicable)			

Exploitation:	
Please describe how you have exploited the knowledge and progress developed and obtained in the project period so far. *This can be internal (within one of your companies) or external.*	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

What was most successful in your exploitation activities? Briefly expand on the action and success	
Please indicate what your plans are for future exploitation beyond the SecurIT support program. *Please be specific in your description.* *Please remember that the Final event organized in the Spring 2024 (as mentioned in the introduction to this report), also is an opportunity for you to exploit the knowledge obtained in the project period and to develop your project further.*	
Demonstrations:	
Please describe the demonstrations executed during the entire project period (timings, end-users, physical places and in which environments the demonstrations have been conducted during the project period). In addition, please elaborate on the lessons learnt from the demonstrations. Lastly, please address how you ensured to remain GDPR compliant, and please be specific in your description.	
Ethics self-assessment:	
Please address any ethical issues that you have identified (if any) in the project period and describe how counter measures have been put in place to mitigate any potential issues.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Please explain in detail to avoid any misunderstandings.	
Risks:	
Please describe the risks you have identified during the project period (for instance technological, collaboration or external factors) and explain how you have overcome these challenges.	
Gender balance:	
What was the gender balance in your project team? Please indicate the number of male and female members involved in your project execution (provide aggregated numbers for all partners).	- Number of female team members: - Number of male team members:
If there was a gender misbalance in your project, please explain the reasons behind this.	
Other identified issues:	
Please describe if you have encountered any issues during the project period e.g. technological gaps, technical components (supply), system integrations, market immaturity, lack of market, funding etc.	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Sustainability of the Project:	
What are the challenges you need to overcome to ensure a successful future of the project? *Please describe 3-5 challenges and how you plan to overcome these challenges.*	
Do you need any further collaboration partner(s) or new partnerships for a successful commercialisation of your solution. And if yes, which types of collaboration/partnerships do you need? *Please be as concrete as possible, so, if possible, the SecurIT consortium can assist in the facilitation of a collaboration/partnership.*	
Commercialization strategy: please elaborate on your long-term vision of the marketing strategy incl. how do you propose to attract more potential clients, get into the right networks, and create your own brand. What will be the focus of your marketing strategy? *Max. 300 words.*	• **Market approach** • **Marketing strategy** • **Targets (in 1, 3 and 5 year(s))**
Outcomes regarding IPR management: please elaborate how you are planning to handle the Intellectual Property Rights (IPR) deriving from the project activities, and how you in the project consortium expect to collaboration going forward (did you sign a collaboration agreement for future collaboration after the project end, how did you manage IPR based on the project results, and eventually any patents).	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Overall assessment and evaluation of the (up to) 12 months project period:					
Please elaborate and sum up on the entire project period, and identify what has worked well, what has been challenging and what corrective measures you have taken to keep your project on track.					
You are also welcome to include a comment on your relations and collaboration with the SecurIT consortium and let us know if we can improve in some aspects.					
Based on the above provided assessment and evaluation, please provide a rating on a scale of 5-1 for the following aspects:		Please insert an x in the category that fits to your experience:			
Categories:	**5 Highly agree**	**4 Agree**	**3 Neutral**	**2 Disagree**	**1 Highly disagree**
The collaboration with and guidance of my dedicated follow up manager has worked well (regular meetings etc.)					
The SecurIT process and structure has worked well (from the open call process, jury day selection, regular meetings, payment installments frequency, progress reports etc.)					
The SecurIT project created new business opportunities for my organisation (open up new markets, new customers etc.)					
In my opinion, the SecurIT project has helped to strengthen the visibility of					

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

European SMEs in the security market/industries					
In case you want to comment on your abovementioned scores, please elaborate here:					
Follow Up Manager:					
Assigned Follow Up Manager (name, cluster, email)					

Signatures:

1st partner, name and date

2nd partner, name and date

3rd partner, name and date

Follow Up Manager, name and date

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

KPI progress report

	KPI progress assessment form	Max score of 10 (projects with scores under 7 will be discussed more indepth)		
	Project name:			
	Please evaluate the KPIs for the Final report			
KPIs	*Technical performance indicators: 45 %*		Score % (within criterium)	
	Please evaluate the KPIs for the Final Report:		Maximum score: 4,5	Score:
A collected overview and average of the project specific KPIs	How much of the Technical progress was achieved according to what was planned in Follow Up Report M1 *Note: 0%-60% delayed, 70%-80% on time, 90%-100%*	- 0% - 10% - 20% - 30% - 40% - 50% - 60% - 70% - 80% - 90% - 100%	100%	
	Recommendations, observations and justifications of the score made by the dedicated Follow Up Manager:			
Deliverables	*Deliverables quality: 45 %*			
Consider deliverables and milestones	**Please evaluate the deliverables based on the Final report and supporting documents**		Maximum score: 4,5	
	CONTENT:			
	Does the Final report include enough information in order to confirm the completion of the deliverables and milestones?	"- YES (1,35 score) - NO (0 score)"	30%	
	CLARITY:			
	Is the quality of text, graphs and figures acceptable for validati	"- YES (0,9 score) - NO (0 score)	**20%**	
	QUALITY:			
	Is the deliverable and milestone enough to describe the technical objectives in the document for a technically related audience?	"- YES (1,35 score) - NO (0 score)	**30%**	
	CONSISTENCY:			
	Is the deliverable and milestone description consistent with what was inserted into the initial Follow Up Plan M1?	"- YES (0,45 score) - NO (0 score)	10%	
	Do the milestones and deliverables need to be revised?	"- YES (0 score) - NO (0,45 score)	10%	
	Recommendations, observations and justifications of the score made by the dedicated Follow Up Manager:			
Deadline Compliance				
	Deadline Compliance - Maximum total score is 1			
	Please include information about deadline compliance with the following actions:	Yes=33 % // No=0 %	Maximum score: 1,0	
	Submitted the Final report within the specified deadline:	Yes	33%	
	Attends the meetings as planned:	Yes	33%	
	Communication with mentor:	yes	33%	
	Recommendations, observations and justifications of the score made by the dedicated Follow Up Manager:			
			Total score	0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Demonstration questionnaire

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Questionnaire

For demonstration

Deadline: 20, October, 2023

This questionnaire is a tool designed to help you to prepare for the demonstration and to evaluate the possible related issues or obstacles. Your Follow Up Manager will be supporting you in the process of setting up the demonstration environment and framework

Questions related to demonstration

Project title:	
Where will the demonstration take place?	*Please list:* 1. *country(ies);* 2. *name institution, demonstration site or place.*
Date	*When is(are) the demonstration(s) planned?*

	Question	Yes	No	Your Explanation
1.	**Will you have to sign an agreement for demonstration? (with the test site, with an end-user, etc.)**			*If yes, please specify under each question if it includes:* 1. *appropriate measures for personal data and privacy protection,* 2. *ethical compliance;* 3. *applicable law compliance,* 4. *management and regulation of access to testing infrastructure,* 5. *data cleaning, deletion of users after the demonstration.*
2.	**Will the demonstration site/place/institution provide a template of demonstration agreement**			*If no, please inform the SecureIT Follow Up Manager to provide you with a template for the demonstration agreement.*
3.	**Will your demonstration be in restricted environment?**			*Please specify under each question:* 1. *what environment it is;* 2. *which restriction measures may apply;*
4.	**Do you need security clearance for demonstration (if it is required)?**			*Please specify under each question:* 1. *which security clearance do you need;* 2. *have you already received it or when do you plan to receive it.*
5.	**Do you need to comply with any requirements to get access to the site/institution/place where you demonstrate the prototype?**			*Please specify under each question:* 1. *requirements;* 2. *your compliance.*
6.	**What are the procedures you need to take to get the access to testing environment?**	n/a	n/a	*Please provide description of procedures:*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

7.	**Will you use real data for testing?**			*Please specify:* *1. what real data you will use:* *2. will* the testing data be deleted by testing environment (site/institution/place) after the demonstration?
8.	**Will natural persons or their personal data be used for the demonstration?**			*If yes, please provide explanation under each question:* *1. why it is vital for project implementation;* *2. would it be possible to reach the same results by testing with natural persons or their personal data?* *3. what are the measures taken to ensure the legal compliance and protection of persons and/or their personal data.*

Questions related to personal data processing

	Questions	Yes	No	Your explanation
1.	**Will your research involve the processing of personal data?**			*If your project **does not involve** any processing of personal data, the remaining questions are not applicable*
2.	**Does your organisation have a Data Protection Officer (DPO)?**			*Please provide name and second name, contact details*
3.	**Is the personal data you intend to process relevant and limited to the purposes of the project?**			*1) Please explain the purpose of your processing activities in its relation to **both**:* *1.1. The project objectives during the research stage, and* *1.2. The operational objectives of the project output once the project has been finalized.* *2) Please explain how the envisioned data processing will be relevant ("purpose limitation") to these purposes.* *3) Please explain how the envisioned data processing will be limited ("data minimisation") to these purposes.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

4.	**Will personal data be anonymised and/or pseudonymised as part of your project?**			*If yes, please provide a description of the anonymisation/pseudonymisation techniques that will be implemented.* *If no, please justify why your project purposes could not be adequately reached if the data were to be anonymised or pseudonymised.*
5.	**Does your project include any type of processing (in particular using new technologies, and taking into account the nature, scope, context and purpose of the processing) that may be likely to result in a high risk to the rights and freedoms of natural persons?**			*If yes, please verify whether a DPIA (data protection impact assessment) should be conducted. To do so, please consult your DPO (or in absence, with SecureIT Fallow Up Manager).*
6.	**Are there any special derogations pertaining to the rights of data subjects or the processing of genetic, biometric and/or health data, under the national legislation of the country where the project takes place?**			*If yes, please submit a declaration of compliance with respective national legal framework(s).*
7.	**Does your project include profiling*?** ** Please note that Art 4.4 GDPR defines "profiling" as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular (though not necessarily) to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."*			*If yes, please provide an explanation of:* *1. how the data subjects will be informed regarding the existence of the profiling,* *2. the profiling's possible consequences and* *3. how data subjects' fundamental rights will be safeguarded.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292