Project Deliverable

D4.1 Follow Up Report (final review) Open Call 1

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	15 December 2023
Submission date	15 December 2023

	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	01-11-2023	Document Creation	Draft	CenSec
V1	11-12-2023	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

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 1 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 demonstration 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.

Authors (organisation)

CenSec

Reviewers (organisation)

FBA

Keywords

Final review, project progress methodology, open call 1, security, cascade funding.

Legal notice

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

Deliverable D4.1: Follow Up Report (final review) Open Call 1

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 of the projects to the closing of the projects.

Introductions and project methodology

A total of 21 projects were funded during the Open Call 1, based on two instruments that is 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 D3.5.

At project start, all funded projects were allocated a dedicated Follow Up Manager (FUM) among the SecurIT consortium partners, in order to keep a regular dialogue with the projects and ensure a continued progress and support. The projects were allocated to each FUM based on the following methodology – country of origin for lead partner (that is, as a point of departure, projects was distributed among partners based on the country of the lead partner, and when this option was done, the second criteria would be implied), country of origin for 2nd partner, (potential) relations with one of the SecurIT consortium partners, and cluster with expertise on the specific area. This procedure was chosen based on both cultural and language aspects, as well as relations between the SecurIT partners and projects. The reasoning behind this procedure was that some potential issues could be overcome by not having cultural and language barriers to consider, and that some consortium partners had members included between the funded projects and would like to keep the close relations with them.

The regular dialogue between the projects and the dedicated FUM consisted for most of the projects of 30 minutes 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 how they expected to overcome these.

In parallel to these meetings, the SecurIT consortium had bimonthly meetings in the work package "*WP4 Monitoring and Impact*", and these meetings were also used 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.

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

In addition, in order to measures progress in the projects, more formal mechanisms were imposed on the projects as projects 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 in sourcing items, 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.

In order to validate the content of the various reports, the SecurIT consortium established several control mechanisms in order to ensure that all projects delivered what they were expected to. For the Open Call 1 projects, the consortium did not have an initial validation process in order when it came to the validation of the Follow Up Plan at the beginning of the project period, and it was only the FUM who validated the report (this was changed for the Open Call 2 projects). However, for the Midterm and Final Reports, the consortium introduced a “mini-committee” structure that consisted of the FUM and two other consortium partners, and the three partners would go through the report and evaluate if it was clearly describing the project progress both when it came to consistency with the Follow Up Plan and with the content itself. In parallel, a Follow Up Committee meeting was scheduled, and this committee consisted of one partner from each of the consortium members. 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 achievements), deliverables (content, clarity, quality, consistency) and deadline compliance -were considered and a score was given.

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:

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

Evaluation Criteria

Each evaluation criterion will be scored from 0 to 10 and the weight of each one of these criteria in the final score will be as follow:

TECHNICAL EVALUATION (Follow Up Managers)			VALIDATION (Follow Up Committee / Selection Committee)
Deliverable (45%)	Technical Performance Indicator (45%)	Deadline Compliance (10%)	Above threshold ✔ Below threshold >

Total maximum score will be 10.
Threshold is 7.

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

As the overview above depicts, the validation process starts by the the projects sending the Midterm or Final report to the FUM. The FUM reviews the report, and in case there are some issues, it is sent back to the project for further clarification. When the FUM deem that the report is in order, it is shared with the mini-committee members. This process was initiated in order 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, and will continue 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

Regarding the payment for the FSTP 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 one project, the process was slightly different as the whole payment was paid at the end of the project and after the Final Report had been validated. This was due to the fact that the project partners were experiencing some financial difficulty (but improving), and this way, the SecurIT partners were lowering the risk of the project failing during the support period.

Overall, the budget distribution model was chosen to minimize the risk of the consortium partners (as the 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:

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 through out the support period.

Lastly, in order to share public available information about the funded projects and the progress made during the support period, all funded projects can be seen on the SecurIT website: [Open Call #1 Funded Projects – SecurIT (securit-project.eu)]

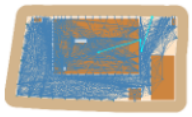
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

On the website (under the tab called “project results”), all projects from the OC1 are described in detail. See below screen shot of how the projects are presented in alphabetically order in the overview list:

List of selected projects for funding

Discover the solutions on progress, the SME partners, and follow here the evolution of each projects.

Find solutions according to your interests by searching key words in the the research-field.

Project name	SME partners (*project leader)	Partners' countries	Domain and challenge solved	Description	Prototype/Demonstrator	Open Call
BIM2SIM 	*APEX solutions Scott Brownrigg Limited	France United Kingdom	**Domain 1**: Sensitive infrastructure protection **Challenge 1.4** : Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions	BIM2SIM aims at developing a prototype digital technology brick to automatically extract security- and safety-related information from standard building description file formats. On the one hand, buildings are core elements for security and safety applications, with a wide range of applications: intrusion, evacuation, optimal position of sensors or safety material, hazard modelling, assessment of structural effects, etc. On the other hand, Building Information Modelling (BIM) is becoming a collaborative must-have for architects, urban planners and in the construction industry. Standard file formats are readily available, and could be extended to provided security-related information as well. BIM2SIM results will be twofold: - guidelines for security-oriented building information modelling, - software converting BIM models into "navigation meshes" used for path-planning, with a first application to the physical security of critical infrastructures.	Prototype	Open Call #1
Cyber Trapper 	*Datatek doo Beograd ADVANCED SECURITY TECHNOLOGIES Avantools	Serbia Greece	**Domain 1**: Sensitive infrastructure protection **Challenge 1.1**: Development of cybersecurity solutions for sensitive infrastructure protection	Through Cyber Trapper platform, we will collect information on ongoing live IIoT attacks at hundreds of locations worldwide. We will collect data from our IIoT clones – traps as well as productions systems, analyse them in real time (in less than 10 milliseconds) and create dynamic threat feed lists with malicious compromise indicators used to prevent attacks at customer premises. This approach achieves the effect of "Crowd Immunity" - after the first attempt of an attacker to interact with the CyberTrapper at one of the group members, the entire group acquires immunity to that attacker and its attack vector.	Prototype	Open Call #1
	*Defora Networks		**Domain 1**: Sensitive	INSIOTA provides an integrated platform, automating a		

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 BIM2SIM project:

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

When you scroll each project page, you can find information about the project when it comes to project partners, project description, status and results from the Midterm and Final report and eventual a few project pictures (when relevant).

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 1

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
1 BIM2SIM	01/09/2022-31/08/2023	• France • United Kingdom	Scott Brownrigg and APEX solutions agreed first on the definition of BIM models of increased complexity, from a single–storey building to a complex site with several multi–storey buildings enclosed by fences. Each model has been refined to help the pre–processing by APEX solutions. These exchanges led to the development of enhanced “BIM guidelines” written by Scott Brownrigg in order to be shared with future partners. A final processing method coded in the Unreal game engine has been developed by APEX solutions in order to perform intrusion simulations, taking the advantage of existing non-playing characters (NPCs) AIs to model the behaviour of “red team” and “blue team” agents. This is a major step towards the full integration of APEX physical security simulations in Unreal Engine (something that was not planned at the beginning of BIM2SIM). As a continuation of the activities of the BIM2SIM project, APEX solutions took a trainee specialising in 3D modelling. The aim is to rapidly develop a “level editor” for our serious game. Last but not least, elements of a post-project strategy have been drawn up by Scott Brownrigg and APEX solutions to capitalise on this prototype project and develop operational applications.	5 - 6

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
2 Cyber Trapper	01/09/2022-01/09/2023	• Serbia • Greece	The goal of our CyberTrapper initiative was to make the internet a safer place for our users, by developing a smart solution that protects everyone. This works like a communal shield, gathering information from our virtual 'traps' worldwide to create a shared protective layer. These traps, which are actually replicas of web services, are stationed on what we call edge devices. They work in tandem with a central server that processes all the collected data to identify and ward off threats. At the start of this project, we selected a type of hardware that would best meet our technical needs. Once we had that sorted, we began creating the system, starting with designing the structure and creating some initial user interface ideas. Once the necessary devices were ready, we began combining everything together – a phase that our technical team found particularly exciting. Once we successfully connected the edge device with our traps, we began testing everything, and we're happy to say that the results have been very promising. We then moved on to developing the central server and integrating all parts of the system. Now, we're eager to build a kind of communal protection for our wide network of users. This is all about everyone pitching in and making the internet a safer place together.	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
3 Insiota	01/09/2022-30/08/2023	• Germany • Czech Republic • Italy	INSIOTA provides an integrated platform, automating a range of IT– Security tests on computer systems and networks. The constant tests help ensure any gap is detected and can be mitigated before a real attacker can abuse them. While the underlying infrastructure of the platform is environment–agnostic, the focus of the project is on systems part of the “Internet of Things.” (IoT) The target environment for the INSIoTA testbed was located in the public space of a European city, monitoring the quality of the environment in a “Smart Street.” Criteria like traffic information and air quality were critical in this context, as the street contained one of few bridges in a city of 100.000 inhabitants, connecting a Police Department to a Fire Brigade on either side. The INSIoTA platform was extended as a solution for the offline analysis of firmware images for these sensors, in order to help protect the infrastructure deployed in case of physical compromise of the sensors deployed publicly. As a result of this project the sensors for this environment can be analysed for the presence of security vulnerabilities prior to deployment, thereby streamlining quality control and strengthening the security posture without requiring additional manpower.	5 - 7
4 Kaleidoscope	01/09/2022-31/08/2023	• Italy • Ireland	The Kaleidoscope platform has been developed by three European ISPs with a large experience in telecommunications and cybersecurity. The goal of the Kaleidoscope project is to provide a future–proof architecture that is able to quickly evolve and adapt to more complex DDoS attacks. The SecurIT open call #1 has permitted to design the whole architecture and to discover the technological challenges as well as establish a long–term path that will enrich the Kaleidoscope platform with new features and more complex traffic analysis modules. At the end of the Kaleidoscope project, the platform has reached a good level of maturity and it will be offered in the near future to European telecom/ISP, service providers, software companies and system integrators. The Kaleidoscope platform is able to scale, thanks to its modular design and the future research will enhance it with AI capabilities. The Kaleidoscope consortium also welcomes companies that want to investigate on how the Kaleidoscope platform can help them in defending their assets (e.g. services, critical infrastructure, etc.) from DDoS attacks.	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
5 SecuRAIL	01/09/2022-31/08/2023	• Slovenia • Croatia	Successful conclusion of the SecuRAIL project – a system aimed at enhancing passenger safety on railway platforms. The final demonstration of the SecuRAIL project and the developed prototype took place at Erdberg metro station, operated by Wiener Linien from Vienna on 23.06.2023. The system provides reliable detection of dangerous situations at railway stations. It automatically detects passengers or objects that fall from the platform onto the track, suspend the traffic and alerts the security staff. New features can be added, such as “trap and drag” accident detection, which prevents a train from dragging behind a passenger or other object grabbed by a train door. The system is particularly well-suited for lines with autonomous trains and stations where installing platform screen doors may not be feasible.	5 - 6
6 SECUVERSE	15/09/2022-15/09/2023	• Italy • France	Secuverse is an autonomous inspection and monitoring system, based on an immersive Metaverse and Artificial Intelligence platform that includes a digital-twin model of a target facility, a LIDAR scanner, an Automated Guided Vehicle (AGV), and AI algorithms for intruder detection. Our goal is to develop an autonomous robotic agent that can patrol sensitive infrastructure, monitoring possible intruders and anomalies, and represent them in the digital twin model of the facility. Remote operators can inspect this rich data ecosystem through a metaverse immersive interface, in order to visualise threats and intruders detected through an AGV–mounted LIDAR scanner and perform mission–control task by communicating with robotic agent on-field.	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
7 VASCREEN	15/09/2022-15/09/2023	• France • Spain	The VASCREEN project has allowed the implementation of the technology developed by MION, based on Explosive Vapor Detection (EVDs), to the suitcases and belongings explosive screening supported by the new ML classification algorithms developed by EZAKO. The final demo has demonstrated the capacity of technology to detect vapors of explosive from real suitcases that contain explosive samples at the level of milligrams. This extraordinary detection capacity has been achieved thanks to the optimal combination of MION vapor detector technology with EZAKO's powerful classification algorithms. During these 12 months of work, we have been working on: – The adaptation and optimization of its technology for luggage screening. – The optimization of the sampling conditions – The implementation of new hardware ideas to increase the sensitivity of the detection – The implementation of ML models for the classification of the results to increase the selectivity – The validation of the algorithms on data from a real environment.	5 – 6

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:

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

	Partners geography	Support period	Demonstration projects Final project update:	TRL Level start - end	Real or near-real environment
8 ARSP	• France • Finland • Spain	15/09/2022-15/06/2023	LMAD robotic management platform has been developed to handle more than logistic use cases and now LMAD can handle security patrols with autonomous robots as well as autonomous deliveries with robots. Moreover, this news platform version will allow LMAD and its partners to manage several robots for several use cases on a single site or over different sites, all managed from a single platform. The final demonstration took place at the EDF sites on 16.06.2023. The purpose was to show how LMAD robotic management platform is now able to handle more than logistic use cases. Indeed SecurIT funding has supported the diversification of these robots from autonomous deliveries to security patrols for the detection of intruders on sensitive sites.	5/6 - 8	Real environment
9 C-Shield	• Poland • Germany	15/09/2022-15/09/2023	The C–SHIELD project is dedicated to the development of an innovative system for chemical hazard detection. The solution is based on two different detection technologies, namely IonMobility Spectroscopy (IMS) and Flame Photometric Detection (FPD). The two commercially available sensors are combined via a hardware unit called a Sensor Node, which is a point detector and can easily be carried by one–person and operated on the move. During the first 6 months of the project, the team of engineers has prepared two dedicated translators, one for each sensor. The translators are responsible for acquiring sensor data, unification of the data into one format, data pre–processing and analysis. During the project lifecycle, all core requirements have been met and the final version of the C–SHIELD system consists of: • dedicated translators for each sensor, • the Sensor Node which is the heart of the system and serves as internal data processing unit, • the data fusion component enabling the system to classify and identify data from different sensors.	6 - 8	Near-real environment

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

10 CyberSec2SME	01/09/2022- 31/08/2023	• Netherlands • Austria	What is new is that the cyber risk data is automatically collected, classified, and analyzed per firm by a set of sensors. These sensors are monitoring the outside and inside of the firm on people, process, and technology. Cyber risk insights can be shown at supply chain level to give the Port of holistic overview. This is important as current measures like surveys and external scanning give an incomplete risk assessment. IT auditors can independently utilize the data to issue (non-)assurance reports, while IT partners gain valuable operational and tactical insights on how to secure firms through alerts and recommendations. Phase 1 and 2 as well as the phishing tests were conducted as described above. The technology & results of CyberSec2SME have been presented by BeiA to the Port of Galati. The Port team were impressed with the results and evaluate future steps. This is a great result as it demonstrates the hard work meets the requirements of the target user group. In conclusion, cyber threats know no boundaries, and it is essential to be proactive in managing these risks. Continuous monitoring of cyber security risks across the supply chain of suppliers is crucial for protecting critical infrastructure from devastating cyber attacks. By implementing a comprehensive cyber security strategy that includes continuous monitoring of cyber security risks, businesses can identify and mitigate potential risks before they become a problem, protect their operations, and ensure the safety of the wider community. The CyberSec2SME project is an excellent example of how businesses can protect their operations and the community from the catastrophic effects of cyber attacks.	6/6 – 7/8	Real enviroment

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

11 DIAC	01/10/2022-30/09/2023	• Germany • Spain	Currently, Access control systems are mainly based on user identification which utilize smart cards (with chip), contactless cards (RFID), biometric systems (fingerprints, face detection, retina scan etc.), PIN codes or physical keys. But these identification systems have privacy and security issues, such as loss of the card, user data breaches, cloning of cards, disclosure of access PIN to another person, etc. Moreover, they are tightly coupled with user's personal information which makes them vulnerable to the privacy attacks. The DIAC project solves most of the problems that current access control systems have, using innovative solution and avoiding direct user interaction with access control through the Disposable Identity Framework. Disposable identities act as an e–ID that can ensure both the anonymity of the identity owner–unlink ability – and the possibility of reliably identifying and verifying a person's identity. Disposable identities are a further step toward minimal data processing: the amount of identity data processed should be adequate, relevant, and limited to what is necessary for the purposes, as it is required by the GDPR regulation. The solution was validated in real environment for its functionality, performance and scalability by 3 demonstrators (in asvin lab, OdinS office and Murcia University building) which involved DID Mobile App, Access Control Terminal attached to a door and the DID Platform deployed on cloud. The DIAC consortium aims to exploit the solution with existing customers by shaping it as a new product in future.	5/1 – 8/8	Real environment
12 Digital Forensics	01/09/2022-31/08/2023	• Denmark • France	During the project, Avian Cloud has evolved from a concept and a desire to meet the next-era requirements to Digital Forensics and eDiscovery labs as cloud adoption evolves into a real product ready to make a great impact in the industry. Now, we offer the world's first one-click Digital Investigations cloud platform that enables government and enterprises to use their favourite Digital Investigations and eDiscovery tools in the cloud 10-100x faster than ever before. A highly secure platform offering isolated tenants per subscription and unique Confidential Computing options. Automatic self-service provisioning in minutes to enable, manage and automatic case tasks using best-of-breed industry technologies within Digital Forensics, Incident Response and eDiscovery.	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

13 FusionSec	26/09/2022-28/07/2023	• Spain • Lithuania	Empowering Secure Collaboration in Mass Events With a help of SecurIT project we were able to built the IoT platform that helps to create a smoother collaboration between public and private forces during mass events. It significantly shortens the communication chain. Moreover, the cloud–based system combines different data sources and allows for real–time monitoring of images from drones, video cameras, and smartphones. This capability helps to create a broader picture of the event and to see it in an integrated way, from different perspectives. Both private and public forces, as well as incident locations, are visible on one interactive map, which improves the coordination of forces. For example, an on–duty police officer can see when forces are misplaced or too far away from a potential incident site. Visual awareness of forces and incidents allows for efficient incident response and, if necessary, coordination of evacuation. The visual sources like cameras, drones and smartphones also provide a better view of emerging congestion or other incidents, providing context and allowing the officer on duty to quickly redeploy the forces and transfer the relevant tasks to the officers promptly. Moreover, this situational awareness can be monitored from different geographically located command and control centres as well as command posts. The testimonies of our users attest to the unmistakable advantages of FusionSec. It's a testament to amplified efficiency, and heightened productivity for security forces collaborating in public mass events. The Lithuanian police and Alytus county police are particularly enthusiastic about FusionSec, recognizing its potential to revolutionize event security, streamline communication, and bolster situational comprehension. Furthermore, the municipality representatives have commended FusionSec for its seamless integration with their operations, enabling them to promptly report incidents like traffic jams through the FusionSec mobile app. The immediate visibility of these incidents to the police officers ensures swift action and resolution.	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

			In essence, FusionSec embodies a transformation that transcends traditional paradigms, enhancing the capabilities of security forces and reaffirming our commitment to safety and efficiency in the face of mass events.		
14 HeliA	01/09/2022- 31/05/2023	• France • United Kingdom	The Helia project is about a 100% made in EU tethered aerostat that can detect early wild fire autonomously based on AI on board. The work was mainly about the development of the payload. The latter is made up of an intelligent box and a gimbal. First steps were to build an enclosure with a visible and a thermal camera controlled by a battery-powered processing board. These cameras and board running an embedded AI process images in real-time, all day and night, and send alert when smokes/fires were detected. This system is very power efficient and datas are safe because after processing, if no alert occurs, images are not kept nor sended. From that we gained the capability to acquire aerial images from Helia to train our AI and set up a deployment procedure. Lastly, we found a gimbal which our electronic board can control autonomously and which scans around the Helia platform by itself. We also managed to decrease the weight (<2kg) and use a 7m3 aerostat instead of the initially envisaged 11 m3, although the 11 m3 was built and always on stand-by. We demonstrated Helia's abilities in multiple events like I-Naval in Toulon, the SecurIT final demonstration in Pourrières (C2RD) or at the International Paris AirShow. Future prospects are in progress. Helia is on track to help fire-fighters in order to avoid other big fires.	5 - 7	Near-real enviroment
15 IDEAS	01/09/2022- 30/06/2023 *(postponed to 30/09 2023)*	• France • Denmark	The objective of IDEAS project: to develop the first solution which guarantees both a level of physical integrity equivalent to that of Datadiode technology, and flexibility of use comparable to firewalls. This new technology must be "by design": 1. Be 100% material 2. Enable two-way communications 3. Be able to reach 1 Gbps for fluidity of data exchanges The POC with a large industrial group has demonstrated those functionalities.	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

16 PIM_SAT-M	01/10/2022-15/09/2023	• Spain • Italy	Within the scope of the project, we developed an AI enabled, platform–based remote sensing tool, which provides reliable and sufficient information on the area or object stability. The underlying technology is InSAR, the key advantages are : – better coverage of large areas as well as “thin” infrastructures – automatically generated early warnings – web–based platform and dashboard. We also were able to showcase the solution. This is a highly cost effective and convenient tool, which equip our customers with valuable and near real time information on the area or object stability and automatic early warnings on a web–based 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

17 RASAD	15/09/2022- 15/09/2023	• Belgium • France	We are thrilled to announce the ground–breaking capabilities of RASAD, an innovative platform that empowers organizations to swiftly build secure applications without writing a single line of code. With RASAD, the traditional barriers of application development are shattered, resulting in an astounding up to 90% reduction in time to market compared to conventional methods. Effortless Creation of Secure Custom User Flows: One of the key highlights of RASAD is its ability to facilitate the effortless creation of secure custom user flows. Developers can now efficiently incorporate essential functionalities like login processes, password resets, consent requests, and much more into their applications. These custom user flows can be seamlessly designed and implemented within RASAD, eliminating the need for time–consuming and error–prone manual coding. Elevating Data Security to New Heights: Ensuring the utmost security of sensitive data is of paramount importance in today's digital landscape. With RASAD, organizations can rest assured that their data remains fully protected. The platform automatically encrypts data classified as sensitive at the application level, eliminating the need for complex encryption algorithms, intricate key management processes, and tedious key rotation procedures. By integrating application–level encryption, RASAD provides a robust security layer, enabling organizations to securely store their data without the typical hassle associated with encryption. Accelerate Time to Market with Confidence: RASAD offers an unparalleled solution for organizations seeking to develop applications with a strong focus on security. With its lightning–fast development capabilities and comprehensive security features such as integrated data classification, RASAD empowers organizations to build secure applications rapidly and efficiently. By choosing RASAD, businesses can accelerate their time to market while ensuring the confidentiality and integrity of their data.	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

			Successful Financial Data Integration Project: We leveraged the power of RASAD to seamlessly move and dispatch critical financial data, including CODA files and bank statements, from the SFTP server of the Bank of Belfius to various destinations within the intricate systems of the Municipality of Koksijde. Streamlining Financial Data Flow with RASAD: The challenge at hand was to ensure a smooth and secure flow of financial data between these two entities. Traditionally, such projects demanded extensive custom coding, time–consuming configurations, and meticulous maintenance. However, RASAD offered an alternative approach that transformed this process. With RASAD's capabilities, we crafted a solution that automated the entire data transfer and dispatch process. Custom user flows were effortlessly designed to handle file transfers, data validation, and destination mapping, all within the secure confines of RASAD's environment. This meant that the Municipality of Koksijde could efficiently and securely access the financial data they required without the need for laborious manual intervention. A Resounding Success: The success of this project cannot be overstated. It not only met the initial objectives but surpassed them in numerous ways. The speed at which the financial data was moved and dispatched was unprecedented, resulting in significant time savings for both the Bank of Belfius and the Municipality of Koksijde. Moreover, the security of sensitive financial data was upheld to the highest standards, thanks to RASAD's automatic data encryption & auditing features. Such a remarkable achievement has not gone unnoticed. Both the Bank of Belfius and the Municipality of Koksijde are now looking into the possibility of continuing their collaboration with RASAD. The effectiveness and efficiency brought about by RASAD have not only streamlined their operations but also laid the foundation for a potentially long–lasting partnership with the platform. In conclusion, the successful implementation of RASAD in this financial data integration project stands as a testament to the platform's transformative capabilities. It not only accelerated data movement but also fostered ongoing collaboration between three important institutions, ushering in a new era of efficiency and		

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

			security in financial data management. Embracing RASAD has proven to be a wise choice, with the potential for even greater achievements on the horizon.		

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

18 ROGID	01/09/2022-31/08/2023 *(postponed to 31/10 2023)*	• Denmark • France	The ROGID project set out to demonstrate how robot guards could add value to high–level security operations for companies when detecting intruders. During the project period, the French video analytics firm Foxstream (FS) and the European robotics company Drone Volt (DV) developed a robot guard solution for an airport in Denmark. Having an airport as an end–user in the project, ROGID addressed specifically challenge 4: "Development of solutions to detect and locate any intruders that had managed to penetrate the perimeter protection and barriers to block intrusions." The airport was, and still is, interested in testing robots as part of their security operations and wanted robots to detect intruders on the perimeter. They hope to eventually replace manual perimeter patrols by car with robots because they believe a robotic solution would be more effective in spotting intruders at night than human guards due to vision impairments. A robotic solution would also have less negative impact on the environment. As the robot was eventually to operate at night, FS and DV suggested developing a solution using thermal imaging technology alongside RGB–based imaging. Furthermore, the solution would patrol automatically the perimeter of the airport and stream live video to a Security Operations Center (SOC) that monitored all the other cameras. Moreover, the solution would send alarms to the SOC if any human intruder was detected. The SOC employees would also have the opportunity to manually control the robot. The solution had a total amount of demonstration hours of more than 32 hours in this project, and 8–hour continuous operation at the airport site was demonstrated (the final demonstration accounted for more than 11 of the total amount of demonstration hours). The partners had obtained a 100% detection rate for intruder detection and 0 registered false positives based on the demonstrations throughout the entire project. The final goal of automatic perimeter patrol and live streaming video data together with the alarms from the intruder detection module was validated at the airport together with the potential end customer, the security department of the airport.	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

			ROGID was presented at SKYDD, Sweden, October 2022, and SIANE, France, October 2022. The ROGID solution was also exhibited at DALO Days, Copenhagen, May 2023. Additionally, Drone Volt plans to attend MILIPOL (November 2023) and Amsterdam Drone Week (May 2024) to showcase the ROGID robot, together with the rest of Drone Volts portfolio within safety and intruder detection. Lastly, the final demonstration site, the airport located in Denmark, expressed explicit interest in further showcasing and testing the solution and pursuing the permanent installation of such a system. Drone Volt had a unique value proposition as one of the few companies that would offer an approved robot guard solution for airports in the EU.		
19 ShowID	15/09/2022-31/07/2023 *(postponed to 01/12 2023)*	• Netherlands • Sweden	ShowID – the universal company badge enabling instant visitor authorization at controlled facilities. Highly secure, adaptable and truly easy. A radical change of the traditional paradigms of the access control market by using ID verification, biometry, liveness detection, cryptography and electronic ticketing. ShowID runs on commonly available devices: standard smartphones, tablets and desktops. No need to purchase, install and maintain specific hardware.	5 - 8	Real environment
20 SLOPEGUARD	01/09/2022-31/08/2023	• Ireland • Italy	The development of machine learning algorithms for anomalies detection and – in the future – for shallow landslides early-warning, has been completed and integrated with the data acquisition system. The AI algorithm has been trained and refined thanks to the data directly collected by the SlopeGuards activated during the project campaign, together with Techcom landslide dataset and other geoscience datasets provided by supportive customers. The Slopeguard system brings the flexibility of an embedded monitoring station and the innovation of integrated AI into the market of landslides monitoring solutions.	5 - 8	Real environment
21 ZENITH	01/09/2022-31/08/2023	• France • France	After 12 months of work, thanks to CHAPSVISION expertise in semantic analysis and to Edicia knowledge of city security, we can extract geo–chronolocalized security relative events from Twitter. The #ZENITH urban security platform aims to detect weak signals from any type of textual data, including social networks, to help cities better anticipate imminent risk situations, and improve the resilience of cities.	6 - 8	Near-real environment

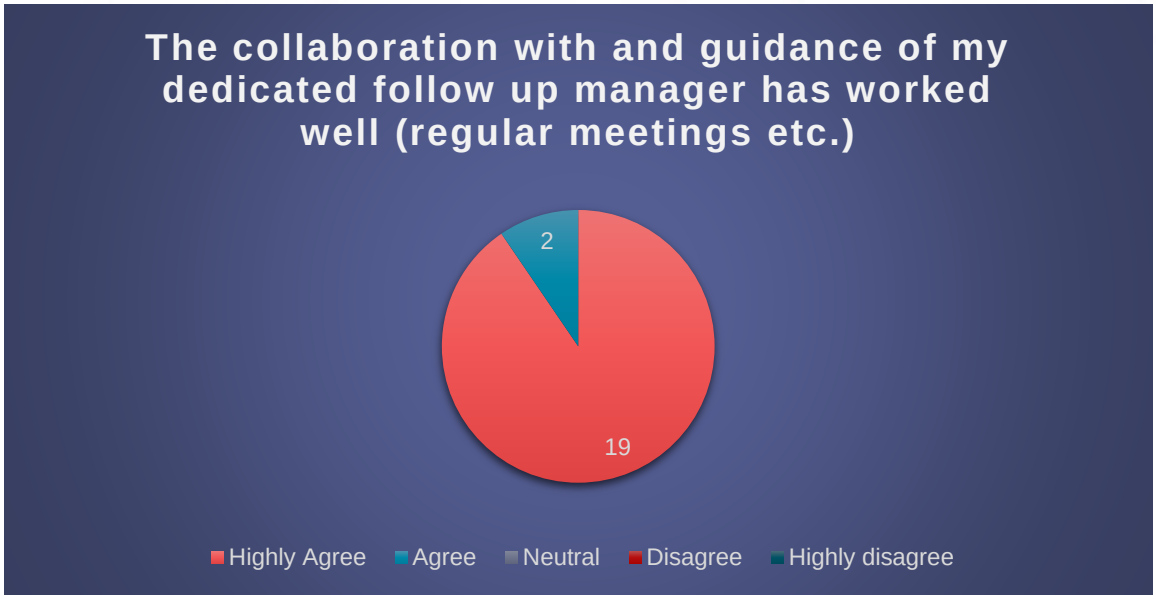
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

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

Quantitative outcomes

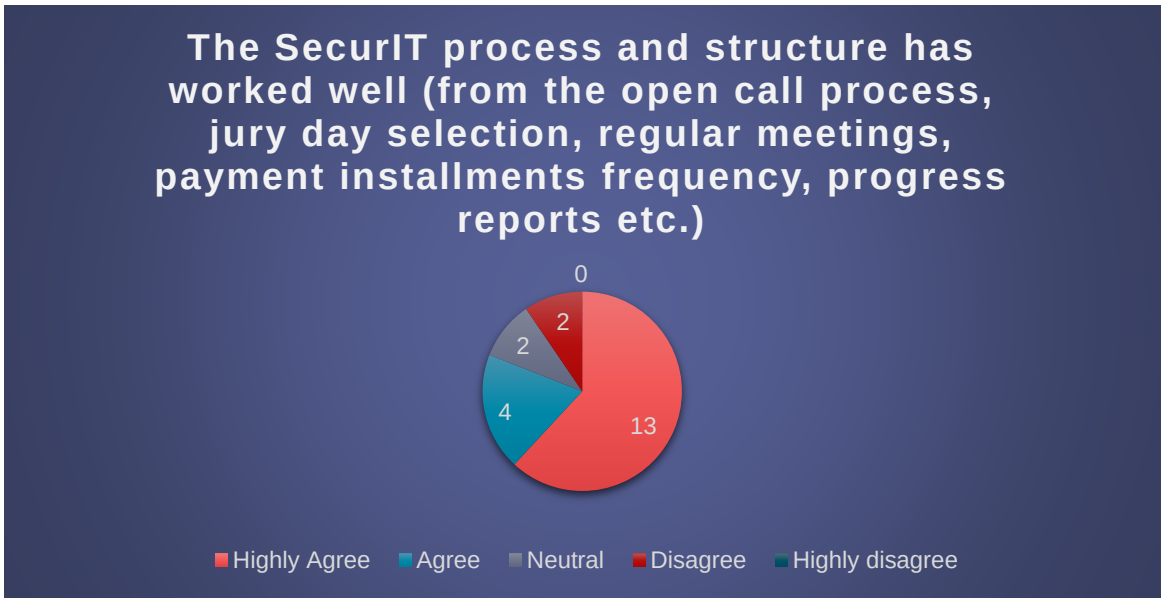
As part of the Final Report, all projects were asked to answer a few questions regarding their assessment and evaluation of the (up to) 12-month support period. All questions could be rated 1-5 where 1 was “highly disagree” and 5 “highly agree”.

The questions and results were as follows:

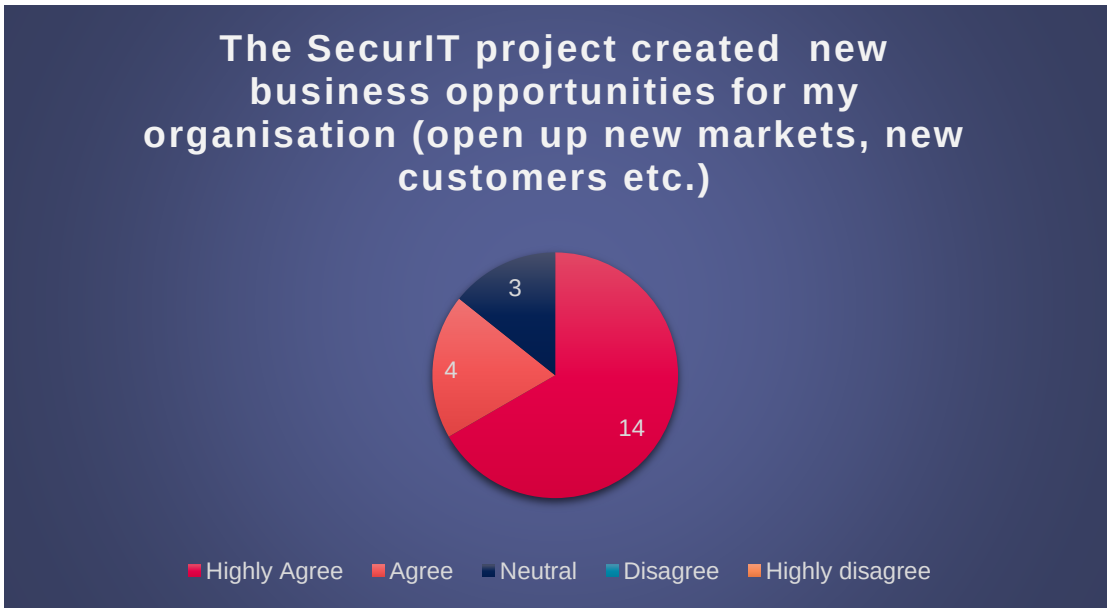


In the abovementioned question, a majority of projects have stated that they “highly agree” in the question concerning that the collaboration with the dedicated follow up manager and the regular meeting structure has worked well as 19 projects have given the highest grade, and two project have stated that they “agree”.

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

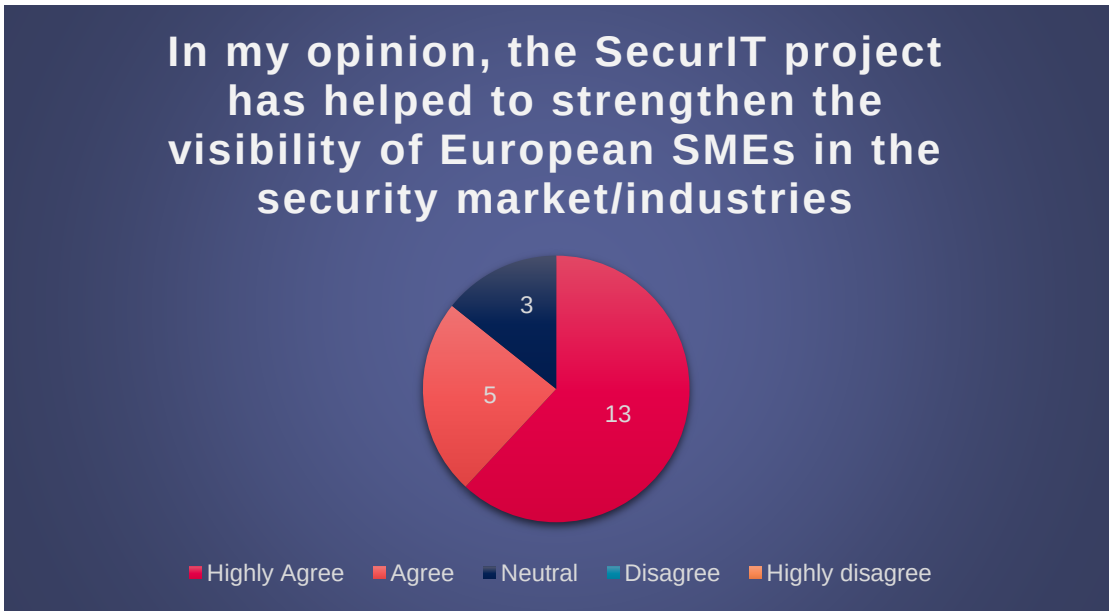


In the abovementioned question, a majority of projects have stated that they highly agree with the statement that the SecurIT process and structure has worked well, four have stated that they agree, two have given a neutral score and another two disagree. Compared with the first question, there is a higher distribution in the answers in this second question, and part of it can be due to the payment installments frequency as some projects have stated that they are unhappy with the majority of the budget being paid after the Final Report (and not at the beginning or Midterm).



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

The abovementioned question shows again a high satisfaction with the SecurIT project having created news business opportunities for the project partners with opening of new markets, new costumers etc, with 14 project stating that they highly agree. Four projects agree and three have given a neutral score.



The abovementioned and last question shows an overall large satisfaction with the participation in the Open Call 1 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. Five projects mention that they agree and three are neutral.

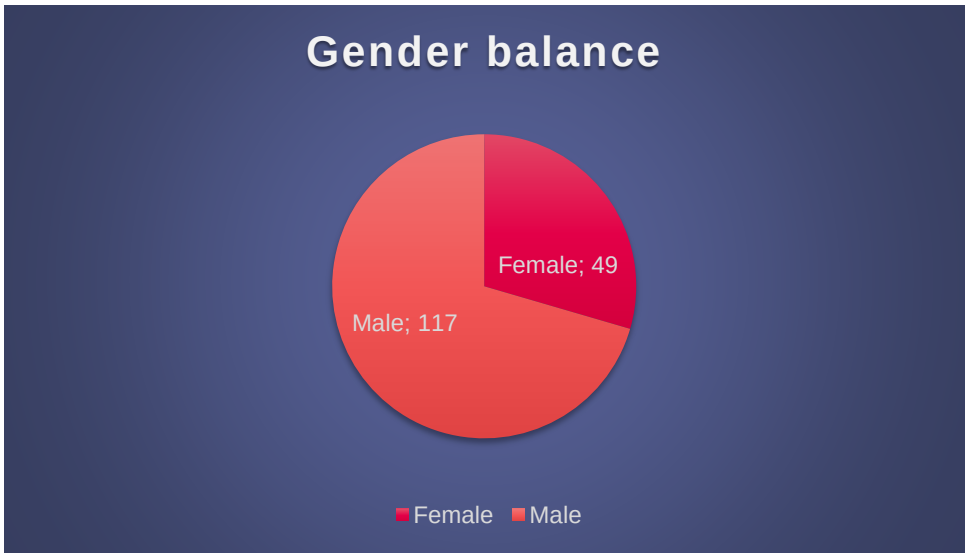
The overall conclusion on the abovementioned questions are that the Open Call 1 projects have experienced a benefit and further strengthening of their position in the European security market by participating in the SecurIT project, and are overall satisfied with the support they have experienced through their support period.

The final aspect we want to mention is the gender balance and involvement for the OC1 projects.

Gender balance

In total, 166 people were involved in the 21 funded projects, and of this number 49 were women, giving a percentage of 29,5 % of women involved. 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 project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292



To sum up of the Open Call 1 and the involved projects, there has been an overall high satisfaction of being involved in the Open Call 1 and the project support that the projects have experienced through the support period. From the SecurIT consortium's perspective, we have gained valuable information that we have further developed and implemented in order to improve in some aspects for the Open Call 2 projects.

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

- Follow up Plans (one for demonstration and one for prototyping projects)
- Midterm Report (one for demonstration and one for prototyping projects)
- Final Report (one for demonstration and one for prototyping projects)
- Demonstration questionnaire (that all projects regardless of instrument were asked to answer)

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

Annex

Follow Up Plan: Demonstration projects

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Follow Up Plan

For demonstration projects

Deadline: M1 (tbc date)

1. 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 interim report in month 6 and the final report in month 12. The two latter reports are based on the information you have inserted in the initial Follow Up Plan in M1.

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 information. 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 (M6) (DD/MM/YEAR):	
Final report due (M12) (DD/MM/YEAR):	
Contact information of lead partner:	Name:
	Email:
	Organisation:
	Title and function:
	Country:
Contact information on 2nd consortium partner:	Name:
	Email:
	Organisation:
	Function:
	Country:
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:
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 - please insert 1-2 pictures	
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) (Doman 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.	

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

Deliverables:	
Please describe the deliverables you will complete during the project period (you can use the description from the proposal). Please be specific in your description.	
Milestones:	
Please describe the expected key milestones that you will achieve during the project and indicate a time for when you expect to achieve them (you can use the description from the proposal). Please be specific in your description.	
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	

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

expected to be achieved e.g. in month 6 or month 12. This will be used to evaluate your progress in the interim and final report in M6 and M12 respectively.		
	M6	**M12**
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 in M12:

	Baseline (current status)	**Expected M12**
1. Employment created / safeguarded due to the Project (stating also the number of employees before the project (baseline) as well as forecasts for M12/2023)		
2. Impact on turnover due to the project (baseline and forecasts for 2023)		

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

3. Market share acquired due to the project (baseline and forecasts for 2023)		
4. Environmental impact (if applicable), (water consumption, energy…) generated by the project (baseline and forecasts for 2023)		
5. Contribution of the project to new or significantly improved products launched (baseline and forecasts for 2023)		
6. Contribution of the project to new or significantly improved methods and processes (baseline and forecasts for 2023)		
7. Advancement of TRL due to the Project (baseline and forecasts for 2023)		
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) 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):	

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

	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 following 12 months. Please be as precise as possible (and please indicate if 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.	

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.	
	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

Follow up plan: Prototyping projects

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Follow Up Plan

For prototyping 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 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 interim report in month 6 and the final report in month 12. The two latter reports are based on the information you have inserted in the initial Follow Up Plan in M1.

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 information. 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 (M6) (DD/MM/YEAR):	
Final report due (M12) (DD/MM/YEAR):	
Contact information of lead partner:	Name:
	Email:
	Organisation:
	Title and function:
	Country:
Contact information on 2nd consortium partner:	Name:
	Email:
	Organisation:
	Function:
	Country:
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:
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 - please insert 1-2 pictures	
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) (Doman 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.	

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

Deliverables:	
Please describe the deliverables you will complete during the project period (you can use the description from the proposal). Please be specific in your description.	
Milestones:	
Please describe the expected key milestones that you will achieve during the project and indicate a time for when you expect to achieve them (you can use the description from the proposal). Please be specific in your description.	
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	

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

expected to be achieved e.g. in month 6 or month 12. This will be used to evaluate your progress in the interim and final report in M6 and M12 respectively.		
	M6	**M12**
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 in M12:

	Baseline (current status)	**Expected M12**
9. Employment created / safeguarded due to the Project (stating also the number of employees before the project (baseline) as well as forecasts for M12/2023)		
10. Impact on turnover due to the project (baseline and forecasts for 2023)		

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

11. Market share acquired due to the project (baseline and forecasts for 2023)		
12. Environmental impact (if applicable), (water consumption, energy…) generated by the project (baseline and forecasts for 2023)		
13. Contribution of the project to new or significantly improved products launched (baseline and forecasts for 2023)		
14. Contribution of the project to new or significantly improved methods and processes (baseline and forecasts for 2023)		
15. Advancement of TRL due to the Project (baseline and forecasts for 2023)		
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) 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:	

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

	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:
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.	
	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 Report: Demonstration projects

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Midterm Report M6

For demonstration projects

Deadline: M6

1. Information about the Midterm report M6

The Midterm report in M6 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, 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 (M6) (DD/MM/YEAR):	
Final report due (M12) (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:

Achieved deliverables:

Please describe the deliverables you have completed during the first half of your project period. Please be specific in your description. If there are any deviations, please explain why this is the case and which corrective measures you will use in order to get your project back on track.	

Achieved milestones:

Please describe the key milestones that you have achieved during the first half of your project period. Please be specific in your description. If there are any deviations, please explain why this is the case and which corrective measures you 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 will use in order to get your project back on track.	

Information on your project progress for public dissemination:

Please describe your project progress within the first 6 months, 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 in M6. If there are any deviations, please explain why this is the case and which corrective measures you will use in order to get your project back on track:

	M6
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. 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 6 months). 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 you have identified (if any) in the first 6 months and describe how counter measures 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 6 months (for instance technological, collaboration or external factors) and explain which	

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

mitigating practices 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 6 months of your project period:	
Please elaborate and sum up on the first 6 month 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.	
	Follow Up Manager:
Assigned Follow Up Manager (name, cluster, email)	

Signatures:

1st partner, name and date

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

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 Report: Prototyping projects

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Midterm Report M6

For prototype projects

Deadline: M6

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 M6

The Midterm report in M6 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, 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 (M6) (DD/MM/YEAR):	
Final report due (M12) (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:

Achieved deliverables:

Please describe the deliverables you have completed during the first half of your project period. Please be specific in your description. If there are any deviations, please explain why this is the case and which corrective measures you will use in order to get your project back on track.	

Achieved milestones:

Please describe the key milestones that you have achieved during the first half of your project period. Please be specific in your description. If there are any deviations, please explain why this is the case and which corrective measures you 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 will use in order to get your project back on track.	

Information on your project progress for public dissemination:

Please describe your project progress within the first 6 months, 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 in M6. If there are any deviations, please explain why this is the case and which corrective measures you will use in order to get your project back on track:

	M6
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. Please be specific in your description.	
Ethics self-assessment:	
Please address any ethical issues that you have identified (if any) in the first 6 months and describe how counter measures 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 6 months (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 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.	

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 first 6 months of your project period:	
Please elaborate and sum up on the first 6 month 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.	
	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 Report: Demonstration projects

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Final Report

For demonstration projects

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. Three financial prizes will be awarded: 7000 € for 1st prize, 4000 € for the 2nd prize, 3000 € for the 3rd prize. These financial prizes will have to be shared among the partners of the awarded project and have to be considered as a "gift". 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.

Contact information on consortium:

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

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:
	Organisation:

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

	Function:
	Country:
	Website:

Achieved deliverables:

Please describe all the deliverables you have completed during the entire project period, based on the deliverables you mentioned in the Follow Up Plan M1. ***Please be specific and exhaustive in your description and include all the information.*** If there are any deviations from the deliverables you planned at the beginning of the project, please explain why this is the case.	

Achieved milestones:

Please describe the key milestones that you have achieved during the entire project period, and when they have been achieved. ***Please be specific and exhaustive in your description and include all the information.*** If there are any deviations from the milestones you planned at the beginning of the project, 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 Plan M1 and additional ones not initially anticipated).	

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

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.* Please follow this format: -10 lines of 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.	

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

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 (baseline), expectations and actual achievements)			

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

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)			

Exploitation:	
Please describe how you have exploited the knowledge and progress developed and obtained in the project period so far.	

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

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:	
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:	

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

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	

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

(supply), system integrations, market immaturity, lack of market, funding etc.	
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))**

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 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.)					

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

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

Final Report: Prototyping projects

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Final Report

For prototyping projects

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

2. 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. Three financial prizes will be awarded: 7000 € for 1st prize, 4000 € for the 2nd prize, 3000 € for the 3rd prize. These financial prizes will have to be shared among the partners of the awarded project and have to be considered as a "gift". 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:

Achieved deliverables:

Please describe all the deliverables you have completed during the entire project period, based on the deliverables you mentioned in the Follow Up Plan M1. ***Please be specific and exhaustive in your description and include all the information.*** If there are any deviations from the deliverables you planned at the beginning of the project, please explain why this is the case.	

Achieved milestones:

Please describe the key milestones that you have achieved during the entire project period, and when they have been achieved. ***Please be specific and exhaustive in your description and include all the information.*** If there are any deviations from the milestones you planned at the beginning of the project, 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.* Please follow this format: -10 lines of 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.	

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

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))**

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 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					

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

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

Questionnaire template

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Questionnaire

For demonstration

Deadline: tbc

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

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**			*Please specify under each question:* 1. *requirements;* 2. *your compliance.*

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

	you demonstrate the prototype?			
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:*
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**:*

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

				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.*
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*			*If yes, please provide an explanation of:* *1. how the data subjects will be informed regarding the existence of the profiling,*

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

	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."			*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