Project Deliverable

D2.1 SecurIT challenges definition linked to 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
Due date	31 December 2021
Submission date	21 December 2021

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	03 December 2021	Document Creation	Draft	SAFE
V1	07 December 2021	Document Update	Review	CENSEC
V2	21 December 2021	Submitted document	Final	SAFE

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 60+ consortiums of European SMEs, that will be granted with a prototype or demonstrator voucher, through a top-notch selective process of 2 Open Calls. *In fine*, the project will support collaborative projects that will create a new industrial value chain.

The project will organise workshops before each open call's launching, reuniting end-users and integrators of security solutions to help structuring the use cases and scenarios that will be addressed by the SMEs projects.

This document details the process that had let to the compilation of the SecurIT challenges that have been defined, and that will consist in the core of the 1st Open Call to be launched in January 2022. These challenges were defined through the work carried out in WP2, related to SecurIT Challenges definition, via the lead of L3CE, as WP2 Leader. The objective of *Task 2.1. Needs analysis and expression of security solutions integrators and end-users* led by SAFE was to obtain a clear definition of the challenges to be addressed in SecurIT project. The work was carried out through an extensive process of consultations of +35 end-users and integrators reunited in thematic workshops that conveyed their challenges to be tackled and expressed their expectations for solutions to be provided from small and medium European companies.

Another process of consultations to end-users and integrators shall also be carried out prior to the launch of the 2nd Open Call of SecurIT in order to submit the Deliverable D2.2 - SecurIT challenges definition linked to Open call 2, due on December, 31st 2022.

Authors (organisation)

SAFE

Reviewers (organisation)

CenSec

Keywords

Challenges, security, domains, use-cases, resilience, disaster, cities, end-users, public space protections, critical infrastructures, territories.

Legal notice

The information and views set out in this application form are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

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

SecurIT challenges definition linked to Open call 1

Process

Upon start of SecurIT project, the consortium early launched a process of consultations at the end of November 2021, that consisted in holding three two-hour workshops, reuniting around the table end-users and integrators, that had been invited by each consortium's members. Due to the travel restrictions and the time-constraints, the consortium opted for online meetings, in lieu of physical events.

The aim of these workshops was to define the needs of integrators and end-users in terms of security for the 1st Open Call. The ultimate expected result was to design a tailored-made call for propositions, suitable for end-users and integrators that had identified the common gaps in security, to be tackled. These challenges are to be inserted in the Guide for Applicants of Open Call 1 (cf. deliverable D3.1), and on the website of the SecurIT project.

The 3 workshops took place on November 18 and 19th 2021, two months prior the opening of Open Call 1, and the invitations were launched at the end of October 2021. In order to generate the most innovations, the workshops were carefully prepared by the consortium through a certain number of dedicated meetings. Several categories of security challenges had been pre-defined: a first list of challenges, segmented in 3 main domains, had been prepared and agreed among the consortium prior to the workshops, in order to have the most representative security challenges presented as a point of departure. An invitation with an agenda with the list of pre-identified challenges was sent out to the integrators and end-users in order to help them specify their needs. The integrators and end-users that had provided a Letter of Support when the SecurIT proposal was submitted also joined in the sessions. All the stake holders had also been invited to provide one or several use-cases through a pre-filled template, sent out with the invitation.

The workshops were co-animated by the partners SAFE and LSEC, and all the consortium members also participated. The tool Mentimeter was used, in order to generate need expressions through polls and votes, engaging the end-users in an active participating way and creating interactivity. The online discussions permitted to collect from the participants their contribution of use-cases, re-orient and prioritize the challenges and identify some key elements that had been forgotten or left apart. The end-users and integrators expressed their views regarding the proposed challenges, discussed their needs while underlining the main issues they were facing.

The 3 workshops took place according to the following schedule and participants:

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

- **Workshop 1: Domain #1: Sensitive infrastructure protection - November 18th 2021 – 3:00 – 5:00 pm CET**

Participants: members from: French Digital Agency for Civil Security, City of Nice, Engie (FR), French ministry of Ecological Transition, INERIS, Ilunion Seguridad S.A, ATOS IT Solutions and Services (DK), The Danish Institute for Fire and Security Technology (DBI), EACTDA, Engie (BE) – Laborelec, Member of CoESS.

During the workshop, the end-users agreed on their major concern around the security of sensitive sites, in a current context of social unrest, pandemics, terrorist threats. Engie expressed the need to have a holistic approach because of the cascading effects of incidents for a sensitive infrastructure. The end-users also suggested to introduce the following notions that had been initially left out from the topic: *Maintainability, supply chain, price, foresight scanning, interoperability.*

- **Workshop 2: Domain #2: Disaster resilience - November 19th 2021 – 10:00 – 12:00 am CET**

Participants: members from: French Digital Agency for Civil Security, City of Nice, Engie (FR), The Danish Institute for Fire and Security Technology (DBI), The Resilience Advisors Network, Member of CoESS.

During the 2-hour workshop, the end-users expressed their views on the topics and the list of challenges that was pre-identified. One of them stressed the need for integrating the 4 related items linked to disaster resilience: anticipation, crisis management, and the “build-back-better” approach, that implies a feedback on crisis. One of them also stressed the importance of social and citizen participation in a moment of crisis, the need of developing some digital tools with citizens, and the citizen awareness needed in decision-making. They separated information and communication, that addresses different publics: while communication is used for internal audience (first responders, etc.), information must be considered as external information to public, citizens and victims of a disaster.

The interactive tool Mentimeter permitted to stress out the following current and future needs such as: *data sharing, cybersecurity, communication, citizen participation, transparency, autonomy, processes, continuity of operations, digital tools, cyber awareness*. The end-users also outlined the following notions that were omitted: *autonomous energy systems, public info sharing, public alerting, multi-source information gathering*.

It was thus decided to stress in the challenges the following elements: convergence of digital tools and solutions to articulate information and management, Convergence of information for crisis centre monitoring for the best-human decisions and the notion of information vs decision with the support of AI.

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

- **Workshop 3: Domain #3: Public spaces protection – major events - November 19th 2021 – 3:00 – 5:00 pm CET**

Participants: members from: French Digital Agency for Civil Security, City of Nice, The Danish Institute for Fire and Security Technology (DBI), Police Department under MoI of Lithuania, CERTH, Lithuanian Armed Forces STRATCOM Department, Dutch Ministry of Defence (Cyber Innovation Hub).

The participants actively expressed their views regarding the protection of public spaces in major events. The Lithuanian Police for example, as representative of a Law Enforcement Agency (LEA), underlined their number 1 priority in case of incidents: evacuating people and organize routes for evacuation and eliminate the threat, and expressed the need for deeper communication between private security companies, suggesting it could be improved through a mobile application for example.
The City of Nice representative also underlined that experimentations must permit to remove doubts and confirm the operational utility.

Through the Mentimenter tool, the needs of end-users outlined these notions: *guide the emergency team, information distribution, social media analysis, targeted video surveillance, brawl detection, crowd detection, prevention of accidents, weapons detection, illegal waste dump, shared information.*
The following notions had been left out from the challenges and added by the participants: *cyber intelligence sharing between SMEs, resilience approach, digital tools with public space, web comportment analysis, consequences, training, evacuation, dashboard, multi partner hyper vision, coordination, misinformation, organizing support to victims, interoperable networks, effect, emergency prep plan, augmented reality*.
All the recommendations made by the end-users were considered in the updated list of challenges.

In the following days, SecurIT partners reorganised the challenges and prioritized them, according to the discussions. They met (online) to agree on the list content of specifications related to the three main domains, and further validated the content once verified by the participants to the workshops and external security experts. The final list is to be inserted into the challenges of the Guide of Applicants of Open Call 1 to be distributed by FBA partner (section 3.2 – What types of activities can be funded?") and also presented on the website of the project.

The objective of the task was to identify common gaps between actors, which later shall be the basis for the call description. It allows SecurIT partners to propose strategic challenges in a cross-border and cross-sectorial industry value chain, and will ensure a real interest for SMEs responding to the Open Call 1, in terms of potential expected market as well as the business and collaboration that will be developed, while matching current and future needs of practitioners.

In the following weeks after the workshops, the consortium members organised national webinars in their ecosystem, prior to the launch of the Open Call to inform about upcoming SecurIT funding

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

opportunities and start engaging them. A total of 160+ SMEs participated in the 5 webinars organised by SecurIT partners (see corresponding annex).

The quantitative outcomes that were set for the task for the total duration of project : *2 Workshops Days; 40 integrators participating; 100 SMEs participating; 300 Expression of Interests (EoI); 5 SecurIT Challenges defined at least,* were adapted to the current situation and led to the achievement of the following Key Performance Indicators (KPIs) for the 1st round of preparation of the upcoming Open Call: *3 workshops organised, 35+ European integrators and end-users participating, 11 SecurIT challenges defined within 3 main topics, 160+ engaged SMEs/Expression of interests received.*

Another process of consultations will be led in the second cycle of the project, prior to the launch of the 2nd Open Call, that will lead to the Deliverable D2.2 - SecurIT challenges definition linked to Open call 2 due on December, 31st 2022.

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

Definition of challenges

The following tables detail the security challenges definition and related-use cases, segmented in 3 categories and 11 sub-domains. They are to be inserted in the Guide for Applicants, under section 3.2 “What types of activities can be funded?”

Challenges – SecurIT – Open Call 1

More than 35 end-users and integrators of security solutions have conveyed their challenges to the SecurIT project and its partners through dedicated workshops. In these workshops, they expressed their expectations for solutions to be provided from consortiums of small and medium sized European companies. Those SMEs will have the opportunity to get direct financial support from the SecurIT project to develop their solutions through individual vouchers up to €60,000 and access to a wide range of tailored professional services.

The challenges have been defined around 3 main domains:

DOMAIN #1

Sensitive infrastructure protection

The security of sensitive sites is a major concern, confirmed by recent events, in a context of social unrest, terrorist threats and even a pandemic.

DOMAIN #2

Disaster resilience

Need of instruments for better prevention and preparedness, technologies for first and second responders, and where relevant for citizens, and overall societal resilience.

DOMAIN #3

Public spaces protection – major events

A more connected city, integrating Artificial Intelligence, Cloud computing and Big Data, where the population takes on a more active role in serving the community.

- **Domain #1: sensitive infrastructure protection**

Sensitive infrastructure protection pertains to the securing of assets and systems that are essential for the functioning of a society and economy. Examples include the provision of gas and oil, agriculture, and telecommunication. The security of sensitive infrastructure is a major concern, confirmed by recent events, in the context of social unrest, terrorist threats and even a pandemic. If this type of infrastructure is exposed to external threats, this will have major consequences for society as a whole.

Targeted end-users: for example, end-users of projects around sensitive infrastructure protection include the safety director of vital importance and Seveso classified industrial facilities, airports, hospital infrastructure, and operators (e.g. electricity, gas, telecommunications, etc.)

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

Solutions: The solutions developed in this domain will have to integrate the following considerations: maintainability, acceptable price, foresight scanning, and interoperability with existing solutions.

- **Domain #2 - Disaster resilience**

There is a need for instruments that facilitate improved prevention and preparedness in crises and natural disasters. The development of technologies for first and second responders, and where relevant for citizens, that increase societal resilience is the second focus-area of the SecurIT project. Innovative technologies can help detect, analyse, treat, and/or prevent major natural events. This domain focuses mainly on climate-related risks and extreme events, geological disasters such as wildfires, earthquakes, tsunamis, and pandemics.

Targeted end-users: for example, first responders, cities and territories, and their governmental structures.

Solutions: The solutions developed in this domain will have to consider citizen involvement and acceptation and transparency. All solutions will also have to ensure the continuity of operations.

- **Domain #3 – Protection of public spaces**

The objective of this domain is to develop innovative tools that create increasingly connected and protected cities in which the population takes on a more active role in serving the community. These solutions should integrate and consider state-of-the-art technologies like in Artificial Intelligence, Cloud computing, and Big Data.

Targeted end-users: for example, cities and territories (security of public roads), and venues open to the public (e.g.: stadiums; concert zone, train stations, etc.).

Solutions: The solutions developed in this domain will have to consider the legal constraints of personal data protection.

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

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #1: sensitive infrastructure protection	**Cybersecurity**	1	**Development of cybersecurity solutions for sensitive infrastructure protection**	To propose effective solutions for: - Cybersecurity of information and communication systems; Data protection; electromagnetic protection; - Cyber Security incident management; - Cybersecurity - Automatic attack detection and remediation; - Quantum - Post Quantum; - Security Bill of Materials - Device - IoT Security - Shared Responsibility; - Secure Sovereign Cloud.
	Operations	2	**Optimisation of communication networks and alert systems**	To optimize solutions for better communication networks (assess, detect and alert both operational forces, LEA or emergency services), the hyper vision and command systems and alert systems.
	Identification and access control	3	**Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk.**	To propose innovative solutions to identify, provide entry for and inspect individuals, vehicles and goods requesting access to the site such as: - Access control for people; - Biometrics & multi biometric systems; - Vehicle control & inspection; - Detecting weapons & explosives: stationary or mobile illicit materials like CBRNE (chemical, biological, radiological, nuclear and explosives) and weapons.
	Zone security and perimeter protection	4	**Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions**	To propose innovative solutions such as: - Data sensors: detectors; system status indicators; IoT; - Video analysis & sensor fusion: deep learning; - Surveillance – Essential components of the decision-making chain are the detection, recognition and identification of land/air/sea vessels and intruders near or inside the protected area – e.g.: optronic solutions; radar sensors; solutions and data processing/analysis software; video protection (embedded AI); - Surveillance Robots: patrol rounds and missions - detection/identification/neutralization of malicious drone; - Securing physical access routes through digital solutions.

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

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #2 - Disaster resilience	**Prior to crisis – prediction:** **Risk knowledge and evaluation**	5	**Optimisation of prediction of disaster**	To propose innovative solutions to: - Enhance exploitation of monitoring data and satellite/remote sensing information as well as artificial intelligence to improve high-level assessment - Production and processing of data by satellite and aerial imagery (UAV/UAS and light aircraft), as well as by sensor networks. This allows for knowledge about areas concerned and potential risks, integrating data about weather and water courses, providing operational maps for decision-makers and rescue managers. - Modelling and geographical information systems: Modelling territories and the simulation of phenomena allow for the substitution of rarely accessible situations by virtual situations in realistic and operational 3D.
	During the crisis: **Communication and warning systems**	6	**Optimisation of communication and warning systems in case of disaster**	These communication systems must be easily transportable and easily deployable within a timeframe compatible with operational demands. The requirement is to have means of communication, which are suitable, diversified, and interoperable such as: - Technology that enables the management and monitoring of communication from news media, social media, and internal communication sources in a crisis situation - Information vs decision with the support of AI To propose innovative solutions to improve forecast / early warning systems, advanced data management, Information update.
	After the crisis: **Post event analysis and recovery**	7	**Development of solutions for a better recovery**	To propose innovation solutions, post crisis and recovery: • Robotics to carry out tasks in hazardous areas for humans • UAV/UAS can view an « area of interest » and give a good understanding of the environment and the situation in the area affected by a disaster • Energy and data network rehability, autonomous and decentralized – to ensure the conservation of the security of data in the context of post-disaster.

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

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #3 - Public spaces protection – major events	**Detection and alert**	8	**Gather and manage real time information**	To propose innovative solutions to gather and manage real time information such as facial and vehicle recognition; CCTVS & cameras (eg: embedded AI for flow detection and crowd surveillance, smart cameras, etc.), signal jamming devices for drones, wave scanners systems and anomaly detection systems. To propose warning systems such as innovative tools for public and/or geolocation of public and rescue team.
	Analysis	9	**Analyse and extract pertinent and potentially crucial information as quickly as possible**	To propose innovative tools that can be used in real-time mode (alert, surveillance, or intervention) or in delayed mode (intelligence, investigations, e.g.: audio analytics systems, SOP updates, blind-spot mapping, performance analyses and determining training programmes etc.). To propose innovative analysis tools to support the responsible authorities in monitoring the public information space and quickly identifying disinformation threats
	Command and control (resource management) and decision- making support	10	**Communication networks and post - event analysis**	To produce innovative safe tools that support event planning and resource management during the event. Such tool should support: - connectivity of different authentication level users; - definition of environment (defining time, uploading geo information, defining roles, etc.); - possibility to see location of resources and communicate with all linked entities directly via safe tool; - possibility to provide visual guidance; - possibility to upload new relevant data and share with respective entities; — possibility to manage few events at a time. To propose innovative solutions for better communication networks, post event analysis

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

	Data protection and cybersecurity – cybercrime	**11**	**Detection**	To propose innovation solutions such as: • AI manipulated content analysis: deep fake video detection; deep fake audio detection • Methods for identifying information sources / provenance of information: detection of similar information appearing in different venues / platforms; attribution of information to a single source • Media forensics: image forensics (content manipulation detection; copy-move, splicing, inpainting, enhancement) • Video forensics (content manipulation detection; traditional cut, delete, paste attacks, copy-move, splicing, inpainting, enhancement); audio forensics (content manipulation detection, traditional cut, delete, paste attacks) • Textual content analysis: Image content analysis; Audio content analysis; Video content analysis • Security bills of materials device IoT security shared responsibility

Annexes

Agenda Workshop 1

SecurIT EU-funded project'*s 1st cycle of workshops*

Workshop on domain #1: sensitive infrastructure protection

November 18th 2021 – 3:00 – 5:00 pm CET

Context

The EU-funded project SecurIT - *New industrial value chain for Safe, sECure and Resilient cIties and Territories*, aims at funding, with prototype or demonstration vouchers, consortium of European companies that will propose innovative security solutions. SecurIT will support and select 63 best-in-class collaborative projects developed by 126 SMEs across Europe, through two Open Calls) in January 2022 and February 2023.

Led by a European consortium of 8 partners (Pôle SAFE - France; Pôle SCS – France; LSEC - Belgium; L3CE - Lithuania; The Hague Security Delta (HSD) - Netherlands; SYSTEMATIC (SPR) - France; Center for Defence, Space & Security (CenSec) - Denmark; Funding box - Poland), the project will organise online workshops before each open calls launching, reuniting end-users and integrators of security solutions to help structuring the use cases and scenarios that will consist in the core of the upcoming calls.

Topic

Domain #1: Sensitive infrastructure protection

The security of sensitive sites is a major concern, confirmed by recent events, in a context of social unrest, terrorist threats and even a pandemic.

Targeted end-users: safety director of vital importance and Seveso classified industrial facilities; airports; hospital infrastructure; operators (electricity, gas, telecom...)

Moderators

Mr. Philippe LECLERC, Program Director "Security and Safety" – Pole Safe Cluster

Mr. Hubert BERENGER, Program Director "Unmanned and autonomous systems'" – Pole Safe Cluster

Agenda

- Round-table and presentation of the participants – interest in the workshops – 15 min;
- Context: brief presentation of the EU-funded project SecurIT - 10 min;

- Discussion of the main security challenges relevant for the domain and potential technological solutions – 25 min;
- Tackling the legal issues about integrating and/or using security solutions – from a national experience - 25 min;
- Identification of test beds in Europe - 25 min;
- Validation of the targeted sub domains and common use cases – 25 min.

To attend the visio-conference, please connect to:
Join the meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/944231469
You can also call using your phone.
France: +33 170 950 594
Access code: 944-231-469

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

Agenda Workshop 2

SecurIT EU-funded project*'s 1st cycle of workshops*
Workshop on domain #2: Disaster resilience
November 19th 2021 – 10:00 – 12:00 am CET

Context

The EU-funded project SecurIT - *New industrial value chain for Safe, sECure and Resilient cIties and Territories*, aims at funding, with prototype or demonstration vouchers, consortium of European companies that will propose innovative security solutions. SecurIT will support and select 63 best-in-class collaborative projects developed by 126 SMEs across Europe, through two Open Calls) in January 2022 and February 2023.

Led by a European consortium of 8 partners (Pôle SAFE - France; Pôle SCS – France; LSEC - Belgium; L3CE - Lithuania; The Hague Security Delta (HSD) - Netherlands; SYSTEMATIC (SPR) - France; Center for Defence, Space & Security (CenSec) - Denmark; Funding box - Poland), the project will organise online workshops before each open calls launching, reuniting end-users and integrators of security solutions to help structuring the use cases and scenarios that will consist in the core of the upcoming calls.

Topic

Domain #2: Disaster resilience
Need of instruments for better prevention and preparedness, technologies for first and second responders, and where relevant for citizens, and overall societal resilience. The innovative technologies can help to detect; analyze and treat to prevent major natural events. Climate-related risks and extreme events; geological disasters, such as wildfires; earthquakes, tsunamis; pandemics).
Targeted end-users: first responders; cities and territories.

Moderators

Mr. Sébastien LAHAYE, Program Director " Forest Fire Resiliency Program" – Pole Safe Cluster
Mr. Loïc CHANVILLARD, Program Director “Aerospace” – Pole Safe Cluster

Agenda

- Round-table and presentation of the participants – interest in the workshops – 15 min;
- Context: brief presentation of the EU-funded project SecurIT - 10 min;
- Discussion of the main security challenges relevant for the domain and potential technological solutions – 25 min;

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

- Tackling the legal issues about integrating and/or using security solutions – from a national experience - 25 min;
- Identification of test beds in Europe - 25 min;
- Validation of the targeted sub domains and common use cases – 25 min.

To attend the visio-conference, please connect to:

Join the meeting from your computer, tablet or smartphone.

https://global.gotomeeting.com/join/944231469

You can also call using your phone.

France: +33 170 950 594

Access code: 944-231-469

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

Agenda Workshop 3

SecurIT EU-funded project*'s 1st cycle of workshops*
Workshop on domain #3: Public spaces protection – major events
November 19th 2021 – 3:00 – 5:00 pm CET

Context

The EU-funded project SecurIT - *New industrial value chain for Safe, sECure and Resilient cIties and Territories*, aims at funding, with prototype or demonstration vouchers, consortium of European companies that will propose innovative security solutions. SecurIT will support and select 63 best-in-class collaborative projects developed by 126 SMEs across Europe, through two Open Calls) in January 2022 and February 2023.

Led by a European consortium of 8 partners (Pôle SAFE - France; Pôle SCS – France; LSEC - Belgium; L3CE - Lithuania; The Hague Security Delta (HSD) - Netherlands; SYSTEMATIC (SPR) - France; Center for Defence, Space & Security (CenSec) - Denmark; Funding box - Poland), the project will organise online workshops before each open calls launching, reuniting end-users and integrators of security solutions to help structuring the use cases and scenarios that will consist in the core of the upcoming calls.

Topic

Domain #3: Public spaces protection – major events
A more connected city, integrating Artificial Intelligence, Cloud computing and Big Data, where the population takes on a more active role in serving the community
Targeted end-users: cities and territories (security of public roads); train station; venues open to the public (eg: stadiums; concert zone etc.).

Moderators

Mr. Philippe LECLERC, Program Director "Security and Safety" – Pole Safe Cluster
Mr. Hubert BERENGER, Program Director “Unmanned and autonomous systems’” – Pole Safe Cluster

Agenda

- Round-table and presentation of the participants – interest in the workshops – 15 min;
- Context: brief presentation of the EU-funded project SecurIT - 10 min;
- Discussion of the main security challenges relevant for the domain and potential technological solutions – 25 min;

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

- Tackling the legal issues about integrating and/or using security solutions – from a national experience - 25 min;
- Identification of test beds in Europe - 25 min;
- Validation of the targeted sub domains and common use cases – 25 min.

To attend the visio-conference, please connect to:
Join the meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/944231469
You can also call using your phone.
France: +33 170 950 594
Access code: 944-231-469

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

Webinars prior to Open Call launch

Choose your webinar session and save the date! *

The SecurIT Cluster partners are organising webinars in their respective ecosystems:

Safe Cluster, SCS Cluster & Systematic Paris Région

- Language: French
- 07 December 2021 – 15:00-16:00 CET
- Replay available soon in our Media Hub!
- More information

HSD

- Language: Dutch/English
- 15 December 2021 – 15:00-15:30 CET
- More information

CenSec

- Language: Danish
- 17 December 2021 – 11:00-12:00 CET
- More information

LSEC

- Language: English
- 20 December 2021 – 12:00-13:00 CET
- More information

L3CE

- Language: English
- 21 December 2021 – 13:00-14:00 CET
- More information

*extraction from the news #2 of the website: https://securit-project.eu/project-launch-2/

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