



SECURIT

TOWARDS RESILIENT SMART CITIES & TERRITORIES

Project Deliverable

D2.2 SecurIT challenges definition linked to Open Call 2



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 2022
Submission date	19 December 2022

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	6 December 2022	Document Creation	Draft	SAFE
V1	16 December 2022	Document Update	Review	L3CE
V2	19 December 2022	Submitted document	Final	SAFE
V3	19 December 2022	Revised document	Final	SAFE



Table of content

Abstract	4
SecurIT challenges definition linked to Open call 2	6
Methodology	6
Open Call 2 Challenges	10
Domain #1: sensitive infrastructure protection	11
Domain #2 - Disaster resilience	11
Domain #3 – Protection of public spaces	12
Annexes	17





Abstract

EU-funded SecurIT project (standing for New industrial value chain for Safe, sECure and Resilient cities and Territories) aims at supporting innovative digital solutions in the field of security, developed by consortiums of European SMEs, granted with a prototype or demonstrator funding instruments, through a top-notch selective process of 2 Open Calls. *In fine*, the project will support and select the most promising collaborative projects developed by European SMEs, that will create a new industrial value chain.

In this regard, the challenges that the applicants and projects shall address consist in the core of the Open Calls and thus need to be cautiously identified. This document details the second process that was conducted in the second cycle of the project, in order to update the list of challenges that were showcased in the 1st Open Call launched in January 2022.

These challenges are defined through the work carried out in WP2, related to SecurIT Challenges definition, via the lead of partner L3CE - WP 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 a consultation process gathering security experts, to discuss the current gaps and needs in the market.

The 1st Open call led to the funding of [21 projects](#) that entered the 12-month support program provided by SecurIT consortium. These projects are addressing the 3 domains and related challenges that consisted in the core of the Open call 1, i.e. Sensitive Infrastructure protection, Disaster resilience and Public Space Protection. Since the project aims at sourcing innovative solutions with a market pull orientation, a consultations process was carried out in order to improve the features of the 2nd Open call to be launched early 2023.

Authors (organisation)

SAFE

Reviewers (organisation)

L3CE

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.





SecurIT challenges definition linked to Open call 2

The objective of the task is to identify common gaps, which later will be the basis for the calls' description. It allows SecurIT partners to propose strategic challenges in a cross-border and cross-sectorial industry value chain, that will ensure a real interest for SMEs responding to the Open Calls, 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.

Methodology

The process used for the definition of the challenges for the Open Call 2 was slightly revised compared to the 1st cycle. The consultations previously held at the start of the project in M3 gathered needs and gaps from a great number of end-users and integrators, which were consolidated into 3 main domains and 11 related-challenges for Open Call 1.

Lessons learnt and statistics from Open Call 1

In order to improve the methodology for the Open Call 2 and to learn from past lessons, SecurIT consortium decided to draw an analysis from the first selection process.

At the end of the selection process of the 1st Open Call, it was found out that 2/3rd of the 111 applications received in Open Call 1 targeted the 1st domain on protection of critical infrastructure, while the rest of applications (figure 1 below) were equally split between the two other domains.

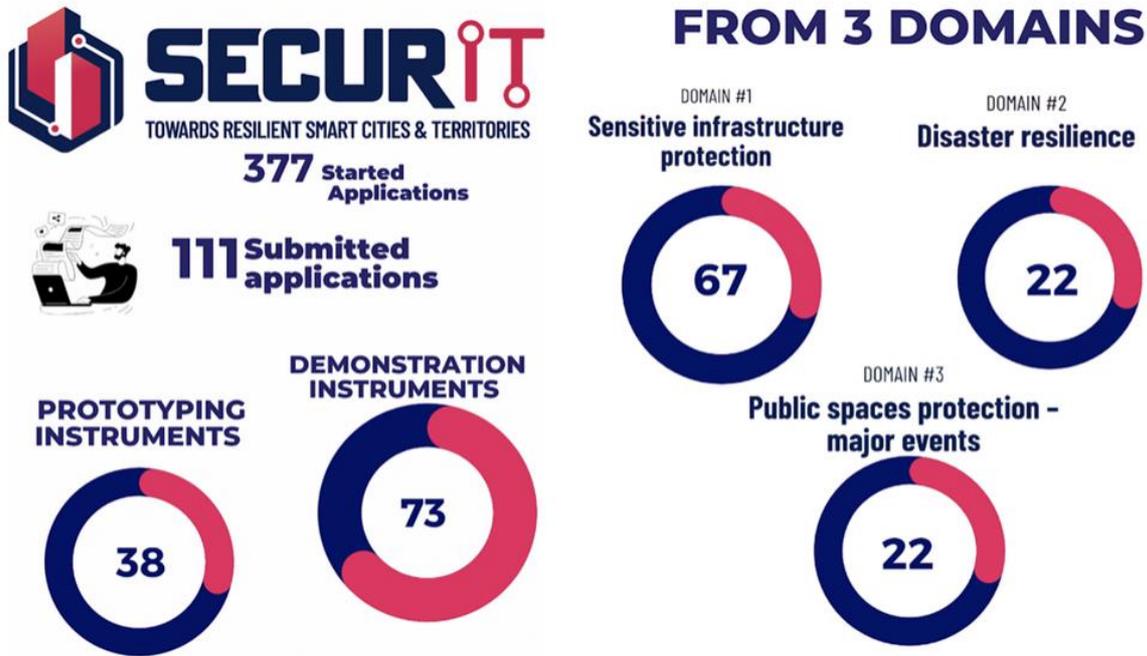


Figure 1 – repartition of applications received under Open Call 1

Also, after the selection of the projects and according to the statistics on laureates, it was found out that 3 challenges were not addressed by the funded projects.

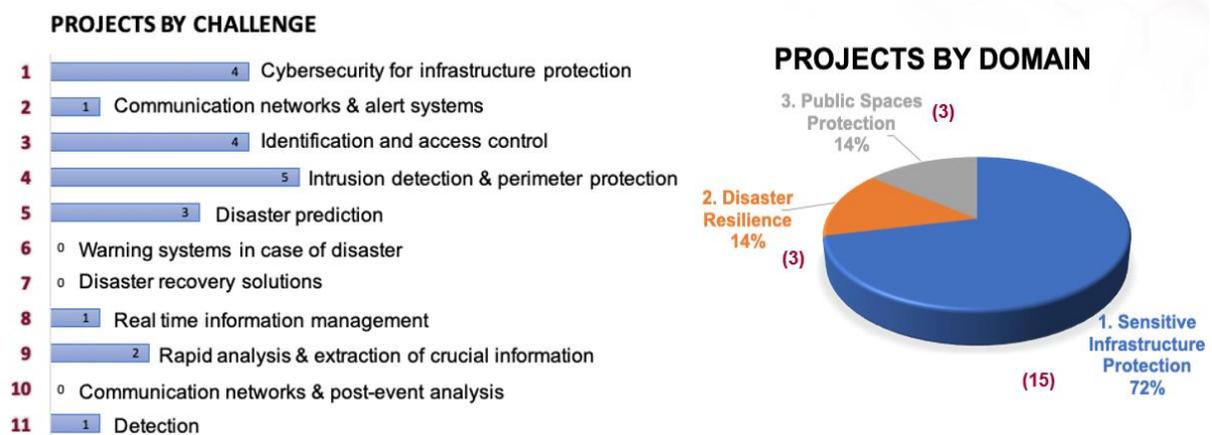


Figure 2 – Statistics from funded projects under Open Call 1

At the end of Open call 1, the consortium of SecurIT produced *Lessons learnt for Open Call 2* document to reflect on the second open call methodology, with the objective of improving processes, and modifying some features of the 1st Open Call that might not have been satisfactory enough for the consortium of SecurIT, applicants or related stakeholders. Feedback of some SMEs applicants showed, that some of the challenges could have been misunderstood or be misleading. Some mistakes of applicants were observed when choosing the challenges and the domains since the challenges on the application platform were not linked to the domains. Lessons learnt document conclusion was to start from the initial list of challenges, and to work on a more precise scope and description.



Advisory Board of SecurIT

Upon start of the project, and in accordance with the Grant Agreement provisions and project's commitment, SecurIT consortium established an **Advisory Board**, in order to pull subject matter experts to provide the project team with valuable support and expertise in achieving strategic objectives of SecurIT project.

In this regard, the Advisory Board (AB) was established with the following role and tasks:

- Provide insights on how to improve the Open Calls organization process
- Contribute to how to reduce the gap between the demand and offering & how to mobilise different networks
- Help to identify the most promising innovations
- Help to establish connections with SMEs, end-users, integrators
- Provide insights on exploitation paths of SecurIT project results
- Help to promote SecurIT project and results

Being involved as an Advisory Board Member within SecurIT can also be valuable and bring a certain amount of benefits, such as:

- Wider exposure to new opportunities of participation in new initiatives
- Opportunity to learn about new products and technologies releases in advance
- AB is an excellent vehicle for establishing valuable professional connections
- Opportunity to participate in exciting networking activities

The Advisory Board was established at the start of the project, composed of 7 members and experts on the security field, from various countries. The Advisory Board held a first meeting at M6 of the project, and the coordination entity of this expert group, L3CE, would organise 2 meetings a year. They were invited to the 1st Jury day that took place at the end of June 2022 in Paris (M10) but due to agenda constraint, they could not attend the pitching session of the pre-selected candidates. When the selection process of Open Call 1 was achieved, they informed and granted access to the description of funded projects under Open Call 1.

In order to engage them in the upcoming activities of the project SecurIT and to benefit from their expertise, it was then decided to involve them in reshaping of the challenges of the 2nd Open Call of SecurIT.

Advisory Board members (position and entity)

1	Professor	KU Leuven
2	Senior Policy Manager	ECSO/YesWeHack
3	Digital Innovation	Agio Capital
4	Founder & Managing Director of the Resilience Advisors Network (RAN)	RAN - a team of some 150 civil protection experts from across Europe.



5	External Relationships & Marketing Executive - Energy Solutions	ENGIE/SIRADEL
6	Associate Professor Department of Materials and Production	Aalborg University
7	Head of Security and Crisis Management	The Danish Institute of Fire and Security Technology (DBI)

Consultations

The Advisory Board members were invited to 2 online sessions, to provide an expert point of view of the challenges that were used for the 1st Open Call, to reshape and improve them for the second Open Call descriptions and selection process.

For that two 1-hour workshops gathering 4 of the Advisory Board members were organized. They took place online on November 17th and 22nd 2022 (M15). Discussions permitted to exchange views and different visions on the innovations and solutions sought out within the project. The experts were invited to provide an external perspective on the challenges, in order to improve clarify and precision of the wording, as well as modify the scope of the challenges accordingly.

The workshops were animated by SAFE as coordinator of SecurIT and leader of the task, and supported by SecurIT consortium members. Some leading questions asked to the experts were used to orient the debates, such as:

- *What are your main gaps and main needs in terms of security or needs perceived from the security market?*
- *what type of digital applications would you expect from SecurIT selection process?*
- *(while keeping the focus on digital innovative solutions), how could the challenges could be rephrased or amended?*
- *what other challenges could be added/ what other needs have you identified?*
- *do you find these challenges relevant to security market?*

The discussions and inputs provided by the experts permitted to redefine the challenges in a better and more precise way, while keeping the 11 challenges and 3 domains (cf. Annex I).

Inputs from the [Deloitte/ Ecorys EC Security Market Study \(May 2022\)](#) were also used to fine-tune the challenges, following the priorities of the European Commission in terms of security segmentation: resilience of critical infrastructures, disaster resilient societies, border management and fighting counter terrorism.



Final list of challenges for Open Call 2

In the following days during a consortium meeting for WP2, SecurIT partners agreed on and approved the final description of challenges for Open Call 2 in a “results session”, discussing the contributions discussed during the workshops. The recommendations made by the experts were reflected in the updated list of challenges. The numbering of challenges was updated to avoid potential mistakes when selecting the right challenge for the right domain (list of challenges from 1.1 to 3.4 instead of 1 to 11). The final list is inserted into the challenges of *the Guide of Applicants* of Open Call 2 to be distributed by FBA partner (section 3.2 – What types of activities can be funded?) and is also presented on the website of the project.

KPI

The quantitative outcomes set for this task were the following (for both rounds):

- 2 Workshops Days;
- 40 integrators participating;
- 100 SMEs participating;
- 300 Expression of Interests (Eoi);
- At least 5 SecurIT Challenges defined.

They led to the achievement of the following Key Performance Indicators (KPIs) for the 2 rounds of preparation of the Open Calls:

- 5 workshops organised,
- 39 European integrators and end-users participating (including the 4 Advisory board members as security experts),
- 11 SecurIT challenges defined within 3 main topics,
- 160+ engaged SMEs/Expression of interests received (during the 1st cycle).

Importantly, KPIs for this task had already been reached through the 1st cycle/process, with 3 workshops organized, gathering +35 end-users, at M3 of the project.

Task 2.1 of the project SecurIT is now completed and achieved.

Open Call 2 Challenges

The challenges of the second Open Call of the SecurIT project have been defined around 3 main domains:



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. The solutions should address hybrid threats, permit to enhance capabilities, and consider the increasingly interconnected, complex and interdependent networks and systems.

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, energy suppliers, and operators (e.g. electricity, gas, telecommunications, etc.).

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, extreme events and natural disasters. In this second focus area of SecurIT, the solutions should focus on development of technologies to strengthen the capacities of first and second responders in all operational phases, and where relevant, to increase societal resilience towards and for citizens. Innovative technologies can help detect, analyse, treat, and/or prevent major natural events. This domain focuses on climate-related risks and extreme events, geological disasters such as wildfires, earthquakes, tsunamis, and pandemics, but also accidental disasters and human-induced disasters (food safety, industrial accidents, infrastructure failures, nuclear accidents, and others).

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

Solutions: The solutions developed under this domain will have to consider citizen involvement and acceptance 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.

Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #1: sensitive infrastructure protection 	1.1	Development of cybersecurity solutions for sensitive infrastructure protection	To propose effective cybersecurity solutions and solutions to increase resilience against cyber-attacks: <ul style="list-style-type: none"> - Cybersecurity of information and communication systems; Data protection and security of data; 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.
	1.2	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.
	1.3	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 digital innovative solutions to identify, provide entry for and inspect individuals, vehicles and goods requesting access to the site such as: <ul style="list-style-type: none"> - 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.
	1.4	Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions	To propose digital innovative solutions such as: <ul style="list-style-type: none"> - 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 and development of physical access control solutions.

Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #2 - Disaster resilience 		2.1 Optimisation of prediction of disaster	<p>To propose innovative solutions and technologies for prevention to:</p> <ul style="list-style-type: none"> - 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: Mass communication and warning systems	2.1 Optimisation of communication and warning systems in case of disaster	<p>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:</p> <ul style="list-style-type: none"> - 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 <p>To propose innovative solutions and technologies for disaster response to improve forecast / early warning systems, advanced data management, Information update.</p>
	After the crisis: Post event analysis and recovery	2.3 Development of solutions for a better recovery	<p>To propose innovation solutions and technologies for post crisis and disaster recovery:</p> <ul style="list-style-type: none"> - 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 rehabilitation, autonomous and decentralized – to ensure the conservation of the security of data in the context of post-disaster.



	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #3 - Public spaces protection – major events 	Detection, alert and behaviour analysis	3.1	Gather and manage real time information	<p>To propose innovative solutions for data and information gathering, exploitation and exchange, surveillance and intelligence: facial, speech, and vehicle recognition; CCTVS & cameras (e.g.: embedded AI for flow detection and crowd surveillance, smart cameras, etc.), signal jamming devices for drones, wave scanners systems and anomaly detection systems.</p> <p>To propose warning systems such as innovative tools for public and/or geolocation of public and rescue team.</p>
	Analysis	3.2	Analyse and extract pertinent and potentially crucial information as quickly as possible	<p>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.).</p> <p>To propose innovative analysis tools to support the responsible authorities in monitoring the public information space and quickly identifying disinformation threats, using emerging solutions for integration of information from multiple and non-traditional sources (e.g., social media) into incident command operations.</p>
	Command and control (resource management) and decision-making support	3.3	Communication networks and post-event analysis	<p>To produce innovative safe tools that support event planning and resource management during the event. Such tool should support:</p> <ul style="list-style-type: none"> - 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. <p>To propose innovative solutions for secure and better public communication and networks, post event analysis, data/information exchange.</p>



**Data protection
and
cybersecurity/
cybercrime**

3.4 Detection

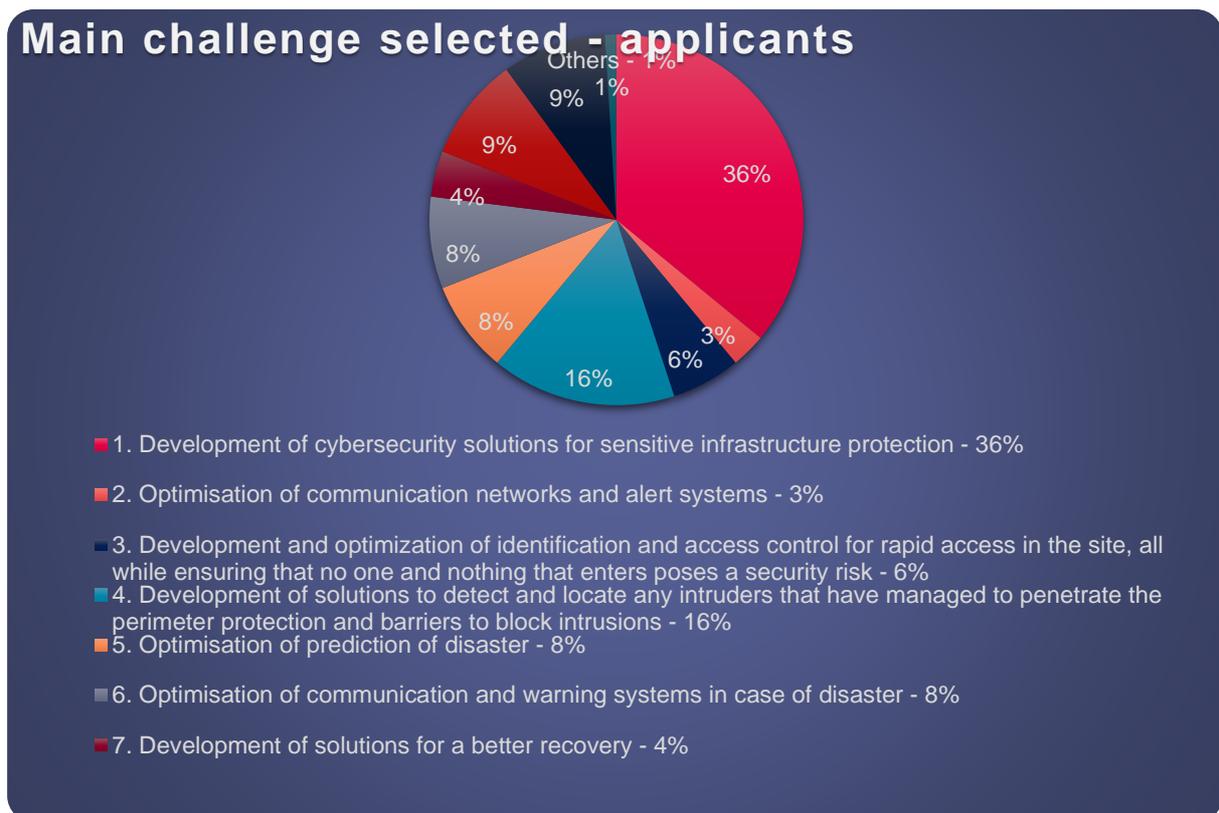
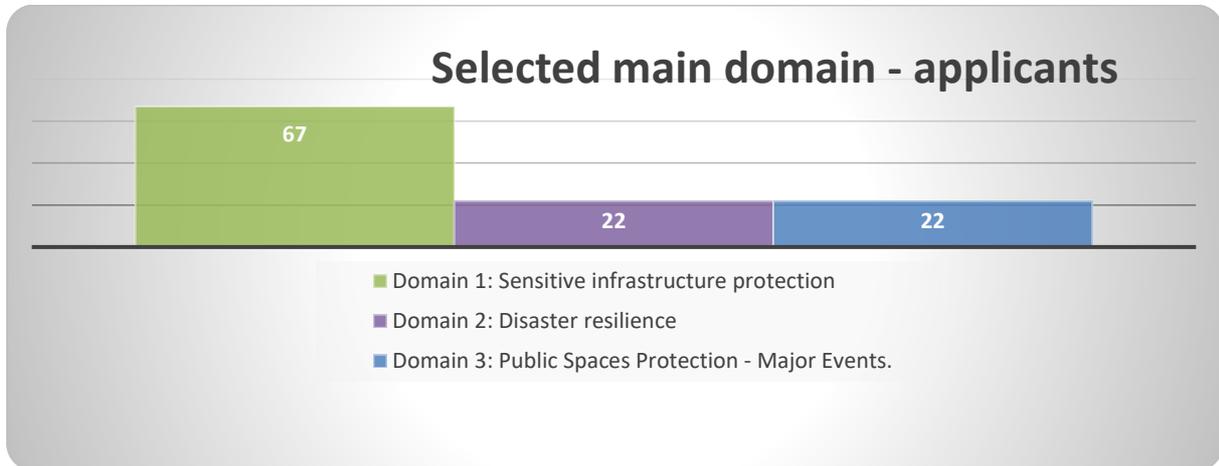
To propose innovation solutions such as:

- 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

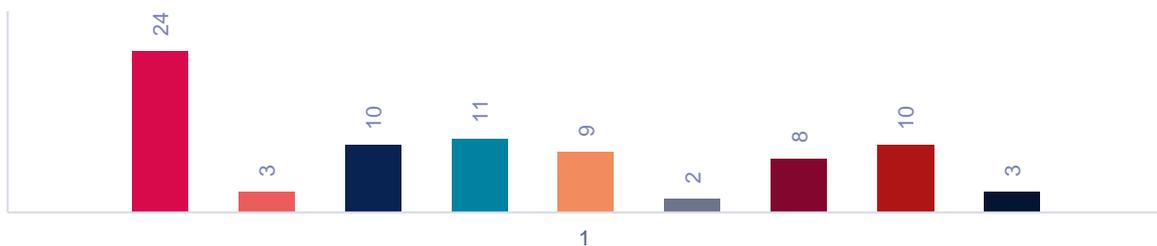
Annex 1 - Statistics from Open Call 1





OTHER CHALLENGES SELECTED (APPLICANTS)

- 1. Development of cybersecurity solutions for sensitive infrastructure protection - 24
- 2. Optimisation of communication networks and alert systems - 3
- 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 - 10
- 4. Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions - 11
- 5. Optimisation of prediction of disaster - 9
- 6. Optimisation of communication and warning systems in case of disaster - 2



Selected Domains

Domain #1 Sensitive infrastructure protection

Domain #2 Disaster resilience

Domain #3 Public spaces protection – major events



Domain 1 – Sensitive infrastructure protection – gathered the most project proposals, with 67 applications on the 111 submitted, against 22 for Domain 2 – Disaster resilience – as well as for Domain 3 – Public spaces protection & Major events.

Most of the submitted projects are tackling the development of **cybersecurity solutions for the protection of sensitive infrastructures** and challenges of **detection and location of intruders in protected perimeters (Domain 1)**.

Proposals tackling the **optimisation of disasters prediction** and of **warning systems** were also numerous (Domain 2), as well as solutions **gathering and managing real time information**, and for the **quick analysis of crucial information** (Domain 3).



Annex 2 – Agenda workshops with Advisory Board members

SecurIT Challenges_Open Call 2

November 17th 2022 2-3 pm
November 22nd 2022 11-12 am
Online via Teams

Agenda breakdown

- Advisory Board introduction
- SecurIT – in brief
- Results from Open Call 1
- Visions for Open Call 2

Context

EU-project SecurIT aims at providing funding to consortium of EU SMEs offering **innovative security solutions** selected through two Open Calls.

In Open Call 1 in 2022, SecurIT funded 21 innovative solutions (14 demonstrators and 7 prototypes) with grants up to 88K€, that addressed the challenges on protection of **critical infrastructure, disaster resilience, and the protection of public space**, with the objective of contributing to safer and more resilient cities and territories: <https://securit-project.eu/1st-batch-of-securit-funded-projects/>. These projects entered the 12-month support program provided by SecurIT consortium.

SecurIT aims at **sourcing innovative solutions with a market pull orientation**. In this regard, we would be happy to count with your support on the reshape of the challenges that will be the core of the next Open Call. (Open call 1 challenges are in the table in pages 3 to 6)

What are your main gaps in terms of security?
What are your main needs in terms of security? /needs perceived from the security market?
What type of digital applications would you expect? (focusing on digital innovative solutions)
*How could the **challenges of the 1st open call** could be rephrased or amended?*
What other challenges could be added/ what other need have you identified?
Would you provide any test beds?
How you find these challenges relevant to security market (with a score for each challenge)?

Thank you for your support!