SECURIT

TOWARDS RESILIENT SMART CITIES & TERRITORIES

Guide for Applicants (GfA)

SecurIT 2nd Open Call for Applicants

Open date for proposals: 10 January 2023 at 13:00 CET (Brussels Time).

Deadline: 14 March 2023 at 17:00 CET (Brussels Time).

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

Table of content

1. Basic Info about SecurIT	**3**
2. What do we offer?	**3**
3. Eligibility Criteria	**4**
3.1 Who are we looking for?	**4**
3.2 What types of activities can be funded?	**5**
3.3 Ideal Project	**8**
3.4 How to apply	**9**
4. How will we evaluate your proposal?	**12**
4.1 Step 1: First Eligibility Check	**12**
4.2 Step 2: Pre-scoring	**13**
4.3 Step 3: External Evaluation	**14**
4.4 Consensus Meeting	**16**
4.5 Jury Day	**17**
4.6. Ethical Review	**17**
4.6 What's next? Sub Grant Agreement and Signature	**18**
5. Our Support Programme and Payment Arrangements	**18**
6. Contact us	**21**
7. Last but not least - final provisions	**22**
8. Extra hints before you submitting your proposal	**23**
Annex 1: SecurIT Challenges and areas of needs	**25**

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

1. Basic Info about SecurIT

SecurIT (https://securit-project.eu/) is an EU-funded project aiming to create a new global competitive security industry (product & service) by supporting a better integration of innovative security systems.
This will be achieved by:

- supporting the **development and integration of innovative security solutions** in a new industrial value chain (and services);
- co-financing and supporting the **development of collaborative projects** allowing the **prototyping and experimentation** of technological solutions in the field of security, taking into account the ethical, legal and societal challenges of this sector;
- promoting **cross-border cooperation** between SMEs and other innovation actors in this sector.

SecurIT aims to focus on **increasing the security of current applications, services and infrastructures** by **integrating state-of-the-art security solutions or processes**, supporting the creation of lead markets & market incentives in Europe, following an end-user driven approach.

The SecurIT project is coordinated by **SAFE CLUSTER** and involves eight partners from six EU countries.
The total SecurIT budget is € 4 958 031,25, out of which € 3.521.000 will be distributed to SMEs as financial support. The budget of 2nd SecurIT Open Call is € 1.750.000.

This document summarizes the main points of the 2nd Open Call for Applicants, under the SecurIT project, which will be **open from 10 January 2023 at 13:00 CET (Brussels Time) with a deadline on 14 March 2023 at 17:00 CET (Brussels Time).**

Where can you find key information regarding this Open Call?

- SecurIT website for general information about the program,
- If you have any technical problems or doubt when filling in the online Application Form at FundingBox, tell us directly at info.securit@fundingbox.com
- Application website https://securit2.fundingbox.com/

2. What do we offer?

Under 2nd Open Call SecurIT will select up to **21 projects aiming to develop new prototypes or demonstrators in the security and cybersecurity domain** with financial and mentoring support from the SecurIT consortium**.** Projects must be submitted by consortia of at least 2 SMEs (at least one SME

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

should be a technology provider) and must address one of the challenges described in Section 3.2.

SecurIT is offering **2 types of Instruments**:

- **Prototyping Instrument:** for the development of prototyping solutions for end-users or/and cybersecurity integrators at the MVP (Minimum Viable Product) stage at least. Under this instrument SecurIT will support you in translating your feasibility plan into a prototype,

- **Demonstration Instrument:** for new application solutions in cybersecurity and digital applications applying to security solutions ready to piloting at a large scale in the short-term. Under this instrument, SecurIT will support the piloting and validation of your solution in the relevant environment.

Selected consortia will enter up to 12-months Support Programme and receive:

- **Up to € 74.000** per 1 prototype project (maximum € 60.000 per SME),
- **Up to € 88.000** per 1 demonstration project (maximum € 60.000 per SME).

You (SME/consortium) can apply only to one of the instruments offered by SecurIT, based on the maturity of your solution (TRL level).

The final number of projects selected per each instrument will depend on the overall quality of the proposals.

Apply here: https://securit.fundingbox.com/apply

3. Eligibility Criteria

We will check the eligibility of all proposals submitted before the deadline via our online application form (https://securit2.fundingbox.com/). All the eligibility criteria are listed in this Section of this Guide for Applicants.
The projects that do not comply with those criteria will be excluded and marked as ineligible. We will check the eligibility criteria based on the information provided in your application during the whole evaluation process.

3.1 Who are we looking for?

We are looking for consortia of at least 2 SMEs[1] [registered legal person] established in:

[1] An **SME** will be considered as such if it complies with the European Commission's Recommendation 2003/361/EC. As a summary, the criteria defining an SME are:

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

- The Member States of the European Union and its Overseas Countries and Territories (OCT) or
- Associated Countries to H2020
- The United Kingdom

At least one SME in the consortium should be a **technology/IT solution provider**.

All SMEs applying as one consortium should be autonomous to one another (without capital or personal links).

The SecurIT partners or their affiliates or employees, are NOT considered as eligible applicants and can NOT apply for funding.

An SME already supported under SecurIT 1st Open Call cannot receive funding under 2nd Open Call, thus it is not eligible to participate in the SecurIT 2nd Open Call.

If at least one SME in a consortium was already supported under the SecurIT 1st Open Call, it disqualifies the consortium from participating and receiving funding in the 2nd Open Call.

The exception to the above is an SME that received only the mini-grant of €1k to participate in Jury Day in the SecurIT 1st Open Call. Thus, SMEs which received the Jury Day mini-grant in SecurIT 1st Open Call but were not selected for the entire SecurIT 1st Open Call Support Programme, can participate in the 2nd Open Call. More information can be found in the Frequently Asked Questions document.

3.2 What types of activities can be funded?

SecurIT is looking for projects that address the development and implementation of technology and systems related to the specific challenges (listed below) defined in collaboration with end-users and integrators. The development of the solutions within the project should have a clear focus on **civil applications** and is limited to them. SecurIT **will not accept** proposals with a military focus.

Depending on the maturity of your solution, you can choose between 2 different types of Instruments offered by SecurIT:

- if you are interested in **building the prototype/MVP** of the solution: apply to **Prototyping Instrument,**
- if you already have a prototype/MVP and would like to **pilot** them: apply to **Demonstration Instrument.**

What are the challenges to be addressed by SMEs?

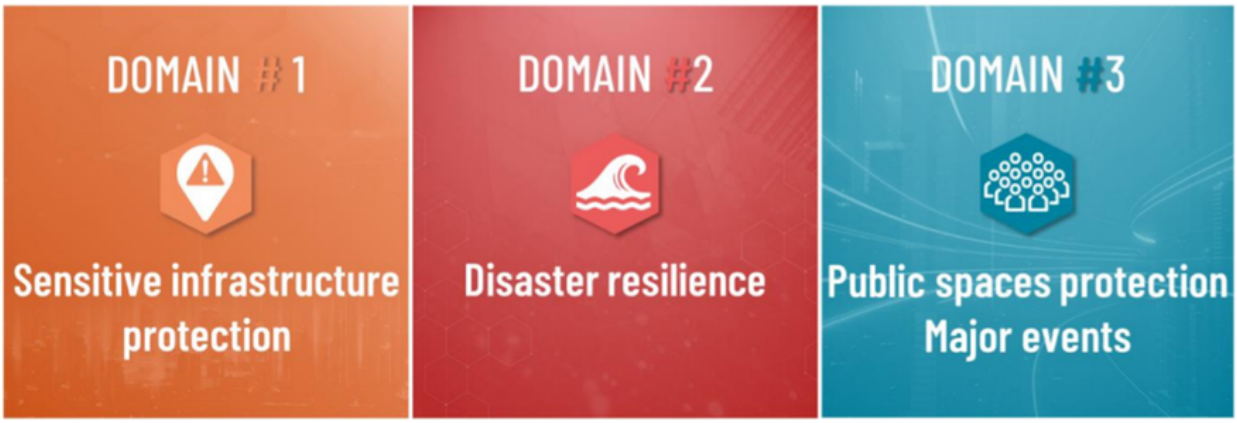
- Headcount in Annual Work Unit (AWU) less than 250;
- Annual turnover less or equal to €50 million OR annual balance sheet total less or equal to €43 million.

Note that the figures of partners and linked enterprises should also be considered as stated in the SME user guide. For detailed information check EU recommendation:
https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

The challenges 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.

 CHALLENGES and potential areas of needs:

1.1 Development of cybersecurity solutions for sensitive infrastructure protection

1.2 Optimisation of communication networks 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

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

1.4 Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions

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.

CHALLENGES and potential areas of needs:

2.1 Optimisation of prediction of disaster

2.2 Optimisation of communication and warning systems in case of disaster

2.3 Development of solutions for a better recovery

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.).

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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 consider the legal constraints of personal data protection.

CHALLENGES and potential areas of needs:

3.1 Gather and manage real time information

3.2 Analyse and extract pertinent and potentially crucial information as quickly as possible

3.3 Communication networks and post -event analysis

3.4 Detection

The challenges listed above can be broadly interpreted/are non-exhaustive. Detailed descriptions of each challenge are included in the Annex 1.

3.3 Ideal Project

The ideal project is a use case of prototyping or demonstration of the security solution that addresses at least one of the challenges in the following domains:

- cybersecurity,
- digital applications applying to security solutions.

The demonstrators that will be implemented should be tested in operational environments. The demonstrations can be considered very near to market exploitation.

For Prototyping Instrument it is expected that the initial TRL (**Technology Readiness Level**[2]) is a minimum of 5 while the TRL reached by the end of the project will be a minimum TRL 6/7.
For Demonstration Instrument it is expected that the initial TRL is minimum 5 while the TRL at the end of the project is minimum TRL 8/9.

The ideal applicant is a consortium composed of 2 (two) SMEs from different eligible countries, however, we also accept consortia of SMEs registered in the same country. Please be aware that international consortia will get a bonus in the scoring process (1 extra point) and will be granted the maximum score in criterion “Consortium composition at the geographical level” during the pre-scoring step (see section 4.2).

[2] TRL, Technology Readiness Level. Technology Readiness Levels (TRLs) are indicators of the maturity level of particular technologies. This measurement system provides a common understanding of technology status and addresses the entire innovation chain. There are nine technology readiness levels; TRL 1 being the lowest and TRL 9 the highest. In our project, we refer to Annex G of the General Annexes to the Work Programme 2016/17 for a full description of TRLs.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

At least one SME must be a **technology/IT solution provider**. It's also recommended that at least one consortium member has **experience in the domain or sector** that the consortium is applying to.
We also encourage you to provide the Letter(s) of Intent from the potential end-users to strengthen your application. The letter(s) can be uploaded in your application form.

Ideal Project Examples

Example 1 (challenge to solve: identification and access control of domain):
A consortium of 2 SMEs from Austria and Spain proposes a digital system that permits access control with an intelligent badge system for authorized persons in charge of protection of critical or sensitive venues. The consortium applies to the demonstrator instrument, in order to test in a near-real environment their solution, addressing challenge 3 - identification and access control. They are assisted for this by the safety director of an industrial SEVESO site that will provide the field for experimentation and testing of the solution.

Example 2 (challenge to solve: Prior to crisis – prediction/Risk knowledge and evaluation)
1 SME from the Netherlands and 1 SME from Bulgaria gather into a consortium to develop tools to map the vulnerability of the territory, i.e. the conjunction between natural disaster potentiality and human capability to face the event. The product they develop here goes beyond the state of the art, uses AI and integrates aerial imagery and past event consequences analysis or a societal filtered analysis.

Example 3 (challenge to solve: Detection of alert)
An SME provider of AI solution from Italy and a small company from Sweden, specialized in analysing human behaviour are developing a prototype of an intelligent flow management system, that could detect suspicious and abnormal behaviour. Their innovative solution is selected in SecurIT open call to participate in the support program and receive an FSTP grant of € 74.000 for delivering the MVP. AI solution provider will receive € 50.000 and its consortium partner from Sweden will get € 24.000 during the 12-month program.

For more inspiration, please check the 21 projects selected for funding under the SecurIT 1st Open Call here: https://securit-project.eu/funded-projects/.

3.4 How to apply

Applying to an open call takes time and dedication and we are grateful you take up the challenge of applying to the SecurIT Open Call. Because we care, we simplified the process as much as possible and

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

we would like to make sure you understand what are some of the eligibility requirements with which you have to comply.

- **Have a European dimension:** your proposal should have a clear European dimension meaning that the challenge is to fully exploit the potential of the European economy and society. Building notably on Europe's Scientific and Technology strengths in the field. The supported activities should reinforce industrial competitiveness across security solutions. The ambition is to bring development and integration of innovative security solutions in a new industrial value chain (and services).

- **Submit on time:** Make sure you submit your proposal through the online form dedicated to the right type of Instrument: https://securit2.fundingbox.com/ before the **deadline** (Deadline: 14 March 2023, 17:00 CET). If you submit the form correctly, the system will send you a confirmation of your submission. Get in touch with us if it is not the case. It is important for you to know that we will not be evaluating any proposal sent after the deadline and submitted outside the dedicated form.

- **Be exhaustive:** Have you answered all the sections of the form? It won't be possible to add any information after the deadline. However, you will be able to modify the form as much as you like even *after* the proposal is submitted, **as long as it is done before the deadline**.

- **Less is more:** You can apply to only one type of Instrument and submit **only 1 proposal** (as a single SME and as a consortium). If more than one proposal is submitted by you, your consortium or your consortium partner (taking into account all applications submitted in both Instruments), only the last edited proposal which has been submitted will be evaluated. Other proposals will not be eligible. So no point in multiplying your chances this way, it is better to submit only one proposal and focus on it.

- If your SME has already **received funding** from SecurIT under the 1st Open Call, you are not eligible to be funded in this Open Call (this will not apply to SME(s) that received only a Jury Day mini-grant (1K€)in the 1st Open Call).

- **Only civil applications will be accepted.** Your project must focus on the development of civil applications and must be limited to them. SecurIT will not accept proposals with a military focus.

- Your proposal must be written in **English** in all mandatory parts in order to be eligible. Only parts written in English will be evaluated.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

- **Every question deserves your attention:** all mandatory sections of your proposal - generally marked with an asterisk - must be filled in. Make sure that the data provided is true and complete. This is crucial for us to properly assess your proposal. Conversely, any additional material that is not specifically requested in the online application form will not be considered for the evaluation so no point overdoing it.

- **Conflicts of interest:** we will take into consideration the existence of the potential **conflict of interest** between you and one or more SecurIT Consortium partners. Indeed, consortium partners, their affiliated entities, employees and permanent collaborators cannot take part in the SecurIT programme. Although, being a member of an association participating in the execution of the SecurIT programme does not mean that you are not allowed to submit an application. All cases of potential conflict of interest will be assessed case by case.

- **Healthy finances and a clean sheet are a must:** we won't accept entities that are under liquidation or enterprises in difficulty according to the Commission Regulation No 651/2014, art. 2.18. Neither will we accept proposals from entities that are excluded from the possibility of obtaining EU funding under the provisions of both national and EU law, or by a decision of both national or EU authorities. Before applying you need to check your financial situation by filling out this questionnaire: https://ec.europa.eu/research/participants/lfv/lfvSimulation.do. It is mandatory to attach the results to your application form (more information can be found in the Frequently Asked Questions document).

- **It is *your* proposal:** your project should be based on your original work. If not, please make sure your right to use the IPR is 100% certain. Going forward, any foreseen developments must be free from third-party rights and if not, these third-party rights must be clearly stated.

SecurIT planned a certain number of online webinars about this open call. They will be announced at the SecurIT website. You are also welcome to reach out to the project partners for more information.

Eligibility criteria checkpoint:

- You are applying as a consortium of at least 2 SMEs from eligible countries, at least 1 of consortium member is IT/technology provider,
- You are addressing at least one of the SecurIT challenges, and choosing one of two instruments (Prototyping or Demonstration Instrument) at appropriate TRL level,
- You are submitting only 1 proposal (as single SME and as consortium), which has a clear European dimension, focus on civil applications and certain IPR rights,

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

- You haven't received financial support from SecurIT under 1st Open Call (this will not apply to SME that received only a Jury Day mini-grant (1K€) in 1st Open Call).
- Your proposal is in English and all mandatory sections are filled in,
- You are using the online application form and submit your application before the deadline,
- You and your consortium member(s) are not under liquidation or in financial difficulty,
- You and your consortium member(s) are not excluded from the possibility of obtaining EU funding,
- You and your consortium member(s) do not have a conflict of interest with any of SecurIT Consortium partners.

4. How will we evaluate your proposal?

Our evaluation process is transparent, fair and equal to all our participants.

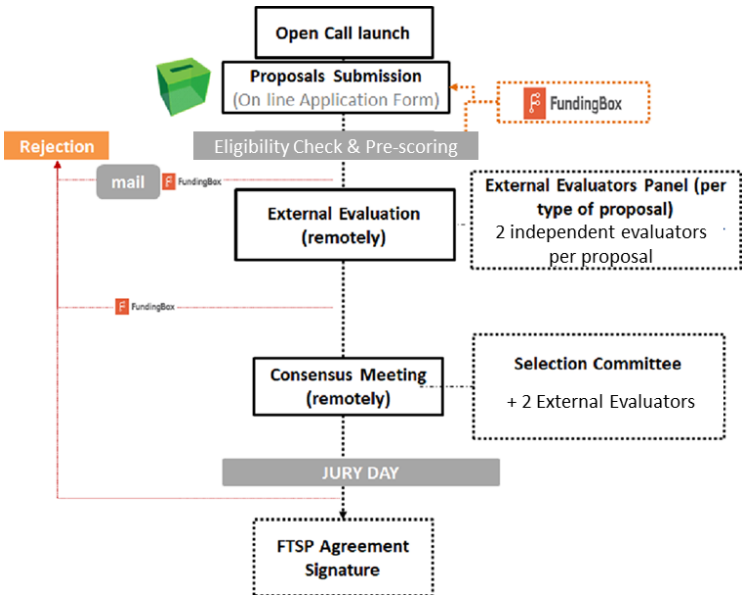


Figure 1. Selection Procedure

We will be evaluating your project in 5 phases. The evaluation process of applications submitted to each Instrument will be done separately (it means that your application will be competing only with applications submitted to the same Instrument).

We expect a high number of applications so if you want to stand out, quality is the way to go. What does it mean? In short, provide as many details as possible while being extremely clear and structured.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

This will help us to identify properly the key points of your application and see how it fits within the overall SecurIT scope.

4.1 Step 1: First Eligibility Check

The first evaluation step is about verifying some basic requirements based on the statements from your proposal. Your proposal will be admissible for the next phase if it:

- Is **complete, readable and in English** in all mandatory sections.
- Has been submitted via the online form: https://securit2.fundingbox.com/ within the **deadline** (14 March 2023, 17:00 CET). You won't be multiplying your chances by applying several times, it is only the last application that you edited (after submission) that we will be evaluating in case there is more than one application that you are part of.
- Has not been submitted by SME already funded under the SecurIT 1st Open Call.
- Includes the properly filled declaration of honour. Read carefully the **Declaration of Honour** template included in the application form here, as we will check the related submitted statements. You will not be able to change them after the deadline.

Moreover, a first check regarding the eligibility of the participants specified in section 3 will be carried out.

Following this first step, we will move on to the pre-scoring phase described below.

4.2 Step 2: Pre-scoring

If we receive more than 80 eligible proposals (in total for both Instruments), a pre-scoring system may be included to help us make a pre-selection.

What does this mean? The FundingBox Open Call Management System (FundingBox Enterprise) will automatically assign a score to the eligible proposals according to the following criteria:

- Security by design principles followed by applicant (consortium as a whole) - 10% weight / up to 10 points
- Background experience of consortium - 5% weight / up to 5 points
- Proven experience in the target market - 15% weight / up to 15 points
- Scalability of the solution (number of potential individual end users) - 10% weight / up to 10 points

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

- Target market for your solution in 2 years from going to the market (number of countries reached) - 10% weight / up to 10 points
- End users involvement (interaction with end users) - 10% weight / up to 10 points
- Status at technological level (innovative maturity of the technological solutions) - 10% weight / up to 10 points
- Consortium composition at the geographical level - 15% weight / up to 15 points
- Partnership experience - 10% weight / up to 10 points
- Previous projects funded by EU - 5% weight / up to 5 points

As an applicant, you should:

- select the option that best describes the characteristics of your project in relation to each criterion,
- confirm that no false declarations are made.

In total, your project can receive up to **100 points**. If your score places you in the best-marked applications (up to **80 top-ranked** applications will be selected in total), well done! As a next step, we will forward your application to an external pool of experts for a more detailed and qualitative evaluation and scoring.

We will inform you about the results of the eligibility check and the pre-scoring phase soon after these steps have been completed, generally in 2 weeks that follow the deadline to submit the application.

4.3 Step 3: External Evaluation

You have reached the external evaluation phase: bravo! And if not, be persistent: there may be other open calls for this project and other funding opportunities may suit - even better - your proposal.

For those who have been selected: from now on, each project will be evaluated by **2 external and independent** evaluators appointed according to the specific characteristics of your project.
These are the criteria they will consider to complete the evaluation:

(1). EXCELLENCE will evaluate:

- **Ambition.** The applicants have to demonstrate to what extent that proposed project is beyond the State of the Art and describe the innovative approach behind it (e.g. ground-breaking objectives, novel concepts and approaches, new products, services or business and organisational models).
- **Innovation:** applicants should provide information about the level of innovation within their market and about the degree of differentiation that this project will bring.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

(2). IMPACT will analyse:

- **Market opportunity:** The applicants have to demonstrate a clear idea of what they want to do and whether the new/improved product/service has market potential, e.g. because it solves a problem for a specific target customer.
- **Competition:** The applicants have to provide information about the degree of competition for their particular product/service and if the idea is disruptive and breaks the market. i.e. the products/services to be brought to market can be clearly differentiated from the competition.
- **Commercial Strategy and Scalability:** The applicants have to demonstrate the level of scalability of the new/improved product/service, meaning that it doesn't address the solution of a specific problem but it's able to be commercialised to solve a structural problem in a specific sector/process/etc.

(3). IMPLEMENTATION will consider:

- **Team:** The applicants have to demonstrate their management and leadership qualities, their ability to take a concept from ideas to market, their capacity to carry through their ideas and understand the dynamics of the market they are trying to tap into as well as their technical capabilities to reach the defined objectives. The team should be a balanced and cross-functional team, with a strong background and skill base.
- **Resources.** Demonstrate the quality and effectiveness of the resources assigned in order to get the objectives/deliverables proposed.
- **Risk management**: the applicants have to present the risk assessment and propose measures to overcome them, especially the applicant should provide information about the legal constraints related to the project execution.

Transversal criteria such as 'Environment and low carbon economy contribution', 'Equal Opportunities including Gender Balance' and 'Social Impact' will be also considered by evaluators when scoring the proposals.

The evaluators will score each criterion on a scale from 0 to 5:

0 = The proposal fails to address the criterion or it cannot be assessed due to missing or incomplete information.

1 = Poor – The criterion is inadequately addressed or there are serious inherent weaknesses.

2 = Fair – The proposal broadly addresses the criterion, but there are significant weaknesses.

3 = Good – The proposal addresses the criterion well but there are a certain number of shortcomings.

4 = Very good – There is a small number of shortcomings but overall, the proposal addresses the criterion very well.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

5 = Excellent – The proposal successfully addresses all relevant aspects of the criterion with no or minor shortcomings.

Each evaluator will produce an **Individual Evaluation Report.** The final scores will be calculated as an average of the individual assessments provided by the Evaluators.

Each criterion will be scored out of 5 points. The threshold for individual criteria will be 3 points. The overall threshold, applying to the sum of the three individual scores, will be 10 points.
In case the scores provided by evaluators differ by 3 points or more in at least 2 of the criteria, this difference will be solved by involving the third evaluator in the process.
In the case of ties, the following criteria will be used to rank the projects, in order:

- Transversal Criteria,
- Impact score,
- Implementation score,
- Excellence score.

All proposals obtaining a score above the threshold will move on to the next stage.

In addition, applications submitted by SME **applicants registered in 2 different eligible countries will be given 1 extra point** to the overall score.

After the external evaluation process 2 types of 'Ranking Lists' will be defined:
- the ‘General Ranking List’ where all the applications will be ranked according to their scores,
- the 'Ranking List of Projects per Instrument' for each type of funding instrument (2 lists in total).

Do note that the evaluation phase takes time as it implies a more personal, qualitative and thus non-automated approach.

4.4 Consensus Meeting

Following the external evaluation, a ‘Selection Committee’ formed by selected consortium partners and, at least, two external experts, selected from a pool of experts that evaluated individually the proposals, will decide by consensus (minimum ⅔ of the votes), and based on the Ranking Lists per Instrument gotten as a result of the External Evaluation, the ‘List of finalists’ per each Instrument **(up to 40 projects in total)** to pass to the next phase.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

Although the goal of SecurIT is to select for the Jury Day of the 2nd Open Call indicatively 13 projects per Prototyping Instrument and 27 projects per Demonstration Instrument, the exact number of proposals selected for Jury Day per each Instrument might be different and will be decided based on the overall quality of the proposals included on each ranking list.

Bear in mind that even if it is normally the best-marked proposals that are selected for funding, the Selection Committee may have fair reasons for objecting to the selection of a specific candidate. These reasons can relate to:

- The alignment with SecurIT goals and scope.
- The ability to achieve the strongest possible impact.
- The low level of innovation.
- The existence of significant ethical concerns.
- The existence of a potential conflict of interest[3].

In case a top-ranked application is rejected, we will consider selecting the next best-ranked proposal.

4.5 Jury Day

If your proposal has been selected following the Consensus Meeting, well done!

You will be invited to an online Jury Day (in mid-May 2023), participation of at least one consortium member will be mandatory. It's recommended that both consortium members are present at the Jury Day. During the Jury Day, you will have the opportunity to pitch your project in front of the SecurIT Jury composed of the Selection Committee Members. The Selection Committee could be supported by security experts and ethical expert(s).
Before Jury Day your consortium will be requested to submit an ethical self-assessment form and send the pitch presentation.

After the Jury Day, the SecurIT Selection Committee will undertake the **final evaluation** taking into account the following criteria:

- Quality of the team
- Innovative step in solving the challenge
- Feasibility of the project implementation
- Transversal criteria (final criteria in case of ties).

[3] Please note that this is not a closed list of reasons for objecting

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

The Selection Committee will decide by majority votes (⅔ from all members) on the "**Provisional Lists of recipients per Instrument"** as well as the '**Reserve Lists per Instrument'**.
Up to 21 proposals in total will be selected. The goal is to select 7 projects for Prototyping Instrument and 14 projects for Demonstration Instrument, however, the exact number of proposals approved per each Instrument might be different, depending on the overall quality of all proposals invited to the Jury Day. After the Jury Day, we will communicate the results.

4.6. Ethical Review

All the selected projects shall comply with ethical principles and relevant national, EU and international legislation. To ensure that each project is compliant with it, all selected projects will undergo an initial Ethics Review before signing the Sub Grant Agreement. The ethical implications of projects are assessed at the proposal evaluation stage, particularly with regard to:

- The use of data that is potentially traceable to a person,
- The use of, or interaction with, vulnerable individuals and groups,
- Potential physical or mental harm to operators, users and / or third parties,
- The development of systems liable to maintain or amplify societal disadvantage or discrimination based on race, gender, sexuality, social class or economic standing.

Where potential issues are identified, the applicants will be required to detail any mitigating actions which will be included in the 'Ethics Summary Report', and an Ethical Committee will be established to supervise and monitor the ethical concerns during the bottom-up project's implementation.

4.6 What's next? Sub Grant Agreement and Signature

You made it! You are part of the **final 21 selected** for the SecurIT open call. It has been a long journey. Or has it actually just started?

In any case, before you get started with SecurIT programme, you need to sign the Sub Grant Agreement with the SecurIT Consortium.

Before signing the Sub Grant Agreement, you should provide documents regarding your formal and financial status (please check the list of documents in the Frequently Asked Questions Document). The SecurIT Consortium will proceed to a **verification of these documents** to make sure you are eligible.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

Be extremely vigilant with respect to:

1. **The nature of the documents** we request. If the documents you provide us with do not prove your eligibility, the adventure will end here.

2. **The deadlines** that we will give you to hand us these documents. If you do not deliver the requested documents on time, without a clear and reasonable justification, we will have to exclude you from the further formal assessment. Another applicant from the Reserve list will then replace you.

5. Our Support Programme and Payment Arrangements

Once your eligibility has been confirmed following the formal check and the Sub Grant Agreement signed, you would be an official beneficiary of the SecurIT Programme. It is now that the adventure begins and it is now high time to understand how the funding is going to be distributed.

Support Programme

The Support Programme can last up to 12 months, but no longer than until 30 June 2024. During this period you will be supported by the Experts from Top Security Clusters for bringing new technologies for security applications. We will support you in the prototype development or demonstrations (depending on the Instrument you selected) in the real condition in security domains.
At the beginning of the Support Programme, you will be invited to participate in a 2-days physical Kick-off Meeting hosted by one of the SecurIT partners to learn more about the Programme, meet other beneficiaries and get matched with your Follow-Up Manager from one of the Clusters, who will guide you through the whole process. Attending the Kick-off Meeting by at least one representative of your consortium is mandatory and the grant shall cover your travel costs.

As a beneficiary, you will receive a **fixed lump sum of**:

- **Up to €74.000 per project** (with a maximum up to €60.000 per SME under Prototyping Instrument),
- **Up to €88.000 per project** (with a maximum up to €60.000 per SME under Demonstration Instrument).

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

It's up to selected SMEs to agree on how the fixed lump sum will be distributed among SMEs under the funded project (but no more than 60k per entity). At the same time please keep in mind that you should reserve part of the grant to cover the costs of your travel to the Kick-off Meeting.
Please note that any SME cannot receive more than 60k€ in total from the SecurIT project. In case you already got a mini-grant during the 1st Open Call, this amount will be deducted from your total grant in case it exceeds 60k€ (please check the example in the Frequently Asked Questions document).

The lump sum is a simplified method of settling expenses in projects financed with Horizon 2020 funds. It means that you are not required to present accounting documents to prove the investment-related costs incurred (e.g. invoices). However, you are obliged to demonstrate that the implementation of the project is in line with the milestones set for it.
It is necessary to provide an explanation in the application on how the lump sum will be used and distributed to reach the defined objectives but detailed reporting of the spending, cost statements and time sheets are not requested after the end of the project. Since the granting of a lump-sum doesn't foresee the delivering of a cost statement, the use of the project budget will be controlled only considering the technical advancements by the SecurIT experts.
The application form must include information how the grant will be distributed between consortium members. When preparing your budget split, please remember that it is strongly recommended that subcontracting is limited to a maximum 30% of the lump sum.

The milestones (deliverables, KPIs and ethical recommendations) will be defined and calendarised in the '**Follow Up Plan**' elaborated at the beginning of the programme with the support of the Follow *up Manager* assigned to guide through the whole Support Programme.

In short, we will carefully assess your progress and the quality of your work during Interim Reviews but we will not review your accountancy.

Bear in mind that the lump sum does not release you from the obligation to collect documentation to confirm the costs under fiscal regulation.

The *Follow Up Plan* will become an Annex to Sub Grant Agreement and establishes the budget planned for the execution of your projects, KPIs and Deliverables that will be taken into account when evaluating your project's performance during Interim Reviews at M6 (Interim Report) and M12 (Final Report).

The payments will be done once the deliverables are approved by the 'Mentoring Committee' and validated by the 'Selection Committee'.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

The corresponding evaluation criteria are as follows:

• Deliverables quality (based on the Deliverables established in the *Follow Up Plan*).

• Technical performance indicators (based on the KPIs established in the *Follow Up Plan*).

• Deadline Compliance.

Each 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:

• Deliverable quality (45%).

• Technical performance indicators (45%).

• Deadline Compliance (10%).

According to this final score:

• Beneficiaries over the threshold (7 points) will successfully receive the next payment and continue in the program.

• Beneficiaries under the threshold will be reviewed by the 'Selection Committee' who will take the final decision taking into account all possible objective reasons for underperformance (i.e. external factors which might have influenced the beneficiaries' performance).

Those not passing this examination will not receive the next payment and will be invited to leave the Program.

The beneficiaries will receive the funding as follows:

- 1st instalment: up to 20% of maximum grant amount (at M1 after validation of the *Follow Up Plan*),
- 2nd instalment: up to 80% of maximum grant amount (at the end of the support program, after validation of the MVP or Pilot).

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

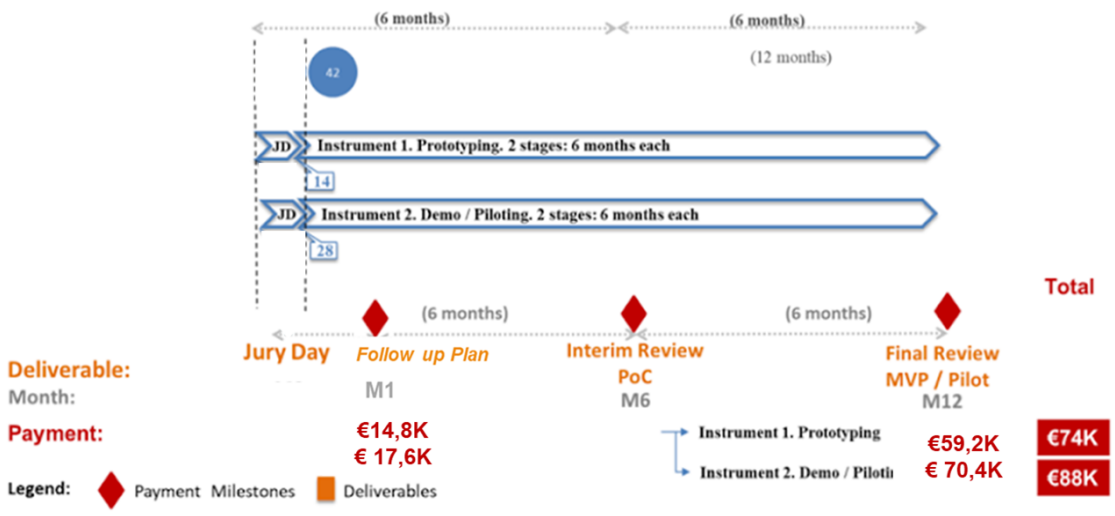


FIGURE 2 SUMMARY OF THE SUPPORT PROGRAM AND MAXIMUM AMOUNTS OF GRANTS PER EACH STAGE

Lastly, for a more detailed payment schedule, you can read our Frequently Asked Questions.

6. Contact us

If you still have any doubts regarding our Open Call process, feel free to get in touch with us and send us an email to the following address: info.securit@fundingbox.com.

If ever you face any technical issues or problems, make sure you include the following information in your message:

- Your username, telephone number and your email address.
- The details of the specific problem (error messages that appeared, bug descriptions such as a dropdown list that isn't working, etc.).
- Screenshots of the problem.

Complaints

First of all, be aware that we won't be reviewing your complaint **if**:

- It is anonymous.
- The information is incomplete.
- It is not related to the results of the evaluation phases. Indeed, most of the evaluation process is run by **independent experts** in the given field. The project consortium does not interfere with their assessment.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

If, after receiving the results of one of the evaluation phases, you consider that a mistake has been made, resulting in the rejection of your application, you have the right to send us a complaint. You can email us in English to: info.securit@fundingbox.com including the following information:

- Your contact details (including email address).
- The subject of the complaint.
- Information and evidence regarding the alleged mistake.

Important note regarding the timeline:

You have **3 calendar days** to submit your complaint starting from the day after the communication was sent. On our side, we will review them within no more than **7 calendar days** from its reception. If we need more time to assess your complaint, we will inform you by email about the extension.

We will not review anonymous complaints as well as complaints with incomplete information.

Please take into account that the evaluation is run by external experts in the field of security and digital solutions and we do not interfere with their assessment, therefore we will not evaluate complaints related to the results of the evaluation other than related to the mistakes in the evaluation of the eligibility criteria and/or pre-scoring.

7. Last but not least - final provisions

Any matters not covered by this Guide will be governed by Polish law and rules related to the Horizon 2020 programme and European Union grants regulations.

We do our best to keep all the applicant data confidential. However, to avoid any doubts, you are entirely responsible to indicate what information is confidential.

Your IPR will remain your property.

For the selected beneficiaries, the agreement will include the set of obligations towards the European Commission (for example: promoting the project and giving visibility to the EU funding, maintaining confidentiality, understanding potential controls by the EC/ECA and OLAF, providing non-confidential information /summary on the project that receives financial support).

The SecurIT Consortium might cancel the call at any time, change its provisions or extend it. In such a case we will inform all applicants about such change. The signature of the agreement is an initial

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

condition to establish any obligations among applicants and any Consortium partners (with respect to the obligation of confidentiality of the application).

You didn't find what you were looking for? You may want to check our Frequently Asked Questions.

8. Extra hints before you submitting your proposal

A proposal takes time and effort and we know it. Here a few crucial points you should read before hitting the "Submit" button in order to maximise your chances of success:

- Is your project in line with what SecurIT is looking for? Not 100% sure? You can consult this section as well as this one.
- Did you present your project in a way that will convince evaluators? Go back to this section if you have any doubt.
- Is your project fulfilling all the eligibility requirements described in the Guide for Applicants? Check again this section.
- Are you able to cope with our signature agreement process and payment arrangements for the selected proposals? You may want to go over this section.
- Did you check our Sub Grant Agreement Template? Check it here.
- Do you need extra help? Get in touch!

And as a bonus: You can read our R.E.C.I.P.E. for an outstanding European Funding Opportunity application for additional advice. Good luck!

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

Annex 1: SecurIT Challenges and areas of needs

Table with Challenges to be addressed *(with examples)

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #1: sensitive infrastructure protection	**Cybersecurity**	**1.1**	**Development of cybersecurity solutions for sensitive infrastructure protection**	To propose effective cybersecurity solutions and solutions to increase resilience against cyber-attacks: - 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.
	Operations	**1.2**	**Optimisation of communication networks and alert systems**	To optimise 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.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

Identification and access control	**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: - 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	**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: - 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/neutralisation of malicious drone; - Securing physical access routes through digital solutions and development of physical access control solutions.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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**	**2.1**	**Optimisation of prediction of disaster**	To propose innovative solutions and technologies for prevention 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: **Mass communication and warning systems**	**2.2**	**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

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

				To propose innovative solutions and technologies for disaster response to improve forecast / early warning systems, advanced data management, Information update.
	After the crisis:			To propose innovation solutions and technologies for post crisis and disaster 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 rehabilitation, autonomous and decentralised – to ensure the conservation of the security of data in the context of post-disaster.
	Post event analysis and recovery	**2.3**	**Development of solutions for a better recovery**	

	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**	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. To propose warning systems such as innovative tools for public and/or geolocation of public and rescue team.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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

	Analysis	**3.2**	**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, using emerging solutions for integration of information from multiple and non-traditional sources (e.g., social media) into incident command operations.
	Command and control (resource management) and decision-making support	**3.3**	**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 secure and better public communication and networks, post event analysis, data/information exchange.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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	**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.

SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES

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