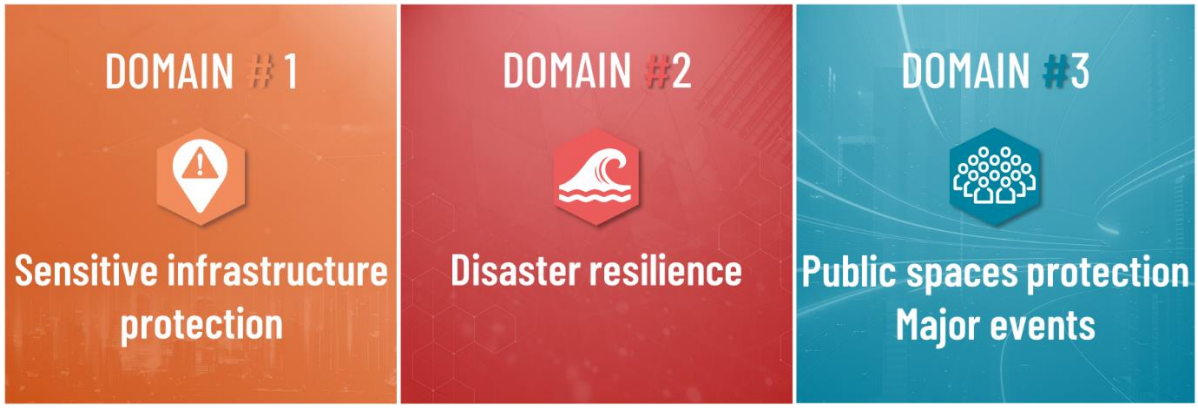
SecurIT – Open Call 1 Challenges

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

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.)

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

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

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

Tables of challenges to be addressed

	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

Tables of challenges to be addressed

	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

Tables of challenges to be addressed

	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

Tables of challenges to be addressed

	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

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