SECURIT

New industrial value chain for **safe, secure and resilient cities & territories**

INNOVATIVE DIGITAL SOLUTIONS FOR SECURITY

Safe & Secured Critical Infrastructures

Disasters Resilience

Public Spaces Protection

Through SMEs support

- Access to market
- 3 521 000€ funding available
- Matchmaking
- Visibility & Support

2 Open Calls/3 funding instruments

Preselection Grant
Up to 1 000€/project
Up to 63 projects - 126 SMEs

Prototyping Voucher
Up to 74 000€/project
Up to 14 projects - 28 SMEs

Demonstration Voucher
Up to 88 000€/project
Up to 28 projects - 56 SMEs

securit-project.eu

SecurITproject SecurIT20 securit-project

SAFE LSEC POLESCS L3CE HSD Systematic CenSec FundingBox

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

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Funded projects

Domain 1 : Sensitive infrastructure protection

AIA GUARD – Demonstration – OC2

AIA GUARD is an end-to-end solution that automatically analyses machine learning workflows and AI systems to detect and protect them from various threats such as data poisoning, model interpretability, data leakage and adversarial machine learning. The solution offers three modules: defence against adversarial attacks, data anonymisation, and improved model interpretability.

AIRA– Demonstration – OC2

AIRA is a software platform that automates evidence-based security risk assessment. It improves the accuracy of investigations, reduces time and increases productivity in proactive risk detection and breach response. This is achieved through features such as automated data collection, analysis and reporting.

ARSP – Demonstration – OC1

ARSP has developed a platform for the unified management of all security robots, which are often used for different security tasks and in different environments. This robot-agnostic platform will enable security companies to manage a diverse fleet of robots across different locations and missions.

BIM2SIM – Prototype – OC1

BIM2SIM is a digital tool for automatically extracting safety data from standard building plans. This technology uses Building Information Modelling (BIM) to capture relevant information from existing file formats. BIM2SIM aims to achieve two key outcomes: to establish guidelines for safety-focused BIM and to develop software for safety applications.

CYBERSEC2SME – Demonstration – OC1

CyberSec2SME provides a continuous cyber risk monitoring software solution for critical infrastructure to assess the cybersecurity posture of their contractors and service providers, enabling them to ensure that their entire supply chain has appropriate and high cyber security standards.

CYBER TRAPPER – Prototype – OC1

CYBER TRAPPER protects Industrial IoT systems from cyberattacks by deploying a network of 'traps'. The traps mimic real systems and collect real-time data on ongoing attacks, creating dynamic threat feeds with malicious compromise indicators. This creates a "crowd immunity" effect that protects all participants once an attack attempt is detected.

DIAC – Demonstration – OC1

DIAC proposes a new approach to the existing access control systems and their limitations (lost cards, data breaches, unauthorised PIN sharing, ...). This system, called the *Disposable Identity Framework* uses temporary, limited-scope digital identities that grant specific access based on context, time, and location.

Domain 1 : Sensitive infrastructure protection

DIGITAL FORENSICS – Demonstration – OC1

The project simplifies digital investigations for governments and businesses. This cloud platform allows users to access their preferred digital forensics, incident response, and eDiscovery tools in a secure environment that can be set up quickly and easily. It automates tasks such as installation, log management, and event monitoring, allowing investigators to focus on core investigative activities.

DISCGRID– Demonstration – OC2

DISCGRID aims to provide security and auditability mechanisms to protect software supply chains by focusing on firmware updates. Two key components are used : secure authentication with tamper-proof claims for firmware & an immutable record of these claims. This allows the integrity, authenticity and provenance of firmware to be verified, ultimately improving the security of the entire supply chain.

EV-SAFE – Demonstration – OC2

EV-SAFE is developing cybersecurity tools to protect Electric Vehicle Charging Station (EVCS) infrastructure from cyberattacks. This initiative aims to address the growing cyber risks faced by EVCS and protect critical parts of the economy and transport. Ultimately, the solution aims to provide a comprehensive security framework for EVCS infrastructure.

FLOWGUARD – Demonstration – OC2

FLOWGUARD is based on a combination of IoT sensors and Graph Neural Networks (GNNs) to protect public water supplies from cyberattacks. By detecting anomalies and vulnerabilities, GNNs can prevent attacks and ensure an efficient response, ultimately safeguarding water infrastructure and setting a new standard for the use of AI in public utility monitoring.

IDEAS – Demonstration – OC1

Industrial networks face a critical security gap as traditional firewalls leave them vulnerable to cyberattacks. IDEAS is a hardware-based solution that enables seamless communication between Information Technology and Operational Technology systems (like SCADA, DCS, RTUs) while providing the highest level of defence against external network threats.

INSIOTA– Prototype – OC1

INSIOTA provides an integrated platform that automates a range of IT security tests on computer systems and networks. The continuous testing helps to ensure that any vulnerabilities are detected and can be mitigated before a real attacker can exploit them. With a focus on IoT systems and the initial testbed set up in the context of a smart city, the systems need to be protected in an environment that is physically open and therefore exposed to multiple possible attacks.

INVISIBUBL – Demonstration – OC2

INVISIBUBL is developing a cloud storage service that eliminates the need to trust a third-party service provider: the Beyond Trust Cloud (BTC). Through user anonymity, cryptographic key fragmentation and integration with existing services, the solution ensures that users remain in control of their data, even when it is stored on servers that may be subject to data access requests.

KALEIDOSCOPE– Prototype – OC1

Kaleidoscope is a new DDoS mitigation architecture that allows for increased granularity and flexibility in different scenarios. The goal is to provide a scalable, high-performance, future-proof architecture that can evolve quickly and adapt to more complex DDoS attacks.

Domain 1 : Sensitive infrastructure protection

OPTIMIZ NETWORK – Demonstration – OC2

OPTIMIZ NETWORK has developed a solution combining IoT sensors and a monitoring platform to secure telecom infrastructures. This system provides real-time information on potential problems such as unauthorised access or environmental hazards, enabling rapid response. In addition, critical access points are secured with electronic locks and secure data exchange is ensured through encryption and centralised management.

RASAD– Demonstration – OC1

RASAD has created a platform for *Rapid and Secure Application Development* that allows any process to be digitised and automated with a guaranteed level of cybersecurity. In addition to authentication & authorisation, the platform is smart enough to decide whether to apply security measures such as encryption of data at rest, auditing of logs, blocking of unauthenticated access, etc.

ROGID – Demonstration – OC1

ROGID has explored the potential of an automated approach to securing sensitive infrastructure. This involved deploying a robotic guard equipped with AI for real-time intruder detection. The robot successfully completed routine patrols, identifying potential security breaches and reporting them promptly to the control room.

RS2DG – Demonstration – OC2

A timely and accurate view of the current and future electrical behaviour of the electricity distribution grid is provided by the digital twin, connected to heterogeneous IoT data sources. The RS2DG project will ensure the robustness of the digital twin of the electricity grid through novel methods based on machine learning, with a focus on missing data collection and identification of anomalies in the values of energy measurements.

SECUVERSE – Prototype – OC1

SECUVERSE is an autonomous inspection and monitoring system, based on an immersive Metaverse and AI platform that includes a digital-twin model of a target facility, a LIDAR scanner, an Automated Guided Vehicle, and AI intruder detection algorithms. The goal is to develop an autonomous robotic agent that can patrol sensitive infrastructure, monitor for possible intruders and anomalies, and represent them in the digital twin model of the facility.

SHOWID– Demonstration – OC1

The project is revolutionising access control by turning smartphones, tablets and desktops into secure, universal corporate badges. This innovative solution eliminates the need for dedicated hardware and provides instant authorisation for visitors to controlled facilities. SHOWID seamlessly integrates features such as ID verification, biometrics, liveness detection, cryptography and electronic ticketing, ensuring the highest levels of security and user convenience.

SMART DIRI – Prototype – OC2

SMART DIRI aims to democratise cybersecurity by providing a user-friendly, AI-powered platform for cyber risk management. The project focuses on developing a machine learning model to streamline the identification, assessment and mitigation of cyber risks. The solution is targeted at mid-sized companies in critical infrastructure sectors, enabling them to strengthen their defences and ensure the continued operation of essential services.

VASCREEN– Prototype OC1

VASCREEN offers a groundbreaking approach to checkpoint security through vapour analysis. This innovative system uses a unique Multidetector Differential Mobility Analyzer (MDMA) to detect potential threats hidden in luggage or merchandise within one minute. Its capabilities are further enhanced by the addition of an automatic air sampling system and powerful Deep Learning recognition algorithms.

Domain 2 : Disaster resilience

AI DISASTER EMERGENCY COM' – Prototype – OC2

This project provides an AI-powered smartphone-based disaster communication system. Through an interface called "Disaster Mode", citizens can report emergencies by providing their location, pictures and a short description. This information is analysed to categorise the urgency and prioritise critical cases. The aim is to reduce call centre overload during emergencies and help first responders identify people in need of immediate assistance.

ERMINE – Prototype – OC2

ERMINE focuses on the development of a disaster prediction system for first responders. This system analyses various data sources such as historical records, satellite images and drone footage to predict events like forest fires and floods. The project aims to create a fast, accurate and resource-efficient programme with global potential. This could revolutionise disaster preparedness by providing early warnings and improving response efforts.

ERRATA – Demonstration – OC2

ERRATA is developing a robotic system specifically designed for hazardous environments. This solution combines aerial robots, autonomous sensors and reliable communications to detect hazards and transmit information to remote teams. Applicable in situations such as collapsed tunnels or disaster zones, ERRATA aims to improve the safety and efficiency of hazardous space exploration and post-disaster management.

HELIA – Demonstration – OC1

HELIA is a high-altitude, AI-powered tethered aerostat designed for real-time hazard detection. This innovative system addresses wildfires as a primary threat, enabling faster response times for firefighters due to its continuous monitoring capabilities. It can simultaneously monitor multiple hazards in different areas, including national parks, urban centres and coastal regions. This enables rapid response to a wider range of potential emergencies.

NOCCRO – Prototype – OC2

Coastal areas face significant threats from erosion and storm surges due to extreme weather events and rising sea levels. Data collection during these events is challenging, but NOCCRO proposes a solution based on the continuous monitoring of existing beach cameras throughout the year. This will allow the extraction of key data on coastal change, providing valuable insights for beach managers and oceanographers to optimize management decisions and improve response to extreme events.

PIM-SAT-M – Demonstration – OC1

PIM-SAT-M addresses a critical challenge: monitoring the stability of structures using satellite data and AI. While sensor technology is expanding, traditional methods such as visual observation remain widespread and often prove inefficient and uneconomical. PIM-SAT-M aims to bridge this gap by piloting an AI-powered, web-based platform that provides a reliable and cost-effective solution for monitoring the stability of structures and their surroundings.

REBRINET – Prototype – OC2

ReBriNet, "Resilience Bridge Net", is a cutting-edge technology designed to support the coordination and decision-making of first and second responders by providing real-time information directly from disaster-affected communities throughout the operation, as they will be able to report critical information through a digital web module that can be integrated into existing web/mobile emergency solutions, enhancing cross-communication capabilities.

RESPO-C – Demonstration – OC2

RESPO-C is developing a mobile application to provide real-time information on active fires, prevention strategies and response measures. Aimed at people who live near or visit forested areas, the app aims to increase citizens' awareness and responsibility in responding to forest fires. This, in turn, could potentially support firefighting efforts by fostering a more proactive and informed local population.

Domain 2 : Disaster resilience

SERVAL MANAGEMENT– Demonstration – OC2

The project aims to improve the response to environmental and technological disasters by developing a secure hardware-software solution with two key functions: the collection and analysis of environmental data, and the provision of operational teams with the necessary tools to optimise their environmental investigation strategies and ensure an efficient and targeted response.

SLOPEGUARD – Demonstration – OC1

Landslides are one of the most common geological hazards, posing a serious threat to human life and huge costs in terms of infrastructure damage. SLOPEGUARD aims to change the way such landslides are monitored, managed and prevented. The solution combines a bespoke monitoring device with advanced machine learning techniques to provide 24/7 early warning of landslides in a fully automated manner.

SYLVIACARE – Prototype – OC2

Know, Preserve and Protect are the keywords of the project, which focuses on environmental monitoring and very early detection of forest fires to develop a disruptive solution using sensors to collect data, send images and locate alarms. This will support and optimise the actions of firefighters.

WUI-SECURE – Prototype – OC2

Wildfire is a growing threat to communities and infrastructure near wildland urban interface (WUI) areas. WUI-SECURE addresses this by creating a comprehensive modelling tool that combines wildfire behaviour, building vulnerability and risk assessments to help identify the most vulnerable areas within a community during a wildfire event. This will enable key decision makers to take preventative action.

Domain 3 : Public spaces protection – major events

AIR-T4S – Demonstration – OC2

AIR-T4S builds on the strengths of the partners' ground expertise to create a unified platform for public space threat detection and response management. This integrated system addresses crowd safety and security through features such as optimised crowd distribution, real-time evacuation planning, clear situational awareness, efficient resource allocation, and a dedicated mobile app for security personnel communication.

CMD – Demonstration – OC2

CMD is developing a software solution based on deep learning models to support crisis management and make cities safer. It detects anomalous behaviour to help police officers manage crises by sending them alerts and critical information such as video streams, images and geographic metrics.

C-SHIELD – Demonstration – OC1

The project focuses on the detection of chemical hazards with a solution that combines two different detection technologies, namely Ion Mobility Spectroscopy (IMS) and Flame Photometric Detection (FPD), in a hardware device equipped with a data fusion software. This system not only reduces false alarms but also estimates the type ID of the detected substance, thus significantly improving situational awareness for end-users.

Domain 3 : Public spaces protection – major events

FUSIONSEC– Demonstration – OC1

The project overcomes communication barriers during mass events with a cloud-based IoT platform that improves collaboration between public and private security forces by providing real-time data from drones, video cameras and smartphones. In addition, a single interactive map visualises the location of both security personnel and potential incidents, facilitating improved coordination.

SAFE FESTIVALS – Demonstration – OC2

SAFE FESTIVALS addresses security challenges at public gatherings such as festivals. The project uses an immersive training platform that simulates various security scenarios and allows security personnel, event organisers and local authorities to collaborate. This solution helps to improve security planning and response strategies, reduce security costs through more efficient training, and facilitate the sharing and implementation of best practices.

SECURAIL – Prototype – OC1

The SECURAIL project aims to improve railway safety with an intelligent LiDAR sensor. This sensor autonomously detects people or objects falling or being pushed onto the tracks, triggering immediate train stops and safety alerts. The project also envisions an open platform for future safety applications, such as the prevention of 'trap and drag' accidents, where a passenger or object is caught in a train door.

ZENITH – Demonstration – OC1

ZENITH has developed a data-driven security platform aimed at maintaining public safety in cities. It collects and analyses vast amounts of data to proactively alert authorities, anticipate security events and improve public safety. The innovative approach combines semantic and predictive analytics, unlocking the potential of rich online data sources, while prioritising data privacy by complying with GDPR regulations and avoiding the storage of personal data.

Flash the QR codes for further information on the SecurIT-funded projects!

Open Call 1 projects

Open Call 2 projects

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

SECURIT
TOWARDS RESILIENT SMART CITIES & TERRITORIES

Project Partners

SAFE (project coordinator) is a French competitiveness cluster located in the South-East of France where high standard security and defence industries are located, as well as a strong part of the French Civil Protection. It gathers a **network of 450+ members including companies, research and academia partners, mainly from the areas of security, environmental protection and aerospace industry and practitioners.**

LSEC is an industry association bringing together more than 800 industrial CyberSecurity partners and reaching out to over 15.000 end users. Since 2006, LSEC has been an active partner in various R&D projects in Europe in the areas of **CyberSecurity, AI and IoT towards industrial robots and industrial machines, postquantum, Computing on Encrypted data and other Privacy Enhancing Technologies.**

Pôle SCS is a digital cluster based in the SUD region, in France, and promotes the development of competitive R&D projects within a community of **more than 300 members,** including companies research centers and educational institutions mainly **in the fields of Microelectronics, IoT, Big Data, Artificial Intelligence and Digital Security, applied to Health, Smart cities, Industry 4.0, Transport & mobility.**

L3CE is the Lithuanian Cybercrime Center of Excellence for Training, Research and Education. It is a research organization established with mission to support capability development and innovation management of security and defence agencies, with a specific focus on **complex, sophisticated cyber related threats.**

HSD is the Dutch security cluster providing access to knowledge, innovation, market, finance, and talent to nearly 300 businesses, governmental organisations and knowledge institutions since 2013. To make a difference in securing the digitalization of our society, these members share their knowledge and collaborate on innovative and scalable security solutions.

Systematic is a French innovation and technology cluster based in the Paris Region bringing together and promoting a regional ecosystem of excellence in Deep Technologies (Data Science & AI; Cyber & Security; Digital Infrastructure & IoT; Digital Engineering; Drones; Optics & Photonics; Open Source) applied to three challenges – Digital Transformations of Territories; Industry and Services and Society). **Systematic has currently over 900 members.**

Founded in 2004, CenSec is a Danish gold cluster with 173 members covering capabilities within the defence, space and security industry, working on two main missions: to develop business networks among SME-suppliers to the defence, security and space industry and to offer assistance to business members to improve market knowledge, competencies and education, creating business and innovation opportunities.

FundingBox is the go-to platform for deeptech innovators in the quest for funding and investors and corporates hunting for the next unicorn. It champions entrepreneurs and innovators eager to ignite their growth to rewrite their future through **easy-to-apply funding opportunities and tailor-made acceleration programmes. The FundingBox platform gatherss over 30,000 funding stakeholders.**

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