



Horizon 2020 Project

IMPETUS: Intelligent Management of Processes, Ethics and Technology for Urban Safety

FAQ

What is the project about?

IMPETUS will provide city authorities with new means to improve the security of public spaces in smart cities, and so help protect citizens. It delivers an advanced, technology-based solution that helps operational personnel, based on data gathered from multiple sources, to work closely with each other and with state-of-the-art tools to detect threats and make well-informed decisions about how to deal with them.

The project builds on mature, state-of-the-art technologies, refining and extending these to fully leverage new capabilities and avoid potential pitfalls. The technological results are supported by practical guidance on how use of the technologies can be fully integrated in working processes to improve operations for public safety.

Why “smart” cities?

Many modern cities are classified as “smart” – and most of those that are not yet “smart” are evolving to become so. Smart cities make extensive use of advanced systems to monitor and manage day-to-day operations, using things such as multiple types of sensors, cameras, tools and apps (e.g. using Artificial Intelligence - AI), internet, and Supervisory Control And Data Acquisition (SCADA) systems for controlling critical infrastructure.



Smart cities benefit from this approach through more efficient city administration, greater situational awareness (especially in emergencies), and the ability to make crucial decisions quickly, based on comprehensive and up-to-date data. But use of advanced systems generates *dependence* on those systems, leading to increased vulnerability - there can be serious negative consequences if the systems are subject to attack. Advanced systems in many cases make extensive use of large amounts of data, some of it of a potentially sensitive nature. This brings with it the risk that sensitive data might be mis-used.

IMPETUS is developing an advanced technology-based solution that facilitates and promotes the advantages offered by the smart city approach, while at the same time guarding against the potential risks.



This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Who might be interested in or affected by IMPETUS?

Our work is aimed at a broad group of stakeholders consisting of people and organisations who:

- **Regulate**: policy makers (at city, national and European level).
- **Make decisions** about adoption of new technology and ways of doing things: city managers, regional & national security agency managers, critical infrastructure managers, ...
- Are **directly involved in managing security threats**: security actors, police and other security agencies (at city, regional and national levels), contractors, critical infrastructure operators, ...
- **Are impacted by** changes introduced by city authorities: citizens, and groups representing them.

Who is carrying out the work?

Our consortium consists of 16 partners from 11 different EU Member States and Associated Countries. It brings together 5 research institutions, 6 specialist industrial and SME companies, 3 NGOs and 2 local government authorities (the trial sites).

The consortium is complemented by the Community of Safe and Secure Cities (COSSEC) – a group established by the project to provide feedback on the IMPETUS solution as it is being developed and tested, and to help promote IMPETUS more widely. COSSEC consists of potential users of IMPETUS results, and other relevant stakeholders.

What classes of threat are addressed by the IMPETUS solution?

1. **Specific threats** where the nature of the threat is known e.g., a chemical or biological attack, a cybersecurity attack, a physical attack (gun vehicle, bomb, ...).
2. **Evolving threats** where the nature of the threat is not yet known – but where indications of “unusual” activities or measurements lead us to suspect that some kind of threat may be developing.

At what phases during an incident can IMPETUS provide support?

IMPETUS provides different types of support at different phases:

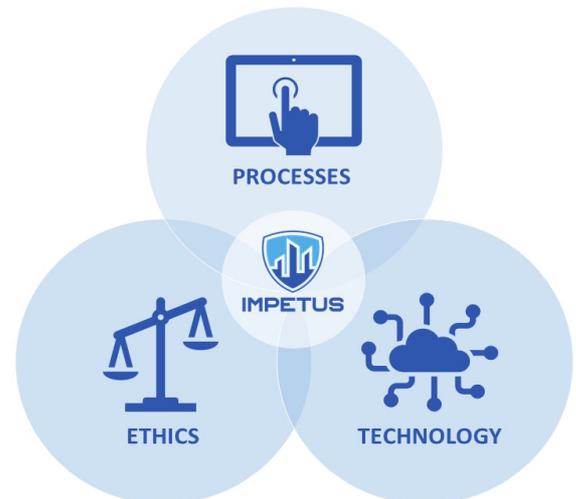
- **Before** any incident has actually occurred: simulation for training and preparedness.
- **Imminent** (i.e., as a threat is developing): detection of signs of a threat emerging.
- **During** (i.e., a threat is on-going). Two distinct types of support are provided in this phase:
 - Gain better *situational awareness*: analyse, monitor, classify and integrate all available data.
 - Use situational awareness, and operational guidelines to *optimise response* to the threat.
- **After**: Use data collected to learn from experience.



What makes IMPETUS special?

As you will read in the sections below, IMPETUS delivers an advanced technology-based solution consisting of multiple tools, an integration platform and a set of practitioner's guides. But other projects and initiatives, individually, also deliver some of these things. The thing that makes IMPETUS special is our *integrated approach* that addresses three complementary but overlapping areas to deliver a single, coherent solution:

- **Technology:** Leverage the power of the Internet of Things (IoT), Artificial Intelligence (AI) and Big Data analysis to provide powerful tools to help operational personnel manage physical and cyber security in smart cities.
- **Ethics:** Balance potentially conflicting needs to collect, transform and share large amounts of data with the imperative of ensuring protection of data privacy and respect for other ethical concerns – all in the context of ensuring benefits to society.
- **Processes:** Define the steps that operational personnel must take, and the assessments they need to make, for effective decision making and coordination – fully aligned with their individual context and the powerful support offered by the technology.



IMPETUS delivers a “technology-based” solution. That means that the project will deliver a set of tools?

Yes – but not only that.

IMPETUS will indeed deliver a set of advanced tools that make use of technical infrastructure (sensors, cameras etc) in smart cities. That's why we call it “technology-based”.

But the IMPETUS solution is more than just technology: it also provides *Practitioners Guides* offering “how-to” advice for all actors involved in dealing with urban security: decision-makers, managers and operational personnel. The practitioner's guides cover:

- **Operations:** The new work processes that operational personnel should follow to leverage advanced technological capabilities and better deal with threats - depending on their specific role, the nature of the threat, and the phase it has reached.
- **Cybersecurity:** Advice on how to guard against, detect and deal with cybersecurity threats.
- **Ethics:** Description of what must be done to make sure that solutions such as the ones developed in IMPETUS are used in an ethical and legal way that respects data privacy concerns. This goes beyond just “advice”: it imposes hard constraints that people and organisations are obliged to follow.

The Practitioners Guides are presented in an integrated Wiki, with an interactive interface facilitating dynamic exploration of the contents.



How can we make sure that IMPETUS technologies are used in a way that respects fundamental rights, addresses privacy concerns and complies with accepted norms and legal requirements?

Balancing the potential benefits of technology with ethical and related concerns is an integral part of the IMPETUS approach. We use several approaches and mechanisms to achieve this, summarised in the table below.

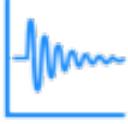
<i>Independent, external inputs & influences</i>	<i>Project results</i>
<p>We consider it important that our work should be subject to external scrutiny with regard to ethics and privacy issues - to point out concerns we may have overlooked or played down, and to propose constraints that need to be put in place. To do this we:</p> <ul style="list-style-type: none"> • Include several external legal experts as members of our Ethics Advisory Board. • Make sure that amongst the external stakeholders represented in COSSEC (the Community of Safe and Secure Cities that we establish during the project) we have some from organisations representing the rights and views of citizens. 	<p>Ways of dealing with ethical, privacy and legal issues are reflected both in technical and in non-technical results:</p> <ul style="list-style-type: none"> • <i>Non-technical:</i> The Practitioner’s Guides include <i>rules</i> (i.e. not just “advice”) about dealing with ethical, privacy and legal issues – expressed in terms of working processes to be followed, and constraints on how/when tools can be used. • <i>Technical</i> (i.e. the tools to be delivered): Where feasible, certain kinds of constraints will be “hard-wired” into tools to ensure protection of privacy and prevent use contrary to ethical guidelines and/or to log all details of usage, to enforce accountability.
<i>Project organisation and activities</i>	
<p>Achieving the three-way integration between technology, ethics and working processes is the core organisational concept of IMPETUS:</p> <ul style="list-style-type: none"> • We have two separate work packages devoted to ethics and privacy: one of them addresses how we deal with these issues <i>during</i> the project itself, the other one looks to the longer term <i>after</i> the project to define the approaches to be taken. • Our requirements gathering and refinement activities in the early stages of the project include ethical and privacy requirements as “first class” requirements – we do not limit the scope to technical, functional requirements. 	



What kind of tool support does IMPETUS provide?

The tools included in the IMPETUS solution are based on existing tools, brought to the project by partners. We refine and enhance these tools to take account of requirements identified in the project, feedback from members of COSSEC and practical experience in using them in our trial cities.

The table below provides short descriptions of the tools, grouped according to their main role:

Role	Tool	
Detecting emergencies needing <i>immediate response</i>		Firearm Detector Continuously monitors surveillance camera feeds and automatically creates an alert if a firearm is detected in a public space.
		Bacteria Detector Continuously monitors air samples to detect abnormally high concentrations of airborne bacteria.
Identifying <i>potential/emerging threats</i>		Urban anomaly detector Continuously monitors data gathered from multiple city sensors and detects cases deviating from the norm - indicating possible cause for concern.
		Social Media Detector Scans large volumes of text on social media and other public online sites, looking for topics/keywords that might indicate potential trouble or threats.
Emergency Management		Evacuation Optimiser Provides instant advice to emergency staff on how to effectively manage an evacuation, based on simulations of different evacuation scenarios.
Cyber protection		Cyber Threat Intelligence Detects, classifies and helps mitigate cyberspace threats to an organisation's IT assets.
		Cyber threat Detection and Response Detects cyber vulnerabilities in IT Systems: raises alerts and suggests countermeasures if they arise.
Ensuring operational efficiency		Workload Monitoring System Measures mental workload and stress of emergency operators using a brain-computer interface, raises alerts if anomalies arise.

Each of the tools can be used independently or via the IMPETUS *integration platform*. The integration platform allows users to access several tools via a unified interface, making it easier to use them together as part of an overall work process.



How and where will IMPETUS be tested?



Oslo, Norway



Padova, Italy

The cities of Oslo and Padova act as trial sites in the project.

Initial trials test the capacity of the tools to collect, analyse and present aggregated data during normal live conditions. Controlled live exercises towards the end of the project are designed to validate the usability and effectiveness of the overall IMPETUS solution in supporting operational performance.

Timing and financing?

The project has a cost budget of 9.3 M€, with financial support of 7.9 M€ from the Horizon 2020 programme for research and innovation of the European Commission. The project started in September 2020 and has a planned duration of 30 months.

Want more information?

Contact:

Project Coordinator: Joe Gorman, SINTEF Digital,
joe.gorman@sintef.no

Dissemination Manager: Harald Drager, TIEMS,
khdrager@online.no



IMPETUS

For the latest news and updates, please visit us at: <https://impetus-project.eu/>

The IMPETUS Consortium

RESEARCH	INDUSTRY & SMES	NGOs	CITIES



This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.