

IMPETUS

A research and innovation project addressing
urban safety

2nd ECSI workshop April 2022



IMPETUS

Intelligent Management of Processes,
Ethics and Technology for Urban Safety



A Horizon 2020
Research and Innovation Project

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

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

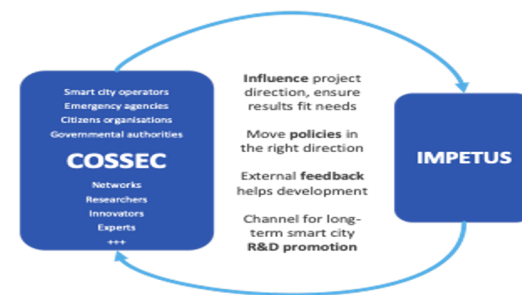
Key facts

- H2020 IA project
- Topic: SU-INFRA02-2019 Security for smart and safe cities, including for public spaces
- Total budget 9.3 M€, EC funding 7.9M€
- September 2020 – February 2023
- Overall goal: **Improve the security of public spaces in smart cities**

Consortium

RESEARCH	INDUSTRY & SMEs	NGOs	CITIES
    	     	  	 

... complemented by
COSSEC:
Community of Safe and Secure Cities
 (extends involvement)



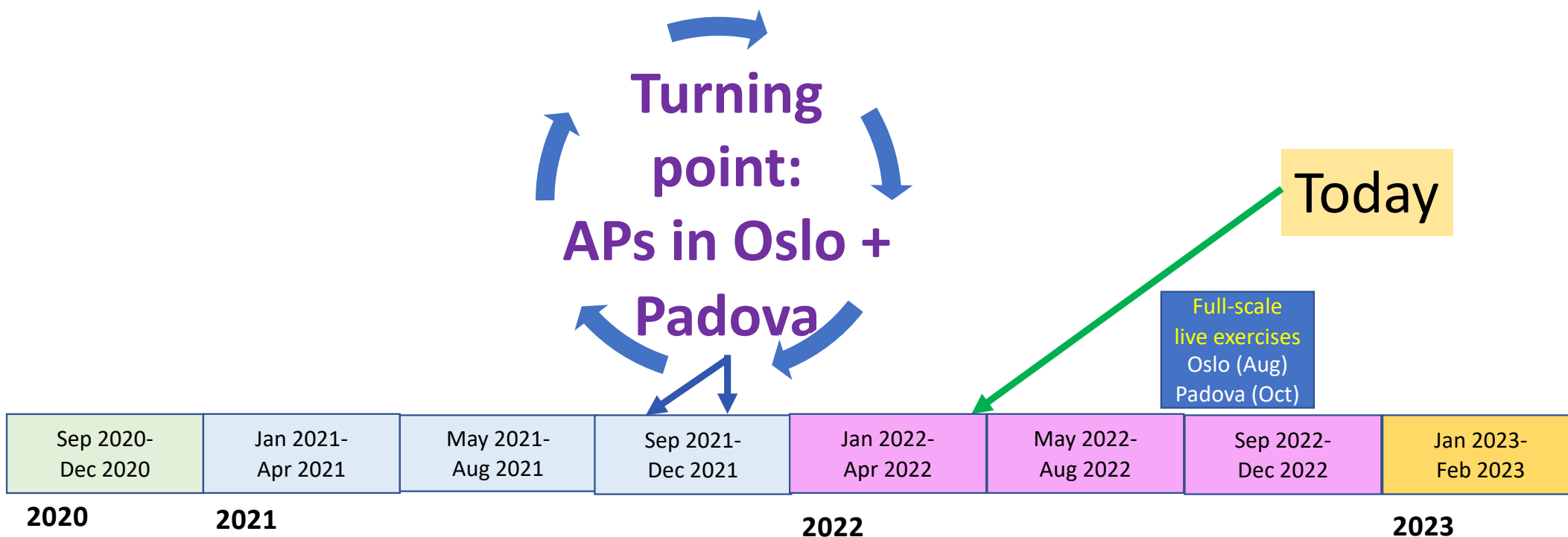
Contact info

www.impetus-project.eu

Project Coordinator: Joe Gorman, SINTEF Digital: joe.Gorman@sintef.no
 COSSEC Manager: Sandro Bologna, TIEMS: s.bologna@infrastrutturecritiche.it
 Dissemination manager: Snjezana Knezic, TIEMS: snjezana.knezic@gmail.co



Challenging 30-months duration





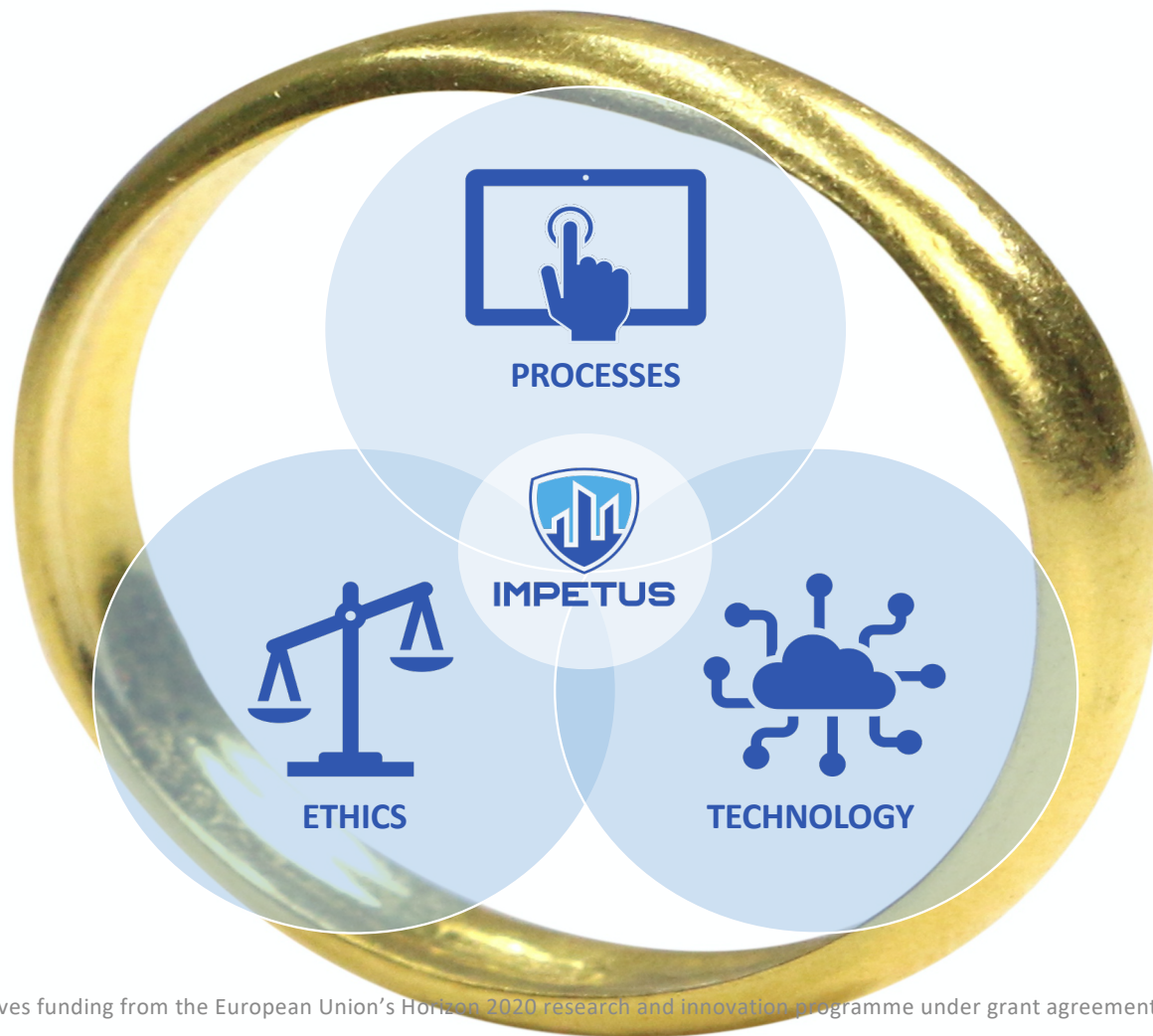
IMPETUS

Motivation / Objectives



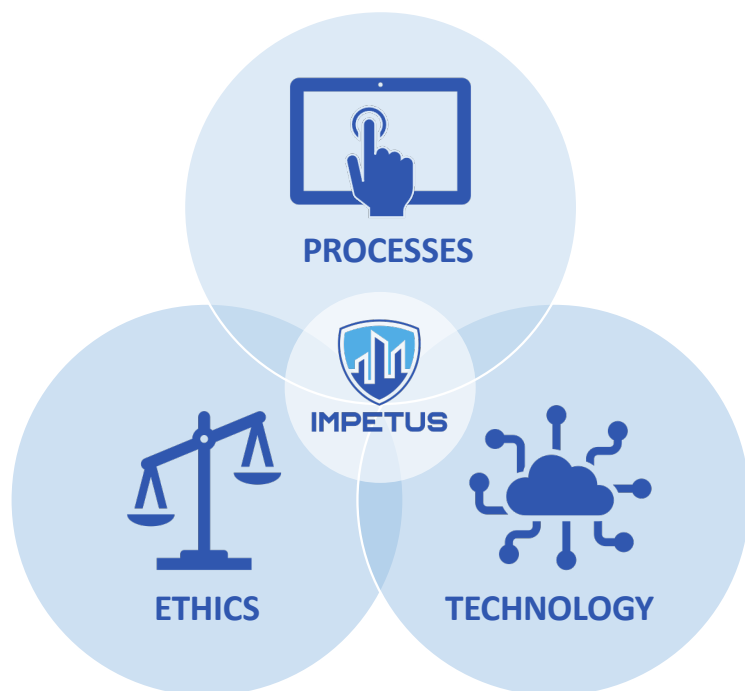
This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

The rings of IMPETUS



WHY IMPETUS: Main objective

The IMPETUS intersection: integrating interdependent solutions and concerns



Improve the security of public spaces in smart cities

- Can advanced **technologies** improve the detection and management of security events?
- How will this affect **processes** used in day-to-day operations?
- How can **ethical** and legal issues be safeguarded and handled?

WHY do Smart Cities need IMPETUS?

Smart Cities

- High-tech grid of sensors (cameras, environmental sensors, traffic sensors, ...)
- IoT ("Internet of Things") – internet is everywhere – not least in everyone's pockets
- IT systems controlling critical infrastructure
- Advanced algorithms and AI (Artificial Intelligence) to help people make decisions

Efficient city administration

Enhanced situational awareness, especially in emergencies

Help authorities make sound decisions, fast

← Enhance



Combat →

IMPETUS

Increased "attack surface" - more vulnerabilities e.g. cyber attacks

Increased risk of unethical use of personal data



IMPETUS

Involving others: COSSEC



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

HOW will IMPETUS achieve its vision?

What do we need?

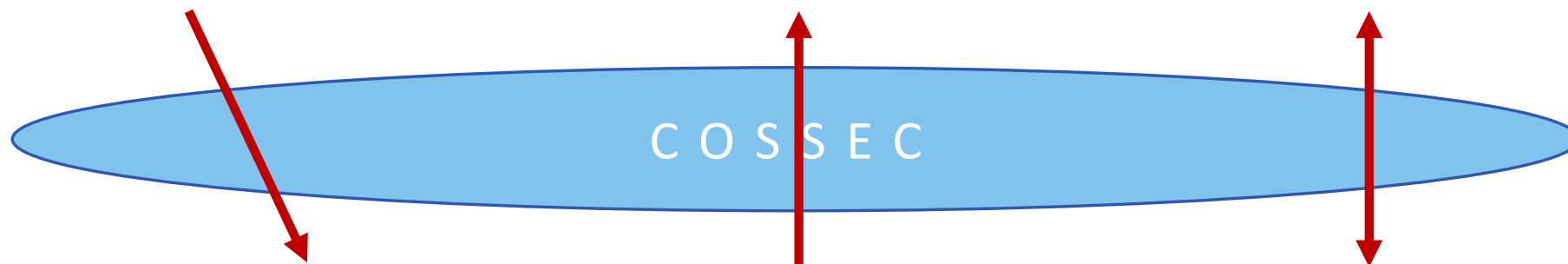
- Identify *risks* and *opportunities* in smart cities
- Formalize *requirements*

What tools can help us?

- *Refine* technologies from partners
- Refine and integrate to provide an *integrated platform*

Does it work?

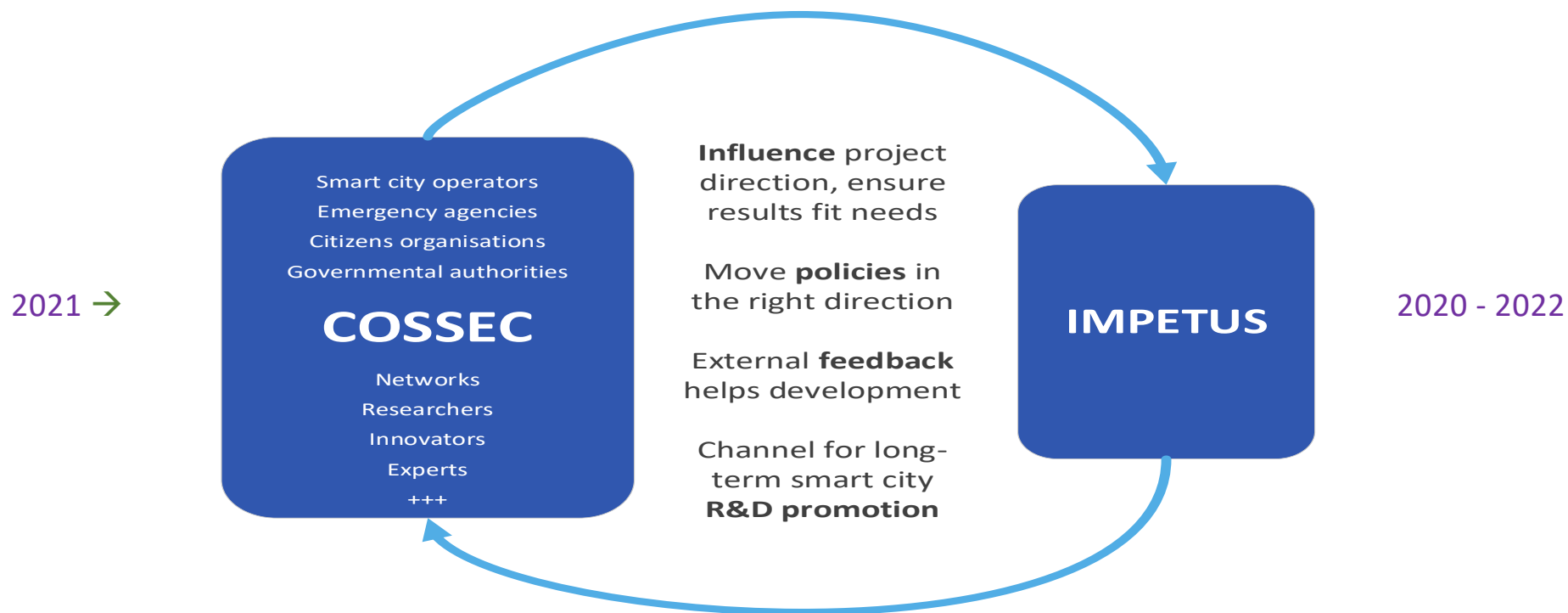
- Validation in *large scale trials*
- Involve *stakeholders* from inside and *outside consortium*



Are ethical, privacy and legal issues understood and respected at all levels?

COSSEC – Community of Safe and Secure Cities

- Extends involvement and influence beyond IMPETUS consortium to wider stakeholders involved in topics of the project



COSSEC Manager: Sandro Bologna, TIEMS: s.bologna@infrastrutturecritiche.it



IMPETUS

Results overview

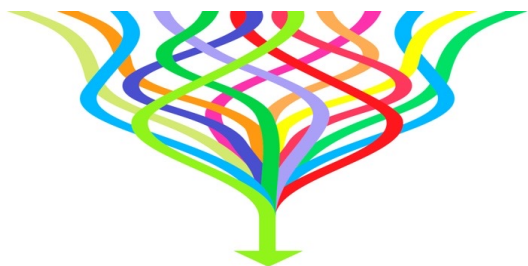


This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

IMPETUS: Key Results

IMPETUS Tools

Phase (w.r.t attack)	Before	Imminent	During	After	
Type of support	<i>Be prepared</i>	<i>Detection</i>	<i>Situational awareness</i>	<i>Response optimization</i>	<i>Learning</i>
Tools	 Breach & attack simulation	 Social media detection Weapon detection Biological risk detection	 Cyber threat intelligence Physical threat intelligence	 Human Computer Interaction Physical threat response optimization	 Cyberthreat response optimization



Integrating Platform

- Tools usable in single interface
- Tools can connect and share data

Practitioners Guides



Practitioner's Guidelines

- Advice
- DOs and DON'Ts
- Reference information
- Training materials



Other projects

First adopters

Policy makers



The IMPETUS solution: Provides the **support** you need



Integrated: for use separately or together, as part of an overall solution

In different phases

For different kinds of threats

Before

Simulation

Chemical/biological attack

Imminent

Detection

Specific

Cyber attack

During

Classify –
monitor -
analyze

Optimize
response

Physical attack (gun, vehicle, bomb, ..)

Evolving

Forewarning of
unusual activity

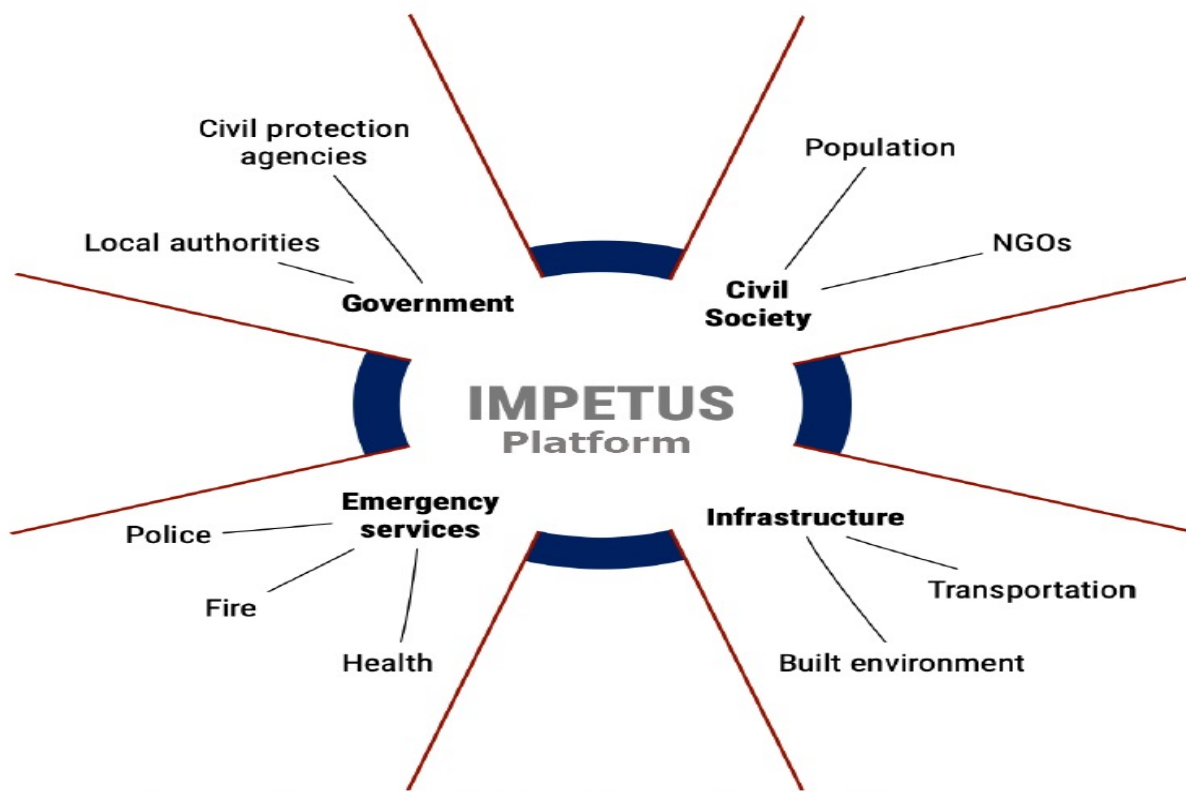


The integrating platform



The Platform - Objectives

Collecting and sharing information between security and emergency actors



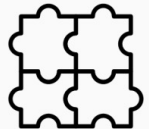
The Platform - Capabilities



Access Control



Alerting



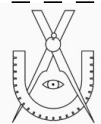
Internal Integration



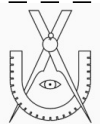
Security



External Integration



UI/UX



Platform: built using Snap4City

The screenshot displays the IMPETUS platform interface. On the left is a sidebar menu with the following items: Dashboards, My Dashboards in All, Dashboards of My Or, My Dashboards in My, Extra Dashboard Wid, Notificator, Data, my Data, Open, Knowledge and Map, IOT Applications, IOT Directory and De, Resource Manager, and Development Tools. The main content area is titled 'Dashboards' and shows a grid of dashboard cards. Each card includes a title, status (Passive), ownership information, and action buttons (Edit, Management, Clone, Delete).

100% OPEN SOURCE

APPLIANCES CONTAINERS

- LOCAL GOVERN
- STAKEHOLDERS
- CITY USERS
- IN-HOUSE
- ENERGY OPERATORS
- MOBILITY OPERATORS
- COMMERCIAL OPERATORS
- SECURITY OPERATORS
- INDUSTRIES
- RESEARCHERS
- START-UPS
- ASSOCIATIONS

SMART CITY LIVING LAB

- GDPR
- SECURITY
- PRIVACY
- ASSESSMENT
- AUDITING
- PENTESTED

- OPEN IOT DEVICES
- IOT EDGE
- IOT GATEWAY
- PAX COUNTERS
- IOT BUTTONS

- TEST CASES, SCENARIOS, VIDEOS, HACKATHONS
- OPEN SOURCES, COMMUNITY OF CITIES
- TRAINING TUTORIALS, COMMUNITY MANAGEMENT

IMPETUS

User: userrootadmin,
Org:
Organization
Role: RootAdmin,
Level:
LOGOUT

Dashboards

Cards [A-Z] [Z-A] [Icons]

Prev 1 Next










Filter by dashboard ti [Search] [Close] **New dashboard**

Dashboard Title	Status	Ownership	Actions
Padova Dashboard	Passive	My own (Organization)	Edit Management Clone Delete
SOC Dashboard	Passive	soc_operator: Private - Organization	Edit Management Clone Delete
Supervisor Dashboa...	Passive	soc_supervisor: Private - Organization	Edit Management Clone Delete
Tool BRD	Passive	My own: Public (Organization)	Edit Management Clone Delete
Tool HCI	Passive	My own (Organization)	Edit Management Clone Delete
Tool PTI	Passive	My own (Organization)	Edit Management Clone Delete
Tool WD	Passive	My own (Organization)	Edit Management Clone Delete



The tools



Phase (w.r.t attack)	Before	Imminent	During		After
Type of support	<i>Be prepared</i>	<i>Detection</i>	<i>Situational awareness</i>	<i>Response optimization</i>	<i>Learning</i>
Tools	 Breach and attack simulation	 Social media detection  Weapon detection  Biological risk detection	 Cyber threat intelligence  Physical threat intelligence	 Human Computer Interaction  Physical threat response optimization	 Cyber threat mapping

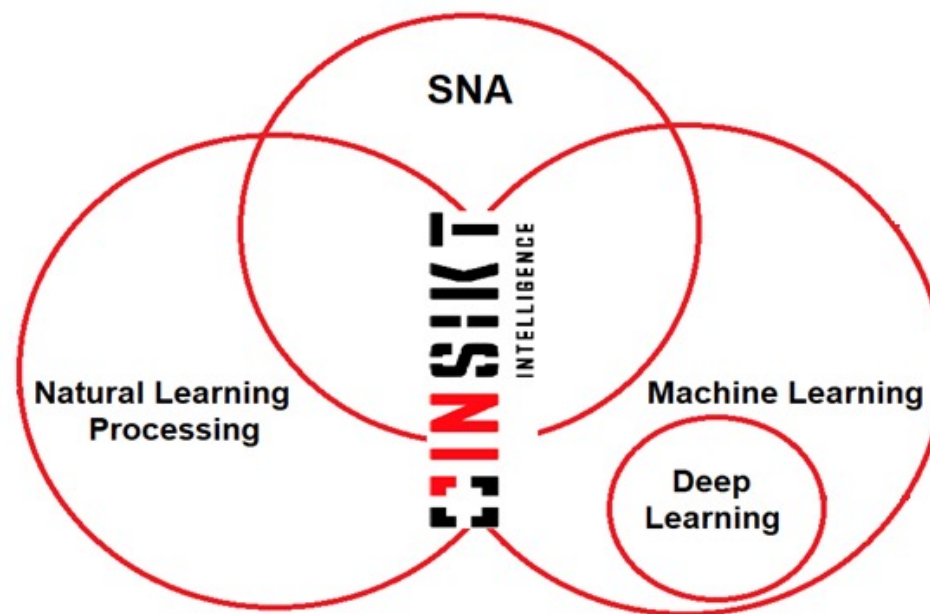


Social media detection tool

Forewarning of unusual activity – based on internet activity observations

Methods & Tools to automatically monitor public online content

- **Automatic text classifiers**
 - Machine Learning and Deep Learning models to classify the messages in domains
- **Data collection technologies**
 - Methods to extract information from web and social networks



- **NLP**
 - Methods to discover insights into the content of the messages
- **Social Network Analysis**
 - Methods to discover relationships between users

Weapon detection tool*

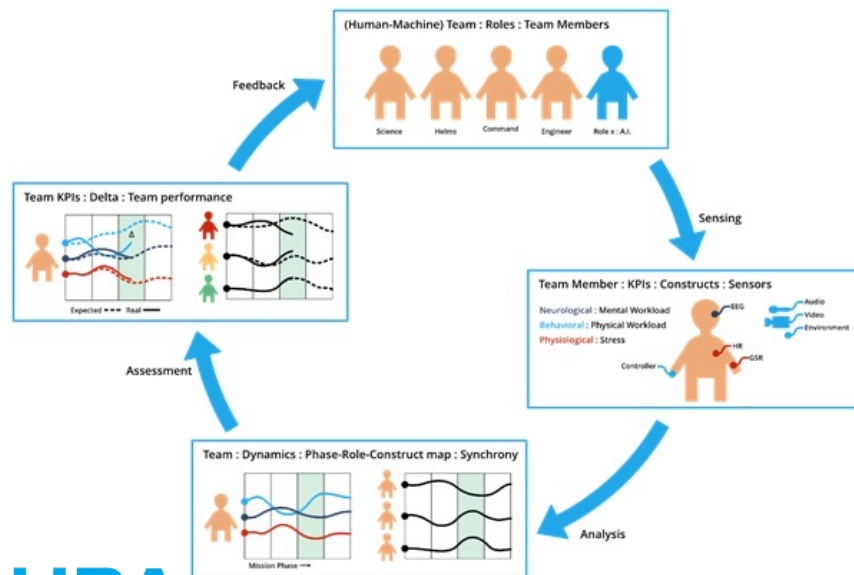
Immediate threat

- Based on AI-based analysis of CCTV images
- Detecting a Weapon With Security Cameras Is **Hard**, Because The Camera Angle And The Environment Is **Never The Same**.

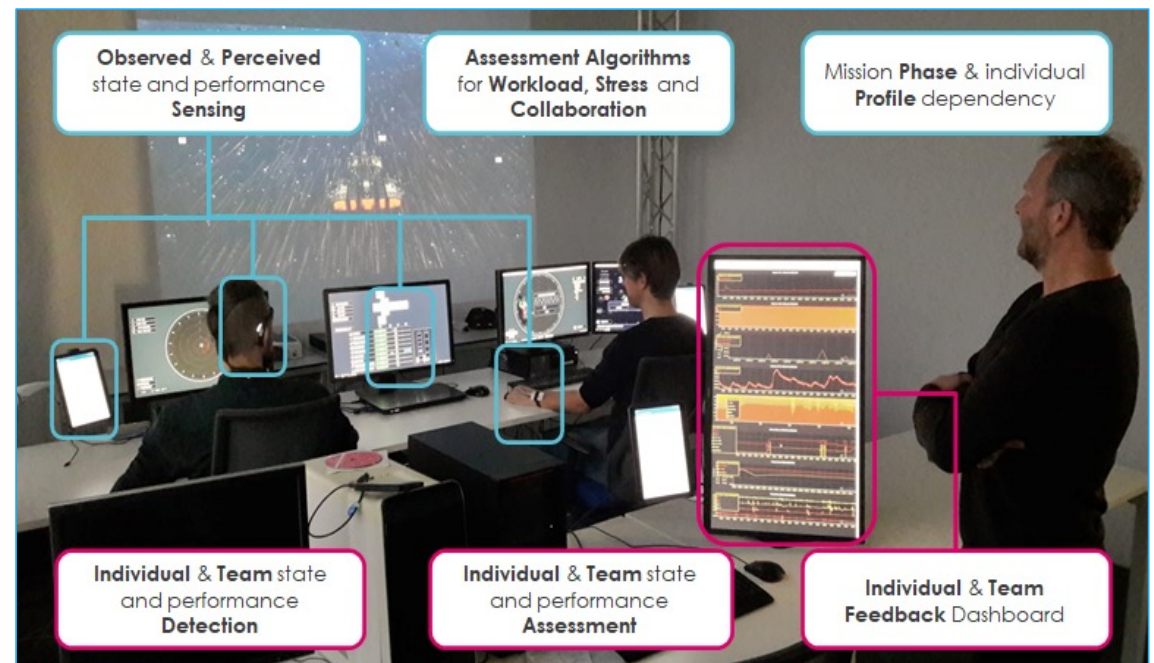
The diagram illustrates the workflow of the weapon detection tool. It consists of five circular icons in a row: a stopwatch for 'Instant', a handgun labeled 'gun' for 'Weapon Detection', the letters 'ai' for 'Via AI', a CCTV camera for 'Through CCTV', and a radio tower for 'With Real-Time Alerts'. Below this diagram are five grayscale images showing the tool's performance in various scenarios. Each image shows a person with a bounding box around them and a smaller bounding box around a detected weapon. The detection confidence scores are: 0.99 (red box), 0.98 (yellow box), 0.97 (yellow box), 0.98 (yellow box), and 0.98 (red box). The labels 'gun,C=0.98' and 'gun,C=0.96' are visible in blue text above the weapon bounding boxes.

Human computer interaction tool

Optimize response – helping IT system users work well under stress



HBAlab
Human Behaviour Analytics
Thales Research & Technology Hengelo



Using (neuro)physiological sensors, machine learning for real-time workload assessment and user feedback

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

The Practitioners Guides



Practitioners Guides



- Practitioner's Guides* are “must reads” for users of IMPETUS solutions
- Each provides:
 - **Guidelines:** “how to...”, “DOs and DONTs”, role definitions, ...
 - **Training materials / services**
 - **Reference information** (tool documentation, relevant regulations, ...)

* Called “Frameworks” in early documentation

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

Practitioners' guide: Ethics and Data privacy

Goal:

*provide **practical advice** about **ethical, legal and data privacy issues** that may arise when using advanced technological solutions to **collect, analyse and manipulate data** in security operations.*

Target audience:

***practitioners** with responsibility for security operations, and who could be **future adopters of IMPETUS results**.*

Format:

a compendium of reports, surveys, guides, brochures, video materials and protocols.



Practitioners' guide: Operations



<https://www.telenor.no/bedrift/sikkerhet/tsoc/>

- Addressing the new **operational concepts**
- Addressing possible **changes to operational strategies**
- Exploring explicitly the **consequences to sense-making and resilience**
- Exploring and defining the **cascading consequences in the SOC-process** and changes in the operational coordination and response
- Exploring new **risks of overdependence** to technology and needs for alternative ways of working

Practitioners' guide: Cybersecurity

Envisioned content

- Theoretical aspects of Cybersecurity for Smart Cities
- Practical guidelines to foster cybersecurity mindset
- Toolkit
- Training material for stakeholders



Image from <https://iiot-world.com/>



IMPETUS

Field trials – trial cities



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

WHERE and how will IMPETUS be validated?

Validation pilots in two cities



- Phase 1: Technical and acceptance testing on non-live systems
- Phase 2: Data collection from live systems, for analysis but no intervention
- Phase 3: Live test with simulated physical and cyber attack

Oslo, Norway



Padova, Italy

General lessons learned:
During the acceptance pilots:
Oslo: Nov 2021
Padova: Dec 2021

Acceptance pilots (APs): lessons learned

- It is a big job to organise an AP for multiple tools and a platform!
- Careful preparation needed to obtain permissions for data sharing/handling:
 - During technical preparations
 - During the APs themselves
- As APs are mostly about checking that the technology works, the “lessons learned” focus mainly on that
- Recruiting and involving potential users:
 - Of crucial importance!
 - Must match tool to end-user with appropriate operational role



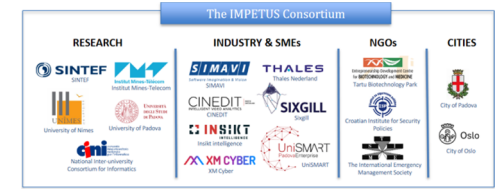
What next? – Long term, post-project

- 
- Promote uptake of results in smart cities throughout Europe and elsewhere
 - Influence policy making to facilitate uptake consistent with ethical and legal principles
 - Establish COSSEC as a permanent community of users



IMPETUS

impetus-project.eu



impetus-project.eu



IMPETUS

HOME • ABOUT IMPETUS • PILOT CITIES • COSSEC • OUTPUTS • NEWS & EVENTS • SURVEY • CONTACTS

Get to know IMPETUS

Our FAQ brochure will help you

READ MORE +



Thank you very much for your attention, and for filling in and sharing the IMPETUS web survey with your colleagues and friends.