



## ***New Emergency Management in a Resilience Era Facing Health, Climate and Energy Challenges***

***6<sup>th</sup> to 10<sup>th</sup> December 2021***

Date and slot of presentation to be filled in shortly

Mathieu Branlat, SINTEF DIGITAL

# H2020 Project IMPETUS: Key Results



**IMPETUS**

Intelligent **M**anagement of **P**rocesses,  
Ethics and **T**echnology for **U**rban **S**afety



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

**New Emergency Management in a Resilience Era Facing Health, Climate and Energy Challenges**



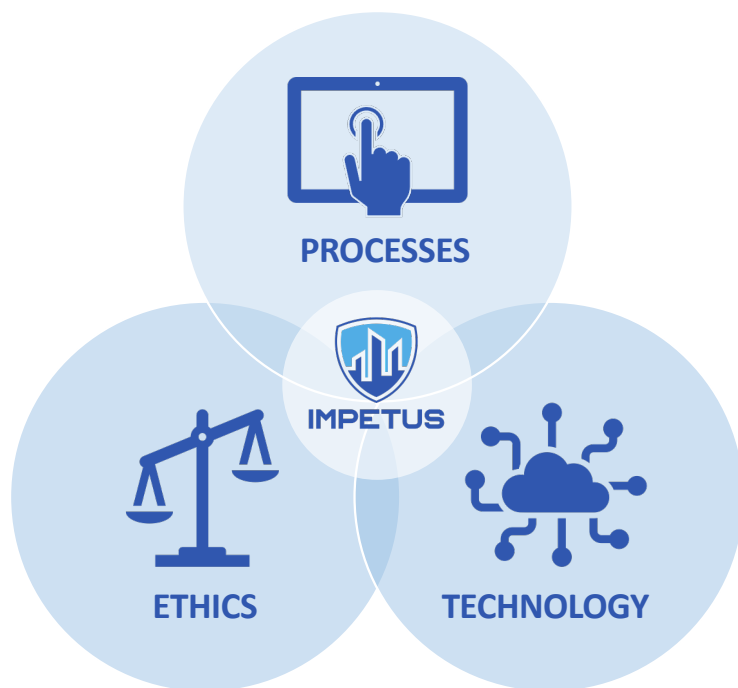
**IMPETUS** project receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883286.

[www.impetus-project.eu](http://www.impetus-project.eu)

RESEARCH	INDUSTRY & SMEs	NGOs	CITIES
SINTEF Institut Mines-Télécom UNIMES UNIVERSITÀ DEGLI STUDI DI PADOVA eni consiglio interuniversitario nazionale per l'informatica	SIMAVI Software Imagination & Vision THALES CINEDIT INTELLIGENT VIDEO ANALYTICS INSIKT INTELLIGENCE XM CYBER SIXGILL UniSMART Fondazione Università di Padova	Entrepreneurship Development Centre for BIOTECHNOLOGY and MEDICINE ISP S-T-I-M-E	Coat of arms of Padua Oslo

## IMPETUS: Main objectives and driving questions

The **IMPETUS intersection**: integrating interdependent solutions and concerns



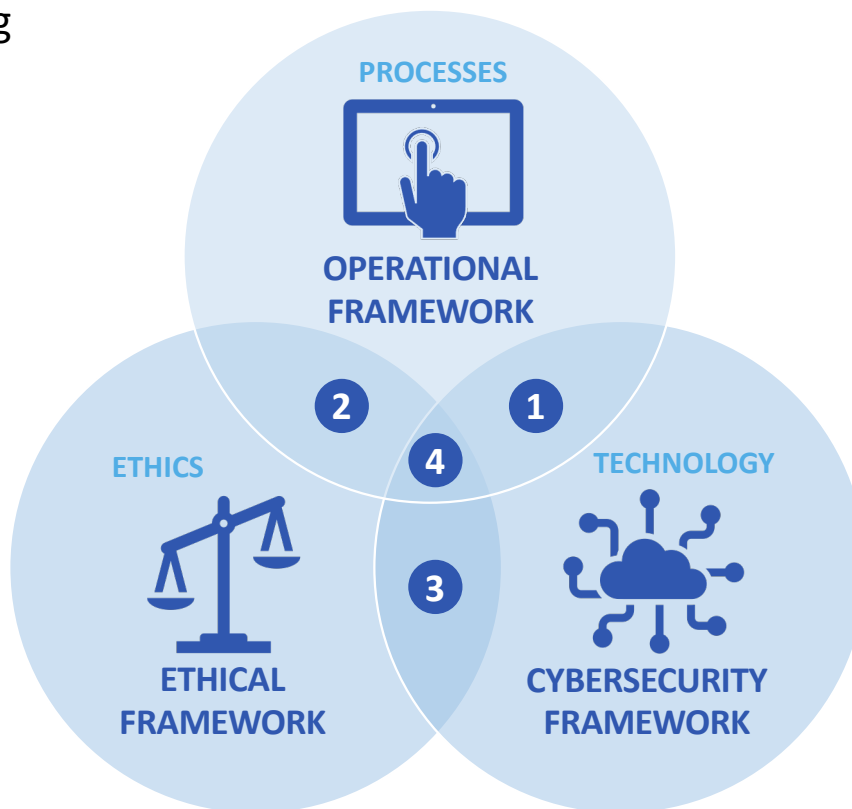
### Improve the security of public spaces in smart cities

- 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?
- Do they create new **cyber security** risks and reliance on infrastructure?



## Different types of results

- **Public safety tools** providing specific capabilities around:
  - Detection
  - Simulation & analysis
  - Intervention
- **Platform:** Integrates tools; common interface/dashboard
- **Frameworks** (aka “Practitioners Guides”) to support deployment:
  - Managing operational change
  - Accounting for ethical and legal concerns
  - Managing cybersecurity



- 1 AI-based threat detection, analysis and intervention  
+
- 2 Privacy-preserving technical and legal framework  
+
- 3 Ethical & explainable AI including security awareness  
||
- 4 Decision-making support tools combining AI + human-in-the-loop

# Results overview

Specific technological capabilities					
Type of support	Be prepared	Detection	Situational awareness	Response optimization	Learning
Tools	Breach and attack simulation	Social media detection	Cyber threat intelligence	Human Computer Interaction	Cyber Threat Mapping
		Weapon detection	Physical threat intelligence	Physical threat response optimization	
		Biological risk detection			



## Integrating Platform

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



## Practitioner's Guidelines

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












Other projects

First adopters

Policy makers



## IMPETUS tools: specific public safety capabilities

Be prepared	Detection	Situational awareness	Response optimization	Learning
 <p>Breach and attack simulation</p>	 <p>Social media detection *</p>	 <p>Cyber threat intelligence</p>	 <p>Human Computer Interaction</p>	 <p>Cyber Threat Mapping *</p>
	 <p>Weapon detection *</p>	 <p>Physical threat intelligence *</p>	 <p>Physical threat response optimization *</p>	
	 <p>Biological risk detection</p>			

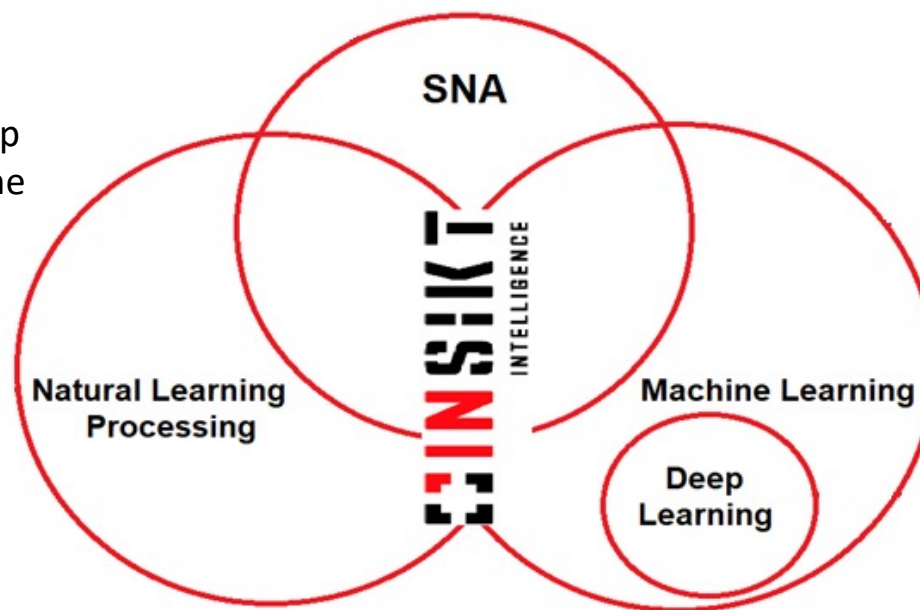


## Social media detection tool\*

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



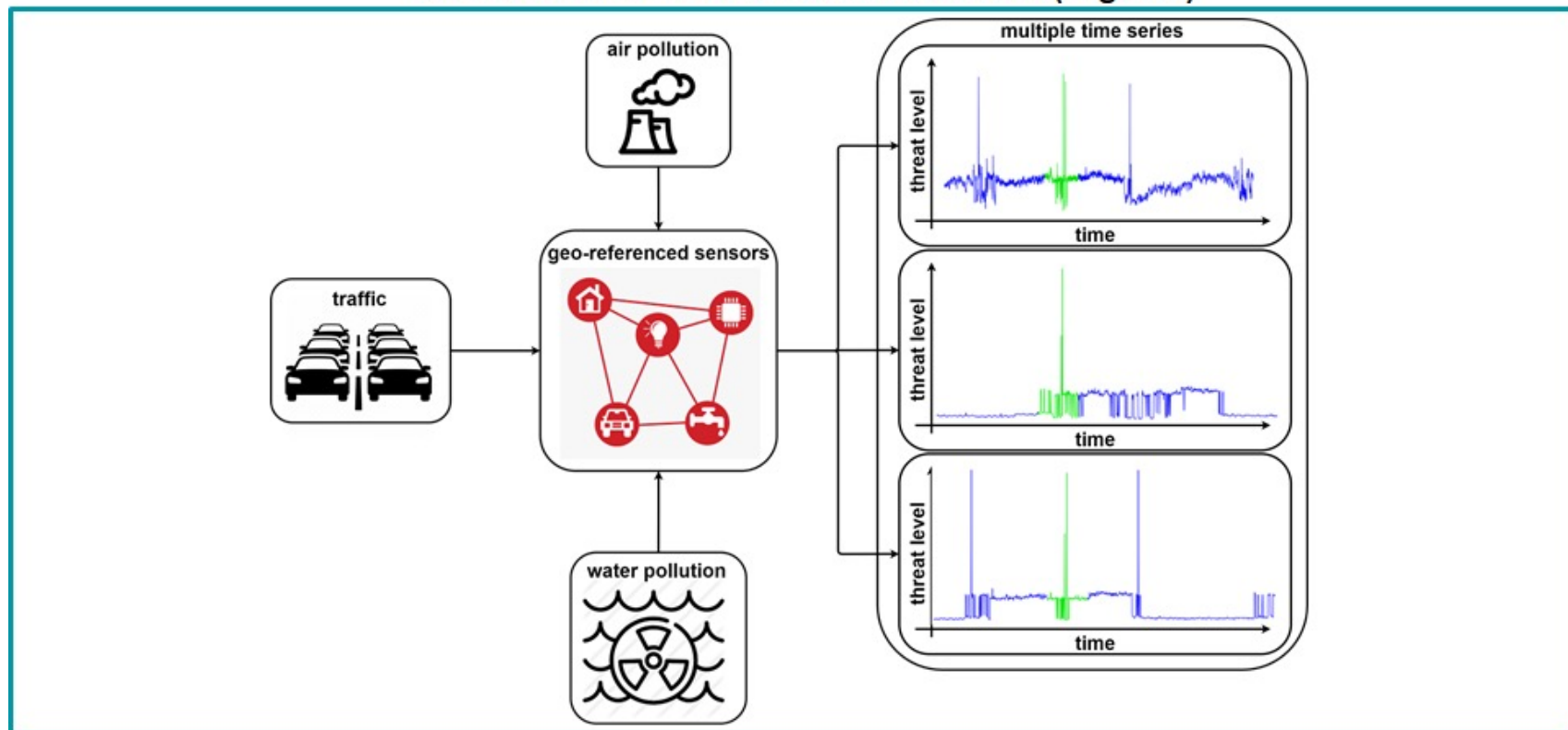
- **NLP**
  - Methods to discover insights into the content of the messages
- **Social Network Analysis**
  - Methods to discover relationships between users



# Physical threat intelligence tool\*

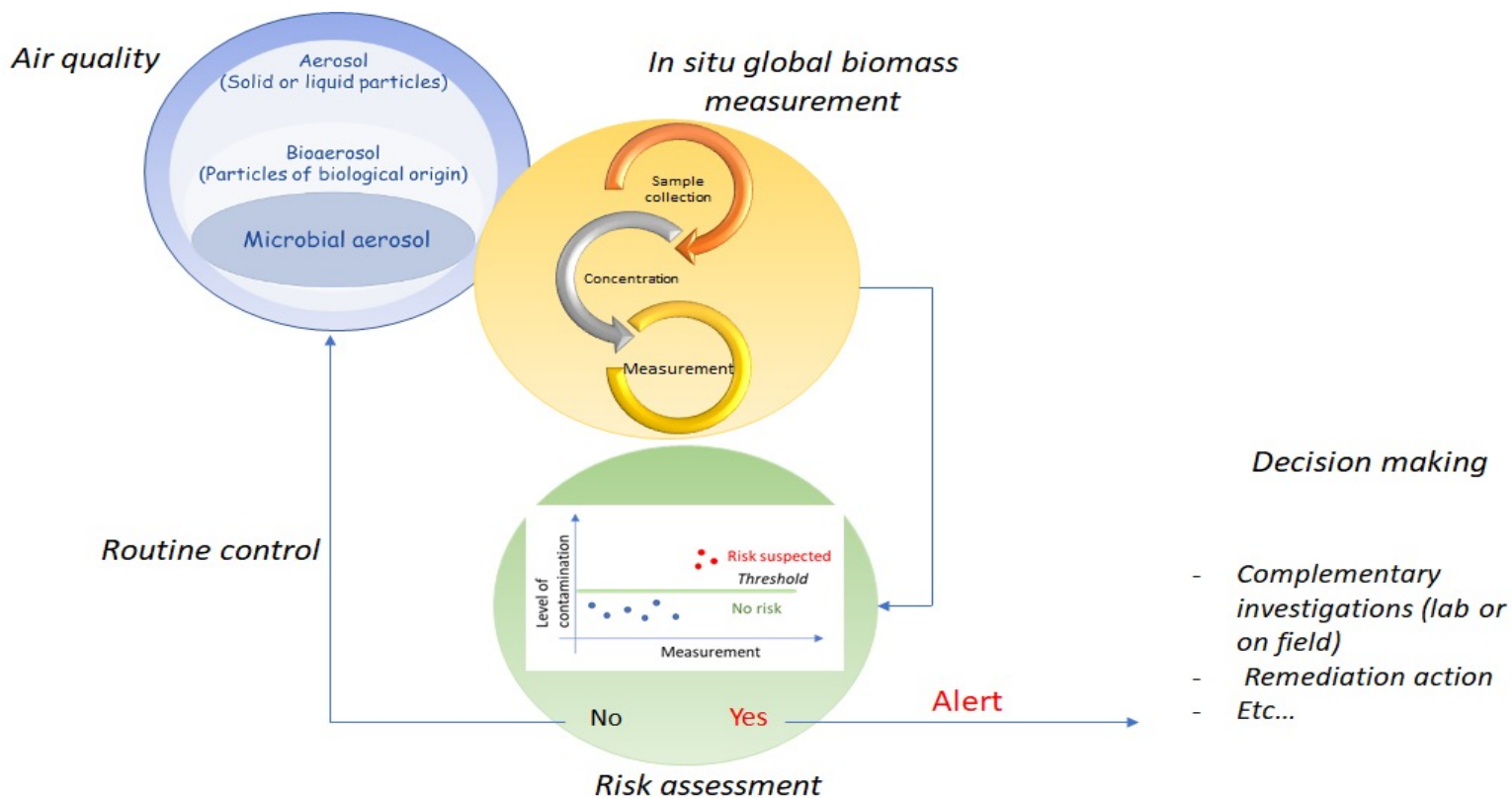
Forewarning of unusual activity – based on sensor data

Anomalies of different time series detected (in green)



# Biological risk detection tool

Chemical/biological attack – collect data, smart assessment of risk level



## Weapon detection tool\*

- 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**.

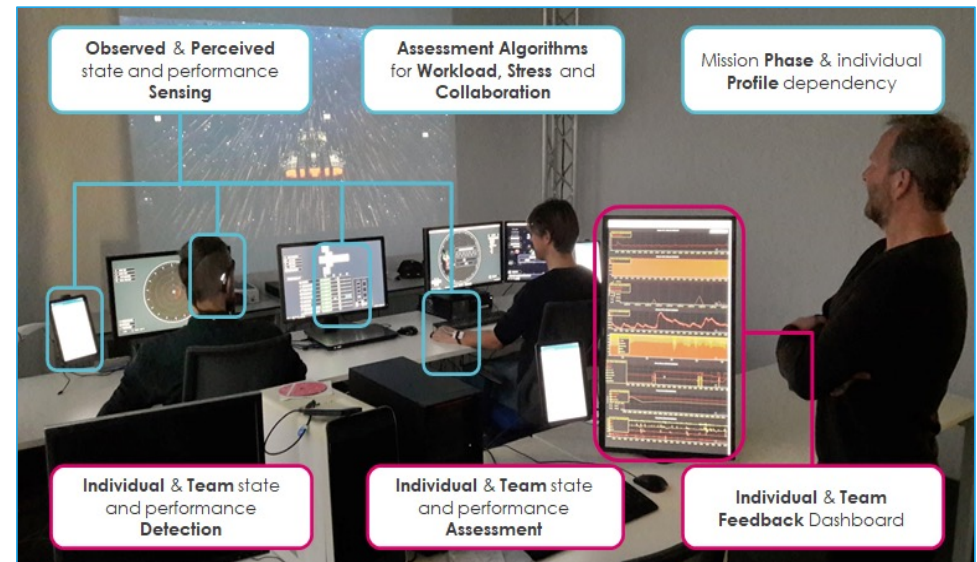
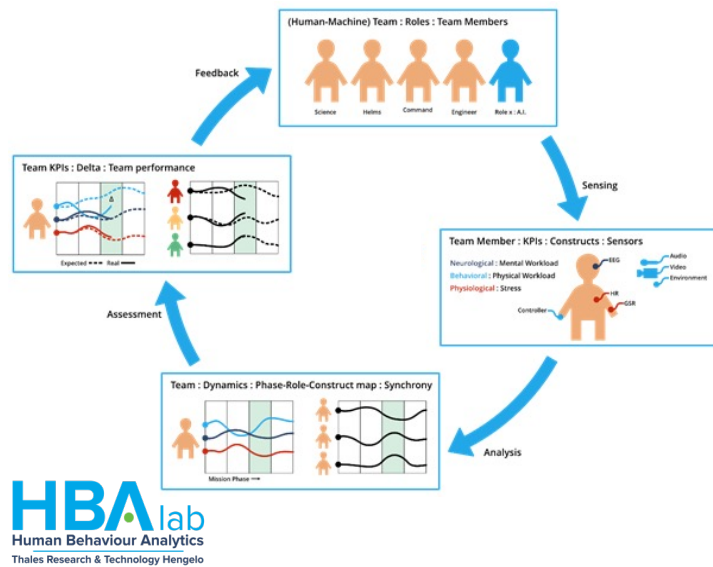
The diagram illustrates the tool's workflow: **Instant** (timer icon), **Weapon Detection** (gun icon with 'gun' label), **Via AI** (ai icon), **Through CCTV** (camera icon), and **With Real-Time Alerts** (tower icon).

Below the diagram are five images showing the tool's performance in various scenarios:

- 1. A person in a black shirt and white pants holding a handgun, with a red bounding box and 'gun,C=1.00' label.
- 2. Two people in a hallway; one is holding a handgun, with a yellow bounding box and 'gun,C=0.97' label.
- 3. A person in a white shirt and dark pants holding a rifle, with a yellow bounding box and 'gun,C=0.97' label.
- 4. A person in a grey shirt and dark pants holding a handgun, with a yellow bounding box and 'gun,C=0.98' label.
- 5. A person in a red hoodie and black pants holding a handgun, with a red bounding box and 'gun,C=0.98' label.

# Human computer interaction tool

Optimize response – helping operational teams manage stressful situations



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

# Platform\*: integration to support public safety operations



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

In different phases

Simulation

Detection

Classify –  
monitor -  
analyze

Optimize  
response

For different kinds of threats

Chemical/biological attack

Cyber attack

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

Specific

Evolving

Forewarning of  
unusual activity

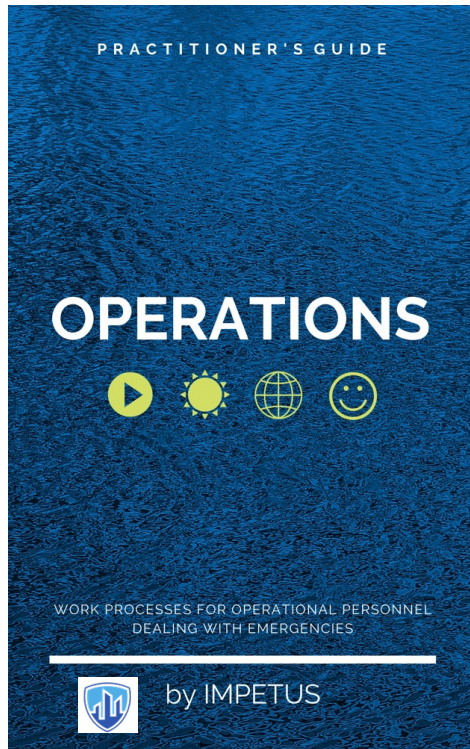


# Platform\*: based on Snap4City

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 features a grid of dashboard cards. At the top left of the main area, there is a user profile section for 'userrootadmin' with a 'LOGOUT' button. The dashboard grid includes: Padova Dashboard (Passive, My own (Organization)), SOC Dashboard (Passive, soc\_operator: Private - Organization), Supervisor Dashboa... (Passive, soc\_supervisor: Private - Organization), Tool BRD (Passive, My own: Public (Organization)), Tool HCI (Passive, My own (Organization)), Tool PTI (Passive, My own (Organization)), and Tool WD (Passive, My own (Organization)). Each card has 'Edit', 'Management', 'Clone', and 'Delete' options. The interface also shows navigation controls like 'Cards', 'Prev', 'Next', and a search filter.



## 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, ...)





**IMPETUS**

# Thank you!



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