



<http://www.impetus-project.eu>

*IMPETUS Project Deliverable: D7.2*

# Acceptance pilot report

Dissemination Status: Public

Editor: Bruno Bonomini (CPAD)

Authors: Giulia Canilli, Arianna Dissegna, Stefano Baraldi, Cinzia Cecconello (CPAD); Martina Ragosta, Andrea Vik Bjarkø, Maria Vatshaug Ottermo (SINTEF); Ian Simon Gjetrang, David Rottingen, Osman Ibrahim, Juan Cabrera, Eirik Bærulfsen (OSL); Keren Saint-Hilaire, Alexia Comte, Sandrine Bayle (IMT); Axelle Cadière, Sébastien Courtin, Mathieu Tur (UdN); Chiara Braghin, Costantino Mele (CINI); Paolo Mocellin, Matteo Bottin (UPAD); Rafal Hrynkiewicz, Johan de Heer, Thomas de Groot (THA); Joachim (Joe) Levy (CINEDIT); Joaquín Luzón (INS); Dor Goshier (SG); Thomas Robertson (TIEMS); Alberto Da Re, Stefano Gallinaro (UNI); Dragos Trifan, Radu Popescu, Gabriel Nicola (SIV); Sachin Gaur (BMA).



## About IMPETUS

IMPETUS (Intelligent Management of Processes, Ethics and Technology for Urban Safety) is a Horizon 2020 Research and Innovation project that provides 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.

IMPETUS provides a solution that brings together:

- *Technology*: leverage the power of Internet of Things, Artificial Intelligence and Big Data to provide powerful tools that 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.

Technological results are complemented by a set of *practitioner's guides* providing guidelines, documentation and training materials in the areas of operations, ethical/legal issues and cybersecurity.

IMPETUS places great emphasis on taking full and proper account of ethical and legal issues. This is reflected in the way project work is carried out, the nature of the project's results and the restrictions imposed on their use, and the inclusion of external advisors on these issues in project management.

The cities of Oslo (Norway) and Padova (Italy) have been selected as the site of practical trials of the IMPETUS solution during the project lifetime, but the longer-term goal is to achieve adoption much more widely.

The work is carried out by a Consortium of 17 PARTNERS from 11 different EU Member States and Associated Countries. It brings together 5 research institutions, 7 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.

The project started in September 2020 with a planned duration of 30 months.

## For more information

Project web site: <https://www.impetus-project.eu/>  
Project Coordinator: Joe Gorman, SINTEF: [joe.gorman@sintef.no](mailto:joe.gorman@sintef.no)  
Dissemination Manager: Snježana Knezić, TIEMS: [snjezana.knezic@gmail.com](mailto:snjezana.knezic@gmail.com)



## Executive Summary

“Acceptance Pilots” (APs) are the formal occasion, at mid-term of the project, to test what has been developed, and to understand what the achievements and the needed corrective actions are.

The Acceptance Pilots took place in the Partner cities (Oslo, 2021 November and Padova, 2021 December) to test the IMPETUS platform and the tools the Partners have been developing and to get feedback, in particular from the end users, to pursue the target of providing a useful and effective support in managing security in public spaces.

Even in front of the serious limitations and constraints due to the persisting pandemic, the APs succeeded: all the Partners gained a more precise idea of the progress of their work and assessed it from the end user perspective. The Consortium, in addition, was able also to involve other stakeholders not only to get their contribution in terms of improvements to be done, but also to let them better understand the potential advantages that the technologies, on which the tools are based, could bring in daily activities related to security and safety.

The 2 events, AP in Oslo and AP in Padova were part of the same validation process and provided a large quantity of significant information and results (not only concerning the technical developments).

One example that clarifies the importance of these tests on the field is the actual personas/roles to whom the IMPETUS Platform and the Partners’ tool are targeted: before the APs, the Consortium was considering as the main end user only the SOC operator (and SOC supervisors). The activities before and during the APs, instead, showed clearly that other kind of end users have to be involved or “created”.

In fact, in addition to the IT specialists that will deal with the cybersecurity and the tools related as CTI, CTM, and BAS (this topic is becoming more and more a critical issue for cities, companies -both enterprises or SME- and for all the other public and private entities), there will be the need to involve/create some “analysts” that could manage different and heterogeneous data and provide information useful to take strategic decisions: so, tools like SMD, PTRO, PTI and HCI are going to provide “new” insights and points of view to improve security.

The SOC operators and their supervisors will get advantages, moreover, from tools like WD and BRD that will potentially provide new alarms, in real time.

The word “new”, used above, in this case means “they currently do not exist”, they are hence additional alarms and information that the safety and security operators will receive, passively. As an example, during the night, when there are no people hanging around and witnessing a danger situation, alarms could be provided by the detection capability of some of the IMPETUS tools.

The IMPETUS platform, that has been tested only partially, from one side could be considered the container of all the tools developed (and other that could be added) and it will let the end users interact with them in the easiest way. On the other side it could be adopted by different agencies and improve coordination providing the same information at the same time to all these different entities.

As an essential part of the project implementation, the APs saw the involvement of nearly 200 people and the implementation of 37 tests (simulations, exercises, “hands on” sessions, etc.) with 21 end users.

To involve and collect the contributions from all these people a huge effort before, during and after the APs, in terms of presentations, brief and debrief sessions, interviews, surveys, brainstorming, discussions and catch-up sessions was needed.

To undertake the above, the Consortium, as a TEAM, worked hard.

This document summarise what have been done and, moreover, underline what emerged as feedback. The results here reported will surely be a precious reference for planning Live Exercises in the cities.



# Table of Contents

<b>Executive Summary</b> .....	<b>3</b>
<b>List of Abbreviations</b> .....	<b>8</b>
<b>List of Definitions</b> .....	<b>9</b>
<b>1 About this deliverable</b> .....	<b>10</b>
<b>1.1 Intended readership/users</b> .....	<b>10</b>
<b>1.2 Why would I want to read this deliverable?</b> .....	<b>10</b>
<b>1.3 Structure</b> .....	<b>10</b>
<b>1.4 Other deliverables that may be of interest</b> .....	<b>11</b>
<b>1.5 Synergy with other projects/initiatives</b> .....	<b>11</b>
<b>2 The Acceptance Pilots – 1<sup>st</sup> part of the Validation process</b> .....	<b>12</b>
<b>2.1 Applicability of the Ethical framework</b> .....	<b>12</b>
<b>2.2 Effectiveness of the IMPETUS Cyber security framework</b> .....	<b>13</b>
<b>2.3 Impact of the IMPETUS Operational framework</b> .....	<b>13</b>
<b>2.4 The Usability of the IMPETUS platform &amp; its tools</b> .....	<b>15</b>
<b>3 (First) Evaluation of the IMPETUS Platform</b> .....	<b>17</b>
<b>3.1 Back-end</b> .....	<b>17</b>
<b>3.2 Front-end: evaluation of the initial interface</b> .....	<b>19</b>
3.2.1 <i>User interface – technical aspects</i> .....	<i>20</i>
3.2.2 <i>User interface – usability</i> .....	<i>21</i>
<b>3.3 Platform cybersecurity</b> .....	<b>23</b>
<b>4 First validation on the field</b> .....	<b>25</b>
<b>4.1 The Acceptance Pilots</b> .....	<b>25</b>
4.1.1 <i>Acceptance Pilots preparation</i> .....	<i>25</i>
<b>4.2 Acceptance Pilot in Oslo</b> .....	<b>26</b>
4.2.1 <i>Planning and Preparation</i> .....	<i>26</i>
4.2.2 <i>The 1st Acceptance Pilot (3 days in Oslo)</i> .....	<i>27</i>
4.2.3 <i>AP in Oslo: Who</i> .....	<i>27</i>
4.2.4 <i>AP in Oslo: What</i> .....	<i>28</i>
<b>4.3 Acceptance Pilot in Padova</b> .....	<b>29</b>
4.3.1 <i>Planning and Preparation</i> .....	<i>30</i>
4.3.2 <i>The 2nd Acceptance Pilot – 3 days in Padova</i> .....	<i>31</i>
4.3.3 <i>AP in Padova: Who</i> .....	<i>31</i>
4.3.4 <i>AP in Padova: What</i> .....	<i>32</i>
<b>4.4 Acceptance Pilot – Tools tested</b> .....	<b>33</b>
4.4.1 <i>BRD – Biochemical Risk Detection</i> .....	<i>33</i>
4.4.2 <i>CTI – Cyber Threat Intelligence</i> .....	<i>35</i>
4.4.3 <i>BAS – Breach &amp; Attack Simulation</i> .....	<i>36</i>
4.4.4 <i>CTM – Cyber Threat Management</i> .....	<i>36</i>
4.4.5 <i>WD – Weapon Detection</i> .....	<i>37</i>
4.4.6 <i>HCI – Human Computer Interaction</i> .....	<i>38</i>
4.4.7 <i>PTRO – Physical Threat Response Optimization</i> .....	<i>41</i>
4.4.8 <i>PTI – Physical Threat Intelligence</i> .....	<i>43</i>
4.4.9 <i>SMD – Social Media Detection</i> .....	<i>49</i>
4.4.10 <i>IMPETUS Platform</i> .....	<i>51</i>
<b>5 Results and Feedback Analysis</b> .....	<b>53</b>
<b>5.1 Feedback from the field (debriefs with end users)</b> .....	<b>53</b>
5.1.1 <i>Internal on-line survey - Partners who attended the APs</i> .....	<i>64</i>
5.1.2 <i>Inputs from people not completely involved – volunteers and local stakeholders</i> .....	<i>65</i>



5.2	Lessons learned .....	67
6	Looking ahead.....	69
6.1	Next Steps .....	69
6.2	Open points.....	71
6.3	Opportunities to be considered/developed.....	72
6.4	Risks Analysis – for Live Exercises planning .....	72
7	APPENDIX A: surveys about APs .....	75
	Members of the IMPETUS Consortium.....	76



## List of Figures

Figure 1 - The IMPETUS platform.....	17
Figure 2 - An example of dashboard made with snap4city - from the web page.....	18
Figure 3 - The Consortium evaluating the IMPETUS platform during Padova AP.....	20
Figure 4 - First version of the User Interface.....	20
Figure 5 - User Interface widget management.....	21
Figure 6 - SOC operator's dashboard, first version.....	22
Figure 7 - Possible configuration of the SOC operator's User Interface: side bar “mock-up”.....	22
Figure 8 - Side bar “mock-up” zoom.....	23
Figure 9 - Alarm pop-up, "mock-up".....	23
Figure 10 - Validation and feedback collection process.....	25
Figure 11 - Oslo City Hall, where Oslo AP took place.....	26
Figure 12 - HCI calibration in Oslo City Hall, before Oslo AP.....	27
Figure 13 - Borggården, outside Oslo City Hall. Location of WD and PTRO test.....	28
Figure 14 - Padova, Piazza dei Signori.....	29
Figure 15 - Simple dashboard designed for the AP. On left the ‘green alert’, on right the ‘red alert’.....	34
Figure 16 - Red alerts as snapshot for the AP. On left in Oslo, on right in Padova.....	38
Figure 17 - HCI devices.....	39
Figure 18 - Operator is using the WDT while the HCI Tool assessed hi workload in real-time.....	39
Figure 19 - Operator is wearing a brain computer interface.....	39
Figure 20 - HCI Tool generates alerts via IMPETUS Platform.....	40
Figure 21 - IT Dept SOC Operator performs calibration test.....	40
Figure 22 - CCTV SOC operator and supervisor interviewed on usability of HCI tool.....	40
Figure 23 - left: CCTV SOC operators simultaneously assessed; right: calibration test.....	41
Figure 24 - left: CCTV SOC operator interacting with PTRO tool while his workload is assessed in real-time; right: explaining the HCI tool dashboard to CCTV SOC operator.....	41
Figure 25 - Location of the considered stations in the city of Oslo.....	44
Figure 26 - Concentrations per hour of NO, NOx and NO <sub>2</sub> pollutants during Oct 2021, from Hjortnes station.....	45
Figure 27 - Concentrations per hour of PM10 and PM2.5 pollutants during Oct 2021, from Hjortnes station.....	45
Figure 28 - Concentrations per hour of PM1 pollutant during Oct 2021, from Loallmenningen station.....	46
Figure 29 - Concentrations per hour of PM1 pollutant during Oct 2021, from Loallmenningen station.....	46
Figure 30 - Concentrations per hour of NO, NO <sub>2</sub> , PM10 and PM2.5 pollutants during Oct 2021, from Loallmenningen station.....	46
Figure 31 - Concentrations per hour of PM10 and PM2.5 pollutants during Oct 2021, from Spikersuppa station.....	47
Figure 32 - Daily vehicle transits with direction “UNKNOWN”, “LEAVING” and “APPROACHING” during December 1, 2021, in the street “Ponte 4 Martiri vs Padova centro”.....	47
Figure 33 - Daily vehicle transits with direction “UNKNOWN”, “LEAVING” and “APPROACHING” during December 1, 2021, in the street “Sito 1 – via Plebiscito”.....	48
Figure 34 - Simulated daily vehicle transits with direction “UNKNOWN”, “LEAVING” and “APPROACHING” during December 1, 2021, in the street “Rotonda Grassi – Maroncelli corsia sinistra vs Grassi/Friburgo”.....	48
Figure 35 - Mention of "Kongsberg" in Norwegian and English.....	49
Figure 36 - Top Entities.....	49
Figure 37 - Relevant concepts, in Norwegian.....	50
Figure 38 - Sentiment and hate speech detected.....	50
Figure 39 - Padova AP, some results of last day survey.....	65
Figure 40 - Many people would like knives detection.....	66
Figure 41 - Improvement areas.....	66



# List of Tables

Table 1: List of Abbreviations .....	8
Table 2: List of Definitions .....	9
Table 3: Operability - from validation criteria to APs guidelines for observations .....	14
Table 4: Usability - from validation criteria to APs guidelines for observations.....	15
Table 5: End-user training dates ahead of OSL AP .....	27
Table 6: Oslo AP, days overview.....	28
Table 7: Tests summary (adding details in 4.1) .....	29
Table 8: From Oslo to Padova .....	30
Table 9: meetings with the end users to prepare Padova AP .....	31
Table 10: Padova AP, days overview .....	32
Table 11: Tests summary (adding details in 4.1) .....	32
Table 12: Feedback and suggestions from end users and operators.....	55
Table 13: D1.2 Requirements addressed.....	61
Table 14: Results from internal on-line survey.....	64
Table 15: Next steps summary .....	69
Table 16: Open points summary .....	71
Table 17: Risks analysis summary .....	72
Table 18: whole list of questions asked after the APs.....	75



# List of Abbreviations

**Table 1: List of Abbreviations**

<b>Abbreviation</b>	<b>Explanation</b>
AP	Acceptance Pilot
LEv/LEx	Live Events/Exercises
BAS	Breach & Attack Simulation
BRD	Biological Risk Detection
CTI	Cyber Threats Intelligence
CTM	Cyber Threats Mapping
HCI	Human Computer Interaction
HMT	Human Machine Teaming
PTI	Physical Threat Intelligence
PTRO	Physical Threat Response Optimization
SMD	Social Media Detection
WD	Weapon Detection
SOC	Security Operation Centre



## List of Definitions

**Table 2: List of Definitions**

<b>Term</b>	<b>Definition/explanation</b>
Acceptance Pilot	The development of a series of dry tests based on use case scenarios designed to validate the performance and the security of tools and platform
Exercise	The development of live tests based on a scenario, designed to evaluate the usability of the platform's tools and interface, as well as impact of the solutions on the performance of security and emergency organisations
Test	A procedure for critical evaluation; in this context a means of determining the quality, and the technological readiness level of tools and platform
Simulation	A realistic imitation of a situation that may occur in reality
End user	An operator working in SOCs or in offices that will be involve in the use of Impetus tools
Stakeholder	Any individual or organisation that may be affected (positively or negatively) by an initiative or a project as a whole.
Technical Provider (or Technical Partner)	Those partners, within the Consortium, whose role is to develop a technical tool. The platform, in this case, must be considered as a technical tool as well.



# 1 About this deliverable

## 1.1 Intended readership/users

D 7.2 will provide an overview of what happened before and during the Acceptance Pilots in Oslo and Padova and, moreover, feedback collected on the field (mainly from the end users) and the following analyses made by the Partners involved with the other stakeholders.

So, with this kind of information (coming from feedback and analyses), the main aim of this document is to define the “route” (the right direction) the Consortium should follow for the actual usefulness and usability of the platform and its tools (without spending time and effort in developing non-reliable, non-effective, non-meaningful things).

The realisation from idea to practice may, often, highlight some difficulties, as well as some opportunities, that are not clear in the first- not on field- phases of the development.

This is the reason why primarily the project Partners may want to read this deliverable, in order to direct their efforts in the right direction. In particular:

- **Cities** expect a platform and some tools that will make the end users job easier and more precise, providing them real time information and analysis of the on-going events. In this document, they can find the results of their evaluation, and they will better understand the contribution they can provide for the final validation.
- **Technical Partners** will be able to define improvement areas, clarify open points and take some critical decisions about how to go on developing.
- **COSSEC members**, given their interest and involvement in security management, will have the chance to follow the development providing their contribution from different points of view, including the deployment of the technologies, the development of new work processes and the ethical implications of the planned changes.
- **Other stakeholders** will have the opportunity to get concrete evidence of what has been developed already and get feedback about the usage of tools, the potential of those new technologies the project has its focus on, the next steps the Partners will undertake and the possible impact that the outcomes of the project could have on operative processes.

## 1.2 Why would I want to read this deliverable?

The Readers will have a clear picture of the progress of works the Consortium Partners undertook till the Acceptance Pilots and, especially, about next steps, missing parts, features and details that need to be modified and improved concerning the IMPETUS platform and the IMPETUS tools.

The main contribution related to this purpose comes directly from the end users that tested the platform and the tools. Other significant feedbacks have been collected from a group of “observers” composed of different other stakeholders as non-technical Partners, COSSEC members, local Authorities and volunteers that helped the Consortium simulate Citizens’ behaviours and their reactions to the scenarios and events drafted to “challenge” the platform and the tools at this stage of the project timeline.

The Reader will also be able to appreciate the progresses made between the two Acceptance Pilots: even if the cities, as mentioned in several other documents, have different characteristics and needs in terms of security in public spaces and considering also difficulties and limitations related to the still ongoing pandemic, the Consortium Partners have demonstrated to be able to work as a team keeping the focus on the Project objectives.

## 1.3 Structure

As already said, this document summarise what has been undertaken in the APs and what emerged in terms of feedback and considerations to be considered both for further developments and for Live Exercise planning.



The document is structured as follows:

- **Chapter 2:** it contextualizes the Acceptance Pilots as a mid-term step of the validation process. It explains how the Validation Plan (D7.1) has been considered the reference for the evaluation activities, considering that the works are in progress.
- **Chapter 3:** it provides an overview related to the platform development status: what is almost ready (and what is still missing) concerning the back-end, the front-end (i.e. the User Interface) and some consideration related to its cybersecurity;
- **Chapter 4:** it is related to the Acceptance Pilots, two “rings of the same validation chain”: there, objectives, preparation, implementation and Partners’ considerations for every tool have been reported;
- **Chapter 5:** in this chapter the feedback and the contributions collected by different stakeholders have been reported, in particular of course the end users’ point of view;
- **Chapter 6:** it groups all the considerations useful for the second part of the project development: lessons learned, open points, risks to be considered in Live Exercises planning.

#### 1.4 Other deliverables that may be of interest

As D7.2 is related to the Acceptance Pilots, several Deliverables should be considered of interest, in particular:

- D7.1, for the methodology and the practical aspects concerning validation;
- D1.1, for information related to the Cities where the Acceptance Pilots have taken place;
- D1.2 to understand requirements and to have a clear idea of what and why has been tested;
- D2.1 to be aware of IMPETUS platform’s features and its state of development;
- D3.1 to be aware of IMPETUS tools’ features and their state of development;
- all D11s because every test, trial, exercise has to be undertaken with the right awareness of the Ethics principles and constraints on which the project is based.

#### 1.5 Synergy with other projects/initiatives

Currently, no synergy; but during the AP in Padova the IMPETUS Consortium met a representative of FASTER Project (<https://www.faster-project.eu/>) and some similarities raised: it, like IMPETUS, addresses the challenges associated with emergency response and the enhancement of the first responders capabilities.



## 2 The Acceptance Pilots – 1<sup>st</sup> part of the Validation process

The Validation process includes all the activities aimed to evaluate the expected project's outputs: the IMPETUS platform and the Practitioner's guides related to Ethical, Operational and Cyber Security frameworks.

The APs have been planned to be a fundamental part of this process: at a mid-term of the duration of the project, according to tasks T7.2 and 7.4, the Consortium have been called to undertake some initial tests to assess what has been achieved.

The reference for the evaluation and validation activities was and is "D7.1 Validation Plan".

According to D7.1, there are four categories of validation criteria, related to:

- The Applicability of the IMPETUS Ethical framework
- Effectiveness of the IMPETUS Cyber security framework
- The Impact of the IMPETUS Operational framework
- The Usability of the IMPETUS platform & its tools

Because of the status of relative maturity of the IMPETUS Platform, the tools and the Practitioner's guides, not all the validation criteria have been considered as applicable for the tests. The same can be said for the requirements collected in "D1.2 Requirements for public safety solutions": only a limited number of them has been fully satisfied, at this stage. The largest part has been approached, some others have been considered to be updated or finetuned.

For this reasons, the main focus of APs has been on the usability and operability of the platform and the tools. The Practitioner's guides based on the frameworks listed above have not been validated because they are still in their development path; the APs have, however, been the occasion to verify if the chosen approach of the Practitioner's guides was correct.

In the following sub-section, the Reader will find some details related to the approach considered, in agreement with the D7.1 Validation Plan's categories listed above.

### 2.1 Applicability of the Ethical framework

According to the Validation Plan, the IMPETUS Platform has to be ensured as a Trustworthy platform, in particular for what concerns Artificial Intelligence. Seven key "macro" requirements have to be, indeed, considered:

(1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) environmental and societal well-being and (7) accountability.

In terms of approach, points (4), (5), (6) and (7) are definitely part of the IMPETUS Consortium's "DNA". They are so deeply rooted in every Partner that are "present in the air" during all the meetings (in particular, before and during the APs) and come out also in every other deliverable already completed. This to underline that it has been more efficient to focus on other topics to be assessed during the APs. It will be an easy task during the Live Exercises, when the Trustworthy Platform will be completed.

Privacy and data governance, point (3), has been central during the preparation phase before the APs and involved all the Partners, not only the Cities. The outcomes of this strong attention have been for instance that only Volunteers who signed an informed consent were involved, data collected and elaborated during APs were only aggregated numbers not referring to people. When some doubt raised, the Consortium chose to avoid the risk completely, finding a different path: e.g. Cinedit, because of Covid restrictions, could not get to Padova AP and the tests related to the WD tool have been undertaken remotely. To avoid any issues related to share real data remotely, some synthetic data were used (thanks to Cinedit problem-solving capability, as the Reader will found in Chapter 4, sub-section 4.4.5).

Point (2), technical robustness and safety, has been the topic of many discussions during the development activities and is also going to be deepened in D6.3. At the moment, it is not possible to validate it. Of course,



the developers have been paying the maximum attention to not harm, to implement something that can be 360 degrees safe for all the stakeholders, in particular for the end user, for the municipality's systems, for the citizens.

Point (1), human agency and oversight, has been hence the one mostly assessed. This mainly because of the possibility of a direct alignment between the developers and the end users. In terms of the approach, no need to verify the respect of Fundamental Rights: same considerations anticipated for (4), (5), (6) and (7).

Indeed, the focus of the APs concerning this point, has been on the human-in-the loop approach. The end users who took part to the APs have been always considered the "centre" of all the tools. The IMPETUS Platform will automatically provide some adding alarms, that currently cannot be detected at all (e.g. because during the night citizens usually do not notify the police a danger because they are sleeping), but the "last word" in handling with them will always belong to the end users (operators and supervisors).

Working together made possible to fine-tune those control mechanisms that let the Platform to detect some issue automatically, but keep strongly in the hands of the operators the responsibility to confirm that the detected issue is actually an alarm, and to decide the consequent reaction to this alarm.

## 2.2 Effectiveness of the IMPETUS Cyber security framework

Cyber-security of the Platform is likely the last thing that can be fully assessed.

But in terms of the approach, after the Oslo AP became clearer that the SOC operators would have not been the right end users for the cybers-security tools and to validate the IMPETUS Platform cyber-security.

Hence, to prepare the Padova AP IT dept specialists have been more involved: in addition to the introductory meetings related to the cyber-security tools, some initial concepts related to Security Culture have been shared. Topics as Attitudes, Cognition, Behavior, Communication, Norms, Responsibility and Compliance were discussed together, even in an informal way: the risk to make the month between Oslo AP and Padova AP too heavy for these people was high. This choice turned out to be correct: the IT specialists during the interviews made during and after the tests provided positive feedback and the right level of engagement has emerged.

## 2.3 Impact of the IMPETUS Operational framework

Waiting for the practitioners' guide, some practical actions have been undertaken.

For instance, to try to evaluate the impact of the IMPETUS tools in terms of operative improvement, during the Padova AP, the same dangerous situation has been simulated twice: during the first round the SOC operators were called to block a person holding a gun in the square without the IMPETUS Weapon Detection tool; in the second round, with the WD tool.

### **Without IMPETUS WD tool**

Before notifying the Local Police patrols present in the square to block the man with the gun, the SOC operators:

- should have waited to receive a phone call from the volunteers acting as "unaware" citizens,
- should have tried to understand the description of the danger and of the person with the gun,
- then via radio he/she should have involved colleagues of the patrols,
- should have transmit what he/she had understood from the phone call regarding the person with the gun

Then the policeman of the patrol should have arrested the man with gun.

Only a small number of the 80 volunteers in the square called the Local Police to notify about the man with the gun. The description of the person was not precise, so the SOC operator took several minutes to understand and to forward the information to the colleagues. The time planned for the test was not enough, the dangerous person was not arrested.

### **With the WD tool**

The detection of the gun has been simulated with synthetic data (so there was a virtual man holding the gun in the square).



The SOC operator was able to confirm that the object detected was a gun (virtual but realistic) and in a few seconds he was able to send a jpeg picture of the man to the colleagues on the field.

So, in a very short time, all the patrols in the square were perfectly aware about the characteristics of the person to be arrested.

Without IMPETUS the gun issue has not been solved (considering the time dedicated), because of so many steps to be undertaken by several different people. With IMPETUS, instead, with only a couple of clicks (so very quickly) the man with the gun had been arrested.

Table 3 reports the validation criteria related to operability and how they have been used as guidelines for observations in the Acceptance Pilots.

**Table 3: Operability - from validation criteria to APs guidelines for observations**

<b>OPERABILITY - Validation Plan criteria</b>		<b>Acceptance Pilots – Guidelines for observations</b>
<b>Criterion ID</b>	<b>Criteria</b>	
PP-EVAL-26. Operational framework, organisational awareness	The operational framework considers if actors have a clear understanding of roles and responsibilities in own and other organisations involved in security management	According to the scope of the Acceptance Pilots, these Operability Criteria have been clustered in: <ul style="list-style-type: none"> <li>• <i>Roles and Responsibilities.</i></li> </ul> Furthermore, the heuristic validation questions have been simplified and used as trigger questions during the debriefings with the operators.
PP-EVAL-35. Operational framework, alternative work methods	The operational framework considers how organisations support the development and maintenance of alternative working methods	
PP-EVAL-28. Operational framework, adapt plans	The operational framework considers the organisations' conditions for adapting plans and procedures during crises and other events that challenge normal plans and procedures	According to the scope of the Acceptance Pilots, these Operability Criteria have been clustered in: <ul style="list-style-type: none"> <li>• <i>Deal with alerts.</i></li> </ul> Furthermore, the heuristic validation questions have been simplified and used as trigger questions during the debriefings with the operators
PP-EVAL-29. Operational framework, resource handling	The operational framework considers how organisations manage available resources effectively to handle changing demands	
PP-EVAL-36. Operational framework, noticing brittleness	The operational framework considers how organisations notice their system performance decline when the system reaches its boundary conditions	
PP-EVAL-24. Operational framework, common ground	The operational framework considers how organisations create common ground for cross-organisational collaboration in security management	According to the scope of the Acceptance Pilots, these Operability Criteria have been clustered in: <ul style="list-style-type: none"> <li>• <i>Interoperability.</i></li> </ul> Furthermore, the heuristic validation questions have been simplified and used as trigger questions during the debriefings with the operators
PP-EVAL-25. Operational framework, networks	The operational framework considers how organisations establish networks for promoting inter-organisational collaboration in security management	



PP-EVAL-32. Operational framework, policy management	The operational framework considers if organisations engage in systematic management of policies (involving policy-makers and operational personnel) for dealing with emergencies and disruptions	These criteria have not been investigated because no unexpected events as well as topics related to resilience (i.e. sources of or community resilience) have been simulated in the Acceptance Pilots. These might be addressed in the Live Exercises and described in "D6.3 – Operational framework – concepts of operations"
PP-EVAL-27. Operational framework, adaptive capacity	The operational framework considers the capacity of the organisation to adapt to both expected and unexpected events	
PP-EVAL-30. Operational framework, community resilience	The operational framework considers whether organisations take into account community resilience to understand and develop their capacity to manage security events	
PP-EVAL-31. Operational framework, learning	The operational framework considers whether organisations identify sources of resilience in order to learn from what goes well	
PP-EVAL-33. Operational framework, communication strategies	The operational framework considers how organisations use communication strategies for interacting with the public	
PP-EVAL-34. Operational framework, public involvement	The operational framework considers how organisations increase the public's involvement in resilience management	

## 2.4 The Usability of the IMPETUS platform & its tools

As anticipated, assessing the Usability has been the main target of the Acceptance Pilots. In the following chapters the Reader will find several information and feedback about how works have been going on.

As for Operability, here below in Table 4 validation criteria and their respective guidelines used during the collection of feedback.

**Table 4: Usability - from validation criteria to APs guidelines for observations**

USABILITY - Validation Plan criteria		Acceptance Pilots – Guidelines for observations
Criterion ID	Criteria	
PP-EVAL-01. Suitability for the task	The IMPETUS platform/tools are suitable for the task when supporting the user in completion of the task.	According to the scope of the Acceptance Pilots, these Usability Criteria have been clustered in: <ul style="list-style-type: none"> <li>• <i>Perceived usefulness.</i></li> </ul>
PP-EVAL-03. Conformity with user expectations	The IMPETUS platform/tools conform with the user expectations if it corresponds to predictable contextual needs of the user and to commonly accepted conventions.	Furthermore, the heuristic validation questions have been simplified and used as trigger questions during the debriefings with the operators.
PP-EVAL-02. Self-descriptiveness	The IMPETUS platform/tools interactions with the user are self-descriptive.	According to the scope of the Acceptance Pilots, these Usability Criteria have been clustered in:



PP-EVAL-04. Suitability for learning	The IMPETUS platform/tools are suitable for learning when it supports and guides the user in learning to use the system.	<ul style="list-style-type: none"><li>• <i>Overall impression of the tool.</i></li></ul> Furthermore, the heuristic validation questions have been simplified and used as trigger questions during the debriefings with the operators.
PP-EVAL-05. Controllability	The IMPETUS platform/tools enables the user to initiate and control the direction and pace of the interaction until the point at which the goal has been met.	
PP-EVAL-07. Suitability for individualization	The IMPETUS platform/tools enables the user to modify interaction and presentation of information to suit their individual capabilities and needs.	
PP-EVAL-06. Error tolerance	The IMPETUS platform/tools supports the user with error control (damage control), error correction, or error management, to cope with the errors that occur.	This criterion has not been investigated because no degraded modes have been simulated in the Acceptance Pilots. This might be addressed in the Live Exercises and described in "D6.3 – Operational framework – concepts of operations"

### 3 (First) Evaluation of the IMPETUS Platform

One of the main objects of the project is to develop and make actually usable by different end users (not only SOC operators) a platform aimed to improve their effectiveness during their daily activities related to public space security.

The IMPETUS platform has to be considered a kind of “virtual box” that in the front-end allows different end users to interact with the Partners’ tools via dedicated User Interfaces, while in the back-end it collects all the information elaborated by Partners’ tools, starting from data coming from the technical equipment (sensors, CCTVs, database, etc.) installed in the cities where the Platform has been installed.

Figure 1 shows the concept behind the IMPETUS platform.

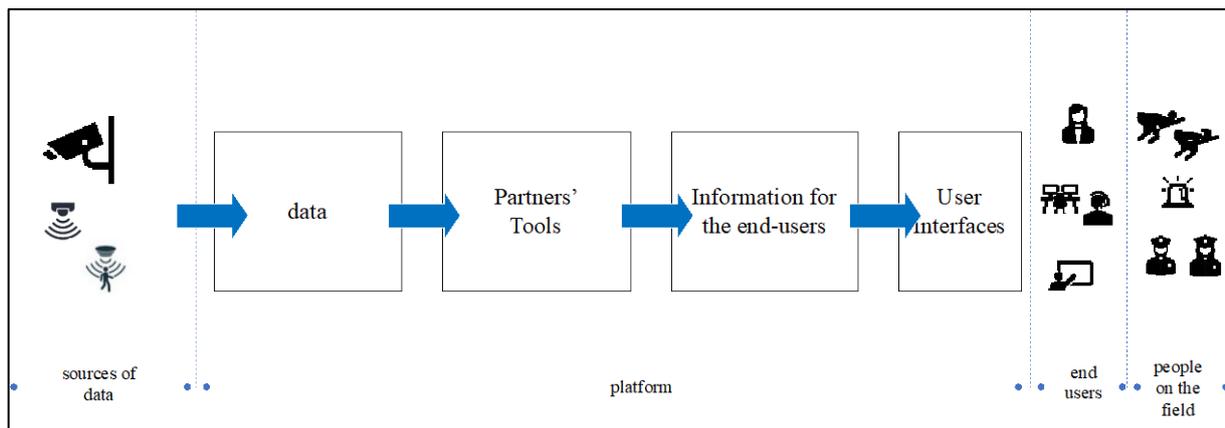


Figure 1 - The IMPETUS platform

Unlike the largest part of the Partners’ tools, the IMPETUS platform is a completely new (software) object. The Consortium has been designing it: the collected requirements and the reference architecture are described in D1.2 and D2.1. The implementation is of course a long path and several continuous inputs coming from all the stakeholders have to be kept in account, almost every day.

At mid-term of the project, as it is easily understandable, several things have still to be defined, some have been implemented, and some instead only require fine-tuning.

Of course, the main effort of the first part of the platform development has been dedicated to the back-end, so to study how to create the “container” of the Partners’ tools, how to collect the data they need from heterogeneous sources and how (and if) this platform could be integrated in the municipalities’ infrastructures and networks. The “engine” of the platform is almost ready.

The front-end, so the interface the end users will see and by which they will interact with the back-end, has to be carefully implemented: it is one of the key-points for the actual adoption/usage of the whole IMPETUS project from the end users.

Better, hence, to involve – the deeper the better – end users. This involvement has started to be effective during the Acceptance Pilots.

Here below, the Reader can understand the status of the platform, in terms of back-end, front-end and cybersecurity.

#### 3.1 Back-end

In a technological application, typically, the back-end is not easy to be evaluated by end users because usually they have limited knowledge of the technical aspects. So, the tests related to the back-end have been undertaken within the Consortium. These tests, aimed to verify the compliance with what is stated in D1.2 and D2.1, confirmed that Platform is:



- Modular
- Interoperable
- Open & Extensible
- Future proofed
- Compliant with IoT & Cloud computing approaches

Where:

<b>Modular</b>	The platform is designed to be the merge of modules. Every module is able to undertake its own operations and activities; they are kept completely separate to be able to run independently (and potentially be swapped out /replaced by other modules if with the evolution of the platform something different or new will arise)
<b>Interoperable</b>	The platform is based on a common data format for data exchange between modules
<b>Open &amp; Extensible</b>	The platform counts on a set of <i>Application Programming Interfaces</i> (APIs), which can be used by third-party developers to add new functionalities to the solution without requiring a major re-design
<b>Future proofed</b>	This derives from the modularity of the platform and from the fact it is open and extensible. This allows to add integrate new modules built on new technologies or to upgrade existing modules in order to keep up with advances in areas they cover.
<b>Compliant with IoT &amp; Cloud computing approaches</b>	Such approach will reduce risks associated with excessive centralisation of large amounts of smart city data

During the requirements definition process some main capabilities have been considered as essential and critical. To fulfill critical and complex topics, the App builder **Snap4City** has been chosen as the technical “foundation” on which to base the IMPETUS platform. Snap4City platform is open source and implements important functionalities that support data integration in various formats, data visualisation and alerting (see D2.1 and [www.snap4city.org](http://www.snap4city.org)). An example of snap4city’s potential is represented in Figure 2.

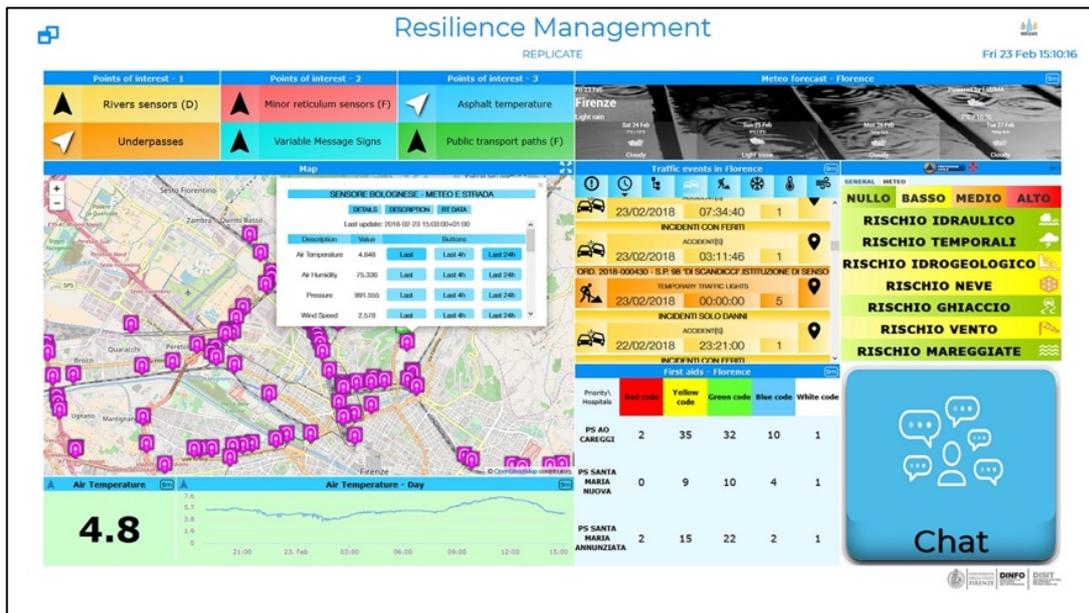


Figure 2 - An example of dashboard made with snap4city - from the web page



What therefore have been implemented is:

- Access Control
- Alerting
- Internal Integration
- Security
- External Integration

Where:

<b>Access Control</b>	<ul style="list-style-type: none"> <li>• <u>Access rights based on roles</u>: within the platform users have associated roles, which allow access only to certain features</li> <li>• <u>Access control policies</u>: who can access information, where and when</li> <li>• <u>Simultaneous users connected</u>: the platform allows the connection of simultaneous users.</li> </ul>
<b>Alerting</b>	<ul style="list-style-type: none"> <li>• <u>Alert centralisation</u>: the platform centralises the alerts produced by the integrated tools</li> <li>• <u>Alerts priority</u>: the alerts have different levels of attention</li> </ul>
<b>Internal Integration</b>	<ul style="list-style-type: none"> <li>• <u>Tools integrated</u>: the platform is modular, individual tools can be added or removed without disturbing the functionality of the platform</li> <li>• <u>Data integration</u>: tool's output is centralised at platform level</li> <li>• <u>Data enrichment</u>: outputs of the tools are combined in order to derive new information or to raise the alert confidence level. This will be done at platform level, through a set of rules.</li> <li>• <u>Standardised communication</u>: data of the tools will respect platform defined format in order to ensure interoperability</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>• <u>Best practices</u>: <ul style="list-style-type: none"> <li>○ Up to date software</li> <li>○ User training and security awareness</li> <li>○ Data protection in transit and storage</li> </ul> </li> </ul> <p><u>Vulnerability assessment</u></p>
<b>External Integration</b>	<ul style="list-style-type: none"> <li>• <u>Sharing of information</u>: sharing information to users from organisations which are not part of the IMPETUS operating environment.</li> <li>• <u>Alerts for different operators</u>: IMPETUS Platform will provide alerts for different operators across different organisations.</li> <li>• <u>Interaction with existing devices and platforms</u>: the IMPETUS platform interacts with existing devices and platforms in the cities.</li> </ul>

### 3.2 Front-end: evaluation of the initial interface

Typically, when a non-technical end user starts adopting new software, his/her first impression is strictly connected to the User Interface: even if the back-end part is perfectly working and the software is extremely powerful, if the User Interface is not well designed or not “comfortable” enough, in a word it is not “user-friendly”, as said above, the risk that the software could not be adopted at all is high.

In addition, one of the main strategic objectives of the project is to help and support the end user to be quicker and more effective dealing with security operations, both in standard situations and exceptional ones.

There are 2 levels of development activities that have to be implemented to let the end users feel comfortable with the platform: one more technical, the other related to usability.



Figure 3 - The Consortium evaluating the IMPETUS platform during Padova AP

### 3.2.1 User interface – technical aspects

The first level is, as said, more technical: the developer has to let every end user “understand”, so the IMPETUS platform is:

- available in multiple languages (e.g., English, Norwegian and Italian);
- able to provide aggregated information and diagrams for strategic monitoring and planning;
- able to adopt a “common” (widely spread) terminology and symbology;
- able to support different forms of interaction depending on the situation and user profile.

These elements of the front-end usually are managed by end users’ administrator who will customize the real User Interface for the end user. An example is shown in Figure 4, here below.

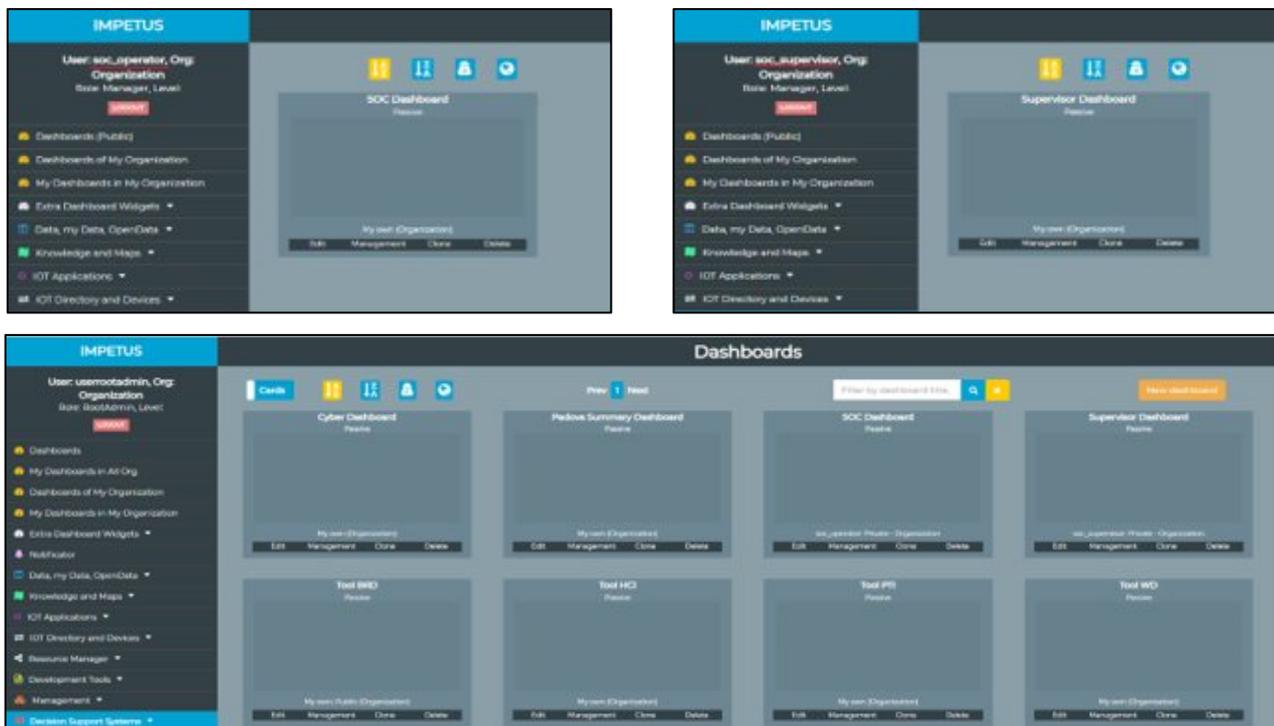


Figure 4 - First version of the User Interface

To manage this technical level of the front-end has been implemented the Dashboard Builder.

It allows to:

- “create” a dashboard based on widgets (that are graphical components that make easier the interaction with the platform)
- control size and zoom of the widgets of the dashboard;
- set and change parameters as: size, the colour of the background, font of the header, the colour of the header, etc.
- compose a set of possible views, by visual interaction, visual composition of widgets;
- allow each single dashboard to be viewed/accessed in “reading mode” by different end users;
- show graphics by using several different kinds of visual paradigms, and parameters.

An example of the widget management interface is in Figure 5.

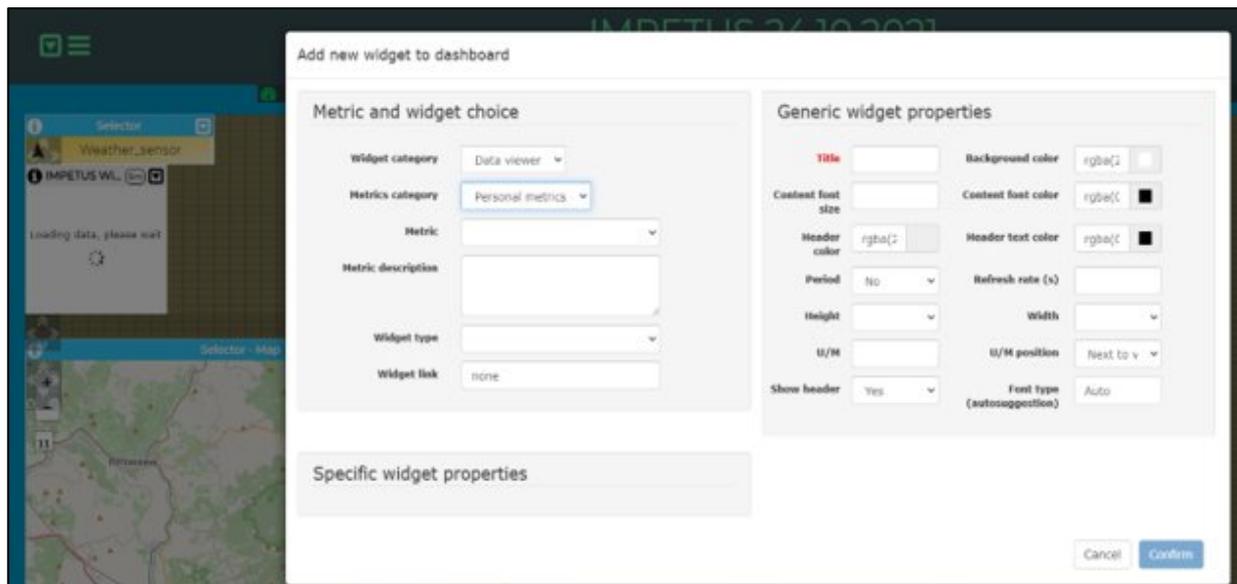


Figure 5 - User Interface widget management

The possible widgets to be used are:

- graphics widgets to present different kinds of information (e.g. alerts received from tools);
- actuator widgets to collect data from authenticated users (e.g. text box, selection box);
- interactive widgets to manipulate data on the dashboard only (e.g. buttons, selectors of events, etc.) and for cross widget interaction (e.g. data drill down).

### 3.2.2 User interface – usability

The second level of the User Interface development is related to the actual usage of the dashboard, according to what the end user has to do in his/her daily activity.

For instance, the SOC operator has to react very quickly to the inputs he/she receives: no time to open several windows or to read long text when alarm occurs.

The very first version of the dashboard thought for the SOC operator has to be revised/refined with, of course, the continuous interaction with the end users (in Figure 6 how it currently looks like).

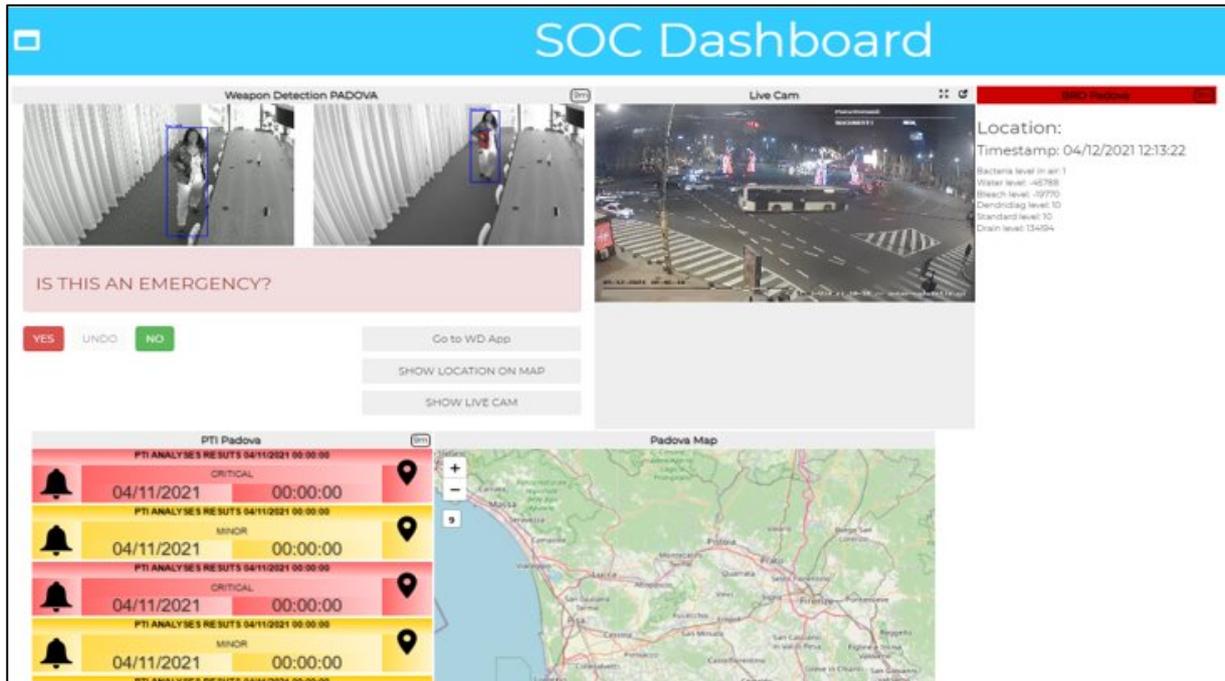


Figure 6 - SOC operator's dashboard, first version

During the APs, in fact, it became clearer how the SOC operators are used to work and which could be the right approach to configure their User Interface, their dashboard.

Indeed, they have to handle with several monitors where different applications are simultaneously displayed and the IMPETUS one cannot be too invasive and “bother” them.

Hence, a possible approach to present information coming from the Partners’ tool could be a kind of “customizable” sidebar that can include what is useful to “keep an eye” on.

In Figure 7 and Figure 8 there are some “mock-ups” the Consortium has been working on:

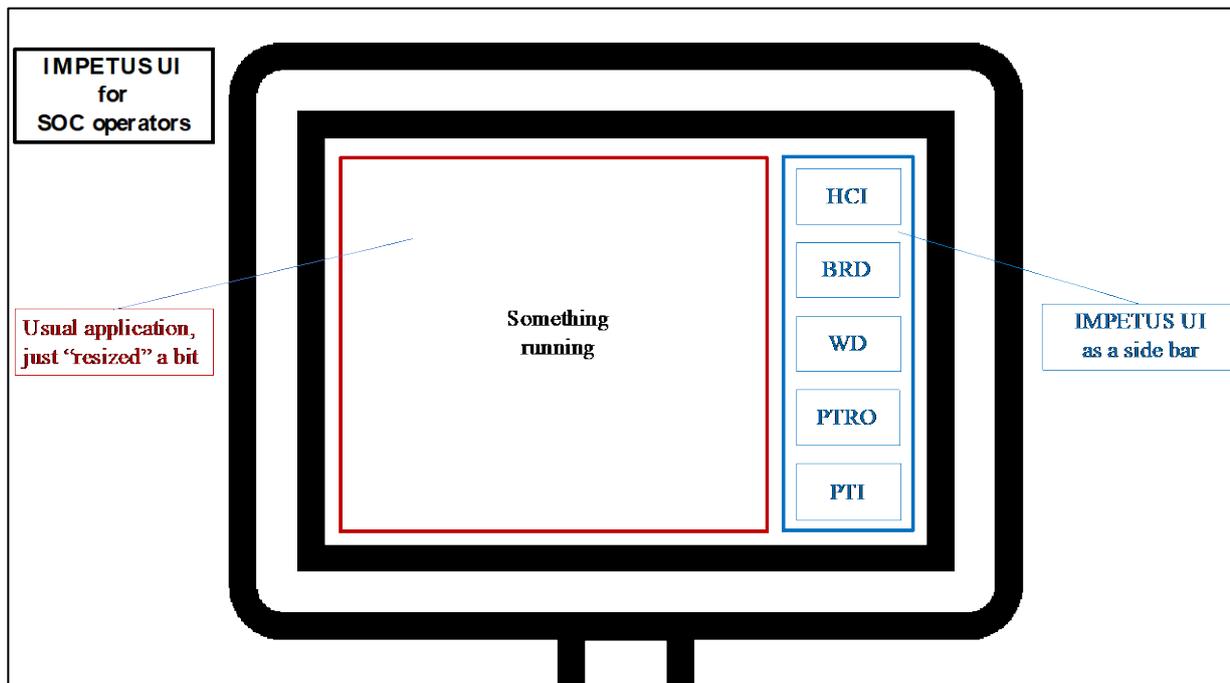


Figure 7 - Possible configuration of the SOC operator's User Interface: side bar “mock-up”

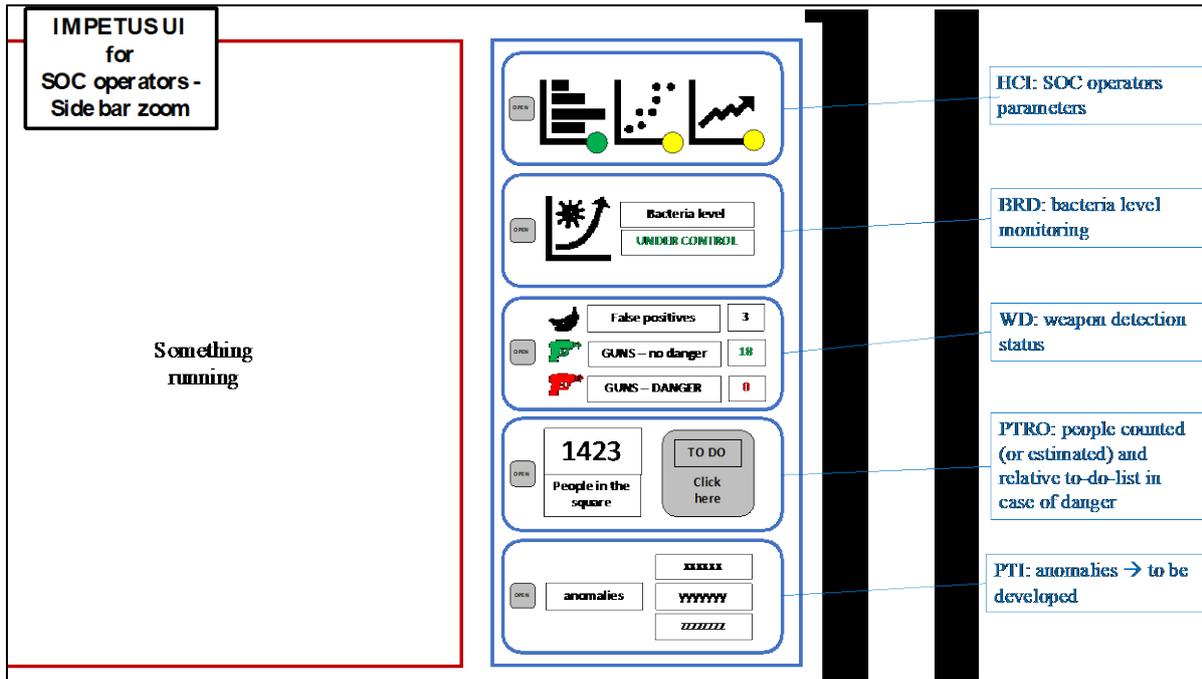


Figure 8 - Side bar “mock-up” zoom

When an alarm occurs, instead, a popup and a specific sound could interrupt the operator’s work, require his/her attention and propose a quick way to take action (Figure 9).



Figure 9 - Alarm pop-up, "mock-up"

Other kind of end users need different information and modalities to interact with the Partners’ tool. This topic will be part of the second development phase, before the Live Exercises.

### 3.3 Platform cybersecurity

The cybersecurity of the IMPETUS platform is a critical issue for any adoption from the cities: using the platform, the security of the local IT infrastructures and networks must not be affected.



It is still not time to fully test these aspects of the platform, but some specific choices to guarantee a safe usage of the platform have already been implemented:

- the platform implements a role-based access: The users have certain roles that will allow them to access specific functionalities of the platform. For example, SOC operators can access the SOC dashboard and not SOC supervisor's one;
- changes to the platform are permitted only to users with administrative roles;
- data minimisation and storage limitation: the platform will not store private data;
- data encryption at database level: if any private data is needed for platform processing, it will be stored encrypted in order to avoid privacy issues;
- encrypted communication: communications between components will be encrypted in order to minimize the risk of data leaking.
- minimize attack surface: the server hosting the platform will be protected by a firewall, only the ports needed for platform operations will be open.

## 4 First validation on the field

As mentioned above, this document provides information collected from the first validation on the field, in particular, concerning what has been achieved and developed at this intermediate stage of the project duration in terms of technological readiness level of the platform and the tools and their integration with the cities infrastructure, in addition to the involvement of the cities.

To improve the quality and the broadness of the feedback, 2 similar-but-different validation sessions have been conducted in Oslo (Norway) and Padova (Italy).

In this document, the reader will find details related to the Acceptance Pilots, the first of 3 iterative steps in the validation process of the project's results.

### 4.1 The Acceptance Pilots

The Acceptance Pilots (APs) are part of the validation process.

This means checking that the developed system meets users` needs and fulfils its intended purpose. The aim of the validation activities is to support the initial design and further development process of the IMPETUS platform.

The target group for validating the IMPETUS tools is the potential users.

The APs consist of a set of tests -undertaken in a limited and controlled environment- of realistic (but not real) situations, planned to challenge the current version of the IMPETUS platform and the Partners` tools. The objectives of these tests are manifold, in particular: (1) to provide feedback to the Technical Partners; (2) to inform the planning of subsequent validation exercises; and (3) to increase the stakeholders` awareness.

The APs took place in Oslo (2021, November 3-5) and Padova (2021, December 1-3).

In the following paragraphs, the Reader can find a summary of what has been implemented to get the most significant and valuable feedback to carry on the development and some useful considerations for Live Exercises planning.

The AP in Oslo was the first step in this feedback collection path, the AP in Padova has to be considered the “answer” to what emerged in Oslo in terms of issues and challenge, as shown in Figure 10 below.

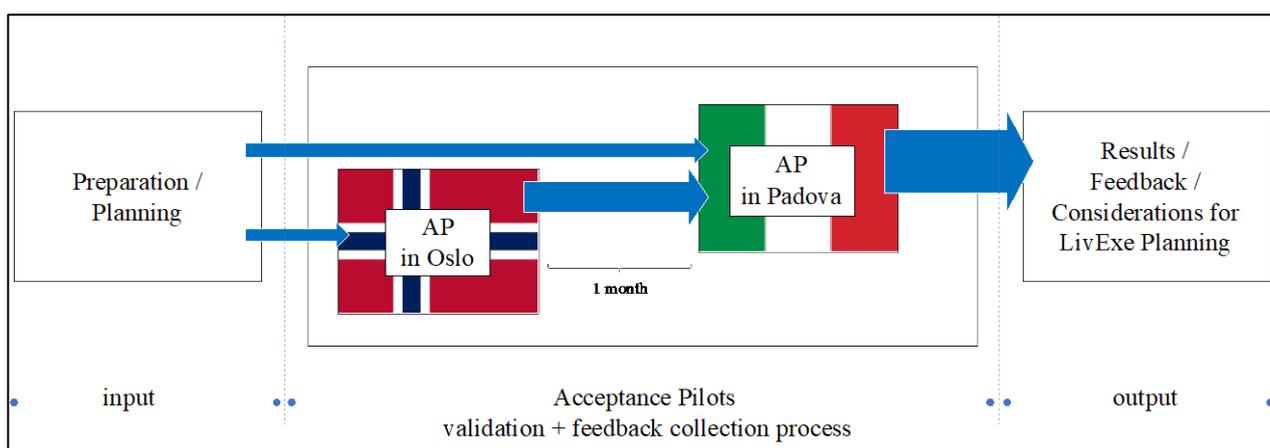


Figure 10 - Validation and feedback collection process

#### 4.1.1 Acceptance Pilots preparation

During the first months of the project CPAD and OSL prepared an analysis of their local contexts (D1.1). This was the starting point to understand the cities` most relevant needs, their current capability in terms of technical equipment and which were the most suitable use cases to test the tools and the overall IMPETUS platform. In



addition, these analyses highlighted which were the people to involve, in terms of local and external stakeholders.

The use cases outlined (in D1.1) were useful for the cities to decide the locations for the tests, the data to be shared with the technical Partners for their developments and the devices to be installed before the APs.

Since then, a continuous dialogue within the Consortium took place. Several collaborative actions have been undertaken and some important deliverables concerning how to start the development of the platform and the tools were finalized (in particular, D1.2 related to the requirements definition, D2.1 and D3.1 where platform and the tools were hypothesized, D7.1, where the validation criteria were planned). Furthermore, the ethic aspects have been addressed in WP11 deliverables (D11.1 – D11.7).

## 4.2 Acceptance Pilot in Oslo

**WHEN: 2021 November, 3<sup>rd</sup> - 5<sup>th</sup>**

**WHERE: Oslo, Norway - City Hall**



Figure 11 - Oslo City Hall, where Oslo AP took place

### 4.2.1 Planning and Preparation

The preliminary work started with the development of simple and locally meaningful use cases to evaluate the applicability and effectiveness of the solutions for different scenarios. End users and other stakeholders involved have been called to evaluate the contribution of the solutions in the scenarios identified within structured workshop sessions.

The **goals** for the AP in Oslo were:

1. Increase awareness and understanding of the scope and features of all tools included in the IMPETUS, as well as the overall platform architecture for both the Consortium and end-users.
2. Test tools in an operational environment, “in the field” (e.g. in the SOCs).
3. Validate all tools to some degree during the AP.
4. Collect first impressions from end-user on tools/platform usability and functionality.
5. Share feedback with the Consortium to further develop tools/platform.
6. Collect feedback from Consortium after the AP in order to reconsider the current status of development of tools/platform and improve planning for future acceptance pilots.

In the Oslo context, the City Hall Security with its related SOC has been identified as a potential end-user for the platform. To get an effective involvement and the best level of feedback, the SOC was hence included in the complete validation process: before, during and after the planned tests.

To get prepared and aligned, some activities have been undertaken before the actual AP in the City Hall:

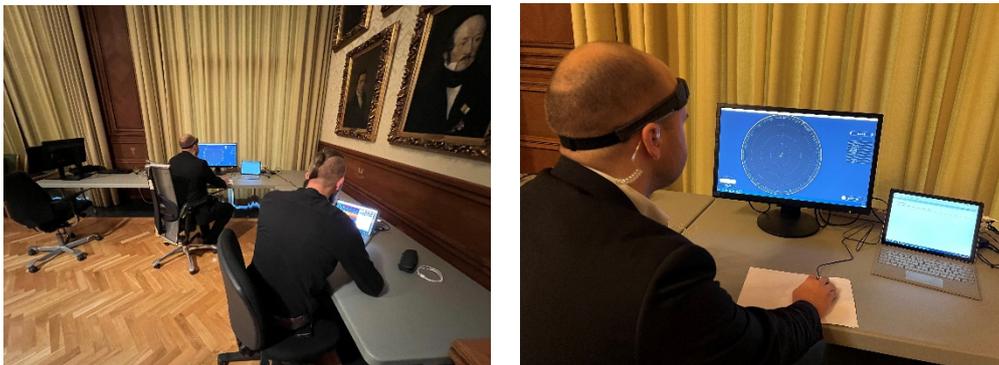


- weekly web meeting OSL + CPAD to plan the APs considering both the similarities and the different characteristics of the 2 cities;
- F2F web meetings with technical Partners to agree the activities related, e.g., trainings to be done, the kind of tests that could be effective and reliable, etc.; (e.g. in Table 5 are reported the training session planned)

**Table 5: End-user training dates ahead of OSL AP**

WHO	WHAT	WHEN
HCI-THALES	<ul style="list-style-type: none"> <li>• Hands on test</li> <li>• Calibration test</li> </ul>	13. October in OSL
PTI-CINI	<ul style="list-style-type: none"> <li>• Online presentation</li> </ul>	19 October 09:00-10:00
PTRO-UPAD	<ul style="list-style-type: none"> <li>• Online presentation</li> </ul>	19 October 10:00-11:00
BDR-UdN	<ul style="list-style-type: none"> <li>• Online video/ppt</li> </ul>	19 October 12:30-13:30
SMD-INSIKT	<ul style="list-style-type: none"> <li>• Video tutorial</li> <li>• Send end user manual</li> <li>• Q&amp;A</li> </ul>	19 October 14:00-15:00
BAS- XMCYBER	<ul style="list-style-type: none"> <li>• Align SOC/IT operator</li> </ul>	TBA
SIMAVI-PLATFORM	<ul style="list-style-type: none"> <li>• Online training</li> </ul>	27 October 09:00-11:00
WD-CINEDIT	<ul style="list-style-type: none"> <li>• Video tutorial</li> </ul>	27 October 12:00-13:00

- Thales’ HCI tool training and calibration sessions with one City Hall SOC operator and Thales specialists (mid-October, 2 weeks before the AP, Figure 12)



**Figure 12 - HCI calibration in Oslo City Hall, before Oslo AP**

- UdN+IMT’s BRD tool set up and installation (2021 Nov 2, the day before the AP)

#### 4.2.2 The 1st Acceptance Pilot (3 days in Oslo)

The Acceptance Pilot in Oslo was held in two main locations: Oslo City Hall (SOC, meeting room and outdoor square) and a floor of a building in the neighbourhood (where there were several meeting rooms), both in the city centre.

#### 4.2.3 AP in Oslo: Who

Around 50+ persons (including 30 project members) participated in the Acceptance Pilot at location. Due especially to restrictions related to COVID-19", the remaining project members engaged via stream.



The local stakeholders involved were:

- Oslo City Hall security and general services (end-user)
- Agency for Emergency planning in City of Oslo (project member, stakeholder)
- Security Manager City Hall and Crisis Manager for City of Oslo (end-user, stakeholder)
- National treatment center for CBRNE from Oslo University Hospital (contribution and participation in BRD test, provided protection equipment).

#### 4.2.4 AP in Oslo: What

Table 6 and Table 7 summarised what occurred during the days in Oslo and the main notes related to the tests undertaken. Figure 13 shows a moment during the tests in front of the City Hall.

**Table 6: Oslo AP, days overview**

<b>2021, Nov. 3<sup>rd</sup></b>	Partner meetups, presentations and tool testing of the BRD sensor and CTM.
<b>2021, Nov. 4<sup>th</sup></b>	Tests of the HCI, WD, SMD and PTRO tools. 20-minute debrief sessions with operators, after each test. Live stream of some of the tests (CTM, SMD) from SOC to the meeting room in order for interaction between test participants and the Consortium. SG and Simavi presented their tools/platform for the Consortium, with a walkthrough of some of its functionalities and visualizations for later discussion.
<b>2021, Nov. 5<sup>th</sup></b>	CINI presented results from their analysis of data obtained from air data sensors in Oslo. The presentation showed some of the PTI tool capabilities with anomaly graphs. Later on, feedback collected from end-user debriefs were presented and discussed in plenary.



**Figure 13 - Borggården, outside Oslo City Hall. Location of WD and PTRO test.**



Table 7: Tests summary (adding details in 4.1)

Tool / Platform	Tested in Oslo	End-user involvement	Notes
BRD	Yes	Partly	BRD sensor tested for 4 hours with 4 different scenarios. Not able to involve SOC-operator during test due to technical issues. End user involved in prior training, facilitation of sensor installation and result sharing.
CTI	Partly	Partly	Not tested live in SOC due complications. Presentation of UI and functionalities performed.
BAS	No	No	Not tested due to tool not being integrated in time for the AP.
CTM	Yes	Yes	Tested in a closed infrastructure at City Hall SOC. Operator with IT competence participated in test.
WD	Yes	Yes	Tested in City Hall SOC in parallel with HCI. Multiple scenarios
HCI	Yes	Yes	Tested in City Hall SOC in parallel with WD. Multiple scenarios
PTRO	Yes	No	Tested in scaled version outside City Hall. 4 scenarios.
PTI	Partly	No	Results from analysis of air data sensors presented during AP. Live data capture not performed.
SMD	Yes	Yes	Use case of predefined keywords presented during AP. No live search on social media conducted during AP, however tool was tested on end user using CSV file.
PLATFORM	No	Partly	Platform not tested by operator during AP. End-user involved in some degree via presentations of UI and pre-arranged training.

### 4.3 Acceptance Pilot in Padova

**WHEN: 2021, December 1<sup>st</sup> - 3<sup>rd</sup>**

**WHERE: Padova, Italy – Piazza dei Signori**



**Figure 14 - Padova, Piazza dei Signori**



### 4.3.1 Planning and Preparation

To get prepared and aligned, several activities have been undertaken before the actual AP, the main ones were:

- some training sessions, just like before the AP in Oslo (weekly meeting OSL + CPAD, F2F meeting with the tech Partners, HCI's tool calibration, BRD setup);
- formal meetings with local authorities to get authorizations and support (*Prefetto, Questore, City Council members, Local Police officers, other Municipality departments, Soprintendenza Archeologia, Belle Arti e Paesaggio, etc.*);
- selection, procurement and installation of additional equipment to increase the data to work with (e.g. 8 CCTV cameras, 9 sensors for counting people);
- Data Protection Impact Assessment.

The Consortium then treasured the experience in Oslo to better finalize what it has been already preparing for the AP in Padova (e.g. the need to use the proper wireless connection to get outputs from some tools).

Table 8 summarises how the main results achieved in Oslo became the “starting point” for Padova AP.

**Table 8: From Oslo to Padova**

What has been achieved by Acceptance Pilot in Oslo?	New Targets for Acceptance Pilot in Padova
Team building	Team-bonding
Better understanding of tools (status, capacity, potential)	Improvement of the status AND sharing the potential with local stakeholders
Meaningfulness of tests score: 4,75/6	Meaningfulness of the tools, for the cities
First evaluation of tools from an operator perspective	A larger involvement: more and different end-users for more feedback
Learning points for AP in Padova and planning of Live-Exercise in Oslo	More info and details for Live-Exercises AND for future a possible/probable adoption

Adding challenge: a broader involvement of the host city in terms of local stakeholders, in order to show them the IMPETUS added value and to get their feedback. While in Oslo it was important to get to know the tools and to be sure that the planned tests were effective, the main focus of the AP in Padova was to verify the meaningfulness of the tools: do they provide a real added value? (e.g., to end users' daily work).

To answer this question a deeper and broader involvement of the local stakeholders has been considered necessary.

During AP in Oslo, it became clear that considering only the SOC operators as potential end-users of the tools and the platform was not correct: only the tools that are able to provide a quick and specific information, as an alarm, provide effective support and value added to the SOC operators. On the contrary, the ones that request more interaction may not be as relevant.

So, other kinds of end users have been identified and involved, in addition to SOC operators and their supervisors:

- IT department analysts and IT supervisors for cyber security tools
- Local Police investigation specialists and safety planners for those tools that provide data-analysing



To get prepared and aligned, some activities similar to those that preceded Oslo AP, have been undertaken:

- weekly web meeting OSL + CPAD to plan the APs considering both the similarities and the different characteristics of the 2 cities;
- F2F web meetings with technical Partners to agree the activities related, e.g., trainings to be done, the kind of tests that could be effective and reliable, etc.; (e.g., in Table 9 are reported the training session planned).

**Table 9: meetings with the end users to prepare Padova AP**

WHO	WHAT	WHEN
<b>HCI-THALES</b>	<ul style="list-style-type: none"> <li>• Hands on test</li> <li>• Calibration test</li> </ul>	30 November in Padova
<b>PTI-CINI</b>	<ul style="list-style-type: none"> <li>• Online presentations</li> </ul>	11 and 18 November 09:00-10:00
<b>PTRO-UPAD</b>	<ul style="list-style-type: none"> <li>• Presentation</li> </ul>	4 October 11:00-12:00
<b>BDR-UdN</b>	<ul style="list-style-type: none"> <li>• Online video/ppt</li> </ul>	15 November 09:30-10:15
<b>SMD-INSIKT</b>	<ul style="list-style-type: none"> <li>• Video tutorial</li> <li>• Send end user manual</li> </ul>	
<b>BAS- XMCYBER</b>	<ul style="list-style-type: none"> <li>• Align SOC/IT operator</li> </ul>	16 and 23 November 12:00-13:00
<b>SIMAVI-PLATFORM</b>	<ul style="list-style-type: none"> <li>• Alignment training</li> </ul>	15 November 11:00-13:00
<b>WD-CINEDIT</b>	<ul style="list-style-type: none"> <li>• Video tutorial</li> </ul>	16 November 12:00-13:00

#### 4.3.2 The 2nd Acceptance Pilot – 3 days in Padova

During the AP in Padova, to get the contributions of all the involved end users, the tests took place in 4 different locations:

- Piazza dei Signori
- Palazzo del Capitano (Nassiriya room and 1<sup>st</sup> floor meeting room)
- the Local Police SOC  
the IT department SOC

#### 4.3.3 AP in Padova: Who

150+ people directly participated (Consortium members, end users, local authorities, other local stakeholders, volunteers and COSSEC members). In addition, some Partners and some other stakeholders provided their contribution remotely, due to the COVID-19 restrictions.

On a local level, these local stakeholders were invited to the Congress and to attend, when possible, the tests:

- Political referents (City Government and City Council members)
- Local Police authorities
- Civil Protection national and local authorities
- National Police local authorities
- Carabinieri local authorities
- Firefighters local authorities
- First Aid local references
- Local Police SOC operators and supervisors
- Civil Protection local volunteers
- Padova IT department SOC operators and supervisors



#### 4.3.4 AP in Padova: What

In Table 10 and Table 11 it has been summarised what occurred during the days in Padova and the main notes related to the tests undertaken.

**Table 10: Padova AP, days overview**

<b>2021, Dec. 1<sup>st</sup></b>	Partners meetup. BRD test. Congress with local authorities, other stakeholders, Consortium members.
<b>2021, Dec. 2<sup>nd</sup></b>	Integrated tests of HCI + CTM + CTRO + BAS tools. SMD hands on training and test. PTI results. Platform status + brainstorming session about UI. Horizon 2020 FASTER project presentation (made by a COSSEC member). Integrated tests of HCI + WD + PTRO tools. 20-minute debrief sessions with operators, after each test.
<b>2021, Dec. 3<sup>rd</sup></b>	Volunteers + local stakeholders + Consortium Partner debrief sessions. Feedback from end users interviews presented and discussed in plenary.

**Table 11: Tests summary (adding details in 4.1)**

<b>Tool / Platform</b>	<b>Tested in Padova</b>	<b>End user involvement</b>	<b>Notes</b>
<b>BRD</b>	<b>Yes</b>	<b>Partly</b>	More data collected in different environments. Possibility to send alarms to IMPETUS Platform. Solved communication issues (wi-fi, 4G).
<b>CTI</b>	<b>Yes</b>	<b>Yes</b>	Right end users involved. From a presentation in Oslo to real interaction with end users. “Hands on” tests after a short training. Real threats detected.
<b>BAS</b>	<b>Yes</b>	<b>Yes</b>	Right end users involved. Real vulnerabilities detected within the municipality network. “Hands on” tests after a short training. Almost integrated with CTM.
<b>CTM</b>	<b>Yes</b>	<b>Yes</b>	Right end users involved. From fully simulated to almost-running system: real countermeasures for real vulnerabilities. Almost integrated with BAS.



<b>WD</b>	<b>Yes</b>	<b>Yes</b>	Use of synthetic data: they will help the development. Real time Telegram message for end users when a detection occurs. Close to real time detection.
<b>HCI</b>	<b>Yes</b>	<b>Yes</b>	More end users and supervisors involved. Comparison between data collected from customized system vs general model. Unbiased/objective outputs.
<b>PTRO</b>	<b>Yes</b>	<b>No</b>	More people involved. More precise data collected from different realistic scenarios. Some unexpected behaviors initially not considered. Further data collected for model input and tuning.
<b>PTI</b>	<b>Partly</b>	<b>Partly</b>	More data collected from different sources confirmed the potential of the algorithm. The more data the better in terms of anomaly detection. From data to info: steps ahead.
<b>SMD</b>	<b>Yes</b>	<b>Yes</b>	Right end users involved. “Hands on” tests after a short training: from scratch to results. Some false-positive detected. Need for different sources of data.
<b>PLATFORM</b>	<b>No</b>	<b>Partly</b>	Some more tools integrated and able to share data. User Interface

#### 4.4 Acceptance Pilot – Tools tested

In this paragraph the Partners describe what they wanted to test, how they plan to arrive fully prepared to the APs, what they undertook and which results they got at this point of the project duration (mid-term).

##### 4.4.1 BRD – Biochemical Risk Detection

<b>BRD</b>	
<b>Objectives</b>	1. Testing the BRD tool in real conditions: BRD is still under development (TRL6) and all tests are performed under laboratory conditions.

<p><b>Preparation</b></p>	<p>Four simulations/scenarios have been designed to test the BRD tool in "real life conditions":</p> <ul style="list-style-type: none"> <li>• to get the baseline: each room has its own bacterial signature concentration which depends on the size of the room, the air conditioner, the geographical orientation;</li> <li>• people in the room for an hour (people just talking like in a meeting): the concentration of bacteria in the room increases with "human activity".</li> <li>• people in the room but in panic: this step was to test the sensitivity of the BRD tool.</li> <li>• to spread the bacteria around the room.</li> </ul> <p>For all these simulations, an alert was sent to the platform in real time. For the different simulations, it was expected two different alerts: green when the concentration in bacteria in the air it's under the threshold, the red alert for the "biologic attack".</p> <p>The different simulations were tested in IMT Alès laboratory: the challenge was for the "biologic-attack" to find non-pathogenic bacteria, which are airborne and to find the right tool to spread the bacteria in the air. Additionally, the team did not have access to a microbiology lab during AP, so they had to find equipment to grow the bacteria in "travel" conditions.</p> <p>The team decided to use yogurt bacteria: not pathogenic and easy to cultivate. It was used a mini-incubator to grow the bacteria, but without agitation. The first step was to adapt the bacteria to the culture medium, in the mini-incubator and to obtain a sufficient volume for the propagation of these in the air. The second step, to spread the bacteria in the air, an atomizer was chosen allowing a good distribution in the air. The "biologic-Attack" was tested in laboratory conditions in a kind of box, and in a room in "real conditions".</p> <p>On the other hand, the BRD tool has been modified to optimize the space in the biocollector and the Kafka has been implemented to send the alert to the platform. A simple dashboard (Figure 15 below) has been designed to understand the different alerts and to have a quick reactivity of the end-operator in case of red alert.</p> <div data-bbox="443 1176 1356 1608" data-label="Image"> </div> <p><b>Figure 15 - Simple dashboard designed for the AP. On left the 'green alert', on right the 'red alert'.</b></p>
<p><b>Things actually done</b></p>	<p>All simulations planned were realised during both Oslo AP and Padova AP.</p> <p>Only the "panic" simulation in Oslo and Padova was transformed into a "game" simulation: easier to organize and to avoid traumatizing the people. A "giant memory game" in Oslo and a "foosball" tournament in Padova were organized.</p> <p><u>Simulation in Oslo (Nov 3<sup>rd</sup> at City Hall)</u></p> <ul style="list-style-type: none"> <li>• The first simulation to obtain the baseline was not validated: some technical issues appeared.</li> </ul>



	<ul style="list-style-type: none"> <li>For simulations b (with people) and c (game): the concentration of bacteria in the air increases with the activity of people in the room but the team did not validate these results because the baseline was not validated.</li> </ul> <p>Then:</p> <ul style="list-style-type: none"> <li>The concentrations of the three simulations were closed: not possible ensuring that the BRD tool did a difference between non-human and human activity.</li> <li>For biological attack the BRD tool detected a significant increase of the concentration of bacteria in the air.</li> <li>The alerts were not sent to the IMPETUS platform in Oslo: the WIFI failed and the team tried to find an alternative to send the alerts to the IMPETUS platform without success.</li> <li>The Oslo AP has seen some problems, but this is normal in "real life conditions"; some experiments have been validated and some points were improved for the Padova AP.</li> </ul> <p><u>Simulation in Padova (Dec 1<sup>st</sup> at UniSmart)</u></p> <ul style="list-style-type: none"> <li>A 4G router was installed in the BRD tool to avoid WIFI issue.</li> <li>The BRD tool was installed overnight before the simulations to get more baseline data and test the automatic mode. This test was a success: it is obtained 9 bacteria concentrations in the air very consistent with the result observed before. This automatic mode works.</li> <li>All the simulations were also a success: the BRD tool detects an increase of bacteria concentration in the air over time, with "human activity" to "biological attack". With the 4G router device the alerts were sent to the IMPETUS platform during the AP in Padova.</li> </ul>
<b>Results and feedback analysis</b>	<p>Objective achieved:</p> <ul style="list-style-type: none"> <li>to test the BRD tool in "real conditions"</li> <li>the alerts have been sent via 4G with the kafka protocol to the IMPETUS platform.</li> </ul> <p>However, these simulations do not allow to validate the sensitivity of the BRD. But the BRD detected an increase in the concentration of bacteria in the air over time with "human activity" and "biological attack".</p> <p>It is better to use an automatic mode all day long to get more data and not to "cut" the different simulations.</p>
<b>Next steps</b>	<ol style="list-style-type: none"> <li>Get more data outside of lab conditions.</li> <li>Design a new dashboard that is understandable to end users and get more feedback from the SOC.</li> </ol>

#### 4.4.2 CTI – Cyber Threat Intelligence

<b>CTI</b>	
<b>Objectives</b>	<ol style="list-style-type: none"> <li>To make the end users of the IT department aware of the potential of the tool</li> <li>To show potential vulnerabilities of the networks</li> </ol>
<b>Preparation</b>	<p>For Oslo AP it has been decided to use virtual machines and to provide some prepared data to undertake a simulation with IMT tool.</p> <p>Before the AP in Padova, ~80 software agents have been deployed in the municipality network (some non-critical devices) to find in real time real vulnerabilities.</p> <p>Some training meetings have been undertaken to provide info about how to deal with the software agents and which could be the results using the tool</p>
<b>Things actually done</b>	<u>Simulation in Oslo</u> (Nov 4 <sup>th</sup> at SOC)



	<ul style="list-style-type: none"> <li>Presented results of the simulated use case, in collaboration with IMT <u>Hands on in Padova</u> (Dec 2<sup>nd</sup> at the IT department)</li> <li>Worked with the end users and IMT to detect vulnerabilities and countermeasures</li> </ul>
<b>Results and feedback analysis</b>	<p>Objective achieved:</p> <ul style="list-style-type: none"> <li>Positive feedback.</li> <li>IT specialists during Padova AP really interested in better understanding the potential of the tool</li> </ul>
<b>Next steps</b>	To be agreed

#### 4.4.3 BAS – Breach & Attack Simulation

<b>BAS</b>	
<b>Objectives</b>	1. Investigative Portal aims to allow SOC's to input their own assets and search for terms that relate to their needs.
<b>Preparation</b>	Before the AP in Padova, the team had a meeting with the managers of the SOC where they requested them to send their assets in order to input it into the platform.
<b>Things actually done</b>	<p><u>Simulation in Padova</u> (Dec 2<sup>nd</sup> at the IT department)</p> <ul style="list-style-type: none"> <li>During test day the team presented to Padova the results that we got, including real alerts on the assets that they requested to search for.</li> </ul>
<b>Results and feedback analysis</b>	<p>Objective achieved:</p> <ul style="list-style-type: none"> <li>Very positive feedback.</li> <li>Longer training was provided to the SOC team, followed by a month POC on the system.</li> </ul>
<b>Next steps</b>	<ol style="list-style-type: none"> <li>Additional feedback from the team needed.</li> <li>Actionable alerts and dark feed to integrate into IMPETUS platform.</li> </ol>

#### 4.4.4 CTM – Cyber Threat Management

<b>CTM</b>	
<b>Objectives</b>	<ol style="list-style-type: none"> <li>To generate based on network information received from sensors installed on the network.</li> <li>To enrich the pro-active attack graph based on a vulnerability ontology and the alerts from the monitored system.</li> <li>To calculate the optimal remediations to apply as response to the detrimental events.</li> </ol>
<b>Preparation</b>	<p>Meetings with involved Partners for integration. Meetings with cities.</p> <p>Installation of the tools and virtual machines on Oslo machine. Attack graph generation for a virtual network for Oslo. Attack simulation on the virtual network in Oslo. Attack graph enrichment based on monitoring the virtual network.</p> <p>Integration with XMCyber tool for AP in Padova. Attack graph generation with real data from Municipality network. Attack simulation on Padova network. Attack graph enrichment based on monitoring of Padova network.</p>



<b>Things actually done</b>	<p><u>Simulation in Oslo</u> (Nov 3<sup>rd</sup> at City Hall)</p> <ul style="list-style-type: none"> <li>• Installation of the tools and virtual machines on Oslo machine.</li> <li>• Attack graph generation for a virtual network for Oslo.</li> <li>• Attack simulation on the virtual network in Oslo.</li> </ul> <p><u>Simulation in Padova</u> (Dec 2<sup>nd</sup> at the IT Department)</p> <ul style="list-style-type: none"> <li>• The team installed the tools on Padova network</li> <li>• Integration with XMCyber tool for Padova</li> <li>• Attack graph generation with real data from Padova network</li> <li>• The attack graph was generated with data from Padova network.</li> <li>• The enrichment was done with false data as the could not simulate the attack because of network policy.</li> <li>• Feedback received in Oslo has been useless for AP in Padova.</li> <li>• The difficulties faced in Padova allow the team to learn a lot of lessons for the live exercises.</li> </ul>
<b>Results and feedback analysis</b>	<p>Objective achieved:</p> <ul style="list-style-type: none"> <li>• The team tested the usability of CTM solutions: good feedback from the end users in both cities.</li> </ul>
<b>Next steps</b>	<ol style="list-style-type: none"> <li>1. For the live exercise it is probable that the firewall of the cities does not allow the developers to simulate the attack or install the tools necessary for the test.</li> <li>2. For the live exercise it would be better if the team will have some meetings with the IT department to talk about the policies and how they could launch the attack simulation. It would be also great to do a test before the live exercise.</li> <li>3. Analyse other tools for network scans to choose which one will be better for the integration with our solution (as XMCyber is no longer part of the Consortium).</li> </ol>

#### 4.4.5 WD – Weapon Detection

<b>WD</b>	
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. Testing the Weapon Detection tool in real conditions.</li> <li>2. The Weapon Detection Tool is still under development in TRL 6 and will be reaching TRL 7 by the end of IMPETUS.</li> </ol>
<b>Preparation</b>	<p>One scenario was designed to test the Weapon Detection Tool in each Partner city using a real and relevant environment.</p> <p>The first step was to provide input and consult with the Partner cities in order to have them deploy video security cameras in an outdoor location where weapons can be detected.</p> <p>Once the video cameras were deployed, we requested video data from both partner cities in order to calibrate and make one AI per Partner city. The data includes Partner cities employees pulling out a gun in a public space.</p> <p>Using an edge device, the weapon detection tool processes all the data onsite issuing the same LAN (local area network). For the AP, when in red alert mode, that is when a weapon enters the camera field of view, we planned to push the alerts locally. At a later stage, the alerts will be sent to the SOC using kafka messaging.</p> <p>Weapon was successfully detected, as shown in Figure 16: guns are in the yellow square.</p>



	 <p style="text-align: center;"><b>Figure 16 - Red alerts as snapshot for the AP. On left in Oslo, on right in Padova.</b></p>
<p><b>Things actually done</b></p>	<p>Both scenarios were realized in Oslo and Padova. The alerts were not shared to the IMPETUS UI, as further development is required.</p> <p><u>Simulation in Oslo</u> (Nov 3<sup>rd</sup> at City Hall)</p> <ul style="list-style-type: none"> <li>• The first scenario where a security guard pulled out a gun was validated. It included 4 people: 3 passers-by and one attacker. The weapon detection tool successfully detected the instances of the gun.</li> <li>• It did generate false positives on a person wearing black leather gloves: these false positives were taken into consideration. The developers are working on a new AI that does not generate false alerts for the city of Oslo.</li> </ul> <p><u>Simulation in Padova</u> (Dec 3<sup>rd</sup> at the SOC)</p> <ul style="list-style-type: none"> <li>• In Padova the developers shared the alerts using telegram to show the real-time situational awareness capabilities of the tool.</li> <li>• Due to Covid-19 travel restrictions, during the Padova AP, the team processed previously recorded videos from Padova at R&amp;D lab in Israel and they shared the alerts in real-time. They did so using telegram and the response was satisfying as it allowed the first responders at the SOC to also receive alerts on their smart devices, therefore gaining time.</li> </ul>
<p><b>Results and feedback analysis</b></p>	<p>Objectives achieved:</p> <ul style="list-style-type: none"> <li>• In both cases, the weapons were successfully detected and the purpose of these scenarios as to test the accuracy and UX (user experience) of the Weapon Detection tool.</li> <li>• We were told there is an imminent need for Padova to have an AI that detects knives on top of guns.</li> <li>• Partner Cities are facing challenging compliances when using security cameras and AI's. It therefore takes time to exchange data.</li> </ul>
<p><b>Next steps</b></p>	<ol style="list-style-type: none"> <li>1. A new AI that does not generate false alerts when people wearing black gloves will be delivered for May 1<sup>st</sup> 2022 for the Partner city of Oslo.</li> <li>2. Deploy and install an edge device at each SOC and share our alerts using kafka.</li> </ol>

#### 4.4.6 HCI – Human Computer Interaction

<b>HCI</b>	
<p><b>Objectives</b></p>	<p>1. Overall evaluation HCI tool from the Cities of Oslo and Padova.</p>
<p><b>Preparation</b></p>	<p>Before the AP a questionnaire was sent out to the cities and their operators in order to better configure the HCI Tool according to the acceptance criteria of the operators: they were questions about comfort and feelings in using different sensors and providing personal psychological data.</p>

Based on the results (and current insights) the developers decided to use the Muse S brain computer interface that has two sensors: an EEG sensor and a PPG sensor. PPG: Heart beats per minute and between-heartbeat times (heart rate variability), EEG: Brain activity signal as oscillations = Brain wave band (Alpha, Beta, ...) power (amplitude squared).



Figure 17 - HCI devices

### Things actually done

#### Simulation in Oslo (Nov 4<sup>th</sup> at City Hall SOC)

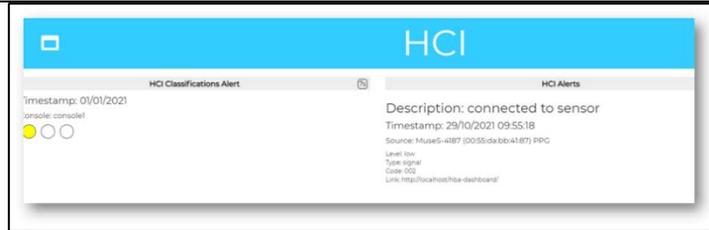
- Calibration test 3 weeks before Oslo AP: one operator participated in the (calibration) test and performed it. The calibration test took approximately 2 hours, after which Thales trained the workload models (physical, emotional and mental) for the specific operator.
- During the AP the operator was using the weapon detection tool during several roleplays just outside city hall (Figure 18). In parallel the HCI Tool captured the operator neurophysiological data using a brain computer interface (Figure 19), which was processed in real-time resulting in a workload classification (low, mid, high) for each workload dimension (physical, emotional, mental) and if deviations in these classifications occurred over time, then alerts were generated a visualized in the HCI Tool dashboard.
- During the AP no connection was made available to test the integration with the IMPETUS platform. Integration between HCI Tool and IMPETUS Platform was technically tested prior to the AP (Figure 20).



Figure 18 - Operator is using the WDT while the HCI Tool assessed hi workload in real-time



Figure 19 - Operator is wearing a brain computer interface



**Figure 20 - HCI Tool generates alerts via IMPETUS Platform**

**Simulation in Padova** (Dec 3<sup>rd</sup> at the IT Dept SOC and at Local Police SOC)

- Test at the Cyber SOC: one operator participated in the test. One day prior to the AP the operator performed the calibration test for training the operators' workload model (Figure 21).
- During the test the operator was working on her laptop (not performing cyber risk assessments). She was interviewed on the usability of the HCI Tool dashboard that visualizes her assessed workload in real-time while being interviewed (Figure 22). In addition, the Cyber SOC supervisor was joined the evaluation discussion on the usability and added value of the HCI Tool (Figure 22).



**Figure 21 - IT Dept SOC Operator performs calibration test**



**Figure 22 - CCTV SOC operator and supervisor interviewed on usability of HCI tool**

- Test at the CCTV SOC: two operators participated in the test (Figure 23). One day prior to the AP they performed the calibration test (Figure 23). Their personalized workload models were trained off-line and implemented in the HCI Tool for the AP.
- Both operators were performing their normal daily activities as well as remotely viewing some of the IMPETUS tools (Figure 24). The test included an explanation of the HCI tool dashboard. Both operators and their supervisor were included in the debriefing/interview afterwards.

	<div style="text-align: center;">  <p><b>Figure 23 - left: CCTV SOC operators simultaneously assessed; right: calibration test</b></p> </div> <div style="text-align: center; margin-top: 20px;">  <p><b>Figure 24 - left: CCTV SOC operator interacting with PTRO tool while his workload is assessed in real-time; right: explaining the HCI tool dashboard to CCTV SOC operator</b></p> </div>
<p><b>Results and feedback analysis</b></p>	<p>Objectives achieved:</p> <ul style="list-style-type: none"> <li>• Usability Sensor Set: the brain computer interface was considered comfortable and unobtrusive.</li> <li>• Data collection and model training: Took in total about 2-3 on average per person, which was less than expected and can be done on the same day as running the AP.</li> <li>• The dashboard of the HCI tool is considered easy to use by supervisor and operator.</li> <li>• Workload classification: personalized workload models made sense given the current task and situation at hand.</li> <li>• Platform integration: technical test was successfully performed.</li> <li>• HCI tool clearly showed operational value.</li> <li>• Embedding the HCI Tool in a SOC environments requires new operational procedures regarding what to do and how to handle situations where operators are under or overloaded that is affecting their level of performance during crisis management situations.</li> </ul>
<p><b>Next steps</b></p>	<p>To be agreed</p>

#### 4.4.7 PTRO – Physical Threat Response Optimization

<b>PTRO</b>	
<p><b>Objectives</b></p>	<ol style="list-style-type: none"> <li>1. To support end users in optimizing the response to a critical event</li> <li>2. To optimize the management of crowds in open public spaces</li> <li>3. To deliver guidelines dealing with the choice of the most suitable egress routes</li> <li>4. To enrich the planning and the early post-event management of events involving crowds</li> </ol>
<p><b>Preparation</b></p>	<p>Meetings with end users and municipalities to:</p> <ul style="list-style-type: none"> <li>• Discuss expectations and limitations from the APs on the following aspects: number of people involved in the tests, number of tests required, properties of each test, logistic issues (where, when, what, how, who).</li> </ul>



	<ul style="list-style-type: none"> <li>• Investigate the most appropriate reference scenarios to be simulated and tested during the APs of Oslo and Padova, based on the number of people to be involved.</li> <li>• Analyze the physical context (place, routes, egress gates, configuration of spaces)</li> <li>• Meetings with municipalities and involved Partners for building the reference scenarios.</li> <li>• Numerical pre-simulation of egress scenarios based on information collected from municipalities and relevance concerning the context. Pre-simulations are used and compared to data collected during the tests.</li> <li>• Discussion on how to retrieve statistically valid data.</li> <li>• Discussion on how to enroll and integrate the participants into the tests.</li> </ul>
<p><b>Things actually done</b></p>	<p>Different activities have been performed in Oslo and Padova.</p> <p><u>Simulation in Oslo</u> (Nov 3<sup>rd</sup> at City Hall)</p> <ul style="list-style-type: none"> <li>• Four egress tests in rectangular open space (size 5.5 x 4 m) with three normally available egress gates (0.8 m). Total number of people involved in the tests: 33. <ul style="list-style-type: none"> <li>• Test 1. All egress gates open.</li> <li>• Test 2. One egress gate hindered.</li> <li>• Test 3. One egress gate hindered (different from previous).</li> <li>• Test 4. Two egress gates hindered.</li> </ul> </li> <li>• The following material was collected during the test: photo and video footage, the time of egress start, the total number of people across each egress gate, the time for the first and last person crossing each gate.</li> <li>• Tests in Oslo were intended to collect specific parameters used to tune and improve pre-simulated scenarios and associated rules.</li> </ul> <p><u>Simulation in Padova</u> (Dec 3<sup>rd</sup> at Piazza dei Signori square and at the Local Police SOC)</p> <ul style="list-style-type: none"> <li>• 8 tests in rectangular open space (size 20 x 11 m) with three normally available egress gates (1 m). Total number of people involved in the tests: 68. <ul style="list-style-type: none"> <li>• Test 0. Initiating event: actor walking with a weapon.</li> <li>• Test 1. Initiating event: multiple gun shots made by an actor.</li> <li>• Test 2. Initiating event: multiple gun shots made by two actors in two different locations.</li> <li>• Test 3. Initiating event: firecracker. The smoke hinders one egress route.</li> <li>• Test 4. Initiating event: brawl staged by three actors.</li> <li>• Test 5. Initiating event: weapon raising. This test is used to check the time-to-first call to the police rising the issue.</li> <li>• Test 6. Initiating event: no initiating event (normal egress across all available egress routes).</li> <li>• Test 7. Initiating event: coloured signal indicating the egress route to be selected.</li> <li>• Test 8. Initiating event: screaming actor with gun shots at one egress route.</li> </ul> </li> <li>• The tests had different purposes: <ul style="list-style-type: none"> <li>• Test 1,2,8: acoustic initiating event and threat.</li> <li>• Test 3: acoustic initiating event + hindering of one egress route.</li> <li>• Test 4: initiating event with different people acting.</li> <li>• Test 0,5: detection of an initiating event and communication.</li> <li>• Test 6: typical scenario requiring non-threatened egress.</li> <li>• Test 7: initiating event induced by visual signals.</li> </ul> </li> <li>• The following material was collected during the test: photo and video footage, the time of egress start, the total number of people across each egress gate, the time for the first and last person crossing each gate.</li> <li>• Tests in Padova were intended to compare experimental data with simulations in the case of more complex scenarios.</li> <li>• All tests in Oslo and Padova were performed in complete agreement with what had been expected.</li> </ul>

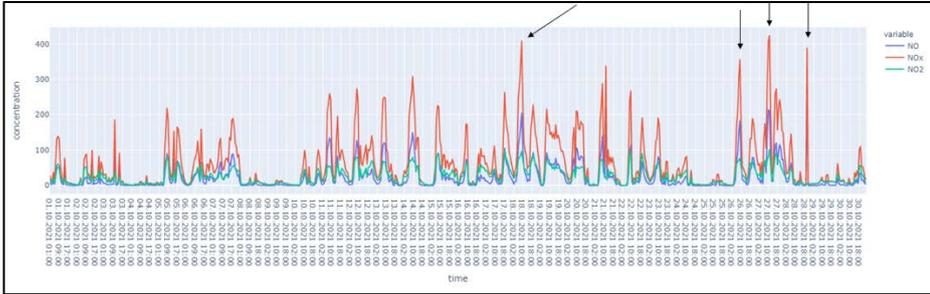
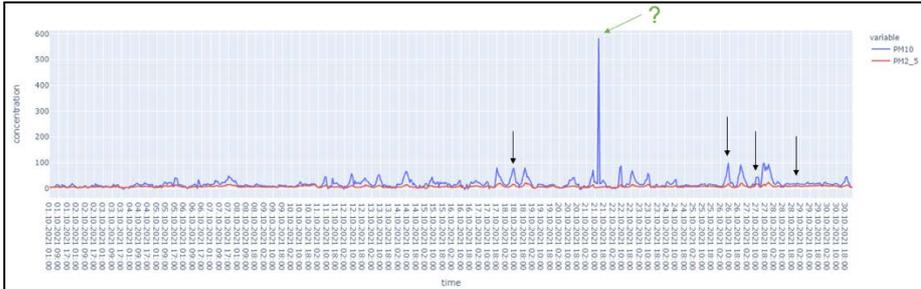


	<ul style="list-style-type: none"> <li>No tests did not take place.</li> <li>Numerical simulations were re-tuned (where required), and all tested scenarios have been numerically reproduced.</li> <li>De-briefing with the public that had attended the tests, feedback collection.</li> </ul>
<b>Results and feedback analysis</b>	<p>Objectives achieved:</p> <ul style="list-style-type: none"> <li>Expected tests were performed both in Oslo and Padova.</li> <li>Data valid for model predictions and analysis of egress performance have been collected.</li> <li>These data have been used to re-tune models for egress, provide the first insight on guidelines to be adopted in optimizing the egress scenario, estimate performance indicators of egress.</li> </ul> <p>Collected feedback:</p> <ul style="list-style-type: none"> <li>Significance of tests performed.</li> <li>Curiosities on observed people behaviour.</li> <li>How sounds and visual items can determine the egress of crowds.</li> <li>How actors and participants perceived the context.</li> </ul> <p>Improvement Areas:</p> <ul style="list-style-type: none"> <li>Involvement of people with different characteristics (distribution of ages, behaviours, etc.).</li> <li>Include additional initiating events (e.g., knife, etc.).</li> <li>Include bigger areas and different people density.</li> <li>Improve simulation reliability by means of improved mathematical models.</li> <li>Quantitative comparison of response with and without the PTRO tool.</li> </ul> <p>During the tests in Oslo and Padova, relevant and crucial data were collected to support modelling approaches to be included in the PTRO. Egress models were tuned with actual data from the activity, and the models successfully reproduced the observed events.</p> <p>Risks Analysis:</p> <ul style="list-style-type: none"> <li>Conditioned behaviour of participants to the tests (same participants in all the tests) – low risk (this aspect can be included in the modelling).</li> <li>Challenging generalization of rules to other contexts – medium risk (at this stage).</li> <li>Human error in collecting manual data and observing the event – medium risk (human error can never be neglected, but the risk can be reduced by cross-checking).</li> </ul>
<b>Next steps</b>	<ol style="list-style-type: none"> <li>According to the GDPR, prior to the live exercise would be useful to collect anonymous data concerning people participating in the tests useful for parametrizing and characterizing the crowd.</li> <li>Formulation of guidelines for end users of Oslo and Padova.</li> <li>Classification of behavior and vulnerability of egress gates.</li> <li>Extension to other contexts and open public spaces.</li> </ol>

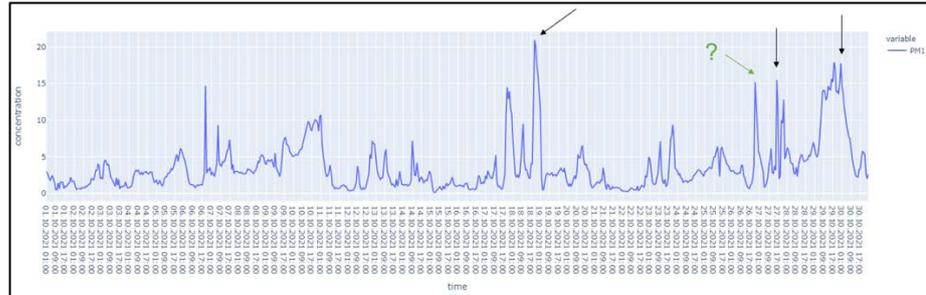
#### 4.4.8 PTI – Physical Threat Intelligence

<b>PTI</b>	
<b>Objectives</b>	<ol style="list-style-type: none"> <li>It is expected to observe instances considered anomalous by the tool, whose feature ranking contains in first positions features that have most contributed to the detection of the anomaly and in the last positions the least relevant features. For instance, in the case of a road accident, the expectation is to observe relevant features such as CO2 levels, pedestrian concentrations, or road traffic levels to be at the top of the feature ranking,</li> </ol>

	<p>rather than pollen or rainfall concentrations, which are less determinant for the detection of the abnormal situation.</p>
<p><b>Preparation</b></p>	<p>The testing session has been organized into the following stages:</p> <ul style="list-style-type: none"> <li>• Initialization stage. The PTI tool is trained using a batch-learning approach and, then, ready to detect anomalies or classify certain events.</li> <li>• identification stage (normal working mode). The PTI tool will detect anomalies or classify events using data coming from the real scenario.</li> <li>• Model adaptation stage (optional stage, if needed). Starting from the model generated after the initialization stage, the tool can be further trained using more recent data. This action is recommended if data distributions tend to change over time and there is not enough time or data availability to train a new model from scratch.</li> </ul> <p>The process described is not necessarily sequential, but iterative: it is possible to switch stages at any time.</p> <p>The evaluation methodology chosen for the testing session is the qualitative analysis, due to the unsupervised nature of the task. Qualitative analysis is more intuitive and interpretable to non-experts.</p>
<p><b>Things actually done</b></p>	<p><u>Simulation in Oslo</u> (Nov 4<sup>th</sup> at City Hall)</p> <ul style="list-style-type: none"> <li>• The PTI tool was tested using data coming from air quality monitoring sensors to identify pollutant concentrations deemed abnormal by the tool. Below is reported the list of stations used during the PTI tool test session, together with the list of pollutants that each station can monitor: <ul style="list-style-type: none"> <li>• Hjortnes. NO, NO<sub>2</sub>, NO<sub>x</sub>, PM10 and PM2.5 pollutants.</li> <li>• Loallmenningen. NO, NO<sub>2</sub>, NO<sub>x</sub>, PM1, PM10 and PM2.5 pollutants.</li> <li>• Spikersuppa. PM10 and PM2.5 pollutants.</li> </ul> </li> <li>• The considered stations are close to the Oslo Town Hall, where the Acceptance Pilot was held.</li> </ul> <div data-bbox="671 1196 1225 1503" data-label="Image"> </div> <p><b>Figure 25 - Location of the considered stations in the city of Oslo.</b></p> <ul style="list-style-type: none"> <li>• Period considered for PTI training: January 2021 - September 2021, with an acquisition per hour, totaling 18.286 acquisitions from the chosen stations.</li> <li>• Period considered for PTI test: October 2021, with an acquisition per hour, totaling 720 acquisitions from the chosen stations.</li> </ul> <p><u>Simulation in Padova</u> (Dec 3<sup>rd</sup> at the SOC)</p> <ul style="list-style-type: none"> <li>• The PTI tool was tested using data coming from number plate monitoring system to identify vehicle transits deemed abnormal by the tool. The system can monitor the transit of vehicles at a total of 94 points in the city of Padua. For each transit, the system records the following information: <ul style="list-style-type: none"> <li>• Date: the date of the transit (dd-MM-yyyy).</li> <li>• Time: the time of the transit (HH:mm:ss:SSS).</li> <li>• Cameraname: the name of the street where the sensor is located.</li> <li>• Hash: result of applying a hash function to the licence plate number.</li> </ul> </li> </ul>

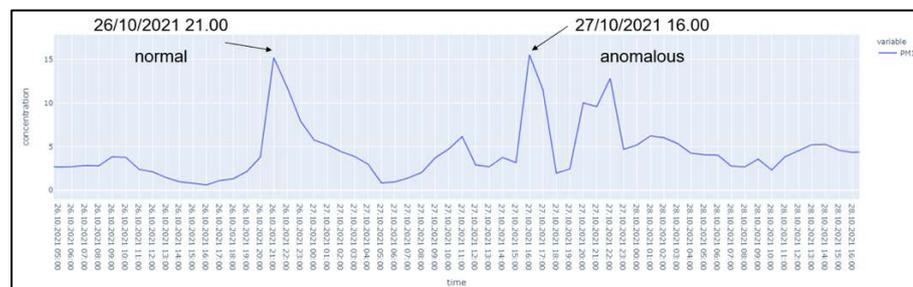
	<ul style="list-style-type: none"> <li>• Direction: vehicle direction, allowed values are respectively “UNKNOWN”, “LEAVING” and “APPROACHING”.</li> <li>• GPS: gps coordinates of the sensor.</li> <li>• Vehicle transits have been aggregated in 15-minute time windows, for each sensor involved, to detect more relevant situations. The aggregation just described allowed the addition of the following derived descriptive variables:             <ul style="list-style-type: none"> <li>• numVehicles: number of vehicles passing through the 15-minute time window.</li> <li>• numUNKNOWN: number of vehicles passing through the 15-minute time window, with direction “UNKNOWN”.</li> <li>• numLEAVING: number of vehicles passing through the 15-minute time window, with direction “LEAVING”.</li> <li>• numAPPROACHING: number of vehicles passing through the 15-minute time window, with direction “APPROACHING”.</li> <li>• The sum of numUNKNOWN, numLEAVING and numAPPROACHING for each time window considered is equal to numVehicles.</li> </ul> </li> <li>• Period considered for PTI training: November 23, 24, 25, 26, 27, 29, and 30, 2021 considering only the weekdays of the chosen week.</li> <li>• Period considered for PTI test: December 1, 2021.</li> </ul>
<p><b>Results and feedback analysis</b></p>	<p>Objectives achieved:</p> <p><b>Oslo AP</b></p> <ul style="list-style-type: none"> <li>• Figure 26 shows the concentrations per hour of NO, NOx, and NO2 pollutants during the identified test period, i.e., October 2021, from Hjørtnes station. The choice fell on these pollutants because they are present within the top-3 of the feature ranking, for those time instants considered anomalous by the PTI tool, indicated with black arrows within the graph.</li> </ul>  <p><b>Figure 26 - Concentrations per hour of NO, NOx and NO<sub>2</sub> pollutants during Oct 2021, from Hjørtnes station.</b></p> <ul style="list-style-type: none"> <li>• As shown in the graph, higher NO and NOx concentrations were recorded at the time points identified by the PTI tool.</li> <li>• Figure 27 shows the concentrations per hour of PM10 and PM2.5, the pollutants considered less relevant for the detection of situations deemed abnormal by the PTI tool, that occurred during the test period.</li> </ul>  <p><b>Figure 27 - Concentrations per hour of PM10 and PM2.5 pollutants during Oct 2021, from Hjørtnes station.</b></p>

- As in Figure 27, the black arrows indicate the time instants when the PTI tool found abnormal situations: the PTI tool did not find an abnormal situation during October 21 at 10 a.m., indicated with a green arrow in Figure 27, when very high concentrations of PM1 were recorded, even though at this time point the pollutant PM1 is correctly present in the first position of the feature ranking.
- The motivation is because several pollutants are being observed by the PTI tool and the sudden increase of concentrations of one of them is sometimes not sufficient to classify the time instant as a potential abnormal situation.
- Figure 28 shows the concentration per hour of PM1 pollutant during the test period, from Loallmenningen station. For this station, PM1 is the most decisive pollutant for the detection of abnormal situations that occurred during October 2021.



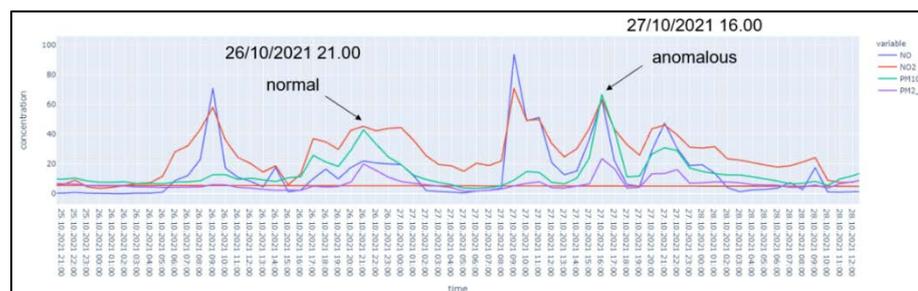
**Figure 28 - Concentrations per hour of PM1 pollutant during Oct 2021, from Loallmenningen station.**

- The black arrows indicate the time instants in which the PTI tool detected abnormal concentrations of the pollutants considered. As expected, the PTI tool was able to correctly detect high concentrations of the PM1 pollutant.
- However, on October 26 at 9 p.m. (green arrow), the concentrations of PM1 were very similar to those of October 27 at 4 p.m., but only in the latter case, an anomalous situation was found by the tool. A more detailed graph is shown in Figure 29.



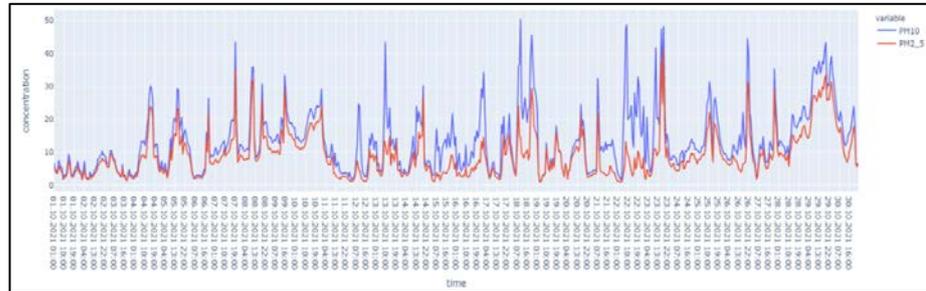
**Figure 29 - Concentrations per hour of PM1 pollutant during Oct 2021, from Loallmenningen station.**

- The reason is due to a sudden increase in concentrations of the remaining pollutants, which occurred on October 27 at 4 p.m. This situation, as shown in Figure 30, allowed the PTI tool to identify an anomalous situation during this time.



**Figure 30 - Concentrations per hour of NO, NO2, PM10 and PM2.5 pollutants during Oct 2021, from Loallmenningen station.**

- Figure 31 shows the concentrations per hour of PM10 and PM2.5 pollutants during the test period, from Spikersuppa station. The pollutants shown in the graph are the only ones the station can monitor.

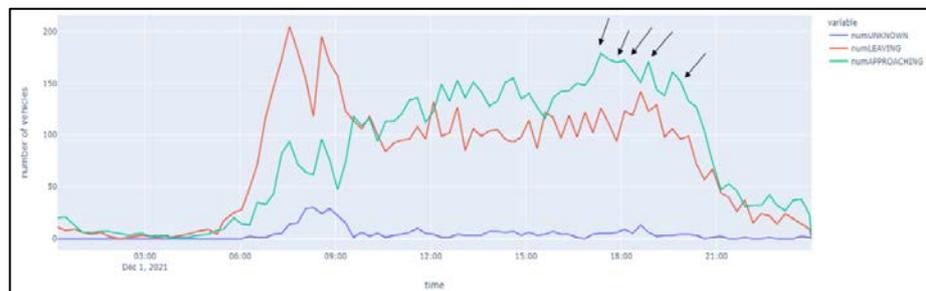


**Figure 31 - Concentrations per hour of PM10 and PM2.5 pollutants during Oct 2021, from Spikersuppa station.**

- As expected, the PTI tool did not identify any situation deemed abnormal for this station, as the concentrations of October are quite regular.

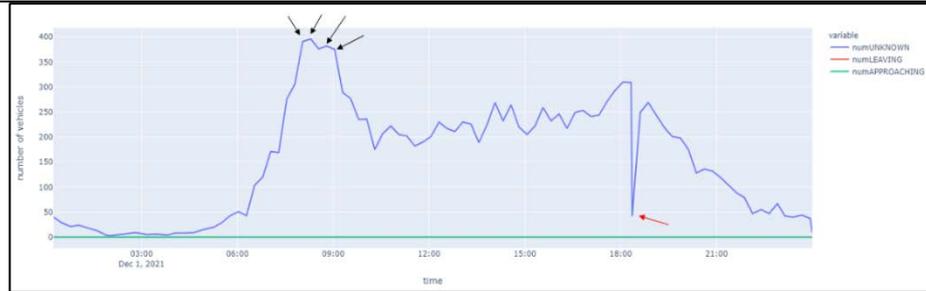
### Padova AP

- Figure 32 shows daily vehicle transits with direction “UNKNOWN”, “LEAVING” and “APPROACHING” in the street “Ponte 4 Martiri vs Padova centro”, during the identified test period, i.e., December 1, 2021. The black arrows indicate the time instants when the PTI tool found abnormal situations: anomalies were found on this day between 5 p.m. and 9 p.m, a time slot when people tend to go home after the working day. In this time slot, it is possible to observe a high number of vehicles with directions “APPROACHING” and “LEAVING”.



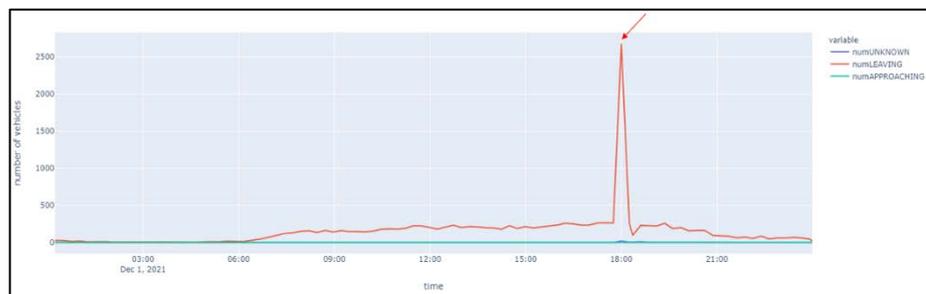
**Figure 32 - Daily vehicle transits with direction “UNKNOWN”, “LEAVING” and “APPROACHING” during December 1, 2021, in the street “Ponte 4 Martiri vs Padova centro”.**

- Figure 33 shows daily vehicle transits with direction “UNKNOWN”, “LEAVING” and “APPROACHING” in the street “Sito 1 – via Plebiscito”, during December 1, 2021. The black arrows indicate the time instants when the PTI tool found abnormal situations.
- As shown in the graph, a high number of vehicles with direction "UNKNOWN" passed between 8 and 9 a.m., the time slot when people tend to head for work. The PTI tool was able to identify this situation as abnormal.



**Figure 33 - Daily vehicle transits with direction “UNKNOWN”, “LEAVING” and “APPROACHING” during December 1, 2021, in the street “Sito 1 – via Plebiscito”.**

- To test the robustness of the PTI tool, it was decided to simulate several anomalous situations to understand whether, in its current state, the PTI tool was able to detect them.
- The red arrow in Figure 33 indicates one of the simulated time instants. However, the PTI tool was not able to classify the time instant as anomalous.
- A different simulated time instant is shown in Figure 34, indicated with the red arrow. In this case, the PTI tool has correctly classified the time instant as an anomaly.



**Figure 34 - Simulated daily vehicle transits with direction “UNKNOWN”, “LEAVING” and “APPROACHING” during December 1, 2021, in the street “Rotonda Grassi – Maroncelli corsia sinistra vs Grassi/Friburgo”.**

- During the Acceptance Pilots, the PTI tool was able to identify potential situations deemed to be abnormal.
- In the city of Oslo, higher than normal concentrations of pollutants were identified. In the city of Padua, on the other hand, abnormal vehicle transits were identified, corresponding to time slots in which people tend to go to or from work.

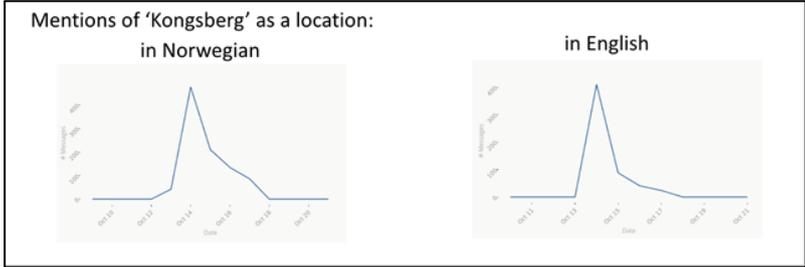
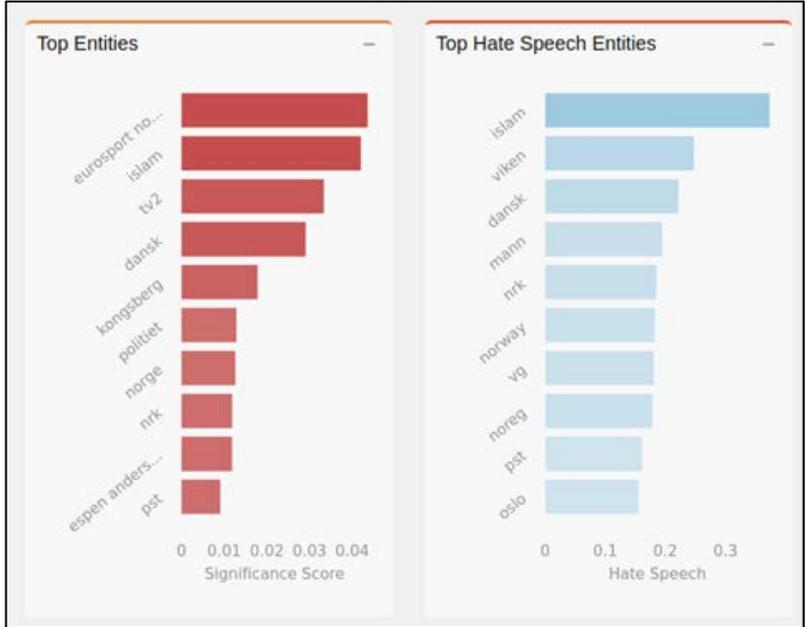
**Next steps**

1. In other circumstances, including simulated ones, the PTI tool was unfortunately unable to detect the anomalous situations. As a possible extension, it is being considered to include time information among the descriptive variables, to identify potential variations in data distributions at certain times of the day.
2. Future developments of the PTI tool include the possibility to identify predefined events using data provided by the geo-referenced sensors.
3. Starting from a predefined set of threats (e.g., fire, car accident, attack with guns), similarly to the anomaly detection task, the event classification task aims to classify the current unclassified sensor data under analysis as a particular threat or as a normal case. Therefore, in addition to the anomaly detector, the event classifier would be able to also indicate the type of threat under analysis.
4. For this task, similarly to anomaly detection, a training phase and an event identification phase are foreseen. The main difference with the anomaly detection task is that usually the classification of an instance is guided by the learning of a predictive model in a supervised manner. This means that the data set used for the training of the model must be annotated by describing the possible threats for the real scenario. However, this could be demanding to obtain.
5. To overcome this problem, unsupervised algorithms could be also considered for the classification task as for the anomaly detection. These algorithms are usually less accurate



	than the supervised ones since they exploit less informative data avoiding considering predefined classes.
--	--

#### 4.4.9 SMD – Social Media Detection

<b>SMD</b>	
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. Show how the tool works and showcase the technologies underlying: the SMD tool is a complex tool and a project-wide explanation was considered necessary.</li> <li>2. Test the tool functionalities and understand their validity for the security professionals' needs.</li> </ol>
<b>Preparation</b>	<p>Cloud deployment of the SMD tool accessible for the testers.</p> <p>Training material for the end users: Mini-video and workshops</p> <p>Prepare use cases relevant to the Acceptance Pilots: OSL AP - Kongsberg use case.</p> <p>Development of a timeline (from 2021/10/13 to 2021/10/19) studying the social media insights that the SMD could extract after a recent violent episode.</p> <ul style="list-style-type: none"> <li>• Configure proper keywords.</li> <li>• Definition of phase 1: Attack itself and 1st release of information.</li> <li>• Definition of phase 2: Details released and Slow-burn reactions on social media.</li> </ul> <p>Relevant Entities in Figure 35 and Figure 36 here below.</p> <div style="text-align: center;">  <p><b>Figure 35 - Mention of "Kongsberg" in Norwegian and English</b></p> </div> <div style="text-align: center;">  <p><b>Figure 36 - Top Entities</b></p> </div>

Relevant concepts in Figure 37, sentiment and hate speech in Figure 38.

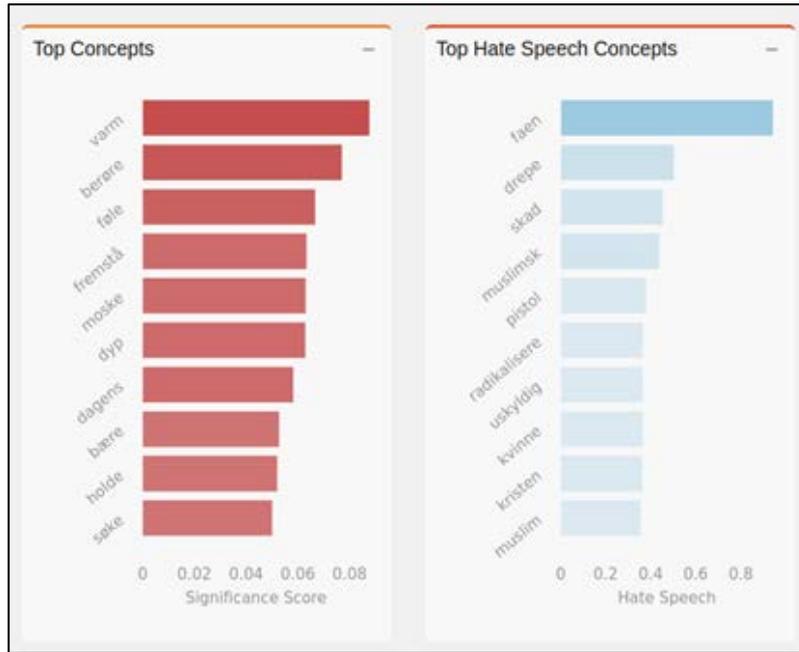


Figure 37 - Relevant concepts, in Norwegian

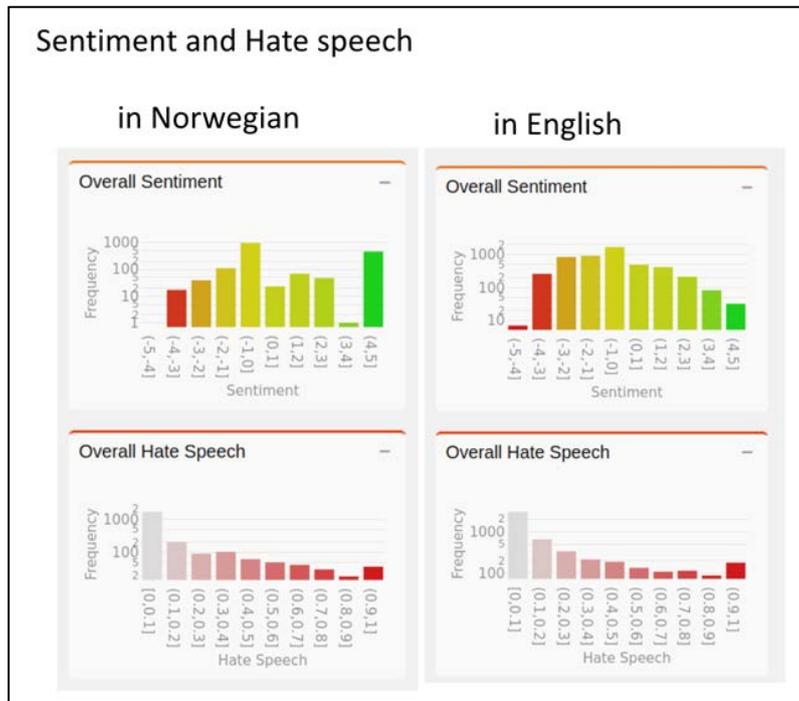


Figure 38 - Sentiment and hate speech detected

Expected Results:

- Find a proper user profile for the SMD.
- Validate that the analysis performed by the SMD are relevant for investigative professionals in the municipalities.

**Things actually done**

Simulation in Oslo (Nov 4<sup>th</sup> at City Hall SOC)



	<ul style="list-style-type: none"> <li>• SOC Operator tested the tool hands-on. After an explanation of how the tool works and how to use it, the testers were left alone -with INS support- with a computer that had opened a version of the SMD.</li> <li>• The SOC Operator confirmed that the information displayed in the SMD was not relevant to his day-to-day work. So, it was decided to change end user and try with investigators for the Padova AP.</li> <li>• The tool has a lot of potential for the planning stage (e.g., for the Head of Security).</li> <li>• Operational context needs to be more clarified.</li> <li>• The team realized that for the CPAD AP, INS had to configure a more relevant scenario (for testing).</li> </ul> <p><u>Simulation in Padova</u> (Dec 2<sup>nd</sup> at Piazza dei Signori)</p> <p>Investigators (CPAD AP) tested the tool hands-on: they confirmed that the tool was very relevant for them and their work and that their role was the correct for the SMD.</p> <ul style="list-style-type: none"> <li>• The tool was considered: <ul style="list-style-type: none"> <li>• useful and easy to use</li> <li>• Comprehensive system</li> <li>• good for a planning phase, not for a real-time operation</li> <li>• few models needed a refinement to improve accuracy in Italian.</li> <li>• More search options will be added to expand or narrow searching: OR to expand and AND, NOT/ ANDNOT to narrow down</li> </ul> </li> </ul>
<b>Results and feedback analysis</b>	<p>Objectives achieved: the SMD tool was a success in many ways.</p> <ul style="list-style-type: none"> <li>• Investigative professionals from the municipalities had the chance to test the tool hands on. It was the first time those professionals used a tool for Social Media monitoring, since currently all the work is done manually.</li> <li>• The tool was considered user-friendly and easy to use.</li> <li>• The tool helped the investigators to understand a general mood in the social media spaces looked at by monitoring e.g. sentiment, support for or rejection of certain topics and keywords. They considered it a very useful preparation tool.</li> <li>• The end users created several projects with certain keywords, that were centred on 1) checking the general mood among citizens, and 2) monitoring political reactions for specific decisions of the municipality government.</li> <li>• The investigators were able to detect hate speech in the messages retrieved.</li> <li>• It was clear that the municipalities would need to specify their necessities and narrow down their specifications to find information in specific areas and detect specific threats and risks.</li> <li>• INS was able to obtain recommendations on preventing false positives.</li> <li>• OSL confirmed that the use case based on the Kongsberg attack was very valid for them, as the conclusions extracted were similar to their own investigation, even if none in INS understood the local language (Norwegian).</li> <li>• It was developed an idea of a messaging system between investigators and SOC operators for coordination.</li> </ul>
<b>Next steps</b>	<ol style="list-style-type: none"> <li>1. To improve the search tool to enable expanding and narrow search options.</li> </ol>

#### 4.4.10 IMPETUS Platform

<b>PLATFORM</b>	
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. To present the interface: the way of working and organizing the platform, how the tools are integrated</li> <li>2. To collect feedback, suggestions, comments from all participants to the APs (both Partners and end users or other stakeholders) regarding possible improvements</li> </ol>



	3. To improve the integration of the tools: the platform is still under development and not all the tools have been integrated before the APs.
<b>Preparation</b>	<p>First Installation of the platform on internal test environment (SIV).  Preparation of test data for displaying in the platform various data or alerts received from tools.  Training sessions.  Gone through some test scenarios:</p> <ul style="list-style-type: none"> <li>• receive an alert on the platform</li> <li>• display details.</li> </ul>
<b>Things actually done</b>	<ul style="list-style-type: none"> <li>• Completed the installation of the platform on internal test environment (SIV).</li> <li>• Preparation of test data for displaying in the platform various data or alerts received from tools.</li> <li>• Training - Due to Covid-19 travel restrictions, the APs' training has been conducted remotely.</li> <li>• A user manual for managing users' profiles and their dashboards has also been prepared.</li> <li>• Introduction about how the platform display information/alerts, as a result of integrations, was presented for BRD + HCI + PTI + WD.</li> <li>• Dashboard management: creating and managing dashboards within the organization.</li> <li>• User management in the platform. How to create users and associate different roles.</li> <li>• Widget management. How to create widgets in the platform.</li> </ul>
<b>Results and feedback analysis</b>	<p>Final analysis:</p> <ul style="list-style-type: none"> <li>• If live cameras will be integrated in the platform, then a standard has to be found: if no, this integration depends on the specific software of each live cameras, impossible to manage all the existing ones</li> <li>• Regarding the WD tool, it will be possible to send pictures or screenshot from the platform to a group of selected people. To be better defined how (via which means)</li> <li>• User Interface development has to be prioritised: dashboards should be rethought, in agreement with the end users' indications</li> <li>• Regarding alerts, it should be defined a workflow to understand -working with the end users- which event could cause an alert and how the platform could support the operator in taking action</li> <li>• To be defined -with end users- which kind of reports and aggregated information they need and if they prefer to visualise them or download a dedicated file. For instance, at the end of the day, HCI statistics could be displayed on the interface of each user</li> <li>• To be defined which is the best way to present the information coming from each tool: there is the risk to block or bother daily activities of the end users</li> <li>• As underlined above, a deeper collaboration with the end users is recommended.</li> </ul>
<b>Next steps</b>	<ol style="list-style-type: none"> <li>1. To be organised working groups of end users, technological Partners to define (other) tests scenarios</li> <li>2. To be completed the integration of all tools in the platform</li> <li>3. To be defined roles, dashboards will be developed according to these roles</li> <li>4. To be share a final decision about where the applications will be installed (some could be hosted in Partners' infrastructures, some could be deployed in the Cloud, and others could be installed locally, on the city's servers).</li> </ol>



## 5 Results and Feedback Analysis

The validation and feedback collection activities have been undertaken in different moments and contexts: during and at the end of the APs, several debrief sessions have been undertaken; after the APs, instead, surveys, and open discussions provided additional contributions (e.g., lessons learned).

### 5.1 Feedback from the field (debriefs with end users)

To be sure to collect the largest set of contributions, ideas, indications, corrective actions and improvement areas, several different stakeholders have been involved: end users of both the cities, the Partners who attended the APs, volunteers and other local stakeholders who took part in the tests.

Results and “spur of the moment” feedback in Oslo and Padova have been collected in some different moments:

- 20-minute dedicated debriefs with the potential end users after each session/test. The debriefs aimed at collecting feedback on the tool's usability and operational aspects, and providing suggestions for possible improvement for the tools as well as for the next validation activities. Indeed, the feedback collected in Oslo were taken into consideration and implemented during the Padova AP.
- After each test, the operators and the observers gathered in a meeting room to delve into, through semi-structured interviews, operators' thoughts, feelings and beliefs about the tools.
- After the APs, in addition, a one hour debrief session with the main operator involved took place for a deeper elaboration and to discuss about usability and functionality of the tools.

As mentioned in Chapter 2 (sub-sections 2.3 and 2.4), the predefined topics were:

- Usability of the tool
- Impact on the operational framework

For the discussion about **usability of the tool**, the focus was on the operator's perceived usefulness and overall impression of the tool; in particular, whether the operator could envision any difficulties in using the tools and if new or specific competencies would be required. The interview set of questions related to this topic have been based on the Table 4: *Usability - from validation criteria to APs guidelines for observations*.

Regarding the **impact on the operational framework**, the focus was on how the tool might impact and/or improve the workflow; for instance, if the use of the tool would require any new procedures, information flows or responsibilities. The interview set of questions related to this topic have been based on Table 3: *Operability - from validation criteria to APs guidelines for observations*.

For all debriefings, except the first one conducted in Oslo where the tool provider asked to join in, only the operator and the observers were present. Based on the experience from this first debrief, it was suggested that the tool providers should have separate debriefings with the operators (if time permitted) for the remaining tools (and for Padova APs too). The reasons for this were that the operator was only available for a short period before moving on to the next tasks and that it was desirable to limit the focus area of the debriefings to the ones mentioned above without going into technical details and capabilities of the tools.

Several specific results and suggestions were provided for each tool, but the following findings applied on an overall level:

- The test scenario for each tool should be presented in a step-by-step manner both to the operator and the observing audience before each test.
- Realistic and simple scenarios are important to fully engage the operator
- Operator training is important to ensure that the test is performed by the operator (or the role the tool is intended for), not by the tool provider
- The operators involved in the APs would like to take part in the future validation activities to monitor the project progress and how their feedback as well as suggestions have been implemented.



At the end of the APs, the results from the debriefings were presented during a general assembly session. All participants were encouraged to provide any additional suggestions and observations during this session. Table 12 provides a summary of the feedback and suggestions collected during the debriefings with the end users and operators after each tool test.



Table 12: Feedback and suggestions from end users and operators

TOOL	AP OSLO			AP PADOVA		
	Usability	Impact on operational framework	Suggestions for improvement	Suggestions from OSLO AP implemented?	Usability	Impact on operational framework
BRD	The operator has not tested this tool, but received training/presentation of usability and tool functionalities.	Very interesting tool in relation to biological threats. Perhaps BRD sensors can be used during a large event in Oslo City Hall.			The operator has not tested this tool, but received training/presentation of usability and tool functionalities.	
	The intended user interface seems intuitive with simple alarm features.	New procedures required.	60 min interval between each run, the SOC receives an alert every hour.		The dashboard received by the SOC is intuitive, but it could be improved with other information allowing a better understanding and action by the operator.	
CTI	Not tested	Not tested		Tested with CTM		Please see the comments below
BAS	Not tested	Not tested		Tested with CTM		Please see the comments below
CTM	End user thinks the usability works well. Three main UIs are intuitive.	Showed something that wouldn't have been found from other tools (or time consuming to do manually).	If possible, the end user should operate the tool during the simulation. (Could the attacker be played by tool provider and work from another machine?). A specific	Partly done	End users think the usability works well. It is quite intuitive.	Showed something that wouldn't have been found from other tools (or time consuming to do manually).



			task can be given to the end user.			
	Could possibly be challenging when more vulnerabilities are detected at the same time or if integrated with other systems and tools (feeding information back and forth between tools and getting the full overview etc.).	End user not in position to answer question about work processes and new information flows.	If simulation is done as a demo: explain each step and especially when switching between dashboards and windows. Possibly prepare step by step guidance and instructions for the operator to follow (and possibly read out loud).	Done	Could possibly be challenging when more vulnerabilities are detected at the same time or if integrated with other systems and tools (feeding information back and forth between tools and getting the full overview etc.)	It would require new work processes, new information flows and new roles
	End user did not have any experience with similar cyber security tools and no previous training was given.	High level of confidence from what is shown so far.	Explain central terms and concepts such as attack graph/vectors in more detail in briefing.	Done	End user had limited experience with similar cyber security tools and no previous training was given.	High level of confidence from what is shown so far.
	Sorting of vulnerabilities/categorization could be beneficial to be able to prioritize tasks.	Will require training and cyber security/IT competence, need to know what the recommendations mean and what the consequences are.	Explain central terms and concepts such as attack graph/vectors in more detail in briefing.	Done	Sorting of vulnerabilities/categorization could be beneficial to be able to prioritize	Will require training and cyber security/IT competence, need to know what the recommendations mean and what the consequences are
	Customization is needed for realistic cost-benefit calculations for each organization				Customization is needed for realistic cost-benefit calculations for each organization	Implementation in the current infrastructure might be challenging.



<b>WD</b>	Operator thinks that the tool would be very useful, especially in situations when the operator is not 100% focused on CCTV.	Confidence/level of trust in tool is very dependent on few false positives.	Could alert video be a few seconds longer, for the operator to have more time to identify the perpetrator?			
	Challenging to use since the operator only got a glimpse of the perpetrator due to the obfuscation (GDPR). Could miss useful information about the perpetrator, such as appearance etc.	It was clear what the next steps expected from the operator was.	Testing different scenarios.	Done	The use of synthetic data gave the opportunity to test different scenarios.	
	In current simulation, the operator had to click on the alert video to remove the obfuscation, this was "too" time consuming given the urgency of the situation. If obfuscation is removed automatically, this will increase the usability a lot.	Would require some new procedures to incorporate into the daily operations (due to dealing with the alerts), but same response as today.	More than one camera to test different angles/distances			
		Would require no new competence or roles.				
<b>HCI</b>	Easy to use and comfortable to use if properly fitted.	Would require new procedures, due to the rotation of operators (every 30-45 minutes).	Test distribution of work (more operators).	Done	Easy to use and comfortable to use	Would require new procedures (i.e. human machine teaming – Platform and AI – handover).



	Thinks it would work well for larger events, because then the operator stays in the SOC the whole shift.	Would require some additional competence and experience from the manager stand point (what is the best thing to do in each specific situation when alert is given?)	Test the manager role (the supervisor operating the tool.	Done	It would work well for larger events or for training.	No new competence needed.
	Operator was given a short briefing of indicators and alerts, easy to understand.	No new competence needed.			Operator was given a short briefing of indicators and alerts, easy to understand.	Unbiased/objective stress and workload assessment.
	Could forget that you have to put it on when returning to SOC (if under stress)	Could perhaps be used for evaluating stress of operators after an incident/event.			Adaption has to be done to each user.	Would require some additional competence and experience from the manager stand point.
	Can be impractical to switch between operators, usually they change after 30-35 minutes. Adaption has to be done to each user. Can the user's profile be recognised automatically (future development)?					
<b>PTRO</b>	The operator has not tested this tool, but received training/presentation of tool functionalities.	Relevant tool for planning of large events.		Presentations and introduction done	The operator has not tested this tool, but received training/presentation of tool functionalities.	Investigation of further initiating events (e.g. attack with knife, coordinated action made by groups of people)
	Not familiar with its intended user interface.	Data on egress scenarios before an event can help planners in dealing with an egress/evacuation setting later.	Classes of risk should be minimized in the number and based on measurable quantities (i.e. number of people,	Further data of relevant scenarios collected	Not discussed with end-users	A combined effort among pilot cities and tool developers is required to understand how data from sensors acquire meaning within PTRO.



			number and size of egress routes)			
	In current step, the end-users can be supplemented with general guidelines to improve the management of egress from public spaces.	Would require some new competence in dealing with the tool. Guidelines are of general meaning and do not require specific additional competences.	Guidelines should give univocal indications (i.e. which gates to be opened/closed).	Analysis of the specific contexts of Oslo and Padova performed.	End-users find valuable the availability of a set of guidelines tuned on the specific city.	Generalization of the set of guidelines to different contexts.
<b>PTI</b>	The operator has not tested this tool, but received training/presentation of usability and tool functionalities.	Very relevant tool in terms of securing a space/building. Interesting with its capabilities in dealing with multiple sources of data like CCTV or temperature sensors.			The operator has not tested this tool, but received training/presentation of usability and tool functionalities.	
	The integration of PTI in the platform: Looks intuitive with a map of the sensors with GPS coordinates.	Could contribute to enhanced situational awareness.				
<b>SMD</b>	Very exciting tool and especially relevant for events and demonstrations to help plan the level of security.	Would require a new role if used in daily operations (one additional operator in the SOC).	The briefing was clear and easy to follow, the demo as well, but maybe a more realistic example could be used?	Done	The tool is very exciting and it might be helpful in the planning phase of large events such as demonstrations.	system that requires some training
	At the moment more relevant for planning and preparing for events, not practical in real time operations (would require a dedicated operator,	Complex and comprehensive system that requires quite a lot of training.	Would maybe be useful to give the operator a bit of training before the simulation and then give the operator specific tasks to		Done	It seems to be more relevant for planning and preparing phases rather than real time operations



	not enough time otherwise).		“solve” during the simulation.			
	It was difficult to understand the meaning of all the terms for content analysis (concepts/key ideas etc.).				Easy to use, easy to understand and navigate	More data sources and decrypting feature for intelligence activities
<b>PLATFORM</b>	The operator has not tested the platform but received training/presentation of usability and platform functionalities.	The platform is relevant for the SOC-operator duties.			The operator has not tested the platform but received training/presentation of usability and platform functionalities.	Different alerts and information details to be shown on the Platform
	Would require training for operation of the platform.	Widget setup is more relevant for the supervisor role. Widget setup depends on sensor integration in the city.			Customize the interface according to the different end users	
	Would require new competence for supervisor				Would require training as well as new competencies	



Considering the requirements listed in D1.2, Table 13 provides an overview of the main requirements addressed and how.

**Table 13: D1.2 Requirements addressed**

ID	Requirement	How the Requirement has been addressed
117	The project should implement a progressive testing and validation of the platform	The APs in Oslo and Padova have been useful to make a first round of tests of the tools and the first version of the Platform, as planned.
118	The IMPETUS platform should be mainly validated through pilots conducted in the partner cities	<p>LEv/LEx will take into consideration all the achievements and feedback obtained from the APs.</p> <p>LEv/LEx will include some different situation and tests but the approach, in terms of Consortium effort and passion will be the same!</p>
68	Relevant sensor data should be provided by the smart cities to properly train AI/ML-based tools.	<p>The 2 Cities have provided data collected with the currently present sensors to the Tech Partners, e.g. data from environmental sensors (mainly pollens and pollution) in Oslo and Padova and car-plates readers in Padova for the PTI tool.</p> <p>For the LEv/LEx. the cities will be able to share data collected by other kind of sensors (counter-people sensors, transport means tracking, etc.) with bigger advance.</p>
70	Sensors should be made available (potentially installed) in the smart cities to support the use of the individual tools	<p>Three air data sensors monitoring pollutants were used for testing the PTI tool in Oslo, see (ch. 4.4.8)</p> <p>A CCTV camera sensor was installed and connected to the WD tool prior to the AP.</p> <p>Six virtual machines were set up to create a closed IT infrastructure for the CTM test.</p> <p>During Padova AP environmental sensors and license plate reading sensors already present in the city have been used. In addition, 8 new-generation CCTVs and 9 people-counters sensors have been installed in Piazza dei Signori square, ready for LEv/LEx.</p> <p>More than 80 software “agents” installed in Padova municipality network for testing in a real environment BAS and CTM tools.</p>
42	IMPETUS platform should have 2 different interfaces, one for physical events SOC operators, another for cybersecurity SOC operators	During the Oslo AP it emerged that not only SOC operators will be the end-users. So, during Padova AP different additional end-users have been involved (e.g. in addition to Local Police SOC, IT dept specialists, judicial Local Police officers).
101	The IMPETUS platform should support users in creating personalized aggregated data and diagrams to perform specific analyses	After the APs, the Consortium has been considering 6 different kind of end users. For each of them a specific UI will be prepared and tested before LEv/LEx.
94	Information generated from the IMPETUS platform should be accessible from different emergency services and operational stations	



50	The IMPETUS platform should be able to provide access rights for end users based on roles, responsibilities and operational needs	This requirement has been already addressed before the APs. During the APs end-users with different roles (operators, supervisors and analysts) were involved in the tests, with the aim of collecting their feedback. The software to meet this requirement is almost completed.
83	Division of responsibilities should be defined clearly relative to the use of tools in the platform, including who is using which tool(s) based on authority and skillset	This topic was addressed in the months previous the APs, and the end users who took part in the tests were indeed involved depending on their roles and their responsibilities.  To improve the current status, the Consortium has been working on the definition of 6 “personas” (the 6 end users identified). These definitions will be essential to a proper <i>ad hoc</i> development of the UI and use of the platform during the LEv/LEx.
44	When something suspicious or alarming is detected, the platform interface should provide an alert that effectively grabs the attention of the operators	Apart from the WD tool, that is already able to provide a “real” alarm, the Consortium has been working to make also PTI, HCI and BRD able to provide alarms.
46	The change detector should raise an alert when sensor data do not follow an expected behavior, according to historical data for any variable under observation	SMD, PTRO and the cybersecurity tools (BAS, CTI and CTM) are able to provide information that could be considered source of danger or warnings to be handle with.
47	The event classifier should raise an alert when sensor data represents a previously defined class of threat	
11	The IMPETUS project should develop an ethical framework to support Smart Cities in addressing ethical and legal issues associated with technology for safety	
14	The ethical guidelines should thoroughly examine the ethical issues connected to the deployers category	The ethical guidelines, work in progress, will be able to provide all the aspects that have to be considered and the points of attention.
15	The ethical guidelines should consider certain relevant aspects concerning the collection of data on one side, and privacy and personal data protection on the other	
16	The ethical guidelines should consider the role of State, its obligation toward use of all available means (including technology) to protect its citizens, and its obligation to protect citizens personal data and privacy	
18	The ethical guidelines should assess the risks to fundamental data rights and data privacy.	
25	Operations supported by the platform should comply with the national/international (if applicable)	
		Specific deliverables (WP11) and documents related to the ethics have been prepared and approved.



	security frameworks, including legal and cyber related frameworks.	Before the APs the cities have shared adding specific documentation to strengthen the effort to protect data (e.g JDPIA) in the research scope of the tests.
26	Smart cities should develop a methodology and process to monitor social media and open news sources.	Apart from the proper end users to be involved (as said, they are not SOC operators), during the APs emerged the need for a preparation path: to work properly, in fact, the SMD tool needs some specific information and a specific plan of detection. The end users involved, in particular the ones that faced the SMD tool for the first time, considered the tool really easy to use: so, a methodology has to be clearly defined and reported in a user manual, but it will not be an issue.
23	Training plans for all relevant security actors should be created to address the concepts of operation with the public safety platform.	Training sessions have been planned and undertaken before the APs with the end users and other stakeholders.
81	Training plans should be created to prepare operators and first responders for using the platform during complex and stressful scenarios.	The Partners worked in small groups composed by both technical and non-technical partners: non-technical partners provided their feedback with the aim to make the presentation “understandable” for all the possible audiences (so, anybody without a technical background).  This appreciated approach, likely, will be used also to prepare updated presentations before the LEv/LEx.
82	Roles, tasks and responsibilities in the decision-making process should be defined clearly in the new concepts of operation.	A process to define the “personas” that will interact with the IMPETUS Platform and tools has already started.
20	The security actors should lead the definition of new concepts of operation taking advantage of new technological capabilities.	During the APs tests without-IMPETUS vs with-IMPETUS have been undertaken with the aim to start considering new operative concepts (in particular, related to a more effective collaboration/synchronization between the players involved)  Revising the current operative procedures, in particular the ones that involve more Police forces or other emergency players (first aid, firefighters, etc.), is to be considered a definitely challenging process, even if expected. The more the Consortium will be able to involve all the stakeholders the more effective will be this improvement path. In any case, it must be said that it could become a topic to be discussed at a higher level than the local context. For this reason, it could be out of the scope and the boundaries of the Project.
93	The IMPETUS platform must be protected from outside intruders	A profiling policy has already been implemented (so, only the authorized people will allowed use the platform, in addition, end users will accede to a dedicated area: not anybody will be able to use everything within the platform).  Specific countermeasures to avoid intrusions, as for cyber-attacks, have been implementing since the beginning of the project.
9	The IMPETUS Cybersecurity framework should provide a response system, to handle both proactive and reactive mitigation of threats and attacks	BAS, CTI and CTM tools providers have been already working on these topics. In particular, BAS is able to detect vulnerabilities, CTM is able to provide countermeasures.



107	The cyber security framework should include tools enabling smart city operators to simulate, validate and remediate cyber-attack paths to critical assets	<p>Tests made during Padova APs have been considered interesting and promising (in particular, regarding critical assets protection).</p> <p>The Cybersecurity framework, work in progress, will share all the possible considerations, e.g. constrains and points of attention, useful to address cybersecurity issues in the more up-to-date way.</p>
106	The cyber security framework should include a security awareness training	<p>Some specific training sessions with the IT dept specialists (in particular before Padova AP) have already been undertaken.</p> <p>There will be the need to involve other stakeholders (e.g. in Oslo) and to update the training topics according to what will be developed before the LEv/LEx. The cybersecurity framework will take into account these work-in-progress elements.</p>
12	The response system should benefit from the use of anomaly detection, in order to derive new attack patterns	<p>PTI tool has been considered one of the most versatile tool because it can work independently form the type of data.</p> <p>Some interesting insights come out the APs: works before LEv/LEx will be aimed to transform the anomalies that can be detected into information useful in an operative context (e.g. new alarms due to non-intuitive thresholds crossed)</p>
49	The IMPETUS platform should be a modular platform where the individual tools can be added or removed without negating the functionality of the platform as a whole	<p>Modularity is one of the “foundations” on which the platform is based. These requirements have been already fully satisfied.</p>
95	The Impetus modules must be easy to integrate with other tools if needed	<p>The adoption of snap4cities as referring architecture made this tasks easier.</p>

### 5.1.1 Internal on-line survey - Partners who attended the APs

Even if the common feeling has been that the Consortium succeeded in both the APs, after each event a sort of “auto-evaluation” has been undertaken via the same internal survey. The purpose has been, firstly, to confirm that the effort provided and the results were effective and really useful to go on developing.

In Table 13 is reported an extract from the surveys: the Partners who attended the APs attested with high scores the value of the work done and the impressive improvement the Consortium was able to get in only one month from one AP to the other. Scores are based on a 1 (poor) to 6 (excellent) rating system.

The complete surveys are reported in APPENDIX A: surveys about APs.

**Table 14: Results from internal on-line survey**

Question	Survey after Oslo AP	Survey after Padova AP
How do you rate the relevance of the tech Partner presentations before each tool test?	5.00	5.29



How do you rate the meaningfulness of the tool tests?	4.75	5.23
How do you rate the evaluation processes during the AP. (Debriefs, evaluation presentations etc.)	5.00	5.17
How do you rate the protection of ethical aspects during the AP? (GDPR, consent etc.)	5.13	5.29
How was your overall experience of the Acceptance Pilot? 1-5	5.00	5.47

### 5.1.2 Inputs from people not completely involved – volunteers and local stakeholders

Some adding interesting topics emerged from another survey made - via an application for smartphones - on the last day of the AP in Padova involving volunteers and other local stakeholders (some samples of the survey results in Figure 39).

This kind of feedback can be considered precious, also for the Live Exercise planning, because it comes from people who are not daily impacted by the Consortium’s activities and/or (deliberately) received limited information about the project and the tests of the Acceptance Pilots: so, interesting because of the different point of view.



Figure 39 - Padova AP, some results of last day survey

The people involved in this survey underlined:

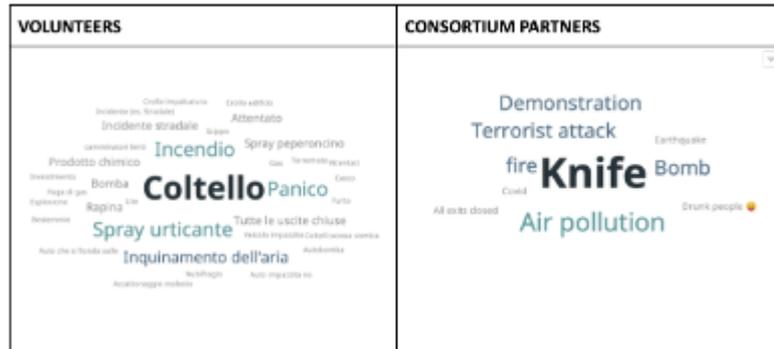
- the importance and/or the opportunity to detect knives (as reported in Figure 40).

This topic has been already discussed within the Consortium and all the Partners agreed: it could be really important and useful because in Europe the largest number of physical attacks is done with a knife. Considering that for gun detection is needed a completely different development, knife detection could be a topic for other research, further development and implementations, or adding projects.

- the importance and/or the opportunity to plan more tests and/or exercises, in particular those exercises that involve citizens.

This suggestion likely rose because people had fun in acting/playing a role on the field, but it can be read also as a need: people would like to be more prepared to face dangerous situations, maybe also to act in the best way possible. This could hence be considered not only a message for the Consortium in planning Live Exercises, but also for local administrations/governments.

- Apart from knives detection, both volunteers + local stakeholders and Partners consider relevant issues - in terms of security and safety - fires and air pollution.



**Figure 40 - Many people would like knives detection**

These of course are topics more related to civil protection or fire-fighters' activities than to Police forces' ones. To address them, in addition to some (more) specific sensors that should be installed, PTI and PTRO tools could definitely provide help in dealing with these emergency situations.

This is another indication that the IMPETUS platform and the Partners' tool should be ideally adopted from all the SOCs of the city to improve coordination and effectiveness in the interventions.

- Volunteers and local stakeholders rated useful and meaningful the kind of tests undertaken in Piazza dei Signori square, more than the Partners did.

This likely means that the tests that took place in Padova AP have been correctly oriented to the local context and local needs (e. g. testing evacuation from the square in occasion of a dangerous ramble may be considered worth of a test by the people that consider it possible, or worst, frequent, while the Partners that come from different countries and different contexts, may consider the ramble an event with limited likelihood or with a different impact).

- Improvement areas could be several, as summarised in Figure 41.

VOLUNTEERS		CONSORTIUM PARTNERS
<input type="checkbox"/> BETTER COMMUNICATION	8%	<input type="checkbox"/> BETTER COMMUNICATION 27%
<input type="checkbox"/> MORE TESTS	21%	<input type="checkbox"/> MORE TESTS 55%
<input type="checkbox"/> LESS TESTS	2%	<input type="checkbox"/> LESS TESTS 0%
<input type="checkbox"/> DIFFERENT PLACES	35%	<input type="checkbox"/> DIFFERENT PLACES 9%
<input type="checkbox"/> DIFFERENT EQUIPMENT	17%	<input type="checkbox"/> DIFFERENT EQUIPMENT 0%
<input type="checkbox"/> OTHER	17%	<input type="checkbox"/> OTHER 9%

**Figure 41 - Improvement areas**

Volunteers, who of course cannot have the whole picture in their mind, suggested to consider different places and different equipment. This topic could be considered as a sort of non-requested (but significant) report: there is more than one place that deserves to be more “protected”, hopefully with the IMPETUS outcomes and other sources of data.



## 5.2 Lessons learned

Even if the APs have succeeded and the largest part of the things planned and undertaken provided useful feedback and a certain satisfaction, there are some aspects that can be approached in a better/different way and there some improvement areas. Here below, the main considerations emerged.

### Before the APs:

- In the preparation phase, one of the main difficulties that the cities faced has been understanding the **needed equipment and the data** that had to be provided to the technical Partners. This topic, furthermore, were tightened by two factors: the impossibility to meet in person and the language gap among Partners and end users. This led to a further difficulty, that was the local stakeholders' engagement. Without a clear understanding of what the project was about, it was not easy to involve end users and some local stakeholders (e.g., authorities). The main lesson learned was the importance of **a strong involvement of the local stakeholders**, with as many meetings as necessary. Meetings, when possible, should happen in person, since it is a much more effective modality.

During the two APs, it raised clearly that meeting in person is a huge boost to the project: it quickly creates a good connection among Partners, it facilitates the mutual understanding and smoothens the development of the project activities. It is hence recommended, to consider **meeting in person as much as possible**, even if only in reduced groups - compatibly with the limitations that the pandemic continues to impose.

- For the AP in Padova, the limitations due to the **pandemic** were an additional complication in terms of looking for **available and suitable spaces** where to safely host the event (both tests and meetings). A lot of time was spent in finding spaces to host all the Partners, especially because of the required "social distance" and the limited number of people allowed to get in. The lesson learned is to book with a significant advance the spaces.

### During the APs:

- Some Partners reported that the schedule was too busy and the days too long: the last day of the APs, in particular, some people that attended were really tired. The lesson learned is to **spread the activities in a longer period** and to keep the Partners focused on the validation activities, limiting other ones (e.g. moving from different locations, meeting the authorities only with the project executive board, etc.)
- During the tests of the tools, it was made clear that an improvement area could be of **proper time allocation**. Even if an agenda has been shared before both the APs, likely too many activities have been planned.
- **Proper time allocation for debriefings** is also important, even if this could imply that more operators or actors are required to be able to perform all tests. In fact, including more operators would most likely be beneficial, as the pressure on them was quite severe especially during the Oslo AP. This could have impacted both the training and the understanding of the different tools as well as avoiding fatigue and the ability to maintain focus, even if the operators are trained in stress handling.
- While some of the tested scenarios were both simple and clearly explained, in some of the scenarios, it could have been beneficial to define the tasks in more detail before the actual test, both to save time and to guide the end user and enable them to see the actual capabilities of the tool. In other words, both better planning of the scenarios and more detailed testing programs could have benefited both APs.

### After the APs:



- Another lesson learned is to **improve end-user training** ahead of testing, in order to increase meaningfulness of tests. From feedback and post-AP reflections, it emerged that a more hands-on training approach would be preferred in some cases. This could be training of use cases, step-by step walkthrough of the tools' user interfaces and functionalities with the operators involved, and the possibility for end-users to explore the tool with remote access ahead of next exercise.



## 6 Looking ahead

### 6.1 Next Steps

Getting closer to Live Exercises and the final delivery, the next steps to be undertaken should be related to these topics:

- Integration
- User Interfaces (UIs)
- Standardisation
- Live Exercise Planning
- Practitioner’s guides (Ethics, Operational, Cybersecurity) final editorship
- Practitioner’s guides usage and evaluation (during LEv/LEx) planning

In Table 15 some to-do lists of what should be undertaken in the close future regarding the point listed above are reported.

**Table 15: Next steps summary**

<b>Integration</b>	<ul style="list-style-type: none"> <li>• <b>Integration within the platform:</b> the platform is to be considered the “container” of the tools: the platform has to be able to get information from all the tools and provide/convey it – in the proper manner – to the end user. <u>TO DO:</u> <ul style="list-style-type: none"> <li>○ Complete the bi-directional channel (almost ready for BRD, WD, PTI, HCI). All the tools send information to the platform in the form of alerts or notifications. For some tools it is useful to receive a context description in order to adjust their mode of operation. For example, in case the SOC is dealing with an alert, HCI will take this in consideration when analysing the sensor measurements from the operators. In the same scenario of an alert in the city, PTI will adjust the permission for data access in order to make the data available to more operators.</li> </ul> </li> <li>• <b>Tools integration:</b> some of the tools can be more “connected”. This means, for instance, that one could provide data (or add data) to another, as BAS does for CTM; So, the simultaneous use of more than one tool can provide a wider set of info to the end users. <u>TO DO:</u> <ul style="list-style-type: none"> <li>○ Analyse any possible combined use of the PTRO and PTI: anomalies related to the number of people getting in and out from a public space (like a square) could be used as data for PTRO.</li> <li>○ Analyse possible interactions between CTI and CTM: CTI searches the dark web for new threats and sends the outputs to CTM (a Prelude base SIEM). CTM then publishes to the platform alerts and notifications about the security environment at the city and allows the IT analysts to take preventive actions.</li> <li>○ Analyse possible interactions between PTI and BRD: the weather data that PTI collected from the sensors of the cities can be analysed together with the measurements from BRD. If BRD detected high level of bacteria, weather conditions (e.g. wind) could mitigate the possible danger. The combine usage of the 2 tools could be more effective and permit a lower impact.</li> </ul> </li> <li>• <b>System integration:</b> to be defined how to provide the platform (and the tools) to the cities, not only Oslo and Padova. <u>TO DO:</u></li> </ul>
--------------------	--



	<ul style="list-style-type: none"> <li>○ Define the implementation details (e.g. what can/has to be deployed on a cloud application versus what is better to be installed “on premise”, where/how to ingest data).</li> <li>○ Define which hardware is needed for IMPETUS installation.</li> <li>○ Define a set of services at platform level that can be used by other developers to access the platform in a standard and documented way. In this way the platform can be extended with new functionalities without having to rewrite its core.</li> </ul>
<b>User interface</b>	<ul style="list-style-type: none"> <li>● <b>Customized UI:</b> one for each kind of end users. <u>TO DO:</u> <ul style="list-style-type: none"> <li>○ Implement (starting from the same back-end) and test UIs before the Live Exercises, considering these kind of end users:               <ol style="list-style-type: none"> <li>1. SOC operators</li> <li>2. SOC supervisors</li> <li>3. IT security specialists</li> <li>4. IT supervisors</li> <li>5. Intelligence/planning specialists</li> <li>6. IT Technical admin</li> </ol> <p>For each category of user, a specific dashboard will be created in order to present relevant information. By doing this, information overload will be prevented.</p> </li> <li>○ Edit a UI manual (or a tutorial) to let the end user to customise his/her own UI.</li> <li>○ Edit a UI manual for technical admin (to create adding UIs for any further end user and to fix problems).</li> </ul> </li> <li>● <b>broadcast messages sent from the UI:</b> to be kept in mind as an opportunity. <u>TO DO:</u> <ul style="list-style-type: none"> <li>○ Analyse the integration with messaging systems (like Telegram) and the possibility to send text, images and videos. This will reduce the time needed to get the relevant information to the people that have to intervene in case of alerts.</li> </ul> </li> </ul>
<b>Standardisation</b>	<ul style="list-style-type: none"> <li>● <b>Installation/adoption</b> regardless of the characteristics of the city and its technical equipment: from Oslo and Padova to the World. <u>TO DO:</u> <ul style="list-style-type: none"> <li>○ Analyse the possible solutions that make the platform “generally adoptable”.</li> </ul> </li> <li>● <b>Compliance with International Standards</b> <u>TO DO:</u> <ul style="list-style-type: none"> <li>○ Verify if there is any Standard to be compliant with.</li> </ul> </li> </ul>
<b>Live Exercise planning</b>	<ul style="list-style-type: none"> <li>● <b>Early planning:</b> the sooner the better <u>TO DO:</u> <ul style="list-style-type: none"> <li>○ Define the dates.</li> <li>○ Verify the opportunity of planning pre-tests activities (e.g. an intermediate testing session before Live Exercises).</li> <li>○ Draft the scenarios paying attention to the meaning of every step, exercise, action (considering the larger scale of the event comparing with the APs) that will be part of the Live Exercises.</li> <li>○ Plan about people (number and roles) needed in terms of end users, volunteers acting (e.g. citizens to be involved in the tests).</li> <li>○ Verify the authorizations needed.</li> </ul> </li> </ul>
<b>Practitioner’s guides (Ethics, Operational,</b>	<ul style="list-style-type: none"> <li>● <b>Finalisation of the works in progress</b> <u>TO DO:</u></li> </ul>



<b>Cybersecurity) final editorship</b>	<ul style="list-style-type: none"> <li>○ Double check of the current status of the Practitioner’s guides.</li> <li>○ Verify that Practitioner’s guides drafts have been updated according to what emerged during APs.</li> <li>○ Collect all the possible adding inputs (e.g from COSSEC members)</li> <li>○ Complete the editorship.</li> </ul>
<b>Practitioner’s guides (usage and evaluation (during LEv/LEx) planning</b>	<ul style="list-style-type: none"> <li>● <b>Frame Practitioner’s guides works assessment planning:</b> <u>TO DO:</u> <ul style="list-style-type: none"> <li>○ Fine-tune of the Practitioner’s guides according to what is stated in the Validation Plan</li> <li>○ Update of the Validation Plan’s part related to the Platform and tools evaluation according to the last version of the Practitioner’s guides.</li> <li>○ Verify the opportunity to set some not-planned specific tests during the LEv/LEx to assess some aspects of the Platform raised with the final version of the Practitioner’s guides).</li> <li>○ Plan a dedicated collection of feedback related to Practitioner’s guides involving end users and other stakeholders (e.g. COSSEC members).</li> </ul> </li> </ul>

## 6.2 Open points

There are still some open points:

- Cybersecurity of the platform and the tools: are the platform or tools safe regarding possible cyber-attacks?
- Dependence on data provided: will the platform and the tools be able to be adopted by all the cities?
- Security of “open” public spaces: are the tools ready for open public spaces?
- Future adoption: will the potential adopter be independent from the Consortium?

In Table 16 some more details about the still-open points listed above are reported.

**Table 16: Open points summary**

<b>Cybersecurity of the platform and the tools</b>	<p>It is mandatory that the platform and the tools do not become a “door” for cyber-attack and/or that they do not increase the vulnerabilities of the local network (i.e. of the city that will adopt them).</p> <p>This topic should have been tested during the APs: it was postponed because of work-in-progress status (e.g. non-completed development of the platform and limited integration with the local IT systems)</p>
<b>Dependence on data provided</b>	<p>Currently, there is a strict connection/dependence with/from data collected by the available sensors (and CCTVs). The technical equipment of the city is currently critical: what could happen in another city with different sensors?</p>
<b>Security of “open” public spaces</b>	<p>Some of the tools seem more easily adoptable in closed spaces (indoor) than in open public one. Is this an issue?</p>
<b>Future adoption</b>	<p>Currently, an adoption of the platform would need a deep interaction with many Partners because of the installation and information about how to use the tools and because of a certain lack of standardisation. Some specific manuals related to how to manage technically the tools and the platform -in addition to the ones for end users already foreseen- are likely needed.</p>



### 6.3 Opportunities to be considered/developed

As said earlier, there are some “technical” opportunities should be analysed in term of possible implementation:

- Broadcast of messages: the operators in case of alert, should be able to involve other kind of people (colleagues on the field, supervisors, authorities, citizens) sending quickly a message directly interacting with the platform. To be defined if it is applicable and how.
- Association between counter people sensors and system of alerting: when it is possible to count the number of people insisting on a place, it could be useful to match this kind of information to a set of thresholds, crossing them could generate an alert and some actions to be taken.

### 6.4 Risks Analysis – for Live Exercises planning

After the APs, the Consortium reviewed what had taken place and some consideration useful to better plan the Live Exercise raised. The most significant ones are reported in Table 17.

**Table 17: Risks analysis summary**

Risks	Mitigation Actions
<p><b>Local context</b></p> <p>The local context can affect the tests in different ways:</p> <ul style="list-style-type: none"> <li>• Each municipality has different sensors infrastructure and equipment, and the tools may have problems being integrated in different technological context.</li> <li>• Each municipality may decide to share different data, due to technological diversities, different legal contexts or different will of the Municipalities them-selves</li> <li>• If equipment purchase is necessary, the Public Administration rules and timing (that can vary from country to country) can be quite long, maybe too much to undertake relevant tests within the schedule of an EU project.</li> </ul> <p>All these factors can affect the tests quite strongly, by reducing the actual tests possibilities and their meaningfulness</p>	<p>The technological Partners and the cities have to agree about the equipment needed to undertake the tests, the kind of data needed vs the data available.</p> <p>If issues of any kind rise, use cases and tests should be planned considering only the existing equipment, as much as possible, that are still meaningful for all the Partners involved.</p>
<p><b>Tools readiness</b></p> <p>Since this is a research project, the readiness of some tools may not be as advanced as expected, and this may affect the test and the scenario by reducing the testing possibilities</p>	<p>While developing the use cases tests, better to consider a plan A (best readiness option) and a plan B, in order to make the test meaningful even if not all the tools are as technologically advanced as expected.</p> <p>At the same time, develop a realistic scenario that fits the cities needs and the actual possibilities of the tools.</p>
<p><b>Covid-19 limits and dynamics</b></p> <p>Due to the pandemic, it has been, at it will probably still be in the future, difficult or impossible to travel and meet in person. This complicates the mutual understanding among Partners and dilates the times of work</p>	<p>Since Consortium meetings are so complicated, and on-line meetings are not as effective, trying at least to organise meetings in person in small groups, maybe even only between two Partners, may be a useful solution.</p>



	This especially among pilot cities and tech Partners and between technical Partners whose tools are related and dependent one to the other
<p><b>Covid-19 or other unforeseen events</b></p> <p>In both the APs some Partners had to cancel their trip last minute due to covid restrictions. This issue could actually happen also for other unforeseen events.</p> <p>If the presence of the Partner is essential for the success of the tests, this can cause the failure of (part of) them.</p>	<p>While developing the use cases tests, better to consider a plan A (best readiness option) and a plan B, where it is still possible to undertake a meaningful test even if the technical Partners cannot participate in person.</p> <p>Train the local end users to let them to have a basic knowledge of the tools and to be able to use them without support.</p> <p>When possible, develop the tools according with the local infrastructure or web applications, to avoid missing essential equipment during the tests.</p>
<p><b>New processes</b></p> <p>Typically, the use or the adoption of new tools implies new processes. There is the risk that the end users do not want to change or they could not understand and appreciate the proposed innovations and the advantages for the daily work. This lack of involvement could cause the complete or partial “rejection” of the new items. Changes, indeed, are “always” painful.</p>	<p>The construction of new processes should not be rigid but take into consideration the local working process and find a way to simplify the daily job of the operators affected by the new processes. To do so:</p> <ul style="list-style-type: none"> <li>• Organize face to face meetings to help the operators feel more confident with new tools and processes.</li> <li>• Test the effective contribution of new tools by comparing the SOC work in the same scenario, but with and without IMPETUS</li> </ul>
<p><b>Language gap</b></p> <p>The Partners that work in the front line in the project are all familiar with English, but the communications with local operators can be complicated.</p> <p>Future collaborations and deployment of the platform and the tools may be threatened by the difficulty in communication between technical Partners and municipalities, especially in view of various cities involved in the future.</p>	<p>To mitigate this risk a manual as “reader-friendly” as possible, and translations to other languages seem important actions to be undertaken</p>
<p><b>Miscommunication to the public</b></p> <p>New tools and new processes may rise doubts and worries in the local population.</p> <p>Most of the people may be worried by the collection of data, if they will not be reassured by the ethical use of them</p>	<p>To inform the citizens and involve them as much as possible, prepare some brochures explaining the scope and goal of the tests, and clarifying the main highlights, to distribute before and during the tests.</p> <p>The same contents should be published in the municipalities’ websites and, if possible, in the local newspapers.</p>
<p><b>Ethics and privacy</b></p> <p>Since during the APs the activities focused on the tools testing, the attention for the ethics aspects could not be properly perceived by Partners and external observers. The risk is that ethics may appear neglected</p>	<p>Before the tests, briefly explain all the passages undertaken to respect all the privacy and ethic aspects of the project, highlighting, in particular, the issues that needed specific care</p>
<p><b>Schedule</b></p> <p>The activities to undertake are a lot, but the risk, with a very busy schedule, is that they are perceived as too many. Furthermore, Partners may be disappointed if,</p>	<p>Avoid a too busy schedule and too long days.</p> <p>When possible, avoid overlapping sessions (this may be hard in order to test tools and platform in a continuous scenario)</p>



due to overlapping sessions, they miss some activities they are interested in.	
--	--

In addition to the above mitigation actions and following the reviewer recommendations, dedicated working groups will be timely established to develop

- i) an effective holistic scenario for the Live Exercises in order to highlight the usability of the Platform and the tools;
- ii) mechanism for recruiting and ensuring an active participation of end users;
- iii) mechanisms for developing COSSEC capability and outputs;
- iv) mechanisms to improve effective communications between Partners; and
- v) contingency plan to mitigate the effects of COVID19 and variants.



## 7 APPENDIX A: surveys about APs

Scores reported in Table 18 are based on a 1 (poor) to 6 (excellent) rating system.

**Table 18: whole list of questions asked after the APs**

Question	Survey after Oslo AP	Survey after Padova AP
How do you rate the travel information prior to the AP in Oslo/Padova	5.07	5,47
How do you rate the facilitation of food/coffee and snacks during the AP?	5.31	4,94
How do you rate the Project Dinner?	5.64	5,68
How do you rate the meeting area as a base for the AP??	5.56	5,27
How do you rate the collaboration with Oslo/Padova prior to AP?	5.71	5.58
How do you rate the collaboration with Oslo/Padova during the AP?	5.75	5.5
How do you rate the digital facilitations during the AP?	5.19	5,41
How do you rate the AP schedule in terms of information, execution and time?	5.50	5,41
How do you rate the information flow provided by Oslo/Padova during the AP?	5,50	5
How do you rate the relevance of the tech Partner presentations before each tool test?	5.00	5.29
How do you rate the facilitations of the tool tests?		
How do you rate the meaningfulness of the tool tests?	4.75	5.23
How do you rate the evaluation processes during the AP. (Debriefs, evaluation presentations etc.)	5.00	5.17
How do you rate the protection of ethical aspects during the AP? (GDPR, consent etc.)	5.13	5.29
How was your overall experience of the Acceptance Pilot? 1-5	5	5.47



## Members of the IMPETUS Consortium

	SINTEF, Strindvegen 4, Trondheim, Norway, <a href="https://www.sintef.no">https://www.sintef.no</a>	Joe Gorman <a href="mailto:joe.gorman@sintef.no">joe.gorman@sintef.no</a>
	Institut Mines Telecom, 19 place Marguerite Perey, 91120 Palaiseau, France, <a href="https://www.imt.fr">https://www.imt.fr</a>	Joaquin Garcia-Alfaro <a href="mailto:joaquin.garcia_alfaro@telecom-sudparis.eu">joaquin.garcia_alfaro@telecom-sudparis.eu</a>
	Université de Nimes, Rue du Docteur Georges Salan CS 13019 30021 Nîmes Cedex 1, France, <a href="https://www.unimes.fr">https://www.unimes.fr</a>	Axelle Cadiere <a href="mailto:axelle.cadiere@unimes.fr">axelle.cadiere@unimes.fr</a>
	Consorzio Interuniversitario Nazionale per l'Informatica, Via Ariosto, 25, 00185 – Roma, Italy, <a href="https://www.conorzio-cini.it">https://www.conorzio-cini.it</a>	Donato Malerba <a href="mailto:donato.malerba@uniba.it">donato.malerba@uniba.it</a>
	University of Padova, Via 8 Febbraio, 2 - 35122 Padova, Italy, <a href="https://www.unipd.it">https://www.unipd.it</a>	Giuseppe Maschio <a href="mailto:giuseppe.maschio@unipd.it">giuseppe.maschio@unipd.it</a>
	Biotehnoloogia ja Meditsiini Ettevõtluse Arendamise Sihtasutus, Tiigi 61b, 50410 Tartu, Estonia, <a href="https://biopark.ee">https://biopark.ee</a>	Sven Parkel <a href="mailto:sven@biopark.ee">sven@biopark.ee</a>
	SIMAVI, Complex Victoria Park, Corp C4, Etaj 2, Șos. București – Ploiești, nr. 73 – 81, Sector 1, București, Romania, <a href="https://www.simavi.ro">https://www.simavi.ro</a>	Gabriel Nicola <a href="mailto:Gabriel.Nicola@simavi.ro">Gabriel.Nicola@simavi.ro</a> Monica Florea <a href="mailto:Monica.Florea@simavi.ro">Monica.Florea@simavi.ro</a>
	Thales Nederland BV, Zuidelijke Havenweg 40, 7554 RR Hengelo, Netherlands, <a href="https://www.thalesgroup.com/en/countries/europe/netherlands">https://www.thalesgroup.com/en/countries/europe/netherlands</a>	Johan de Heer <a href="mailto:johan.deheer@nl.thalesgroup.com">johan.deheer@nl.thalesgroup.com</a>
	Cinedit VA GmbH, Poststrasse 21, 8634 Hombrechtikon, Switzerland, <a href="https://www.cinedit.com">https://www.cinedit.com</a>	Joachim Levy <a href="mailto:j@cinedit.com">j@cinedit.com</a>



	Insikt Intelligence, Calle Huelva 106, 9-4, 08020 Barcelona, Spain, <a href="https://www.insiktintelligence.com">https://www.insiktintelligence.com</a>	Dana Tantu <a href="mailto:dana@insiktintelligence.com">dana@insiktintelligence.com</a>
	Sixgill, Derech Menachem Begin 132 Azrieli Tower, Triangle Building, 42nd Floor, Tel Aviv, 6701101, Israel, <a href="https://www.cybersixgill.com">https://www.cybersixgill.com</a>	Benjamin Preminger <a href="mailto:benjamin@cybersixgill.com">benjamin@cybersixgill.com</a> Ron Shamir <a href="mailto:ron@cybersixgill.com">ron@cybersixgill.com</a>
	City of Padova, via del Municipio, 1 - 35122 Padova Italy, <a href="https://www.padovanet.it">https://www.padovanet.it</a>	Enrico Fiorentin <a href="mailto:fiorentine@comune.padova.it">fiorentine@comune.padova.it</a> Stefano Baraldi <a href="mailto:Baraldis@comune.padova.it">Baraldis@comune.padova.it</a>
	City of Oslo, Grendsen 13, 0159 Oslo, Norway, <a href="https://www.oslo.kommune.no">https://www.oslo.kommune.no</a>	Osman Ibrahim <a href="mailto:osman.ibrahim@ber.oslo.kommune.no">osman.ibrahim@ber.oslo.kommune.no</a>
	Institute for Security Policies, Kruge 9, 10000 Zagreb, Croatia, <a href="http://insigpol.hr">http://insigpol.hr</a>	Krunoslav Katic <a href="mailto:krunoslav.katic@insigpol.hr">krunoslav.katic@insigpol.hr</a>
	International Emergency Management Society, Rue Des Deux Eglises 39, 1000 Brussels, Belgium, <a href="https://www.tiems.info">https://www.tiems.info</a>	K. Harald Drager <a href="mailto:khdrager@online.no">khdrager@online.no</a>
	Unismart – Fondazione Università degli Studi di Padova, Via VIII febbraio, 2 - 35122 Padova, Italy, <a href="https://www.unismart.it">https://www.unismart.it</a>	Alberto Da Re <a href="mailto:alberto.dare@unismart.it">alberto.dare@unismart.it</a>