Grant number: 883286
Project duration: Sep 2020 – Feb 2023
Project Coordinator: Joe Gorman, SINTEF

Horizon 2020: Secure societies
SU-INFRA02-2019
Security for smart and safe cities, including for public spaces
Project Type: Innovation Action

http://www.IMPETUS-project.eu

IMPETUS Project Deliverable: D9.6

Standardisation Report

Dissemination Status: Public

Editor: Sachin Gaur, BMA

Authors:

Radu Popescu	SIMAVI
Joachim Levy	CINEDIT
Osman Ibrahim	OSL
Nesrine Kaaniche	IMT
Manuela Soccol	UNI
Harald Drager	TIEMS
George Markowsky	TIEMS
Brian Holecek	TIEMS
Sandro Bologna	TIEMS

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

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

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Executive Summary

The IMPETUS project, funded by Horizon 2020, is dedicated to the development and promotion of innovative technologies and tools for creating intelligent, sustainable cities and communities. In order to maximize the project's impact, the partners involved have recognized the necessity of aligning their technological advancements with existing Information and Communications Technology (ICT) standards in both the European and Global markets. Ensuring that the tools and technologies conceived by the IMPETUS project are secure, interoperable, and in line with European and Global standardization plans is crucial for facilitating their adoption by a wide range of organizations.

To accomplish this objective, the IMPETUS project has identified and documented various ICT standards already developed or under development by European Standard Definition Organisations (SDOs) and other Global SDOs. This comprehensive report outlines the ecosystem of these standards and disseminates the information to partners and stakeholders. By highlighting the relevant standards connected to technologies in the European and Global markets, the report ensures that partners remain informed of applicable standards and are encouraged to contribute actively to their ongoing development.

Several SDOs and their corresponding standards or regulations pertinent to the IMPETUS project are referenced in the report. The first two SDOs, CEN and CENELEC, host multiple essential committees, including CEN/CLC JTC 13 Cybersecurity and Data Protection, CEN/CLC JTC 21 Artificial Intelligence, and CEN-CLC-ETSI SF Smart and Sustainable Cities and Communities. The report emphasizes the significance of these committees in guaranteeing that the technologies devised by the IMPETUS project are secure, interoperable, and in accordance with European and global standardization strategies.

Additionally, the report cites the European Telecommunications Standards Institute (ETSI), which has established two relevant standards: ETSI TS 103 375 and TS 103 376, associated with IoT standards in smart city use cases and gaps. Other pertinent standards for the IMPETUS project include oneM2M, EN 303 645, ETSI TR 103 375, and TR 103 376, which are also connected to IoT standards in smart city use cases and gaps.

The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) is another SDO mentioned in the report. The ISO/IEC JTC 1/SC 41 Internet of Things and Digital Twin is an essential committee of which IMPETUS project partners should be cognizant.

The report also references the International Telecommunication Union (ITU) Study Group 20 and the Institute of Electrical and Electronics Engineers (IEEE). The latter has developed several germane standards, such as IEEE P7000™ and IEEE CertifAIEd™.

The European Commission (EC) is an additional organization referenced in the report, with several regulations relevant to the IMPETUS project highlighted, including the EU AI Act, GDPR, EU Cybersecurity Act, and Rolling Standards Plan. Adhering to these regulations is vital for ensuring the technologies developed by the IMPETUS project comply with European standards and regulations.

The report refers to the Norwegian Data Protection Authority and the AI Sandbox, a regulatory sandbox that permits organizations to test their AI technologies in a controlled environment to guarantee compliance with relevant regulations and standards.

The report presents the idea of developing a new standard to describe the types of messages that need to be exchanged between tools and central monitoring systems; this could have a major impact on markets and technology uptake.

In summary, the primary aim of the report is to align the IMPETUS project partners with the appropriate standards in the European and Global markets, ensuring that their tools and technologies are secure, interoperable, and in harmony with standardization plans.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Table of Contents

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

1 About this deliverable

1.1 Intended readership/users

The target audience of the deliverable is the project partners, standardisation development organizations regarding the technical IMPETUS results and other stakeholders who are involved in design, development and procurement of similar technologies in the smart city context.

1.2 Why is this deliverable important?

The central objective of this deliverable to promote standardisation among IMPETUS partners and IMPETUS results among the standardisation bodies and cover important regulations that are applicable to IMPETUS tools. The document provides an overview of standards linked with IMPETUS results promoted by global standards organisations. Hence it provides a mechanism to align the further evolution of IMPETUS results with global standards.

For standardization groups and regulatory bodies: in addition to the specific needs of the two pilot cities, the IMPETUS partners present an opportunity to see practical implementations of the standards that are being created by the European standards organisation bodies and to learn from further feedback and extension.

1.3 Basis of the deliverable and limitations

1.3.1.1 Basis of the deliverable:

The activities that were organised by the project partners to source standards linked information and outreach / standards activities listed below:

a. A questionnaire, capturing the awareness of the standards topic among project partners with their feedback.
b. Multiple one to one meetings with the report editor and project partners mentioned as contributors in writing this report.
c. A webinar along with the ETSI expert (Christophe Colinet), title as ‘Relevance of Standards for IMPETUS’ with project partners to discuss standards for IMPETUS on 8th Feb 2023.
d. Multiple consultations with a standards expert (Rene Lindner) from HSBooster.EU (a standards support project from EU) to improve this deliverable.

1.3.1.2 Limitations of this deliverable

Based on the questionnaire (Annex 1) and one to one meetings by the report editor with project partners made it clear two important insights:

a. Project partners have limited awareness of the standards landscape.
b. They also had very limited resources and bandwidth to contribute to standards linked work. IMPETUS project being a short-term project does not allow many years of window it normally takes to create standards. Also, the limited resources of project partners made it evident that they cannot also regularly attend the standards meeting organised by the standards bodies.

Hence, it was agreed that the scope of this deliverable will not focus on upstream activities from the project partner to standards bodies but on downstream ones to improve awareness of the project partners to adopt standards that are prevalent in the global landscape. This document also provides an elaborate coverage of various committees and bodies active in relevant standards space. This enables IMPETUS partners and other organizations involved in the development of similar technology for future contributions in the standards space linked to their products and services. As we have mapped the ecosystem for them and they do not need to start from scratch.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

2 Our approach

We will be explaining in the next sections in this report the “IMPETUS Approach to Standardisation and Regulation”. For Standardisation (1) the report will focus on (a) identifying which standards organizations might be relevant for IMPETUS; (b) Identifying the relevant standards for IMPETUS partners.

For Regulation (2) the report will focus on the tools of IMPETUS project by (a) identifying which regulatory bodies might be relevant; (b) Identifying the relevant regulatory frameworks.

This report also captures various EU funded projects and initiatives which promote a digital single market in EU where standards-driven procurement and development of standards driven technologies play a key role.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

3 Standardisation

Here we will focus on the technical results of IMPETUS by (a) Identifying which standards organizations might be relevant; (b) Identifying the relevant standards and engage IMPETUS partners around the awareness and implementation of these standards.

3.1 Relevant Standardisation Development Organisations

We start by giving an overview on standards development organizations at both the European level (CEN/CENELEC[1]/ETSI[2]) and the ISO[3]/IEC[4] level. We chose ISO/IEC/ITU-T because these standards are among the most used worldwide, and CEN, CENELEC and ETSI because the standards of these two organizations are recognized as European Standards.

3.1.1 CEN

The European Committee for Standardization (CEN) is a pivotal European Standards Development Organization, which operates alongside CEN-CENELEC and the European Telecommunications Standards Institute (ETSI). As one of three organizations officially recognized by the European Union (EU) and the European Free Trade Association (EFTA), CEN is entrusted with the development and definition of voluntary standards at the European level. By providing a robust platform for the creation of European Standards and other technical documents, CEN ensures harmonization and standardization across a diverse range of products, materials, services, and processes.

CEN's comprehensive scope encompasses a wide array of fields and sectors, including air and space, chemicals, construction, consumer products, defence and security, energy, the environment, food and feed, health and safety, healthcare, Information and Communications Technology (ICT), machinery, materials, pressure equipment, services, smart living, transport, and packaging. Through its commitment to fostering standardization activities, CEN plays a vital role in facilitating the efficient and effective functioning of the European Single Market, promoting innovation, and ensuring the safety, quality, and sustainability of goods and services across the continent.

As an essential component of a standards report, understanding CEN's role and objectives is crucial for stakeholders and decision-makers who seek to navigate the complex landscape of European standards. By leveraging CEN's expertise and resources, businesses, governments, and consumers alike can achieve a shared vision of progress, safety, and economic growth, all while adhering to the highest possible standards within their respective industries.

Website: https://www.cen.eu

3.1.2 CENELEC

The European Committee for Electrotechnical Standardization (CENELEC) is a key European Standards Development Organization that focuses on establishing voluntary standards in the electrotechnical field. This organization plays a critical role in facilitating trade between countries, creating new markets, reducing compliance costs, and supporting the development of a single European market. An understanding of CENELEC's objectives and scope is essential for stakeholders and decision-makers when addressing standards-related issues in a report.

CENELEC is committed to supporting standardization activities across a diverse range of fields and sectors, including electromagnetic compatibility, accumulators, primary cells and primary batteries, insulated wire and cable, electrical equipment and apparatus, electronic, electromechanical and electrotechnical supplies, electric motors and transformers, lighting equipment and electric lamps, low voltage electrical installations material,

[1] https://www.cencenelec.eu/
[2] https://www.etsi.org/
[3] https://www.iso.org/home.html
[4] https://iec.ch/homepage

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

electric vehicles, railways, smart grid, smart metering, and solar (photovoltaic) electricity systems, among others.

By providing a comprehensive framework for the development and adoption of electrotechnical standards, CENELEC ensures consistency and compatibility across the European market. This harmonization enables seamless integration of products and services, as well as fostering innovation, safety, and sustainability within the electrotechnical industry.

For standards report, incorporating CENELEC's role and contributions in the electrotechnical field is vital for a thorough understanding of the European standards landscape. By leveraging CENELEC's expertise and resources, businesses, governments, and consumers can work towards a shared vision of progress, efficiency, and economic growth, all while maintaining the highest standards in the electrotechnical sector.

Website: www.cencenelec.eu

3.1.3 European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) is a leading European Standards Organization (ESO) responsible for the development and maintenance of standards in the domains of telecommunications, broadcasting, and other electronic communications networks and services. Established in 1988, ETSI has garnered a reputation for fostering innovation and ensuring interoperability across the European market and beyond. With a membership base of over 900 organizations spanning more than 65 countries and five continents, ETSI serves as a platform for collaboration between a diverse range of stakeholders including manufacturers, network operators, service providers, research bodies, and government agencies.

As the recognized regional standards body, ETSI plays a crucial role in shaping the future of the rapidly evolving telecommunications and electronic communications landscape. By developing harmonized standards and technical specifications, ETSI enables seamless integration of technologies and services, while promoting a competitive environment that benefits both consumers and industry players. Its contributions to standardization efforts have had a profound impact on the global market, with many of its standards adopted internationally.

Website: https://www.etsi.org/

3.1.4 High level overview of committees and standards relevant for Smart Cities from European SDOs

CEN, CENELEC, and ETSI are European Standards Development Organizations that work together to develop and harmonize standards in various fields. For Smart Cities, their focus includes communications, data, and AI. Here is an overview of some relevant committees from each organization:

CEN:

- CEN/TC 442 - Building Information Modelling (BIM): This committee focuses on the standardization of information, processes, and data in the field of BIM, which is essential for Smart City infrastructure.
- CEN/TC 294 - Communication systems for meters: This committee works on standards related to communication systems for meters, which are crucial for smart metering and energy management in Smart Cities.

CENELEC:

- CLC/TC 205 - Home and Building Electronic Systems (HBES): This committee is responsible for standardization in the field of electronic systems for automation, energy management, and security in homes and buildings, which are integral components of Smart Cities.
- CLC/TC 215 - Electrotechnical aspects of telecommunication equipment: This committee deals with electrotechnical aspects of telecommunication equipment, including aspects related to Smart City communication infrastructures.

ETSI:

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

- ETSI TC SmartM2M - Smart Machine-to-Machine (M2M) Communications: This technical committee focuses on the standardization of end-to-end M2M communication technologies, including IoT and smart city applications.
- ETSI ISG CIM - Context Information Management: This Industry Specification Group is responsible for developing specifications that enable interoperability between various systems and data sources, which is essential for Smart Cities.
- ETSI TC ITS - Intelligent Transport Systems: This technical committee works on standards for communication and cooperation between vehicles, infrastructure, and devices, promoting efficient and sustainable urban transportation systems.
- ETSI ISG SAI - Securing Artificial Intelligence: This Industry Specification Group works on understanding the security risks related to AI, as well as developing mitigation strategies and standards for secure AI deployment in various domains, including Smart Cities.

These committees and their respective standards play a vital role in shaping the communication, data, and AI aspects of Smart Cities, ensuring interoperability, efficiency, and security in the rapidly evolving urban landscape.

- CEN, CENELEC, and ETSI have developed several standards relevant to smart cities, particularly in the areas of communications, data, and artificial intelligence (AI). These standards facilitate interoperability, security, and efficiency in the development and implementation of smart city solutions. Some notable standards include:
- ETSI TS 103 463: This standard defines a Smart City ICT Reference Framework that facilitates the development and deployment of smart city services, applications, and devices. It covers aspects such as data models, communication protocols, and interfaces.
- ETSI TS 103 264: Known as the oneM2M standard, it provides a common framework for machine-to-machine (M2M) communications and the Internet of Things (IoT) applications. This standard enables seamless integration and interoperability of IoT devices and services within smart cities.
- ETSI TS 103 645: This standard outlines the cybersecurity baseline requirements for consumer IoT devices, which are crucial components of smart city infrastructure. It helps ensure the security and privacy of smart city services that rely on IoT devices.
- CEN-CENELEC Smart City Standards: CEN and CENELEC have developed various smart city-related standards, such as EN 50600 (data center infrastructure), EN 15182 (hand-held branch pipes for firefighting), and EN 17210 (accessibility and usability of the built environment). These standards contribute to the efficient functioning and safety of smart cities.

The focus topics for IMPETUS project that are relevant from ETSI´s work are of IoT, IoT Security and Smart City linked standards. We have already mentioned them in the rolling plan in the sections below.

ETSI also organises an annual event which is called ETSI IoT Week[5]. Such an event is free to attend and presents excellent opportunities for solution developers and municipalities, to follow the latest in the Standardisation topics and also meet other relevant stakeholders from other regions which are leading the standards driven IoT deployments.

3.1.5 International Organization for Standardization (ISO)

"The International Organization for Standardization (ISO) is based in Geneva, Switzerland, and is an independent, non-governmental international organization with a membership of 167 national standards bodies. and 783 technical committees and subcommittees to take care of standards development"[6].

Website: www.iso.org

[5] https://www.etsi.org/events/2060-etsi-iot-week-2022
[6] https://www.iso.org/about-us.html

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

3.1.6 International Electrotechnical Commission (IEC)

"Founded in 1906, the IEC (International Electrotechnical Commission) is the world's leading organization for the preparation and publication of international standards for all electrical, electronic and related technologies. These are known collectively as "electrotechnology"[7].

Website: https://www.iec.ch/homepage

3.2 Overview of Standards development in EU-Global: EU Rolling Plan for Standardisation 2022[8]

The EU provides a centralised up to date resource for understanding the ICT Standardisation work across various standards defining organisations and topics that are of strategic important to the EU. The resource is called the rolling plan for Standardisation, and it is already available for 2022[9]. It is a comprehensive resource which captures the priorities set by EU and the mandate given to EU Standard Definition Organisations by the EU. It captures various topics of interest including cyber security, information security, e-privacy, IoT, AI and Smart cities. Many of the IMPETUS solutions are around cyber security, IoT, AI and smart cities and hence they may be relevant to be followed.

3.2.1.1 IoT Standards

Many of the IMPETUS solutions involve connecting sensor technologies to the platform for real-time data exchange. As a result, these solutions can be considered Internet of Things (IoT) devices, making it essential to adhere to relevant standards. Highlighting the significance of IoT topics, the report states that the number of connected devices is projected to grow to 50 billion by 2030. Consequently, interoperability among various IoT networks has become a key focus area, with the document emphasizing the continued efforts of standards development organizations (SDOs) to work on standards such as ISO 13584-1 (Industrial automation systems and integration - Parts library - Part 1: Overview and fundamental principles) and IEC 61360 (Standard data element types with associated classification scheme for electric items) in relation to semantics. The report also mentions large-scale pilots initiated since 2016, which have facilitated the enhancement and testing of IoT solutions by the public. The IoT section highlights the work of the European Telecommunications Standards Institute (ETSI), specifically ETSI TS 103 375 (SmartM2M; Smart Cities; Standardization landscape and future developments) and TS 103 376 (SmartM2M; Smart Cities; Standardization landscape and future developments; IoT networks), which are linked to IoT standards in smart city use cases and gaps. On the global level, the report refers to ISO/IEC JTC 1/SC 41 (Internet of Things and related technologies), oneM2M (a global partnership project that develops technical specifications to enable the interconnection of IoT devices and applications), and the International Telecommunication Union (ITU) Study Group 20 (IoT and its applications, including smart cities and communities).

3.2.1.2 AI Standards

Since 2018, EU has published important plans and whitepapers to clarify its strategy and objectives. The overall EU objective it to have an ecosystem of excellence and trust. Trust is the keyword here when it comes to EU policy and it is based on EU values and fundamental rights. AI is also a field which has seen very little standardisation in the past. However, it is a hot topic where we can anticipate a large amount of standards work will take place in the coming years. CEN-CENELEC have a joint technical committee on AI called as JTC 21[10]. Similarly on global level, ISO and IEC both have started a joint committee on AI called as ISO/IEC JTC 1/ SC 42[11].

IEEE also has a special focus on ethics in AI[12]. The Standard series of P7000 focus on ethics considerations for autonomous systems. As per IEEE communication, "the IEEE P7000™ series of standards projects under development represents a unique addition to the collection of over 1.900 global IEEE standards and projects. Whereas more traditional standards have a focus on technology interoperability, functionality, safety, and trade

[7] https://www.iec.ch/who-we-are
[8] https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2022
[9] https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2022
[10] https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/
[11] https://www.iso.org/committee/6794475.html
[12] https://ethicsinaction.ieee.org/wp-content/uploads/ead1e.pdf

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

facilitation, the IEEE P7000 series addresses specific issues at the intersection of technological and ethical considerations. Like its technical standards counterparts"[13].

The IEEE also has now a certification program for ethical AI. IEEE CertifAIEd™ is a certification program for assessing ethics of autonomous intelligent systems (AIS) to help protect, differentiate, and grow product adoption. The resulting certificate and mark demonstrate the organization's effort to deliver a solution with a more trustworthy AIS experience to their users[14]. A certification like this could be relevant to IMPETUS stakeholders and partners in improving trustworthiness of their AI products. The IEEE CertifAIEd webpage provides links to 4 short videos of twenty minutes in total, which is a great start for getting awareness on the topic[15][16][17][18]. We highly recommend IMPETUS partners to go through this awareness module.

In 2020, ETSI also released a white paper on AI, called as AI and future directions for ETSI[19]. The document captures standardisation work at ETSI and covers many of the topics relevant for IMPETUS for example related with Societal relevance for emergency communications.

The rolling plan also mentions the future direction for EU when it comes to AI standards. The focus topics mentioned are data governance and data quality, record keeping, provision of information and transparency, trustworthiness, robustness, accuracy and cybersecurity, human oversight, risk management and testing, conformity assessment, quality management system, lifecycle monitoring, users' conduct.

3.2.1.3 IoT Security Standards

While there are a broader range of security standards that are valid for security of any system like ISO 27000 family of standards[20]. IMPETUS pilot cities and target cities in general have already been following these standards in securing their operations.

Here we would like to particularly highlight the standard EN 303 645[21], which was published in June 2020 by ETSI. The Internet of Things is getting adopted very quickly and many of the integrations in the IMPETUS project built upon a sensor technology that sends the data via a connected device to the city authorities. This is a classic IoT deployment scenario. IoT devices are also vulnerable as security is not the primary consideration when designing such devices. Hence, EN 303 645, Cyber Security for Consumer Internet of Things: Basic Requirements is a first step in the right direction. Something that IMPETUS partners should follow and the cities that deploy tools from IMPETUS like projects should demand.

3.2.1.4 Smart City Linked Initiatives and Standards

Projects like IMPETUS find their abode in proactive and leading cities. We often find an overlap of such cities in what is popularly called as smart cities. The term "smart cities" has different origins and broader objectives than the IMPETUS project. However, the cities aiming / already in the smart city category are relevant for IMPETUS partners for future development and adoption of IMPETUS tools. Hence, we mention the EU standards work and initiatives which directly target smart cities.

The rolling plan mentions the smart cities marketplace where 110 cities and 93 Industrial partners are backing the initiative[22]. It mentions many projects and relevant information for IMPETUS project.

[13] https://standards.ieee.org/industry-connections/ec/autonomous-systems/
[14] https://engagestandards.ieee.org/ieeecertifaied.html
[15] https://www.youtube.com/watch?v=9_zbg0_p5G4
[16] https://www.youtube.com/watch?v=ppyA3vRPeLk
[17] https://www.youtube.com/watch?v=S8U79pRuJQo
[18] https://www.youtube.com/watch?v=IJxtCs9bN5U
[19] https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp34_Artificial_Intellignce_and_future_directions_for_ETSI.pdf
[20] https://www.iso.org/standard/73906.html
[21] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
[22] https://smart-cities-marketplace.ec.europa.eu/

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Another important EU initiative that has been organised in the past is Synchronocity[23]. It enabled the trial of standards driven IoT technology pilots for cities. it resulted in the creation of 10 MIMs[24] (Minimum Interoperability Mechanisms) and that are now hosted by Open and Agile Smart Cities (OASC).

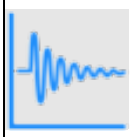
OASC is another very relevant city led grassroot body which is enabling standards driven deployment and procurement in smart cities. Many of the Norwegian and Italian cities are members. Unfortunately, the IMPETUS pilot cities are not yet OASC members.

LivinginEU[25], the latest EU initiative is continuing the previous technical standards work, building upon MIMs and has now version 5 available of MIMsPLus for cities and tool developers to consider[26]. This document is highly relevant for IMPETUS partners to consider and refer.

A special mention of oneM2M and SAREF4City[27] standards by ETSI are mentioned in the rolling plan. Which we would also highly recommend for IMPETUS project partners to consider in their implementations.

The Joint Technical Committee (JTC) 1 Working Group (WG) 11 of ISO/IE[28]C is also mentioned in the rolling plan as JTC1 WG11 focuses on Smart Cities.

3.3 What are the IMPETUS tools and quick link to them about standards?

Role	Tool	
Detecting emergencies needing *immediate response*		**Firearm Detector** Continuously monitors surveillance camera feeds and automatically creates an alert if a firearm is detected in a public space.
		**Bacteria Detector** Continuously monitors air samples to detect abnormally high concentrations of airborne bacteria.
Identifying *potential / emerging threats*		**Urban anomaly detector** Continuously monitors data gathered from multiple city sensors and detects cases deviating from the norm - indicating possible cause for concern.
		**Social Media Detector** Scans large volumes of text on social media and other public online sites, looking for topics/keywords that might indicate potential trouble or threats.
Emergency Management		**Evacuation Optimiser** Provides instant advice to emergency staff on how to effectively manage an evacuation, based on simulations of different evacuation scenarios.

[23] https://european-iot-pilots.eu/project/synchronicity/
[24] https://mims.oascities.org/
[25] https://living-in.eu/
[26] https://living-in.eu/sites/default/files/files/MIMs-Plus-LI.EU-Tech-Specs-v5.pdf
[27] https://saref.etsi.org/saref4city/v1.1.2/
[28] https://jtc1info.org/sd-2-history/jtc1-working-groups/wg-11/

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Cyber protection		**Cyber Threat Intelligence** Detects, classifies and helps mitigate cyberspace threats to an organisation's IT assets.
		**Cyber threat Detection and Response** Detects cyber vulnerabilities in IT Systems: raises alerts and suggests countermeasures if they arise.
Ensuring operational efficiency		**Workload Monitoring System** Measures mental workload and stress of emergency operators using a brain-computer interface, raises alerts if anomalies arise.
Overall Platform		Integrates the output of all the above tools in a cohesive and easy to operate manner.

Below is the list of IMPETUS tools and platform, along with possible communication standards from international standards bodies that may be relevant to each one of them.

Detecting emergencies needing immediate response

a. Firearm Detector

This innovative solution is designed to leverage video feeds from surveillance cameras for firearm detection, thus playing a vital role in enhancing public safety. To ensure its seamless integration, interoperability, and reliability, the Firearm Detector should align with a number of global ICT standards. Some relevant ones are mentioned below:

[1] https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

[2] https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

ISO/IEC 23009 (Dynamic Adaptive Streaming over HTTP)

This standard defines the delivery of multimedia content over the internet using adaptive streaming techniques, allowing seamless playback of video content even with fluctuating network conditions. It is relevant to the Firearm Detector for streaming video feeds from surveillance cameras to the detection system.

IEC 62676 (Video Surveillance Systems)

This standard series covers the design, installation, and operation of video surveillance systems, including performance requirements and specifications for video transmission, storage, and analytics. It ensures that the Firearm Detector's video processing and analysis components adhere to established guidelines and deliver reliable performance.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

ISO/IEC 2382-28:2015, Information technology — Vocabulary — Part 28: Artificial intelligence, aids in the development and application of AI in the Firearm Detector, providing crucial definitions and terminologies.

Moreover, IEEE 7000 - Model Process for Addressing Ethical Considerations in System Design, ensures ethical considerations are incorporated throughout the development and operation of the AI in the Firearm Detector.

IEEE P7003 - Standard for Algorithmic Bias Considerations, ensures the AI system within the Firearm Detector is transparent and eliminates any potential biases in its functionality.

Furthermore, the ITU-T Y.3172 standard for Architectural Framework for Machine Learning in Future Networks including IMT-2020, provides guidance on how machine learning technologies can be applied in the Firearm Detector's system, particularly in the context of data analysis from surveillance feeds.

The solution developer have already developed a privacy preserving method which follows GDPR for on ground deployment by masking the person in the camera surveillance. If the fire arm is detected then only the relevant city authority can remove the mask.

Some of the important guidelines and reports that are relevant for the solution developer are:

The High-Level Expert Group on Artificial Intelligence (HLEG AI), an independent advisory body set up by the European Commission, has published Ethics Guidelines for Trustworthy AI[1]. The guidelines offer a robust framework for achieving ethical AI, emphasising principles such as transparency, fairness, and accountability, among others.

Furthermore, the European Union Agency for Cybersecurity (ENISA) has published a report on 'Artificial Intelligence Cybersecurity Challenges[2],' which provides recommendations for securing AI systems.

b. Bacteria Detector

ISO/IEC 17025 (General Requirements for the Competence of Testing and Calibration Laboratories)

This standard outlines the general requirements for the competence, impartiality, and consistent operation of testing and calibration laboratories. By adhering to ISO/IEC 17025, the Bacteria Detector can ensure accurate and reliable measurements and promote confidence in its testing results.

ISO 16000 (Indoor Air Quality)

This series of standards focuses on indoor air quality, addressing various aspects such as sampling strategies, measurement methods, and evaluation of results. By complying with the ISO 16000 series, the Bacteria Detector can effectively assess bacteria levels in indoor environments and contribute to maintaining a healthy and safe atmosphere for occupants.

Identifying potential/emerging threats

a. Urban Anomaly Detector

The Urban Anomaly Detector, another crucial technology developed under the IMPETUS project, uses Artificial Intelligence (AI) to identify irregularities or anomalies within urban environments. To ensure its efficient, reliable, and ethical operation, it should align with various global and European AI and ICT standards.

Global Standards:

ISO/IEC 27001: This standard for Information Security Management ensures the integrity and security of data processed and analysed by the Urban Anomaly Detector.

ISO/IEC 2382-28:2015: This standard provides crucial definitions and terminologies for the development and application of AI in the Urban Anomaly Detector.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

IEEE 7000: This standard ensures that ethical considerations are incorporated throughout the development and operation of the AI in the Urban Anomaly Detector.

IEEE P7003: This standard ensures that the AI system within the Urban Anomaly Detector is transparent and minimizes any potential biases in its functionality.

ITU-T Y.3172: This standard provides guidance on the application of machine learning technologies in the Urban Anomaly Detector's system, particularly in the context of data analysis from various sources.

ISO/IEC 38500 (Corporate Governance of Information Technology)

This standard provides a framework for effective governance of IT resources, ensuring that organizations make appropriate decisions about the management and use of information technology. It is relevant to the Urban Anomaly Detector, as it helps organizations establish and maintain effective oversight and control over the tool's operation, security, and data management.

ETSI TS 103 304 (SmartM2M; IoT LSP use cases, security, and privacy) This technical specification focuses on the security and privacy aspects of Machine-to-Machine (M2M) communication and IoT systems in the context of Large Scale Pilots (LSPs). The standard is relevant to the Urban Anomaly Detector, as it provides guidance on ensuring secure data exchange between IoT devices, sensors, and systems, as well as addressing potential privacy concerns related to the collection and processing of urban data.

b. Social Media Detector

The Social Media Detector, an integral part of the IMPETUS project, utilizes Artificial Intelligence (AI) to analyze and interpret data from social media platforms. Given the sensitivity and breadth of this data, the Social Media Detector must adhere to various global and European AI and ICT standards to ensure its operation is efficient, reliable, and ethically sound.

Global Standards:

ISO/IEC 27001: This Information Security Management standard ensures the integrity and security of the social media data processed and analyzed by the Social Media Detector.

ISO/IEC 2382-28:2015: Providing crucial definitions and terminologies for AI, this standard aids in the development and application of AI in the Social Media Detector.

IEEE 7000: This standard ensures that ethical considerations are incorporated throughout the development and operation of the AI in the Social Media Detector.

IEEE P7003: This standard ensures that the AI system within the Social Media Detector is transparent and works to minimize potential biases in its functionality.

ITU-T Y.3172: This standard provides guidance on how machine learning technologies can be applied in the Social Media Detector's system, particularly in the context of data analysis from social media sources.

ISO/IEC 27018 (Protection of Personally Identifiable Information in Public Clouds)

This standard provides guidelines for protecting personally identifiable information (PII) processed by public cloud service providers. It outlines best practices for data handling and storage, ensuring the privacy and security of personal data collected and processed by the Social Media Detector tool.

ETSI TR 103 305 (Big Data Security and Privacy)

This technical report addresses security and privacy challenges related to big data, providing recommendations for best practices, risk management, and data protection. The Social Media Detector tool, which processes large volumes of social media data, can benefit from the guidance provided by this standard to ensure the privacy and security of collected information.

Emergency Management

Evacuation Optimiser

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

ISO 22320 (Emergency Management - Guidelines for Incident Command System)

This standard provides guidelines for an Incident Command System (ICS), which is a standardized approach to managing emergency response operations. The ICS helps to ensure effective communication, collaboration, and decision-making during emergencies, which is crucial for the successful implementation of the Evacuation Optimiser.

CEN/TS 17091 (Crisis Management and Business Continuity)

This Technical Specification focuses on the process of crisis management, including the detection and assessment of crises, decision-making, communication, and coordination. Adhering to this standard ensures that the Evacuation Optimiser aligns with best practices in crisis management and supports the overall goals of maintaining safety and minimizing the impact of emergencies.

Cyber protection

a. Cyber Threat Intelligence

ISO/IEC 27001 (Information Security Management Systems)

This standard provides a systematic approach to managing sensitive information by applying risk management processes, ensuring that the information remains secure. It includes guidelines for establishing, implementing, maintaining, and continually improving an organization's information security management system (ISMS).

IEC 62443 (Industrial Communication Networks - Network and System Security)

This standard series addresses the security of industrial automation and control systems, providing guidelines and technical specifications for securing critical infrastructure from cyber threats. The standard covers aspects such as risk assessment, system design, secure development, and operational security, making it applicable to both existing and new systems.

b. Cyber Threat Detection and Response

ISO/IEC 27035 (Information Security Incident Management)

This standard provides a structured approach to managing information security incidents, including the detection, reporting, assessment, response, and learning phases. It helps organizations effectively respond to security incidents, minimize their impact, and prevent their recurrence.

ETSI EN 303 645 (Cyber Security for Consumer Internet of Things)

This standard establishes a baseline set of security requirements for consumer IoT devices, ensuring that these devices are designed, developed, and maintained with cybersecurity best practices in mind. It aims to protect consumer privacy and the wider digital ecosystem from potential cyber threats originating from IoT devices.

Ensuring operational efficiency

Workload Monitoring System

ISO/IEC 11073 (Health Informatics - Personal Health Device Communication)

This standard series focuses on personal health device communication, which can be applicable for transmitting brain-computer interface data.

IEC 62304 (Medical Device Software - Software Life Cycle Processes)

This standard is applicable for the development and maintenance of medical device software, including brain-computer interfaces used in the workload monitoring system. I

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

IMPETUS Platform

The IMPETUS Project's integrated platform, which consolidates the output of all tools developed by partners and provides a visual interface for data, requires effective communication and interoperability between various tools and systems. The following communication and ICT standards could be relevant to the platform:

ISO/IEC 27000 Series (Information Security Management Systems)

This series of standards is essential for ensuring the secure exchange of data between various tools and the integrated platform.

IETF RFC 8259 (The JavaScript Object Notation (JSON) Data Interchange Format)

This standard specifies the JSON data interchange format, which could be used for exchanging data between the platform and the tools.

OASIS MQTT (Message Queuing Telemetry Transport)

MQTT is a lightweight messaging protocol designed for limited bandwidth and high-latency networks, which can be helpful for efficient communication between the tools and the platform.

W3C Web Services Description Language (WSDL)

WSDL is an XML-based interface definition language for describing the functionality offered by a web service. It can be used for interoperability between the platform and tools using SOAP-based web services.

ISO/IEC 20547 (Information Technology - Big Data Reference Architecture)

This standard provides a reference architecture for big data systems, which could be relevant for the platform's data management and processing capabilities.

OGC Sensor Web Enablement (SWE) Standards

SWE standards enable the discovery, access, and control of sensors and sensor data. These standards can be relevant for integrating sensor-based data from the tools into the platform.

W3C Web Content Accessibility Guidelines (WCAG)

These guidelines ensure the accessibility of web content for individuals with disabilities. By adhering to WCAG, the IMPETUS Project's integrated platform can provide a more inclusive and user-friendly experience for all users, including those with visual, auditory, cognitive, or motor impairments. Implementing WCAG principles ensures that the platform is perceivable, operable, understandable, and robust for a wide range of users.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

4 Regulation

Here we will focus on the the regulations and regulatory bodies that may be relevant to tools developed inthe IMPETUS project. We do this by (a) identifying which regulatory bodies might be relevant, (b) Identifying the relevant regulatory frameworks.

4.1 Regulatory Organisations

Many of the components within the IMPETUS project process the data and interact with the network. Hence following the regulations for cybersecurity and data protection is a key aspect.

At the highest level the EU Cybersecurity Act[29] strengthens the role of ENISA (European Cybersecurity Agency) and grants a permanent mandate to the agency and gives it more resources with new tasks.

On May 13, 2022, the European parliament reached political agreement with EU Member states[30] on the directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) proposed by the commission in December 2020.

ENISA will have a role in setting up cybersecurity certification framework from a technical standpoint. Getting certified against these schemes would give a market access of the all EU member states as the certification scheme would be EU wide.

Similarly on the data protection aspects the General Data Protection Regulation (GDPR) has been valid since 25 May 2018[31]. Norway although not part of the EU but a member of the European Economic Area also follows GDPR. Thus, GDPR is applicable for EU/EEA countries.

The Norwegian Data Protection Authority[32] provides elaborate guidance on GDPR and linked regulations for data protection. Similarly in Italy, the independent body at the national level is called GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, GPDP[33] provides the elaborate guidance on privacy and personal data protection.

4.2 Regulatory frameworks relevant for IMPETUS

On the topic of cybersecurity, IMPETUS partners should closely follow ENISA and align their products and services (including IMPETUS platform) with the cybersecurity certification scheme in order to make it widely acceptable within the EU region. This will directly impact the adoption of the platform and tools for future.

ENISA also publishes high quality publications[34] from time to time for users like cities. Hence, in case of IMPETUS for municipalities / local bodies who are potential users of the IMPETUS platform they may benefit by following ENISA publications relevant to their topics in future.

In the realm of artificial intelligence, the High-Level Expert Group on Artificial Intelligence (HLEG AI) established by the European Commission has published Ethics Guidelines for Trustworthy AI. These guidelines lay out a framework for achieving ethical AI, emphasizing principles such as transparency, fairness, and accountability. By aligning with these principles, the IMPETUS project ensures its AI components are developed and operated responsibly and ethically.

On the topic of data protection, compliance to GDPR is followed within the IMPETUS project and if we specifically focus on the pilot cities of Oslo and Padova we may have to additionally look to the national bodies for specific guidance. We mention briefly the National organisations of Norway and Italy below and for future

[29] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[30] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2985
[31] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[32] https://www.datatilsynet.no/en/
[33] https://www.garanteprivacy.it/web/garante-privacy-en
[34] https://www.enisa.europa.eu/publications#c3=2012&c3=2022&c3=false&c5=publicationDate&reversed=on&b_start=0

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

adoption and deployments we recommend investigating national agencies in addition to the guidance provided by the EU rules.

Norway although not part of EU (but European Economic Area) also follows GDPR. As noted earlier, Norway follows GDPR as GDPR is applicable for EU/EEA countries. The Norwegian Data Protection Authority[35] provides elaborate guidance on GDPR and linked regulations for data protection.

One interesting initiative to be highlighted by the Norwegian DPA is a sandbox for Artificial Intelligence[36]. The initiative provides a playground for the vendors and users to allow investigation on the working of an AI solution in a safe and transparent manner before it is approved for a wider public use. The Norwegian DPA has recently organised an open event explaining the purpose of this initiative and how to apply for it[37]. There are more than 25 organisations who have applied for the sandbox of Artificial Intelligence.

4.3 How can IMPETUS partners contribute to Standards and Regulations?

AI linked standards are still emerging and the EU has recently proposed an AI act[38]. However, these are still early days for regulating AI solutions and hence policy makers would need feedback from on the ground experiences. We capture some possibilities below where IMPETUS partners can pioneer best practices and share their experience with others.

To highlight this, we discuss one example of challenges and opportunities with the AI systems.

CINEDIT, one of the IMPETUS partners, has done a very good job in data protection and privacy measures by masking the faces when running the AI models for weapon detection.

CINEDIT and others rely on a trained AI model. Which may vary from one deployment to another. Oslo has a different weather pattern than Padova for example. Hence, the training data must provide for different seasons, lighting conditions etc. In order to be more transparent for the buyer of an AI solution, the developer should specify the higher level details of the training dataset of the AI model. These details should include the nature of the population it was trained on (gender, ethnicity, race etc.), the types of weather patterns it was trained on etc. A clear explanation of what metadata is shared by the AI models needs to be provided. This enables the end users (city authorities in this case) to understand better what they are buying.

This is a fast-evolving domain where there are no clear standards and regulations, but best practices are emerging.

a. Model Cards[39] is one approach where the AI models can list various meta data linked with the model. So, along with the Model the developer provides a specification sheet, which specifies the details about the training dataset.
b. AI assurance: Center for Data Ethics and Innovation (CDEI) has published a report[40] on AI assurance which delves into various topics around assurance of AI tools in the public sphere. On similar lines, DNV one of the Norwegian multinationals, which specializes in assurance and certification of industrial systems have also started research on assurance of AI models[41]. On their website they mention topics under assurance of AI systems as data coverage evaluation, AI integrity evaluation, Adversarial testing and continuous assurance. They also mention their framework, DNV-RP-0510 Framework[42] for providing assurance for machine learning based systems. IMPETUS partners may like to discuss more

[35] https://www.datatilsynet.no/en/
[36] https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/
[37] https://www.datatilsynet.no/en/news/aktuelle-nyheter-2022/the-sandbox-seminar-2022/
[38] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence
[39] https://modelcards.withgoogle.com/about
[40] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1039146/The_roadmap_to_an_effective_AI_assurance_ecosystem.pdf
[41] https://www.dnv.com/research/future-of-digital-assurance/artificial-intelligence.html
[42] https://www.dnv.com/software/campaigns-2020/dnvs-recommended-practice-for-machine-learning-assurance-rp.html

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

with organizations like CDEI or DNV to better inform each other on how AI assurance frameworks can be developed in the future. We also again refer to IEEE CertifAIed standard for AI Ethics and Assurance[43].

IMPETUS partners are dealing with choices when it comes to deployment of AI solutions which have to deal with ethics and other aspects linked with public good. These results are captured in the Practitioners Guide[44] on operations, ethics and cybersecurity. These choices can be informative for broader policy and regulation governing AI solutions in general.

Global standards for IoT systems like oneM2M, which provide a seamless integration of heterogenous IoT data to a standardised centralised server also make a good fit for IMPETUS platform architecture. Hence a further extension of the IMPETUS platform could be to enable upstream APIs for cities to allow third party developers to build and innovate on top of the IMPETUS platform and data. However, the scope of the oneM2M standard is "*to allow any IoT application to discover and interact with any IoT device*."[45]. Thus, its focus is at the level of interacting with specific *devices*. For the kind of functionality provided in IMPETUS, where different tools report different types of security-related events to one or more monitoring locations, it would be useful to have a standard at a higher semantic level describing the classes of security information and the form/content of the type of messages that need to be exchanged. There are different types of alerts, priorities, location data, alert-specific supplementary data etc. from different tools – but they all fit within an overall framework of alerts + data. Within IMPETUS, we defined our own format for exchange of messages between the different tools and the central integrating platform. We know that our sister project, S4AllCities, defined an equivalent message format – providing support for the transmission of the same kind of information – but completely different at the detailed level of formats. If the two projects had co-operated to define a format, it would have meant that IMPETUS and S4AllCities tools could be interoperable in the sense that any of them could be "plugged in" to the central interfaces used by SOC operators in both IMPETUS and S4AllCities.

Clearly, we need to go beyond just IMPETUS and S4AllCities. To the best of our knowledge, there is no existing standard in this area. If such a standard could be developed, it would enable interoperability between tools and platforms developed by multiple vendors. We believe this could have a major impact on developing a market and enabling widespread uptake of the type of technology developed in IMPETUS.

[43] https://engagestandards.ieee.org/ieeecertifaied.html
[44] https://impetus-pg.atlassian.net/wiki/spaces/IPG/overview
[45] From "Value Proposition" for onem2m at: https://www.onem2m.org/using-onem2m/what-is-onem2m

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

5 Conclusion, recommendations and next steps

In the inception phase of the project the awareness of standardisation and its benefits was low among the project partners based on a survey that was organised by the city of Oslo, one of the project partners.

The key partners recognise the limitation that standardisation in a tight timeline project is difficult to achieve. Also, many of the partners have resource limitation for attending and contributing to meetings at standards bodies. However, they acknowledge the importance of standardisation and also the value of adopting global standards for market access. Hence, this report provides them an important starting point to engage with the standards ecosystem. Also, the activities held during the preparation of deliverable made this topic accessible to them.

We recommend partners to attend the annual event organised by various standards development organisations. Normally these events are free of charge and participation of the IMPETUS partners will bring them directly in touch with the standards ecosystem.

We find that standardisation work is a long-term commitment that many of the IMPETUS partners would continue to work on the IMPETUS tools beyond the life of the project. We hope and expect that they will be aligned to global standards to take advantage of the wider European market. In time, they may further influence the standard making process as they are pioneering many new technologies and use cases in their own right.

Also, the small medium enterprises part of such projects could gain from a direct support from SDOs that makes it easy for them to engage on the European side. As currently they see their participation as an additional burden on their resources and bandwidth. However, they are most to gain in long run as standards led development will ease their market access and adoption.

In writing of this deliverable, IMPETUS tapped also help from another EU funded project to provide Standards linked support, called as HSBooster.EU. However, the initial response was delayed and took time to engage. But after the initial hiccup it was useful to discuss with standards expert and enhance the understanding of standards for IMPETUS project. Hence, EU should make available such horizontal facilities to other EU funded project in a timely and accessible manner.

Some of the tool developers in the IMPETUS project are also pioneers and shapers of the field they operate in. Hence, they maybe making seminal contributions in how technology is developed and used. Which is important for standards setting. So, it may be a good idea to engage them again in few years to see if they are looking to contribute to standards bodies as currently they do not have resources but as they grow they may have the resources and bandwidth.

We believe that developing a standard for message exchange for the type of technology developed in IMPETUS (see end of section 4.3) would have a major impact on the market and on technology uptake, and we would strongly encourage any work in this area.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

6 Acknowledgment

During the writing of this report many one to one meeting and input sessions were organised, and their inputs were captured in this report. Specifically, we would like to acknowledge meetings with the ethics managers Manuel Soccol and Irene Negri for their contributions on the Ethics topic. We would like to the thanks the Practitioners Guide (PG) team to include inputs on standards, especially Nesrine Kaaniche for the Ethics PG. We are grateful to Osman Ibrahim of the City of Oslo for initial survey and feedback on the report. We are grateful to CINEDIT and SIMAVI for their feedback on the report. Last but not the least, we are grateful to multiple experts from TIEMS, who contributed with their feedback and inputs on this deliverable through various one-to-one meetings.

7 References

CEN/CENELEC www.cencenelec.eu

ETSI www.etsi.org

ENISA www.enisa.europa.eu

European Commission https://commission.europa.eu/index_en

ISO www.iso.org

IEC www.iec.ch

IEEE www.ieee.org

ITU www.itu.int

Norwegian Data Protection Authority https://www.datatilsynet.no/en/

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Partners of the IMPETUS consortium

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

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

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

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.