CREATE-IoT

H2020 Work Programme 2016-2017
H202-IoT-02-2016
Duration: 36 months

European Large-Scale Pilots Programme

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 06.11

Workshop on common IoT standardisation framework

Revision: 1.00
Due date: 31-03-2020 (m39)
Actual submission date: 28-03-2020
Lead partner: ERCIM

European Commission

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Summary					
No and name	**D06.11 Workshop on common IoT standardisation framework.**				
Status	Released	**Due**	m39	**Date**	31-03-2020
Author(s)	D. Raggett (ERCIM), E. Darmois (ETSI), M. Serrano (NUIG), O. Vermesan (SINTEF), R. Bahr (SINTEF), A. Kung (TI), P. Annicchino (AS)				
Editor	D. Raggett (ERCIM)				
DoW	Workshop on "Navigating IoT architectures and standards" - Workshop on common IoT standardisation framework, (final workshop on LSPs IoT standardization activities). This deliverable is part of the work carried out in tasks T06.01 (IoT Interoperability, standards approaches, validation and gap analysis) and T06.02 (Pre-normative and standardisation activities). It is centred around a presentation of the "Navigating IoT Architectures and Standards" workshop organised by the European Commission, CREATE-IoT and the AIOTI and carried out on February 19th to 21st, 2020 in Brussels. During this 3 days' workshop dedicated to the progress in IoT Standardisation, the IoT Large-Scale Pilot projects (LSPs), the CREATE-IoT CSA and the IoT Large-Scale Pilots Programme Activity Group 2 (Standardisation, Architecture and Interoperability) have contributed to a great number of sessions to address IoT Standardisation in general and some specific topics such as Privacy, Semantic Interoperability and the LSP 3D Reference Architecture model.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	02-01-2020	SINTEF	Template/Initial version.
0.01	10-02-2020	ETSI	Document structure and general information.
0.02	23-03-2020	ERCIM	Content from minutes and slides
0.03	26-03-2020	ETSI	Content addition and main rationalisation
0.04	28-03-2020	SINTEF	Internal review and comments considered.
1.00	28-03-2020	SINTEF	Final version released.

Table of contents

1. EXECUTIVE SUMMARY

1.1 Publishable summary

The 3 days' workshop "Navigating IoT Architectures and Standards" has been held on February 19th to 21st in Brussels [1]. This workshop has been organised by the European Commission, CREATE-IoT and the AIOTI.

The purpose of this 3 days' workshop was to address the recent progress made in the definition of IoT architectures and standards, in particular the contribution of the IoT Large-Scale Pilots Programme projects [2]. Multi-dimensional IoT reference architectures are of great importance in the successful development and deployment of IoT solutions since they support a holistic view of IoT systems by addressing the different functional layers, the cross-cutting functions and system properties. This approach allows the largest possible expression of the requirements for data and device security, device discovery, provisioning and management, data normalization, analytics, and services. In this perspective, the IoT reference architectures are key for standardization, as they define guidelines that can be used when planning the implementation of IoT systems in order to address the complexity of IoT solutions and ensure trustworthy, secure, scalable, interoperable IoT deployments.

This very well attended workshop (with an average of over 50 to 80 persons per day) has included keynotes, plenary and expert sessions bringing answers to what has been achieved and what remains to be done by the IoT and DEI Large-Scale Pilots Programme funded under Horizon 2020, which are team up together to develop significant contributions to piloting European platforms, data ecosystems, standardisation and pre-normative activities.

The first day of the workshop was centred around the outcomes of the STF 547 Task Force on IoT standardisation funded by the European Commission and supported by ETSI. The second day focused on the handover of common activities from the IoT LSPs cluster to the DEI LSPs cluster, while the third one was centred around AIOTI approaches to address the upcoming challenges to digitizing European industries.

The event included keynotes, plenary and expert workshop sessions bringing answers to what has been achieved and what remains to be done by the IoT and DEI Large-Scale Pilots Programme funded under Horizon 2020. With the help of the coordination and support actions CREATE-IoT, NGIoT and OPEN-DEI, these projects are expected to team up together in order to have significant contributions to piloting European platforms, Data ecosystems, standardisation and pre-normative activities.

1.2 Non-publishable information

None, the document is public.

2. INTRODUCTION

2.1 Purpose and target group

The purpose of this 3 days' workshop was to address the recent progress made in the definition of IoT architectures and standards, in particular the contribution of the IoT LSPs and the work done in the associated CSAs.

One of the topics addressed - multi-dimensional IoT reference architectures - is of great importance in the successful development and deployment of IoT solutions since these architectures support a holistic view of IoT systems by addressing the different functional layers, the cross-cutting functions and system properties.

This approach allows the largest possible expression of the requirements for data and device security, device discovery, provisioning and management, data normalization, analytics, and services. In this perspective, the IoT reference architectures are key for standardization, as they define guidelines that can be used when planning the implementation of IoT systems in order to address the complexity of IoT solutions and ensure trustworthy, secure, scalable, interoperable IoT deployments.

The topics discussed are of interest to a large range of the IoT stakeholders, to start with the technical community (e.g., IoT systems designers and developers, standardisation community participants). Since part of the workshop can be considered as the hand-over of the work of the first IoT LSPs to their successors, the topics addressed are also useful for the IoT LSPs community at-large.

2.2 Contributions of partners

ERCIM has contributed to the organization of the event, to the content of the document and several presentations during the event.

ETSI has contributed to the organization of the event, to the overall structure of the present document, to its content and to several presentations during the event.

SINTEF has contributed to the organization of the event, to the content of the document and to several presentations during the event.

NUIG has contributed to the content of the document and to several presentations during the event.

TL has contributed to the content of the document and to several presentations during the event.

AS has contributed to the content of the document and to several presentations and sessions chairing during the event.

MI has contributed to the content of the document and to several presentations and sessions chairing during the event.

2.3 Relations to other activities in the project

This event has been organized within the framework of activities of CREATE-IoT WP06 (IoT Interoperability and Standardization). It has also benefited from contributions stemming from on-going work in the IoT LSPs and the IoT Activity Group AG02 (IoT standardisation, architecture and interoperability).

3. WORKSHOP SUMMARY

The 3 days' workshop "Navigating IoT Architectures and Standards" has been held on February 19th to 21st in Brussels. This workshop has been organised by the European Commission, CREATE-IoT and the AIOTI.

The slides of presentations are available in the e-Room of CREATE-IoT and of the IoT European Large-Scale Pilots (LSP) Programme.

3.1 Context of the Workshop

This very well attended workshop (with an average of over 50 to 80 persons per day) has included keynotes, plenary and expert sessions bringing answers to what has been achieved and what remains to be done by the IoT and DEI Large-Scale Pilots Programme funded under Horizon 2020, which are team up together to develop significant contributions to piloting European platforms, data ecosystems, standardisation and pre-normative activities.

The workshop was organised in three days with complementary topics:

- The first day of the workshop was centred around the outcomes of the STF 547 Task Force on IoT standardisation funded by the European Commission and supported by ETSI.
- The second day focused on the handover of common activities from the IoT LSPs cluster to the DEI LSPs cluster.
- The third one was centred around AIOTI approaches to address the upcoming challenges to digitizing European industries.

The event included keynotes, plenary and expert workshop sessions bringing answers to what has been achieved and what remains to be done by the IoT and DEI Large-Scale Pilots Programme funded under Horizon 2020. With the help of the coordination and support actions CREATE-IoT, NGIoT and OPEN-DEI, these projects are expected to team up together in order to have significant contributions to piloting European platforms, Data ecosystems, standardisation and pre-normative activities.

3.2 Overview of the workshop

3.2.1 Day 1 ETSI STF547 Public Dissemination Workshop

On the first day of the workshop, the work was centred around the outcome of the ETSI Specialist Task Force (STF) 547. The Content of the presentations addresses the work carried out, the lessons learnt and the main guidelines for the development of IoT systems especially in the fields of security and privacy.

The STF 547, funded by the EC and supported by ETSI, was launched with the intention of addressing some of the most important issues that the development and the adoption of IoT standards are facing, in particular in the area of privacy, security, semantic interoperability and the availability of standardised platforms.

The workshop gave participants the opportunity to discuss – and challenge – the guidelines and recommendations that STF 547 has developed in 7 Technical Reports (including Teaching Material on privacy and security) which were discussed during the meeting.

The main deliverables of the work of the STF 547 are the following Technical Reports:

- TR 103 591 Privacy study report – Standards Landscape and best practices
- TR 103 533 Security study report – Standards Landscape and best practice
- TR 103 534- Teaching material – Part 1: IoT Security and Teaching material
- TR 103 534-2 Teaching material – Part 2: IoT Privacy and Teaching material
- TR 103 535 Guidelines for using semantic interoperability in the industry
- TR 103 536 Strategic/technical approach on how to achieve interoperability /interworking of existing standardized IoT Platforms
- TR 103 537 Plugtests preparation on Semantic Interoperability

In addition, the STF has developed a Special Report:

- SR 003 680 Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach

This SR is designed as a support for the dissemination of the STF results to a very large audience, beyond the technical community (addressed with the Technical Reports). It analyses a list of issues and provides guidelines and recommendations to all stakeholders involved across the whole lifecycle of IoT systems.

Some of the questions addressed in the discussions were the following:

- How can privacy regulations be supported by standards?
- Is there anything specific to IoT regarding security?
- How to enable a wider adoption of semantic interoperability in various industry sectors?
- Are there available standardised platforms that can reduce the role of proprietary platforms in the development of new IoT systems?

All of the sessions were highly interactive. The work of the STF was presented and followed by and extensive Q&A session with some of the panellists together with the audience.

The results of the STF have given ample room for the presentation of a set of guidelines that may be subject to feedback and to the identification of further work.

3.2.2 Day 2 ETSI STF547 Public Dissemination Workshop

On the second day of the workshop, the work centred around the handover of common activities from the IoT LSP cluster to the DEI LSP Cluster enabling to capitalise on the experience created and ensured the continuation of work on the gaps identified in the new projects' cluster and the AIOTO working groups.

After three years of intensive activity, the IoT European Large-Scale Pilots Programme projects launched in 2017 presented their highlights, best practices and the standardisation activities, and the new DEI Large-Scale Pilots projects launched in 2019 were introduced. The new projects address the Agri-Food sector, Energy, Health and Care and Smart Manufacturing.

Parallel break-out sessions (aka World Café) have been also organised addressing topics of common interest to identify and organise common work teams for the coming year:

- IoT Data Space, sharing and Conceptual Reference Model
- IoT Data lakes, economics of data-driven services and marketplaces
- IoT Security, privacy policy framework

This workshop has been very timely with presentations of old and new projects, with a lot of emphasis on technology for the citizens and stakeholders across different sectors and the visible emergence of vocabularies in support. The presentation of such varied projects is stressing the need to identify best practices and to share them around for effective communication within and across projects, directorates and sectors.

More of the progress will be visible at this year's IoT week in Dublin.

3.2.3 Day 3 EC-AIOTI Workshop: Breaking down the silos for IoT & DEI Standardisation

The Workshop focused on how AIOTI addresses the upcoming challenge for Digitizing European Industry and what are the approaches on standardization to promote open, active collaborations and IoT/IIoT as enabler for platform developments and marketplaces in the industrial sectors.

Challenges like gaps in IoT standardization and IoT enabled data marketplaces were also discussed. In particular the focus was on:

- **Session 1: Digital Transformation:** What are the standardization, regulation and policy needs for the successful implementation of the digital transformation in Europe, considering 5G deployments among others?
- **Session 2: IoT-enabled Data Marketplaces:** Transformative journey from building infrastructure to the local enablement of cross-domain marketplaces is underway across many domains and geographies; What are the standardization, regulation and policy needs associated with these IoT-enabled Data marketplaces?
- **Session 3: Breaking down the technology silos and how the AIOTI approach can address the horizontal harmonization.** This session focused on the work already carried out by AIOTI on the current gaps in IoT standardization and it addressed the opportunities and barriers on leveraging technologies like 5G, IoT/IIoT, AI, Robotics, Cloud and Edge Computing as well as Automation and required standards, governance, policy and rules to address the Horizontal Harmonization.

The conclusion of the sessions and of the workshop have been drawn by the EC:

- We need to find an accommodation between global and local perspectives. We may see some changes in the partnerships, and to review the standardisation approach, to identify gaps and react to market trends.
- The majority of value for the IoT is from cloud. We need to balance the interest to preserve proprietary approaches and open approaches. We have more stakeholders to talk to. More automation at the edge. A larger playground.
- We urgently need standards at the metadata level and not just the data level. We need a mix of private and public money.

4. ETSI STF 547: GUIDELINES AND RECOMMENDATIONS

4.1 Introduction

Emmanuel Darmois started by presenting an introduction to the work of the ETSI specialist task force (STF) 547, which has EC funding to develop a framework for IoT standardisation that addresses interoperability across IoT domains. STF 547 focuses on (semantic) interoperability, an end-user centred approach to privacy, and methods and techniques for secure IoT.

The essential objectives are to identify guidelines and best practices, to build a bridge to potential designers and implementers of IoT systems, and to provide comprehensive material for information, teaching/learning, and demonstration with a practical usage and implementation perspective.

The task force has produced a coordinated set of deliverables with seven technical reports in 2019, including two intended for use as teaching materials. A special report (SR 003 680) will be published at the end of February 2020 that presents a global overview of the technical reports and is targeted broadly at all stakeholders rather than just technical and standards experts. The report covers security, privacy, semantic interoperability, and platforms interoperability. It addresses the main issues that stakeholders have to deal with across the lifecycle of IoT systems, guidelines for strategic, operational and technical aspects, and the major take away messages. It further includes an analysis of relevant use cases in eHealth, smart buildings, industrial IoT and critical communications.

The task force has produced a coordinated set of deliverables with seven Technical Reports (TR) including two intended for use as teaching materials and a Special Report (SR):

- TR 103 591Privacy study report – Standards Landscape and best practices
- TR 103 533 Security study report – Standards Landscape and best practice
- TR 103 534-1 Teaching material – Part 1: IoT Security and Teaching material
- TR 103 534-2 Teaching material – Part 2: IoT Privacy and Teaching material
- TR 103 535 Guidelines for using semantic interoperability in the industry
- TR 103 536 Strategic/technical approach on how to achieve interoperability /interworking of existing standardized IoT Platforms
- TR 103 537 Plugtests preparation on Semantic Interoperability
- SR 003 680 Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach

The special report (SR 003 680) is targeted broadly at all stakeholders rather than just technical and standards experts. It addresses the main issues that all stakeholders have to deal with across the lifecycle of IoT systems, and provides guidelines for strategic, operational and technical aspects, and the major take away messages. It further includes an analysis of relevant use cases in eHealth, smart buildings, industrial IoT and critical communications.

The STF547 website is at: https://portal.etsi.org/STF/STFs/STFHomePages/STF547

4.2 Session 1 - Security

4.2.1 Technical Presentation

This session, moderated by Antonio Kung (Trialog), was fully dedicated to the issue of Security in IoT systems and to the presentation made by Scott Cadzow of the results of STF 547:

- The presentation and discussion of the nature and the role of Security methodologies, in particular Security by Design, in the development of IoT systems and how general-purpose security methodologies are applicable and how far they need to be modified and complemented in order to address the specifics of IoT systems;
- The presentation and discussion of the guidelines proposed by the STF team;
- The presentation of the Teaching Material on Security developed for teachers (in academics or the enterprise) for training students, designers and all stakeholders with an interest in understanding the basics of security in IoT systems.

Scott has described the technical reports that have been produced by STF 547 on security.

TR 103 533: "SmartM2M; Security; Standards Landscape and best practices"

This TR provides an overview of the standards landscape and best practices for applying security to IoT. The report includes:

- A simplified security model of IoT
- An introduction to the security purposes of IoT as a specialization of the generic cyber-security domain and introduces some of the paradigms used in security analysis, design, and implementation.
- An overview of the regulatory domain as it impacts IoT security.
- An overview of the security ecosystem and identifies the stakeholders in standards development and development of best practices.
- An overview of the specific technologies of security that may apply to IoT.

TR 103 534-1: “SmartM2M; Teaching material; Part 1: Security”

- This TR presents teaching material to allow readers, identified by role, to gain knowledge of the fundamentals of IoT security. The document is structured as a set of annexes each containing the outline of training material. The more detailed training material, in the form of a set of PowerPoint slides is provided on demand from ETSI.

4.2.1.1 What is Security?

The question "What is Security?" is very difficult to answer succinctly. In the context of ICT, where IoT is a specialisation of ICT, security is often taken to refer to the prevention of various forms of attack on the system, or elements of the system.

In respect to the main characteristics of IoT Systems: these are often seen as an extension to, and overload of, existing systems given the (potentially massive) addition of networked devices.

IoT systems push for an alternative approach to take account of a set of essential characteristics of IoT, however, IoT should not be treated as “just another node in the system”.

This would appear to advocate for an "IoT-centric" view. The concern here is to identify what is the change in thinking and application, for security, that is necessary to ensure IoT is properly and natively addressed.

Some characteristics of IoT that distinguish it from other ICT domains:

- **Stakeholders**: There is a large variety of potential stakeholders with a wide range of roles that shape the way each of them can be considered in the IoT system. Moreover, none of them can be ignored. Many of the stakeholders have only limited technical ability but considerable technical responsibility
- **Privacy**: In the case of IoT systems that deal with critical data in critical applications (e.g. e-Health, Intelligent Transport, Food, Industrial systems), privacy becomes a make or break property across the eco-system. From an IoT device or service perspective what contribution does each element have to make?

- **Interoperability**: There are very strong interoperability requirements because of the need to provide seamless interoperability across many different systems, sub-systems, devices, etc.
- **Security**: As an essential enabling property for Trust and privacy and safety, security is a key feature of all IoT systems and needs to be dealt with in a global manner and by default.
- **Technologies**: By nature, all IoT systems have to integrate across many diverse technologies. The balance between proprietary and standardised solutions has to be carefully managed, with a lot of potential implications on the choice of the supporting platforms.
- **Deployment**: A key aspect of IoT systems is that they emerge at the very same time where Cloud Computing and Edge Computing have become mainstream technologies. All IoT systems have to deal with the need to support both Cloud-based and Edge-based deployments with the associated challenges of management of data, etc.
- **Legacy**: Many IoT systems have to deal with legacy (e.g. existing connectivity, back-end systems). The challenge is to deal with these requirements without compromising the "IoT centric" approach.

4.2.1.2 Actors and Properties

Scott then introduced some typical actors in ICT and IoT security.

- Alice and Bob who who want to authenticate themselves to each other, to communicate in confidence, to exchange data without fear of it being manipulated
- Eve who is an eavesdropper, or more generally, the adversary
- The trusted 3rd party who introduces Alice to Bob and acts as the trust anchor for their relationship

Security deals with: *authenticity* (how does Alice know that the entity purporting to be Bob is actually Bob), *authority* (how can Bob verify that Alice is allowed to perform some operation), *confidentiality* (Alice wants to know that only Bob can hear what she says), *integrity* (Bob wants to know that a file he's received from Alice hasn't been tampered with by someone else, e.g. Eve), *availability* (is the system working), and finally, the regulatory framework provided by the applicable laws.

Scott noted that the terms security, safety and privacy are massively overloaded. Privacy depends on security: Can private data be maintained as private without knowing the identity of the holder? Is a device an identifier?

He listed things of interest: assets (what a system is composed from and what we want to protect, assets are presumed to have weaknesses and may have vulnerabilities), threats (what a system may suffer from), threat agents (used to attack a system), what objectives we need to secure and how, and the unwanted incidents that we want to avoid.

4.2.1.3 Design principles

Scott turns to design principles. Security combats risk, which can be mitigated in two ways: by reducing the likelihood of an attack and by reducing the impact of an attack. You can do this by redesigning the asset to make it less vulnerable, and by hardening the asset to make the vulnerabilities less accessible. He makes the case that security systems are fractal in nature, with the same kinds of branches at each level: confidentiality, integrity and availability. The means to provide assurance varies at different levels, but the intent remains the same.

It is common to hear concerns about the cost of designing in security, and what's the need as the device in question is considered to be just a toy, app or widget. However, to the attacker, the device is host to a camera, microphone or valuable data, etc. A similar concern is whether it is really necessary to address regulatory requirements such as GDPR, CSA, NIS and RED. This however

is a pre-condition of market access and failure to comply may mean forcible removal from the market.

4.2.1.4 Roles and responsibilities

Scott then talked about security roles and responsibilities: *System protection* involves the least knowledge model for assuring system operation, and the data needed to forecast, resolve and recover; *anti-adversary* to identify who gains from system breaches, *risk management* and *regulatory compliance*, e.g. in respect to technical provisions for GDPR, for the Cyber-Security directive, for law enforcement, support for eIDAS and so forth.

IoT devices may act as security tokens themselves, e.g. RFID tokens and wireless car keys. IoT devices may act as sensors in respect to analytic and forensic examination of attacks. IoT devices may assist in identifying and breaking the attacker's abilities. IoT devices may act as policing agents for regulations.

4.2.1.5 Standardisation landscape

There is a rich and complex standardisation landscape. This is surveyed in relation to IoT security in ETSI TR 103 533. Thought experiments can help to underpin security design. The aim is to thoroughly understand a design, and the potential means for attackers to subvert a system, such that the "unknown unknowns" are minimised.

- What tools does Eve have and where could she apply them?
- What activity of Alice and Bob is Eve trying to subvert?
- What is Eve prepared to do that Alice and Bob cannot, or will not do?

Some related considerations include: what level of knowledge about an asset is available to Eve? How much time is needed to access a system to identify a weakness, and then to develop and apply an attack? What level of expertise is needed in respect to knowledge of the underlying principles, product type or attack methods? How much access is needed to exploit a vulnerability? What kinds of equipment is needed to exploit the vulnerability?

Eve may know about the standards that are commonly used for connectivity and interoperability. Lower cost and wider application of shared capability will give Eve more time to prepare an attack. Eve may find helpful information on IoT attacks on YouTube or the dark web. IoT deployments may involve many devices, thereby giving Eve more chances to experiment and lower cost for doing so.

Attackers and defenders are engaged in an escalating war with each other. Eve tries to stay ahead of the defence forces, whilst they try to stay ahead of her. Eve is not inhibited by ethics, morals or value for money, whilst defenders need to obey the law and any ethical and moral frameworks their society sets.

4.2.1.6 Security and Trust

Good security is expensive, but cheaper than dealing with the consequences of attacks. Good security design requires a security mindset, and a little paranoia helps! Good code is easier to review for security, and to fix, than hacked together code. New regulations bring new considerations, e.g. vulnerability analysis and reporting requirements, and a clear cyber-security lifetime declaration. IoT security costs may be amortized over a larger number of units than other ICT domains.

There needs to be a countermeasure cost-benefit analysis to identify the best fit for security services and capabilities, e.g. for any cryptographic measure there are many unseen costs in respect to key management and both the infrastructure and device level.

Trust underpins security, and trust in hardware is conceptually than for software. We can use hardware as a root of trust, offering hardened security in respect to illegitimate software, networks and any human adversary.

Trust can in turn be defined as confidence in the integrity of an entity to fulfil specific responsibilities. Trust is highly dynamic and contextual. This may be described using assurance levels and elements such as identity, attribution, attestation and non-repudiation. Trust isn't commutative in the sense that if A trusts B and B trusts C then this doesn't imply that A trusts C. Trust is founded on a root of trust, which may involve tamper resistant hardware.

Scott listed some myths and commonly ignored features about trust. Trust isn't binary and may involve various levels of trust. Trust is often relative, i.e. you may trust one part more than another. Trust is rarely symmetric between parties. Trust is dependent on time, i.e. it needs to be dynamically maintained. The trust of a system tends towards the level of the least trusted element.

A trust anchor fixes the point where trust is spread, e.g. the point where cryptographic keys are stored. Software is easy to duplicate, but hardware-based trust can help to identify the original from the copy. A root of trust and a trust anchor provides a means to determine the provenance of data: who generated it, who granted permission to allow it to be generated, who sent it, who allowed it to be sent, who has access to it, and what has been done to it before it arrived?

4.2.1.7 Certification and Guidance

Scott talked about the PKU model of certification authorities – a strictly hierarchical approach to trust. He compared this to webs of trust involving relationships between different entities. This was later raised in questions – in principle non-hierarchical models of trust may be more resilient to attacks and merit further work.

The consumer IoT document from TC CYBER (TS 103 645 "Cyber Security for Consumer Internet of Things" [12]) provides basic guidance for the development and manufacturing of consumer IoT devices: avoid universal default passwords, and provide a means for managing reporting vulnerabilities, and acting on them in a timely manner throughout the lifecycle of products.

All devices should be securely updateable, and consumers should be informed when an update is needed, and preferably agree to secure automatic updates. Credentials and security sensitive data should be stored and communicated securely. The attack surfaces should be minimised.

Software integrity should be ensured through secure boot from a hardware root of trust. Devices should detect unauthorised changes, alert the consumer and/or administrator, and enter a lock down mode to minimise further risk.

Device manufacturers and service providers shall provide consumers with clear and transparent information about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers. If personal data is processed, the consumer's consent should be obtained in a valid way, and such consumers should be provided with access to their personal data at any time.

IoT devices and services should be designed to recover securely from outages of power and networks. Where practical IoT services should be able to continue operating and locally functional in the absence of network connectivity.

IoT telemetry data should be monitored and examined for security anomalies. Transfer of personal data should be kept to a minimum and anonymised. Consumers should be told about what data is collected and why.

It should be easy to remove personal data when the user wants to remove his/her data, when there is a transfer of ownership or when the user wants to dispose of the device. This should come with clear instructions and clear confirmation that the data has been deleted.

Device installation and maintenance should be easy, with minimal steps that follow best security practices on usability along with guidance on how to securely set up the device. Input data should be validated. Scott then talked about basic, foundational and organisational security controls for managing IoT/ICT entities, see figure below:

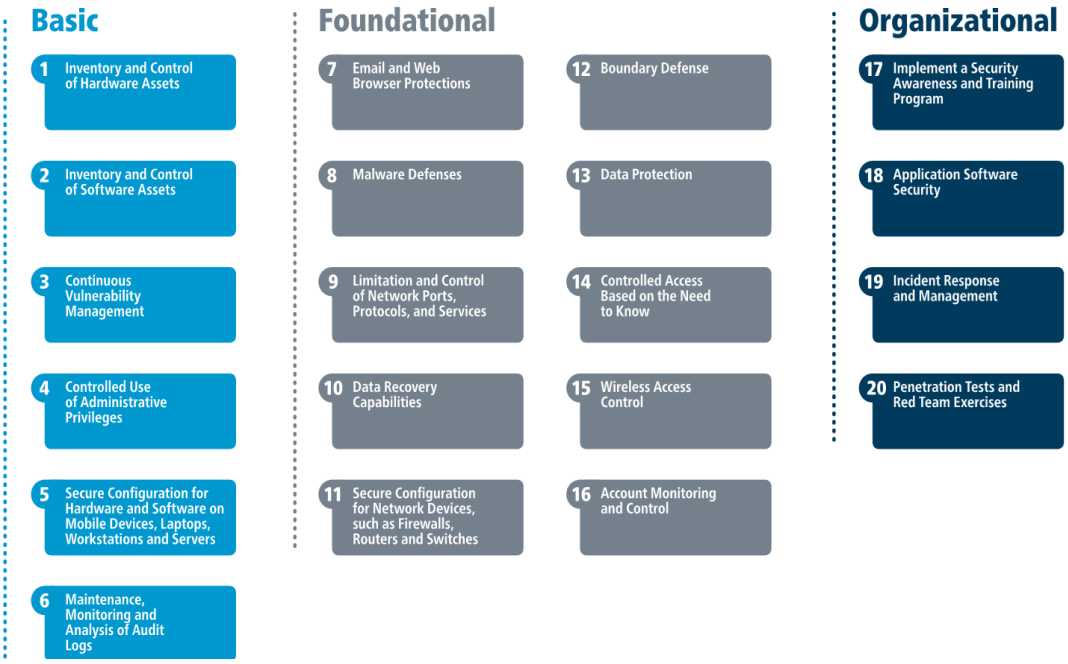


Figure 1: Basic, foundational and organisational security controls for managing IoT/ICT entities

Basic controls include knowing the physical and logical location of assets and their nature (software, hardware, firmware, process, human, …). You need to know how asset dependencies are managed and all IoT devices will require some configuration.

Foundational controls address configuration and reporting aspects for securing entities and systems, including how data is introduced and deleted, and how the elements of the system work together to enable regulatory compliance.

Organisational controls include training, pen-tests and red-teams. This includes having people put themselves in the role of would be attackers to identify and pre-empt real attacks.

IoT security should involve consideration of the entire system, end to end, including constrained devices at the edge. Scott then ran us through his Security FAQ, see the STF 547 report.

4.2.1.8 Conclusion

In conclusion, IoT security is difficult yet essential, with attackers having greater access to the toolkit for exploiting IoT compared to many other ICT systems. Risk, liability and responsibility is shared across a much greater set of actors. IoT is a catch all term covering many complex elements, e.g. virtual networking, mobility, cloud services, composite services and distributed services.

4.2.2 Q&A and discussion

The technical presentation was followed by a Q&A session introduced by Antonio Kung presenting a list of questions structured along the 4 blocks described in the following diagram.

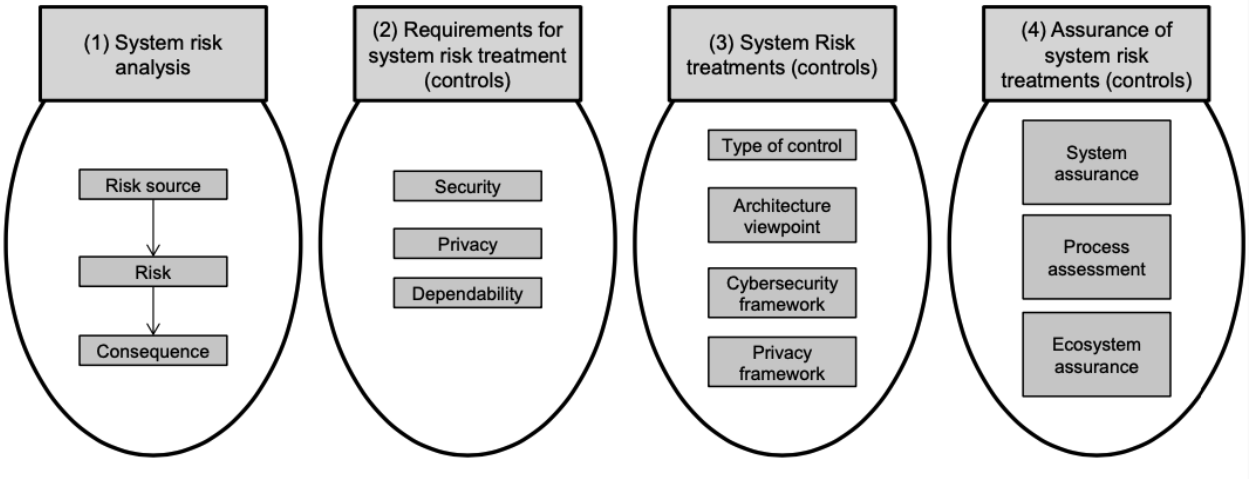


Figure 2: Questions structured along the four blocks

For each block, he presented a (potential) list of questions to be addressed:

Table 1: Potential questions according to blocks

Systems risk and analysis	**Requirements for system risk treatment (controls)**	**System risk treatments (controls)**	**Assurance of system risk treatment (controls)**
• **Method? STRIDE, LIDDUN, TVRA?** • **Consequence? Financial, Organisation, Safety, Privacy** • **System of systems?**	• Properties? • Integration of safety?	• Organisational controls? • Impact of architecture? • Lifecycle approach?	• System assurance? • Process assessment (CMM)? • System of systems/Ecosystem assurance?

Some of the main questions and answers are listed below:

Table 2: Session 1- Main questions and answers

Questions	**Answers**
Isn't hierarchical security a juicy target for attackers as once the centre has failed, the whole system crumbles? Shouldn't we be looking are alternatives that are more resilient and limit the spread of attacks?	Non-hierarchical is definitely interesting, and blockchain is an example.
Can we have further guidance?	You need to take a system level perspective.
How do we manage system risk and analysis?	This is a question of educating people and ensuring that people have a security mindset.
What are the requirements for system risk treatment (controls)? What are the properties? How do we integrate safety?	This should be engineering driven.
What about the liabilities when attacks occur?	Protection insurance is a fallback for handling liabilities but mustn't be used in place of good security.

How do we relate all this to the work in the IoT Large Scale Pilots?	The LSPs are relatively speaking not that large scale. We need to spread the thinking based upon the successes in the LSPs.
System risk and treatment controls: What are the organisational controls? What is the impact of the architecture? what is the lifecycle approach?	Moving from ICT to IoT security should be seen as a major step. This requires education and creates opportunities.
Have you also looked into ways to stimulate different types of stakeholders? One way is through regulations, another is through education.	We're mainly focused on standards. We need to ensure that organizations as a whole understand security. We need to lobby for this.
How will different IoT approaches co-exist in respect to security?	Standards doesn't mean uniformity; it rather means common building blocks. There are lots of ways for accessing the Internet, but they all work on the same framework. We need to realize that there are common goals across similar layers.
In Create-IoT, we've worked on the IoT 3D architecture. How can we frame the concepts and procedures to enable people involved in IoT to develop the necessary mindset?	The multi-layer architecture will help address the coexistence of different IoT approaches.
Assurance of system risk: how do we assure systems? Likewise, for processes and for systems and ecosystems?	You need to provide reasonable (i.e. qualified) assurance. Unfortunately, many people mistake this for absolute assurance.

Before the session came to a close, Rolf Riemenschneider (EC DG Connect, Unit E4) notes that people are building systems independently, and we have to ensure that they think in terms of system of systems.

4.3 Session 2 - Privacy

4.3.1 Technical Presentation

The session was moderated by Pasquale Annicchino (Archimede Solutions) and presented by Jumoke Ogunbekun for the STF 547.

Pasquale introduces the session and notes that Sebastian Ziegler will present tomorrow the common work of the IoT LSPs, CREATE-IoT and U4IoT on “Personal data protection for IoT deployments - lessons learned from the European large scale pilots for the IoT” (see [11]) that bears many commonalities with the work done by STF547.

Jumoke has presented a description of the privacy work in STF547 based a human centric approach to privacy in IoT. The STF has published two reports:

- ETSI TR 103 591: addressing the standards landscape and best practices [1]
- ETSI TR 103 534-2: presenting teaching material [6]

4.3.1.1 Privacy

Jumoke introduces privacy as the ability of an individual to be left alone. This concept overlaps but doesn't coincide with the concept of data protection. He distinguishes between physical privacy (e.g. of one’s home) and informational privacy (information about oneself). The right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12) as well as in the European Convention of Human Rights (Article 8).

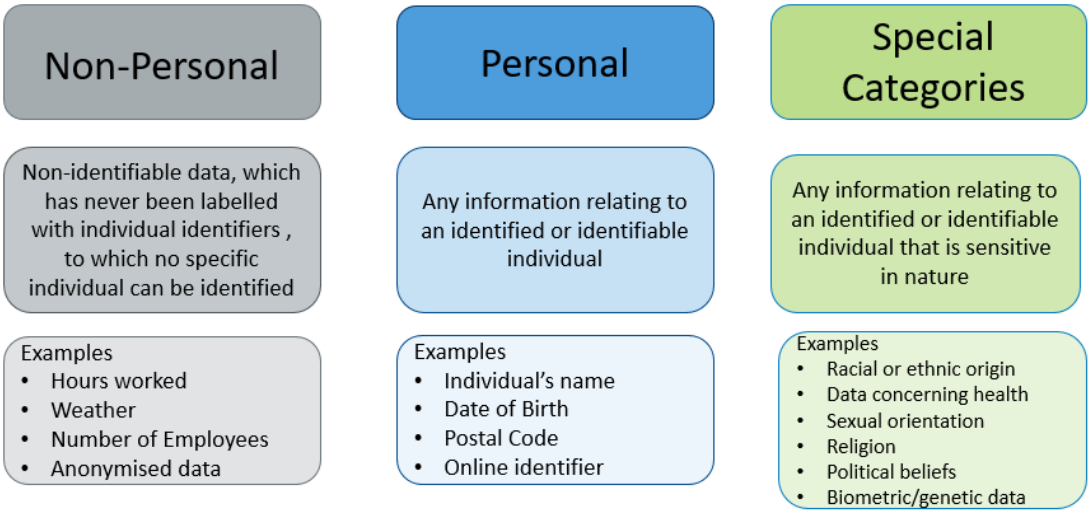


Figure 3: Personal Data categorisation

Personal Data is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity of that natural person. GDPR provides separately for special categories of data, namely, genetic data, biometric data and data concerning health.

4.3.1.2 Categories of personal data

Three categories of data: non-personal (e.g. number of employees), personal data (e.g. date of birth) and special categories (e.g. racial or ethnic origin, sexual orientation, religious affiliation). This was followed by an overview of GDPR, along with some examples of privacy scandals involving Facebook (Portal) and Amazon (Alexa). Non-EU organisations are subject to GDPR if they offer goods or services to EU residents or monitor the behaviour of EU residents.

Examples of personal data processing: in (gathering, recording, amendments), data (storage, structure, organisation), out (use, analysis, transmitting, extraction and profiling). GDPR defines processing as any operations on personal data whether it is automated or not, e.g. collection, recording, organizing, structuring, storage, adaption, alteration, retrieval, transmission, erasure or destruction.

4.3.1.3 GDPR: roles, rights

GDPR talks about profiling and automated decisions involving the processing of personal data to evaluate certain personal aspects relating to a natural person, in order to predict aspects concerning that natural person. Data has to be personal, automated and some form of evaluation must take place.

Roles within GDP, e.g. data subject, data controller, data protection officer (DPO) and data processor. In addition, third parties and supervisory authorities that monitor and enforce the application of GDPR with the aim to protect the fundamental rights and freedom of natural persons in relation to processing and to facilitate the free flow or personal data within the European Union.

Six principles covering how data is processed:

- Lawfulness, fairness and transparency
- Purpose limitation

- Data minimisation
- Accuracy
- Storage limitation
- Integrity and Confidentiality

Six reasons for why data is processed:

- Consent
- Contract
- Compliance
- Vital interest
- Public interest
- Legitimate interest

GDPR provides rights for individuals:

- Right to be informed
- Right of access
- Right of rectification
- Right to data erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Some novel aspects of GDPR include privacy by design, accountability, consent management, data protection impact assessment and data breach notification.

Procedures are required for reporting data breaches, i.e. a breach of security leading to accidental or unlawful destruction. Loss, alteration, unauthorized disclosure, access to personal data transmitted stored or processed.

4.3.1.4 Privacy and security

Privacy and security are separate concepts, but privacy depends upon security. Five principles for privacy by design.

- No personal data by default principle: avoid personal data collection or creation by default, except where, when and to the extent required.
- 'As-If' principle: design and engineer IoT ecosystems as-if these will process personal data, now or in a later phase.
- De-Identification by default principle: de-identify, sanitise or delete personal data as soon as there is valid legal basis anymore.
- Data minimization by default: only process data where, when and to the extent required, and delete or de-identity other data.
- Encryption by default principle: encrypt personal data by default and include digital rights and digital rights management thereto.

Recommendations for reinforcing the role of human users, and putting privacy concerns at the heart of IoT, and as the users and beneficiaries of IoT. Illustration of GDPR roles for ambient assisted living in smart homes.

4.3.1.5 Privacy and standardisation

STF 547 work showed that there doesn't appear to be a need for new standards, but rather a need for better guidance.

Jumoke talked about privacy in the context of the oneM2M architecture. the oneM2M Privacy Policy Manager (PPM) architecture is a distributed authorisation privacy protection architecture that takes into consideration the user's privacy preference. The PPM handles the user's consent, stores the access log, and keeps track of data that was collected. The PPM can store access control policies and with a PPM portal it can give the data subjects the ability to configure their preference. He talked about how GDPR principles apply to the PPM design support.

4.3.1.6 FAQ and key takeaways

The report addresses some FAQ and formulates key takeaways:

- The requirements set under the GDPR are mandatory.
- The effective protection of privacy and (personal) data protection, within the IoT environment requires appropriate technical and organizational measures.
- The implementation, monitoring and optimisation of measures are to be planned and taken in advance during related data collecting, data processing and data management pertaining to the life cycle of the respective IoT ecosystem.
- The GDPR further requires organizations not only to be able to ensure, but also to deliver documented and continuous proof of appropriate levels of compliance – defined in the GDPR as: accountability on a continuous basis.
- A holistic approach of IoT would presume the engagement of all IoT stakeholders and would, therefore, possibly, increase the likelihood of their wide adoption and actual implementation.
- GDPR strengthens the role of standards without necessarily dictating the creation of new standards.
- The STF547 work showed that there does not appear to be any new standards or regulations needed with respect to privacy.
- The effective use of existing standards and regulation in a circular manner would seem to be sufficient to maximize the possible resulting benefits.
- The oneM2M architecture is an example of demonstrated Privacy design for IoT system
- Compliance with GDPR should not be a mere a ''box-ticking exercise'' but should aim at the effective protection of personal information in reality.

4.3.2 Q&A and discussion

The Q&A session was moderated by Pasquale. Harm-Jan and Jumoke have brought most of the answers on behalf of STF 547.

Table 3: Session 2 - Questions and answers

Questions	Answers
Dave Raggett outlined that the Web focuses on tracking people for targeted advertising. He wants to turn that on its head and focus on pull based approaches in contrast with the push-based model inherent in advertising. This is especially relevant to the IoT, particularly in respect to home healthcare.	We see shifts happening as well, with centralized models giving way to more distributed approaches that give users more control. Cites work on distributed identifiers. Consent management and ways to help users with that. Potential role of AI.

Dave Raggett is organising a W3C workshop on pull based approaches to privacy-based business models for later this year. This emphasises user control over personal data and release to pull based services as needed. A further aspect is that users find it hard to deal with details of privacy management, and that this can be delegated to a third party based upon assessing user's attitudes as inferred by his or her behaviour. He hopes to involve the STF in the workshop given its expertise. Today's click through consent is far from the answer	Harm-Jan: we want to encourage data sharing and privacy friendly business models. Jumoke: we need to make consent a lot clearer on what people are consenting to.
A shift from free ad-based services necessitates different business models. This will need ease of use for end users as a key aspect.	The challenge is to mandate/encourage a positive approach that drives new services?
What about opportunities in smart cities?	Harm-Jan: smart cities have plenty of opportunities, cites role of living labs. We may need a global approach to avoid having a proliferation of silos. Pasquale: smart cities are a global battle ground for privacy as other regions around the world have different value systems, cites fears around face recognition in public spaces.

As a conclusion to the discussion, Franck Boissière (EC DG Connect, Unit E4) mentions that further legislative work is under consideration. Day 2's workshop will be very interesting and in line with what will be announced by the European Commission.

4.4 Session 3 - Semantic Interoperability

The session was moderated by Dave Raggett (W3C) and presented by Michelle Wetterwald and Khalil Drira for the STF 547.

4.4.1 Introduction

Dave presents a few introductory slides, starting with a list of background reports from ETSI and AIOTI WG03.

- ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach [10]
- ETSI TR 103 535 SmartM2M; Guidelines for using semantic interoperability in the industry [7]
- ETSI TR 103 537 SmartM2M; Plugtests preparation on Semantic Interoperability [9]
- AIOTI WG03 Semantic Interoperability for the Web of Things (2016) [13]
- AIOTI WG03 Semantic IoT Solutions: A Developer Perspective (Oct. 2019) [14]
- AIOTI WG03 Towards Semantic Interoperability Standards based on Ontologies (Oct 2019) [15]

He then introduced W3C's Web of Things. The IoT us fragmented with lots of technologies and standards. This is holding back the potential by increasing costs and risks, which runs contrary to the aims for a digital single market across the EU.

The Web of Things is an abstraction layer for digital twins. These are locally exposed to client applications as software objects with interfaces involving properties, actions and events,

independently of the physical location of the IoT device, and the communication technologies used to access it.

Things are assigned a URI as an identifier for metadata that describes the kinds of things, their object interfaces, and the context in which they reside.

Communications metadata used to inform client platform how to access a thing. JSON-LD is used as a popular serialisation of RDF.

This shifts the focus from IoT protocols to ontologies for things and requirements for open ecosystems of services.

Companies want to differentiate their products from those of their competitors, and to address varying customer needs across a product line with varying features (maximising profit across different kinds of customers)

Client applications want to easily work with IoT devices from different vendors and across product lines from same vendor and to take advantage of features beyond lowest common denominator.

This requires the consideration of how to describe capabilities in a flexible, modular way. It also means that the initial ontology is likely to be found inadequate. We need to ensure that a broad range of stakeholders are involved in work on standards

He listed some questions relating to semantic interoperability:

- What is it and why does it matter?
- What is the relationship to the Internet of Things?
- What is the relationship to AI and machine learning?
- How to test for semantic interoperability?
- What are we (i.e. you) doing to help this?
- How is semantic interoperability supported by IoT platforms?
- Do we need semantic interoperability in IoT platforms?
- What are the benefits of implementing semantic interoperability in IoT platforms?
- To what extent semantic interoperability can be implemented in IoT platforms?
- Can semantic interoperability be implemented for any IoT platform?
- Is there a reference model for semantic interoperability?
- What are the main interoperability issues due to the lack of a common semantic data model in IoT platforms?
- How can semantic interoperability between two IoT devices, platforms or applications be assessed?

4.4.2 Technical Presentation

The work of STF 547 was presented by Michelle and Khalil. It has addressed the general analysis of Semantic Interoperability (done in TR 103 535 [7]) and the specific issue of testing Semantic Interoperability (analysed in TR 103 537 [9]).

4.4.2.1 General analysis of Semantic Interoperability

4.4.2.1.1 Introduction to semantics

Michelle showed the following figure (from the AIOTI WG03 white paper) regarding the possible approaches to data modelling.

The scope of the STF work was on interoperability by standardisation for the most part.

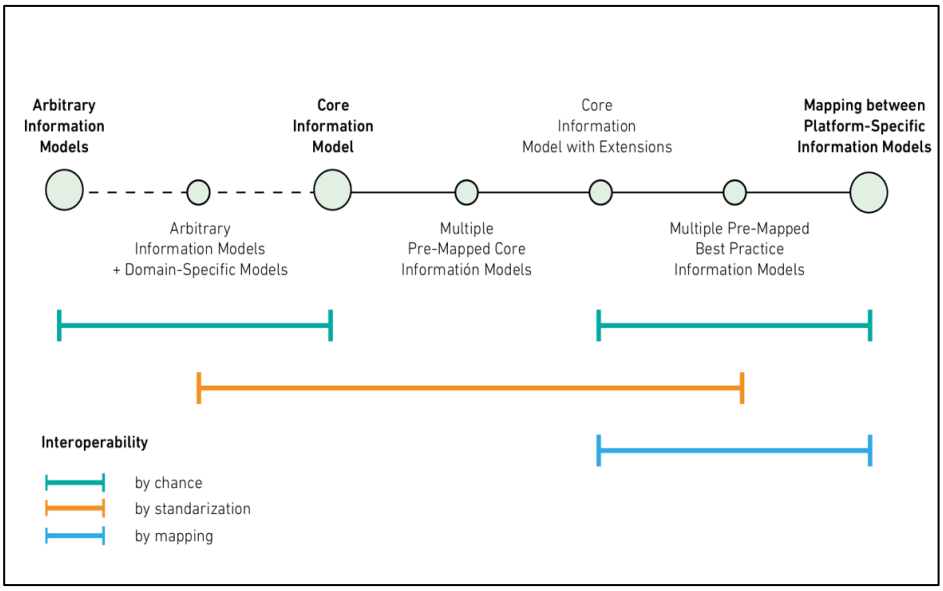


Figure 4: Possible approaches to data modelling (Source: AIOTI WG03)

There are several potential options: glossary, dictionary, taxonomy, thesaurus, topic map, metadata repository, microformat and ontology. Ontologies include concepts, relations, instances and axioms used to constrain values. Upper ontologies model common relations and objects that are generally applicable. Domain ontologies model concepts belonging to a specific domain, e.g. buildings, energy and environment.

There are many existing ontologies that have been developed in European projects, by industry or standards development organisations, e.g. ETSI SAREF, oneM2M, W3C SSN, NGSI-LD, and OPC-UA. Examples are shown from the ACTIVAGE project and the ETSI/oneM2M work on mapping the oneM2M base ontology to the SAREF ontology.

4.4.2.1.2 Semantic Interoperability – why is it necessary?

How semantics can support interoperability:

- Interworking Proxies for cross-technologies interoperability
- Standardised resource structure and URIs, and common services APIs for cross-domain interoperability of standard-specific platforms
- Mapping for cross-domain, cross-standard interoperability

The following roadmap can be defined for agreements on interoperability:

- Prior agreement on generic basic data models
- Rich domain-specific data models
- IoT upper ontology models
- Domain-specific elaborated ontology models

The interoperability layer stack has to be supported by different approaches:

- Organization and process alignment – BPM and process coordination
- Semantic alignment – metadata and ontologies
- Technical – syntax, interaction, transport

Some examples of ontologies: W3C/OGC SSN, W3C/OGC IoT Lite, VTT IoT ontology, FP7 Spitfire, IoT-O, ETSI SAREF, and the oneM2M base ontology.

How do we enable data interoperability between devices and applications without prior agreement? Can we support generic interworking and automated management of devices? Ideas for semantic based discovery/matching and binding of devices and apps. The use of reasoning to

infer new knowledge from facts. Better monitoring and understanding of the surrounding environment. Smart decisions to dynamically adapt to changes in the environment.

Some ideas for self-configuring IoT devices:

- **Monitoring** – runtime discovery of devices and updates to the ontology instance
- **Analysing** – applying semantic rules to find relevant matches between devices and actuators
- **Planning** – querying the ontology instance to find service operations of the matched devices to create actions
- **Executing** – convert actions to protocol messaging (e.g. HTTP), and create any required device subscriptions on service platform

4.4.2.1.3 Achieving Semantic Interoperability

Michelle and Khalil both discussed interoperability in terms of an eHealth scenario, before listing some considerations for achieving semantic interoperability:

- Necessity to provide rich resource and data description models to understand (e.g. units of measurements) and interpret data exchange and service requests (e.g. context-aware mapping of abstract to concrete data values or resource instances)
- Consider the trade-off between high-level semantic interoperability requirements and other scenario-specific NF constraints such as security and privacy enhanced by processing data close to its producers.
- Consider different levels of richness for the data representation models to be able to adapt to device constraints or cloud powerfulness during inference rules execution.
- Avoid defining models from the scratch and give priority to reuse of existing and standardized models (e.g. standardized ontologies: SAREF, oneM2M Base ontology) when defining new specialized models.

These points were then discussed in relation to IoT based mission critical communications. IoT communications and systems must comply with the stronger requirements of emergency services.

Safety organizations need to receive guidelines to prepare their deployments in the safest manner possible across the different services involved (police, firefighters, medical, etc.). IoT devices may not be able to exchange data with service platforms and applications because they were produced by different manufacturers or providers. System may fail because IoT device emergency data not being decodable / understood. Lack of valid data syntax and semantics may prevent data interpretation in the receiving system (e.g. data is out of accepted range)

4.4.2.1.4 Industry adoption of Semantic Interoperability

The next section of the talk addressed adoption by industry and guidelines. IoT service providers are faced with heterogeneous and vendor-specific installations.

Centralized management of IoT solution often forces the owners to go through costly replacements to adopt mono-vendor solutions. Installation of new equipment requires costly system integration because devices are often designed to communicate with specific applications only.

There is no uniform manner to access and filter the huge amounts of datasets that are generated. Huge amounts of data are generated, but never get analysed and used. IoT systems remain isolated from their surroundings and environment, resulting in poor or non-existing synergies

Industry can benefit from semantic interoperability in a number of ways:

- Continuous solution integration/operation: Quickly plug and play new equipment, networks and services in a cost-efficient manner and without disturbing the ongoing IoT system management operations.

- Efficient data exposure: IoT devices generate huge amounts of data. The exposure of these data sets through modern APIs enables proliferation of new services such as situational awareness, energy efficiency, preventive maintenance and smart data.
- Centralized management of heterogenous IoT infrastructure allows increased efficiency by setting global policies, quicker reactions and optimized decisions across all buildings. It also brings down operational costs thanks to a single software set.
- Wider integration allows the IoT system to give rise to fully integrated solution supporting mass scale deployment in multiple domains. The IoT system stops existing on its own and starts to interwork with other verticals.

Possible approaches to integration include:

- Manual file export and import: simplest method = export the data to a file and import the file into the target system.
- Extract, Transform and Load (ETL): copy of data is extracted from a source, then translated to match specific format and loaded into the destination system.
- Point-to-Point integration (P2P): ad-hoc connections between applications for near real time processes such as monitoring, alerting or triggering. As the number of applications increases, it becomes unmanageable.
- Enterprise Service Bus (ESB): hub-and-spoke approach in place of many point-to-point connections. Acts as a central broker, accepting messages from one application and sending messages to another application through near real time communications.
- Integration Platform as a Service (iPaaS): user-friendly dashboard for designing and maintaining connections and integrations, monitoring results and resolving errors. It comes with a broad array of application and technology connectors.
- Semantic interoperability platform: it enables heterogeneous devices and applications to understand exchanged data and system specification in a similar way, implying a precise and unambiguous meaning of the exchanged information.

Some market drivers for semantic interoperability:

- Enhancing existing services: Vendors must be proactive to promote the early introduction of semantic to their customers
- Providing new services: The adoption of semantic resulted from new user requirements such as context-awareness, collaboration, data sharing and automation required today in industrial areas including smart cities and industry 4.0
- Public policy support: Many companies indicated that public sponsorship for the projects and proactive roles of standardization bodies led to increased focus on semantic and its adoption and become a driving force for innovation diffusion
- Wider integration allows the IoT system to give rise to fully integrated solution supporting mass scale deployment in multiple domains. The IoT system stops existing on its own and starts to interwork with other verticals

Some corresponding market inhibitors:

- Lack of familiarity with semantic
  - Often immature supplier technology, weak development capabilities, insufficiency of experts and culture issues in industry.
- Lack of killer applications and successful cases
  - Killer applications and successful cases as guideline for the successful adoption of the semantic adoption.
  - Users want to demonstrate systems or predict test results before they adopt the semantic technologies.
  - Suppliers are suffering from problems regarding demonstration, observation and verifiability of the system.

- Complexity and immaturity
  - Many developers feel that semantic is complex to understand in terms of its application process.
  - Complexity makes developers feel uncertain about the result of semantic adoption.
  - Low opinion of the maturity level of Semantic tools as a result of the perceived gap between academic and industrial perspectives.
- Uncertainty regarding scalability and performance
  - Current semantic reasoning systems have difficulties processing large-scale data.
  - Lack of technology standards and tools supporting project development, difficulty in cost projection and quality assurance.
- Difficulties to perceive immediate value
  - The potential value of a new technology is associated with the perception of its benefits. Semantic interoperability is a long process.
  - Service improvement should be expected in the mid-long future rather than immediate increase in productivity.

Challenges for use of ontologies:

- No generally accepted upper ontology in use today
  - Upper Ontologies are difficult to design compared to domain ontologies because they describe our consensus reality, and the concepts they define are more abstract.
  - The skillsets needed to design Upper ontologies are different from domain ontologies.
- Many fragmented niches of knowledge
  - There are many niches of knowledge containing tens of thousands of class definitions that are still relatively limited in their conceptual breadth, depth and resolution.
  - Today, most vertical domains have yet to be modelled ontologically.
  - Domain ontologies need to be made public and connected together so that they can be normalized and mapped to one another.
- The ontology integration nightmare
  - It seems easier for developers to develop new ontologies from scratch but then, quite hard to make them compatible with other existing ontologies.
  - In theory, we should be able to integrate all ontologies together, however the task of actually doing such integration is difficult in practice.
  - Difficult to express the similarity and difference in meaning between concepts, relationships, attributes and their constraints.
  - The complexity of ontology integration increases exponentially to the number of concepts being integrated.

4.4.2.1.5 Guidelines

Some strategic guidelines have been proposed by the STF:

- Decide adoption and promote it
  - Proactive attitude in analysing trends or technological features and a determined will for a successful introduction is required.
  - Experts must persuade internally their department heads and resolve any conflict with managers who have a negative opinion of the semantic.
- Invest in communication and training
  - Provide educational programs for developers who do not have enough understanding or knowledge of semantic and persuaded them to participate in the programs.
  - Communicate with sales and train them is essential to overcome their knowledge gap and can align the capability of the semantic with the needs of customers.
- Outline expectation upfront

  - There is a gap between the user perspective expecting substantial performance and that of supplier recognizing some limitations due to the early stage nature of semantic.
  - The gap resulted from the frequent promotion that the reasoning engine can enable fantastic services that are not possible with existing technologies such as database and data mining.
- Promote success and expand diffusion
  - Even though semantic is adopted, further efforts will be necessary to make it easier for the system to get disseminated in an organization.
  - A stage model of technology diffusion consists of initiation, adoption and acceptance, adaptation, routinization, and infusion.

And some technical guidelines as well:

- Use an upper ontology
  - Provide a common ontological foundation for semantic interoperability across domains (e.g. oneM2M base ontology).
  - High-level compatibility and plausibility check for domain ontologies and their semantic integration.
  - Fundamental concepts defined by upper ontologies cover space and time, categories and individuals, processes, etc.
- Reuse existing domain ontologies
  - The ability to effectively and efficiently perform ontology reuse represents a potential solution to the problem of standardization.
  - It is more cost effective to build an ontology reusing existing ontologies than from scratch.
  - Reusing an ontology is far from an automated process, and instead requires significant effort from developers and experts.
- Insert ontologies in the development process
  - During the proof of concept phase, the need for semantic interoperability is not necessarily visible.
  - If not initially adopted, semantic interoperability becomes extremely costly and almost impossible to integrate properly in the future.
  - Semantic interoperability in general and ontologies in particular should be inserted at an early stage in the development process to ease the mass scale deployments of IoT systems and avoid vendor-lock in.

4.4.2.1.6 More specific answers and future directions

- Semantic interoperability in IoT platforms is considered as a step towards further global interoperability as required for different domains including industrial IoT, and smart cities. These requirements of interoperability are considered as priorities in Europe. For more details, see: ETSI TR 103 535 Sections: 6.1, 6.3.2.
- Semantic interoperability proceeds by extending the platforms interworking by providing a common data (and resources) representation model allowing platforms and associated applications to have an unambiguous understanding of the meaning of produced / exchanged / stored data (and the underlying resources such as the sensors / actuators producing / consuming such data). For more details, see: ETSI TR 103 535 Sections: 6.1, 6.3.2
- The benefits of implementing semantic interoperability in IoT platforms include extending the technical interoperability at the communication level and allowing efficient operations on data at the level of platforms and intelligent exploitation by applications. A further benefit is to help machine-level decisions by automated reasoning based on inference rules. See: ETSI TR 103 535
- The choice of the level of interoperability to be adopted and the technique to be implemented can be constrained by the computation and the communication capacities. A trade-off between

the richness of the model and the constraints of its implementation should lead to the choice of the appropriate approach and technique to be adopted. See: ETSI TR 103 535

- Semantic interoperability can be implemented for any IoT platform with more or less powerfulness in the exploitation depending on the constraints of the platform and the requirements behind implementing semantic interoperability. Different levels of interoperability are considered, and different solutions are associated. See: ETSI TR 103 535
- Several initiatives are addressing reference models for semantic interoperability. Some of them high level rich models such as oneM2M Base ontology and ETSI SAREF ontology. Others provide more basic models for REST APIs such as the IPSO data model. See: ETSI TR 103 535
- Some questions relating to semantic interoperability include: the lack of a common semantic data model in IoT platforms. There are no common methods to share, process, analyse the huge amounts of datasets generated by IoT devices. This hinders generating useful information and sharing valuable knowledge for different vertical domains and cross-domains applications. The e-health domain is an example.
- The assessment of semantic interoperability should be based on the adopted interoperability approach. For each case, ranging from schema-based to ontology-driven approaches, a specific assessment model is to be implemented. See: ETSI TR 103 537

4.4.2.2 Testing Semantic Interoperability

4.4.2.2.1 Approaches

Different approaches to semantic interoperability include: SAREF and its extensions for the different verticals; oneM2M approaches, for example base ontology, FlexContainer resources, Smart Device Template, and W3C's Web of Things.

Interoperability involves different capabilities: exchange of meaningful, actionable information, shared understanding of the exchanged information, and an agreed expectation for the request and for the response to the exchange of information.

To support this, we have: **ontology management** for the acquisition, storage of the ontologies; instantiation mapped to the node data structure; ontology update [*but not yet dynamically*]; and **data management** to generate a request, understand a request received, understand a gap in the ontology (missing information), generate a response.

4.4.2.2.2 Scenarios

Test configurations include:

- Single IoT platforms that connect multiple applications.
- Multiple IoT platforms using the same ontology, with platform to platform information exchanges; and
- Multiple IoT platforms using different ontologies.

Another scenario considers the cases involving interworking with semantic unaware systems. In this situation, data can be augmented with semantic metadata before being transferred further.

The recommendation is to do so at the border of a system rather than internally. This also applies when there is a need to map data and metadata from one ontology to another.

Testing involves reaching an agreement across stakeholders on the scope and objectives for tests and preparing a test framework that can exercise all relevant aspects, for instance, the ability to correctly process good data, and to reject bad data passing through the specified interfaces.

A methodology is needed for test reporting and if necessary, for updates to the ontologies and mappings.

4.4.3 Q&A and discussion

Table 4: Session 3 – Questions and answers

Questions	Answers
We are confronted with the challenges of making semantics easy to understand	This was the core of the STF approach, hence the guidelines provided.
Shouldn't we consider information management rather than data management?	Georgios: it is important for understanding which data should be open, what the business models are for data exchange.
What you have shown is what we've considered in the last three years. I would have liked to see what's likely to come in the future, e.g. Google's emphasis on knowledge graphs, and what the challenges are around scalability?	Actually, the STF was more tasked to look at the state-of-the-art and how it can be adopted as such by the industry. While the industry struggles to adopt SI, the research community is continuing its work. Some of it may actually simplify the current issues. An example is the use of AI for mapping ontologies.
If you need to convert data, how can you make knowledge itself interoperable? AI would be some help here	The research community is looking at this.
Can we start with existing standards on paper and transform them into ontologies?	This is what we have done in SAREF.

4.5 Session 4 - Platforms and Interoperability

The session was moderated by Georgios Karagiannis (Huawei) and presented by Emmanuel Darmois for the STF 547.

4.5.1 Introduction

Georgios presents a few slides by way of introduction, starting with a high-level definition of the idea of an IoT platform as considered by the IoT European Platforms Initiative (IoT-EPI): an IoT Platform can be defined as an intelligent layer that connects the things to the network and abstract applications from the things with the goal to enable the development of services.

An IoT platform facilitates communication, data flow, device management, and the functionality of applications.

The goal is to build IoT applications within an IoT platform framework.

The AIOTI WG03 high level functional model of IoT platforms defines three layers:

- **Application layer** that contains the communications and interface methods used in process-to-process communications
- **IoT layer** that groups IoT specific functions, such as data storage and sharing, and exposes those to the application layer via interfaces commonly referred to as Application Programming Interfaces (APIs)
- **Network layer** that provides services which can be grouped into data plane services, providing short- and long-range connectivity and data forwarding between entities, and control plane services such as location, device triggering, QoS or determinism.

4.5.2 Technical Presentation

The major point addressed by the STF 547 work on Platform Interoperability is: Are IoT platforms meant to be largely proprietary or is there room for standardised platforms in support of greater interoperability?

The ETSI TR 103 536 [8] published in December 2019 provides a strategic technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms and addresses the following questions:

- What is a platform and what are the relevant ones for IoT?
- What are the main requirements of Interoperability and Interworking?
- How these requirements are fulfilled by typical platforms.
- How those elements are fulfilled in specific sectors such as Industrial IoT.
- Which recommendations can be made for an effective selection and usage?

The essential objectives are to identify guidelines and best practices, and to build a bridge for potential designers / implementers of IoT systems.

4.5.2.1 Platform Interoperability

In more detail, the report starts with an analysis of platform interoperability in the context of IoT, including roles, reference architectures and guidelines. It provides an overview of the landscape of IoT platforms, and the strategic and technical approaches to interoperability, along with associated frameworks. It further addresses industrial IoT from the platform perspective.

IoT platforms address challenges such as:

- Flexibility, versatility
- Semantic Interoperability
- Flexible deployment models
- Open and efficient implementations
- Non-functional properties (latency, etc.)
- Security
- Privacy and data confidentiality

4.5.2.2 Platform Classification

The report considers several dimensions for classifying IoT platforms: scope and breadth, openness, origin and governance, ecosystem and maturity.

Table 5: Platform advantages and drawbacks

Type	Advantages	Drawbacks
SDO-based	• No dominant stakeholder • Open source implementation availability • No dependence from a single company • Formal testing suited available • Global certification program available • Suitable for all the IoT services in the different region of the world • Strongly focused on interoperability • Strongly focus on integration of existing technologies • Global standardization • Competition on the platform is suitable for the users who reduce the associated costs.	• A standard platform makes the platform a commodity. • Competition on the platform is not suitable for the providers, who prefer to invest and focus on the IoT services.

SSO-based	• There is usually an ecosystem of stakeholder representing the whole chain. • Open source solution often available, especially on device and gateway side. • Some have certification programs. • Some have global presence, even in vertical sectors.	• Few of them are focusing on platform interoperability, while more are focused on protocol and devices, so integration effort if expected to be still predominant. • There will be a certain dependency from specific ecosystem.
Open Source-based	• No dominant stakeholder. • Proven high TRL (e.g. TRL-9).	• Cover only parts of requirements. • Limited focus on interoperability validation.
Industry Group-based	• Usually reflect the needs of vertical sections of the industry. • Usually well thought and helpful for the implementation of some interoperability interfaces. • Sometimes no alternatives, either because of extremely widespread acceptance or because they are mandated by regulations in specific areas.	• Cover only parts of manufacturers requirements. • Need to be used i conjunction with other interoperability standards. • May allow for specific extensions by individual manufacturers.

Three IoT software stacks: constrained devices, gateways and smart devices, and IoT cloud platforms. Challenges such as flexibility/versatility, semantic interoperability, flexible deployment models. open and efficient implementations, non-functional properties, e.g. latency, security, privacy and data confidentiality.

One issue is how to find a way through the jungle of IoT platforms, as identified by UNIFY-IOT, IoT-EPI, the European IoT Large Scale Platforms (e.g. ACTIVAGE and AUTOPILOT). The IoT-EPI has produced a white paper with over 360 IoT platforms globally, with over half developed by IoT start-ups. However, though there have been many architectures for IoT platforms, there are many that are now left on the graveyard.

4.5.2.3 Standardised platforms

Standardised platforms have some defining characteristics:
- Their origin: SDO or SSOs; Open Source
- Some structuring elements: Reference Architecture; Set of supported protocols; Set of interfaces or Reference Points.

Examples of standardised IoT platforms (analysed in more details in the TR) are oneM2M, Apache and OCF.

In order to deal with interoperability, platforms have to deal with (all or part) of levels:
- Technical (e.g., communication protocols, etc.)
- Syntactical (e.g., JSON, XML, …)
- Semantic (e.g., oneM2M base ontology, SAREF, SSN)
- Organisational (e.g., the EIF guidance for interoperable digital services.

The IoT community has worked on:
- Technical approaches such as the IoT, Web of Things, Semantic Web of Things.
- Frameworks such as AIOTI, SAREF, EIF.

4.5.2.4 Industrial IoT as a case study

Smart manufacturing is central to digital transformation of industry. Industrial devices, sensors, actuators, automated machines and equipment, robots etc.

Communications backbone for data to flow throughout a factory. Support for business processes including supply chains and opportunities for improving efficiency. Fine grained information on energy consumption.

Challenge to provide better access across the different layers of an enterprise: field level, PLC, SCADA, MES and ERP. The current layered model (IEC 62264) is strictly hierarchical and acts as a brake on innovation, taking too long to implement changes.

IIoT is a major business segment, but tough due to requiring massive and effective integration of data analytics, optimisation when integrating things, devices and networks, and integration with legacy systems. There is a long list of areas where IIoT benefits are expected.

IIoT shows some contrasts with other IoT domains:

- Differences with traditional Operational Technology (OT)
  - More effective data collection capability, from the point of view of costs, speed and scalability.
  - Ability to federate heterogenous data sources, including IT data bases, thus helping to reduce silos fragmentation.
  - Ability to communicate across Factory and Enterprise boundaries.
  - Offering single point of access for analytics to all federated data.
  - Better, more flexible and suitable for self-consumption tools for data visualization are expected by users.
- Differences with consumer IoT
  - Lower number of end nodes.
  - Higher frequency of data acquisition.
  - Higher volume of data managed.
  - Need to ensure contextual consistence among data, both spatially and temporally

Regarding Data Management and Analytics, the focus is shifting from connectivity to data analytics with new offerings for the IIoT flourishing.

Vertical Integration is a key issue:

- To address the “shop-floor divide”
  - Relatively few manufacturing companies have a seamlessly integrated view of operations from shop floor up to the corporate level
  - This happens both for SMEs and larger companies
  - As a result, a very large part of the data that can be generated at the lower levels (devices and control systems) is not currently used to generate actionable insight.
- With approaches to bridge it
  - Lower costs of many of the components.
  - Availability of cloud technologies.
  - More flexible and easily deployment data analytics solutions
  - SMEs are starting to use IIoT solutions to connect ERPs to the shop floor
  - A cloud-centric infrastructure approach is now (more and more) commonly used

IIoT Platform decision criteria lead to several selection scenarios:

- Business case
- Market and product
- Investment capacity
- Product timeframe and expected evolution
- In-house integration vs system integrator
- Position in the value-chain

Table 6: Scenario pros and cons

Scenario	Description	Pros & Cons
Internal development	This is often a solution taken by incumbents that want to be able to integrate the latest technologies within their legacy solutions. The result is a proprietary platform that can become a semi-open platform by offering open components (e.g. APIs) that be used to enlarge its ecosystem.	• Mostly for (very) large companies. • Supports incremental innovation. • Allows for a coherent approach towards the customer. • May become the "de facto" reference in a sector and create an ecosystem of developers and integrators.
Integration with an ecosystem	When a significant (or "de facto") platform provider wants to enlarge the breath of its platform to new use cases(end even to new adjacent sectors), it may be interesting for a company in this new sector to enter the incumbent ecosystem the objective to contribute to the definition of the platform along the lines of its own strategy.	• A possible approach for SMEs. • Possibility to leverage the strength of the platform provider to promote its solutions against its competitors (Provided this strategy is decided and implanted quickly enough). • Difficult to maintain a differentiation in longer term.
Point solutions coupled with cloud service provider(s)	Some companies may have a basis of internal competence sin some sector with a specialized skill set without have the resources (financial and/or human) to build a full-fledge platform. The approach taken is to plug the company point solution on the infrastructure (IaaS, PaaS, and SaaS) of a cloud service provider (CSP).	• A possible approach for SMEs. • Supports the use of open source SW components. • Dependency towards the CSP and limited choice for evolution. • Difficult to generate a differentiation in the longer term.
Standardized approach	With this approach, the choice of a reference (technical) architecture is key with a definition of the layered models chosen, the choice of an information and interoperability strategy and of the reference points and supported APIs. Different parts of the platforms can be served by a combination of some of the above scenarios.	• A possible approach for SMEs. • Supports the use of open source SW components. • Limits (but does not suppress) the dependency towards the "de facto" platforms or CSP platforms chosen.

Regarding platform adoption, OPC-UA, a standard for M2M horizontal communication and vertical communication, is an important decision

- It is promoted as the foundation for digitalization in the context of Industrie 4.0.
- It provides a framework that can be used to represent complex information as objects.
- Many Industry Standards are being developed under the umbrella of OPC UA

Overall, the adoption of IIoT is slow, but steadily increasing. Barriers include security of IoT devices and having to deal with legacy (i.e. brownfield development). For instance, having to work with OS versions that are no longer supported (i.e. no longer getting security updates). Heterogeneity of deployed systems.

4.5.2.5 Guidelines and recommendations

The main lessons learned from the platform landscape analysis and the IIoT case study are:

- A landscape still very fragmented and immature
- Proprietary platforms are not a panacea

- Open platform adoption in the Enterprise is (even more) complex
- Different scenarios possible for platform availability
- A growing role for standardized solutions
- Semantic Interoperability is a key issue and a key enabler for open platform adoption
- Many issues related to platform adoption are cultural

The TR proposes a list of guidelines and recommendations:

- Technical Recommendations
  - Enough Standards to start with
  - Start small on IIoT projects
  - Agree on trade-off for implementable Semantic Interoperability
  - Insert the new technologies in the overall development process
- Recommendations to oneM2M
  - Profiling for IIoT
  - End-to-end Semantic Interoperability in oneM2M-enabled IoT platforms
  - Interworking between oneM2M and open industrial platforms. With the very important example of OPC-UA

4.5.3 Q&A and discussion

Table 7: Session 4 – Questions and Answers

Questions	Answers
Speaking about system of systems, how can we see platform vs system of systems?	In many cases a platform matches a subsystem. Therefore the question of interoperability becomes very critical when the sub-systems have been developed with (possibly completely) different approaches.
Coming back to the CREATE-IoT 3D architecture, AUTOPILOT is a good example. The platform is a necessary component in realising the function of a system of systems.	A security mindset (and a cross-cutting approach) can help to identify how components form parts of a larger system. And, as well, to identify methodologies and criteria for consideration by the various stakeholders. The 3D model can help to provide different ways of looking at things.
Legacy systems are clearly important to deal with, do you have any suggestions for how to do so?	There are technical solutions, but one should also consider servitisation, and how to provide services on top of existing systems and how to clearly define a contractual relationship.

4.6 Wrap-up

A first part of the wrap-up was dedicated to the on-line announcement to the European Parliament of the AI white paper produced by the European Commission.

Emmanuel Darmois has summed up today's workshop and thanks everyone for the part that they have played. ETSI STF 547 has now finished its work. Create-IoT has two upcoming deliverables relating to this workshop's topics. We would like to have a common understanding of what can be expected in relation to standardisation and semantic interoperability (for example). Another workshop will take place in September 2020 in Brussels, and we will seek ways to transfer our results to that event.

Some additional considerations have been brought by the participants:

- An important element on data strategy is work on platforms there are now some 1200 IoT platforms. The IoT LSPs Interoperability Framework is an approach to relate cross-sector

platforms as well as sector-specific ones. One cannot expect a single IoT platform to win out given the differing requirements across different sectors.

- There is a tendency to remain within silos rather than addressing the challenges of a cross platform approach. Indeed, one of the challenges for semantic interoperability is how to best deal with the creation and maintenance of domain specific ontologies.
- ETSI has two other special task forces that will continue after the closure of STF 547, in addition to the AIOTI work on standardisation for the IoT and a subgroup on semantic interoperability. ISO /IEC JTC1 SC41 (IoT) is also active. SAREF is a valuable part of this future. We have created an open portal for people to support its evolution.

Franck Boissière (EC DG Connect, Unit E4) has finally stressed the importance of collaborating across projects to be able to look further into the future and to improve collaboration across IoT, Big Data and AI.

5. IoT AND DEI LARGE SCALE PILOTS WORKSHOP

5.1 Introduction

Franck Boissière (EC DG Connect, Unit E4) outlined that today's workshop is important as it highlights how the IoT Large-Scale Pilots (LSPs) launched in 2016 have produced a very large legacy of results that need to be kept and expanded now that these LSPs come to an end. Today's workshop will take stock of the LSPs, but more time would be needed to do them justice.

The LSP model is now expanded to other areas and the new LSP will quickly present their projects and objectives. On a different note, the EC presented its strategy for a digital Europe yesterday. This is very similar to the way we've approached things in the LSPs.

He thanks the Coordination and Support Action and notes the USB memory cards with the slides and other documents as circulated by CREATE-IoT.

5.2 Session 1 - European Large-Scale Pilots - Presentations

This session started with summaries of the results of EU IoT Large-Scale Pilots which have been running for the last three years as part of the Horizon 2020 programme. We then heard about the Boost 4.0 project on smart factories which has been running for the last two years. And finished with very brief introduction to the newest IoT project that have recently started.

5.2.1 Taking stock of the projects about to finish

5.2.1.1 AUTOPILOT

The project was focused on autonomous driving + IoT + Mobility as a service. The approach taken is summarized in the following figure:

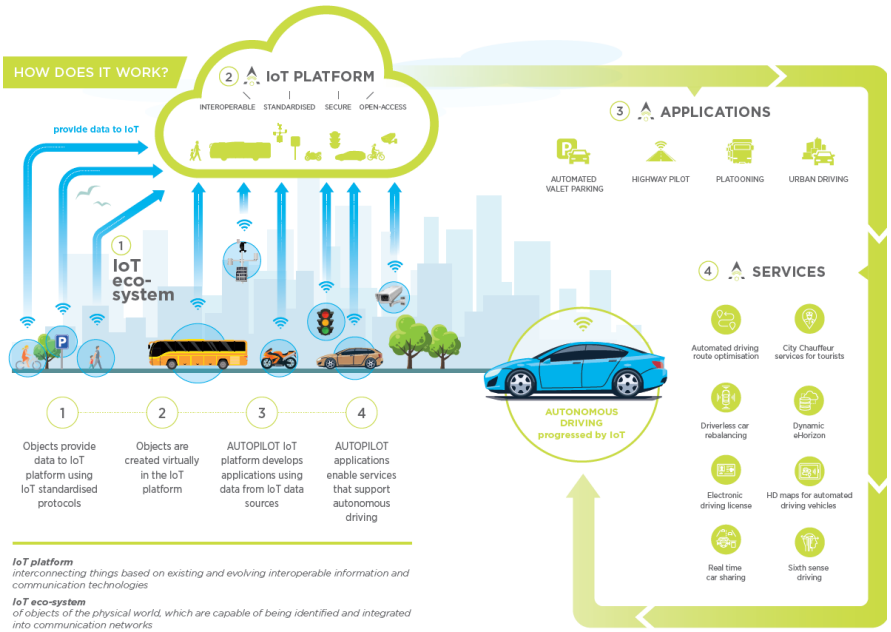


Figure 5: The AUTOPILOT project

IoT can improve mobility - better experience for users to get around, smart cities/mobility, cooperative and connected automated mobility. Related: MaaS, Data Marketplace, AIOTI and Data Lake.

How can we enable different actors to share data? What is the business model for this? Autopilot IoT platform with digital twins for physical objects, and applications that enable services that support autonomous driving. List of 8 such services, e.g. route optimisation, chauffeur for tourists, etc.

The main project results include:

- IoT progressed automated driving functions
- Vendor and Open interoperable IoT platforms
- In vehicle integration (sensor fusion) improved by IoT
- Seven use cases deployed
- New market opportunities
- Commercial business models and user compliance
- String contributions to SDOs - IoT data models and ontologies

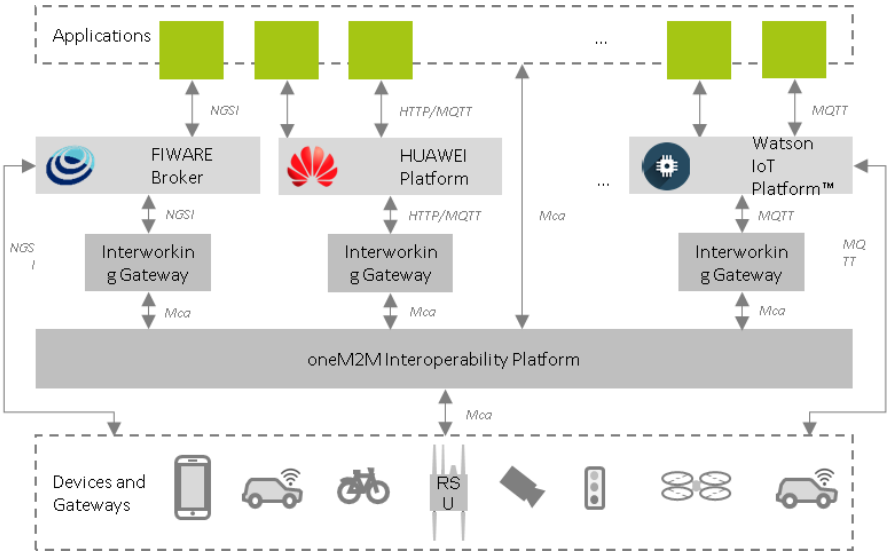


Figure 6: The AUTOPILOT project (Architecture example)

The main perceived project impacts are:

- IoT usefulness proven with proof of concept at Vehicle – Platform and Service Level
- Automotive industry convinced by the IoT benefits for “Managing” Smart Mobility Data in the Cloud
- Seamless replicable and scalable deployment of vendor and Open platform
- Acceptance of IoT at user level
- Progressed vision of Data Market Place based on real Industry and Mobility Service use cases
- Paved the way for automotive data platform for 5G/CCAM deployment

5.2.1.2 MONICA

As an innovation project, MONICA was not supposed to develop new standards and have instead used existing standards and identified gaps where standards are missing.

MONICA has focused on sound management and crowd management for open air events such as concerts. Can we mitigate sound levels outside of the event area? We've demonstrated a 15dB reduction via passive absorbers and secondary speakers for sound cancelation as a larger scale

version of noise cancelling headphones. "Peaceful showers" as metaphor for localized sound reduction.

MONICA makes use of a wireless transmission system with very low latency and time jitter. One challenge was the hurdle of testing novel devices that have yet to be CE-marked. This was addressed through application of Article 9 of DIRECTIVE 2014/53/EU. This requires devices that are not yet CE-marked to be cleared marked as such. In addition, the pilot area for the tests should preferably be gated, so that devices are not allowed outside of the pilot area, and are to be collected after the event. A lack of awareness of this directive hindered pilots in some of the countries used by MONICA.

Here is the helicopter's view of the project:

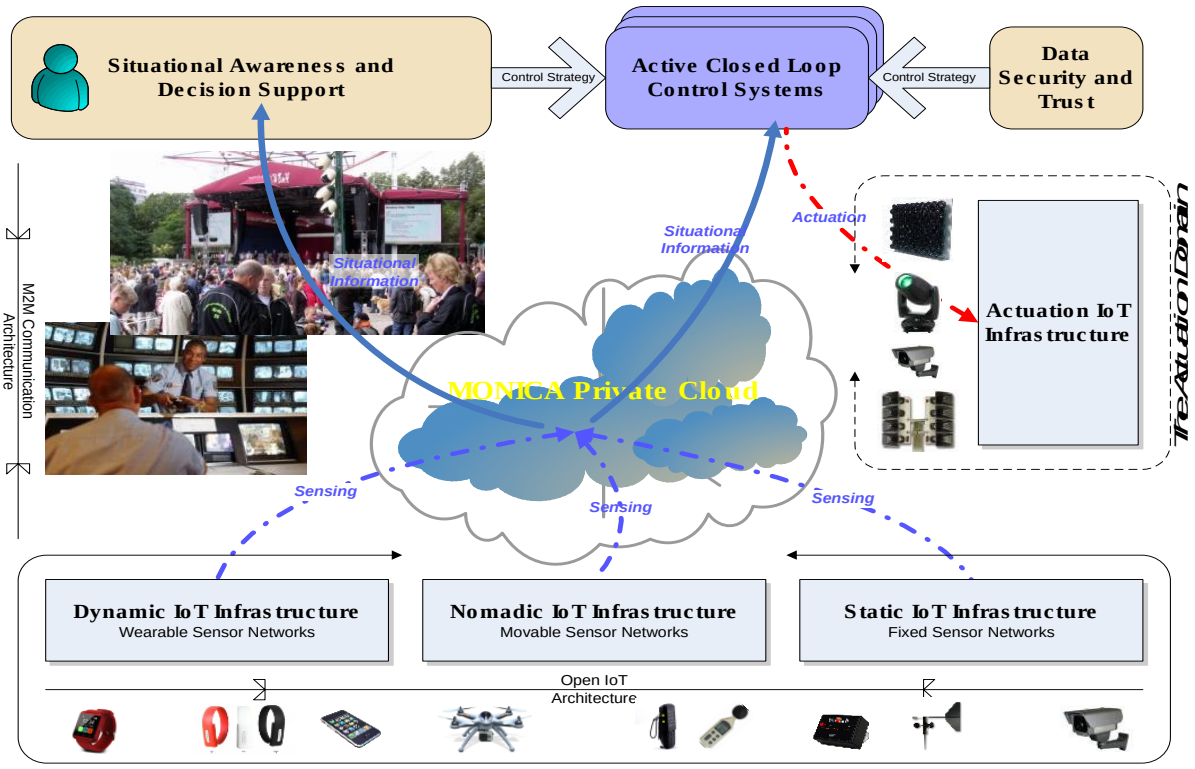


Figure 7: The MONICA project

The project identified the need for even lower latency and jitter for data transmission, along with the need to support a hundred thousand devices in a limited geographical area.

5.2.1.3 SYNCHRONICITY

The SynchroniCity project's main aim is to deliver a market for IoT and AI enabled services for cities and communities. This was broken down into nine objectives:

- Establish technical foundations
- Establish marketplace enablers
- Create reference zones
- Pilot services that serve citizen needs
- Establish ecosystem
- Establish citizen-oriented methods
- Establish holistic quantification of value
- Provide insights into new business models
- Transform city policy-making and planning

The decision was taken early on to maximise the use of existing standards where practical, leading to a focus on the minimal interoperability mechanisms (MIMs) needed to integrate existing solutions. Five MIMs have been addresses: context information management, common data models, ecosystems transaction management, personal data management, and fair AI.

This approach has been demonstrated with 50 services piloted across 21 cities. Some examples include:

- RainBrain – greening of city roofs with collocated sensors and actuators to empty water buffers when storms are imminent.
- NoiseAbility – monitoring different kinds of noise and citizen feedback in urban environments in Eindhoven, Bilbao and Edinburgh. Integration with datasets on events, traffic and waste collection.
- EdgeLights – using live traffic data for energy saving on streetlights (in Porto).

SynchroniCity highlights:

- *Nuvla* secure edge computing platform for smart cities
- Use of node-red to speed development of services.
- Open libraries for machine learning, mapping, visualisation, etc.
- SynchroniCity APIs for context management, data storage, IoT data marketplace and security.
- *OASC* (open and agile smart cities) 140+ member cities across 27 countries. The OASC Catalogue with solutions, products, case studies, value propositions and urban challenges.

5.2.1.4 ACTIVAGE

Healthcare is the maintenance or improvement of health via the diagnosis treatment and prevention of disease, illness, injury, and other physical and mental impairments in human beings. Well-being by contrast is a general term for the condition(s) of an individual or group, to achieve a level of health according to particular conditions/situations, for example, their social, economic, psychological, spiritual or medical state.

- Wheel of well-being with factors contributing to living well: intellectual, social, physical, spiritual, emotional, occupational and environmental.
- Impact, exploitation, dissemination and standardisation.
- Evolving from electronic records for health to connected-health records.
- ACTIVAGE handbook.

Social dimension and impact. People are classified as very fit, well, managing well, vulnerable, mildly frail, moderately frail, severely frail, very severely frail and terminally ill. The aim is to extend the time people have in the first four categories and to reduce the time when people are frail and in poor health. To support this aim, each of the nine ACTIVAGE deployment sites covers two or more of the following aspects:

- Daily activity monitoring
- Integrated care
- Monitoring assisted persons outside the home
- Emergency trigger
- Exercise promotion
- Cognitive simulation
- Prevention of social isolation
- Safety, comfort and safety at home
- Support for transportation and mobility

The deployment sites supported 6000 elderly users and 1200 carers and were built with a variety of IoT platforms from previous European projects (FiWare, OpenIoT, sensiNact, Sofia2 and universAAL). The IoT devices included: indoor sensors and actuators, outdoor sensors, wearable

sensors, health devices and user interaction devices. The use cases covered: social engagement, assistive technologies, housing, transport & mobility, behaviours, age-related changes, disease management.

The ACTIVAGE IoT ecosystem (AIoTES) made use of 3G/4G, WiFi, LoRA and other connectivity technologies to collect data on the AIoTES platform for use by a suite of applications in compliance with GDPR. The project was aware of the many commercial technologies, and therefore focused on providing a bridge between them. Venture Scanner has surveyed the landscape and identified 760 companies active in digital health.

ACTIVAGE had a very active group on standardisation which monitored and aligned with standards development activities, e.g. AHA data model, the ACTIVAGE ontology, and SAREF 4 Health extensions. The project was strongly influenced by ANSI/HL7's standards for electronic health records.

5.2.1.5 IoF2020

This slot focused more on the capabilities of the IoT Catalogue rather than the IOF2020 LSP itself. The following summarises information from the IoF2020 booklet and website.

The IoF2020 project was a really large project with over 120 partners and a 4 years duration. Trials were conducted in five main areas: arable crops, dairy, fruits, vegetables and meat. The project sought to show the additional benefits from high resolution data obtained with ground sensors and drones as compared to remote sensing data obtained from orbiting satellites.

Farm machinery uses precise spatial location together with sensors and actuators, e.g. to measure how yield varies across different parts of a field, and to dynamically tailor delivery of irrigation, fertilizer, pesticides and herbicides to reduce waste, costs and energy expenditure.

Interoperability is a challenge as farm machinery generally uses vendor specific communication. This was addressed using the Agricultural Data Application Programming Toolkit (ADAPT) and the Extended FMIS Data Interface (EFDI) for a cloud-based API with multi-vendor ADAPT plugins, and support for farmers to sell their data from a data sharing platform.

Livestock sensors can be used to monitor grazing time and location, as well as milk yield from individual cows. Leg mounted sensors can be used to identify lame animals, as lameness entails pain and discomfort, with decreased fertility and milk yield. Pregnant cows can be given precise tailored doses of mineral supplements.

IoT provides opportunities for improved traceability and enriched information flows along the supply network as well as the means to monitor temperature, humidity and shocks during shipping and storage. Provenance is of increasing interest to consumers who want to know where and how their food was produced, and to feel a connection to the farms and farmers.

The session included a demo of www.iot-catalogue.com as a means to showcase project results, use cases, technologies and solutions. The catalogue covers many projects not just IoF2020. IoF2020 project use cases divided across arable, dairy, fruit, vegetables and meat. Each use case tagged by validations, places, components, value propositions, team, region deployed, etc. You can see how many times each component has been used across use cases. One can also browse for hardware components and their prices.

5.2.2 A glimpse at the future

At this point the session switched to a brief introduction a number of other IoT related projects, starting with Boost 4.0 on smart manufacturing and shared dataspaces, and followed by the most recent batch of IoT projects which have only just started.

5.2.2.1 Boost 4.0 - towards a European Industrial Data Space environment

Boost 4.0 is a Lighthouse project on big data for factories. Delivering global standards, secure digital infrastructures and trusted big data middleware.

The project has fifty partners and is running many pilots across many companies, covering themes such as zero-defect manufacturing and predictive maintenance through the collection and analysis of big data.

The project focused on the four main open source European initiatives: The Industrial Data Space, FIWARE, Hyperledger and Big Data Europe, along with the development of open connectors and big data middleware with native block chain support for the European Industrial Data Space.

We need to overcome barriers for data sharing

- Trust
- Interoperability (too much effort currently needed on data preparation)
- Secure exchange

5.2.2.2 DEMETER

Demeter is a new H2020 project that started in September 2019 on smart agriculture. Demeter's goal is to lead the digital transformation of Europe's agri-food sector through the rapid adoption of advanced IoT technologies, data science and smart farming, ensuring its long-term viability and sustainability. We seek to enable farmers to produce more food with less, whilst respecting the environment.

The project will focus on large-scale deployment of farmer-centric, interoperable smart farming-IoT (Internet of Things) based platforms, delivered through a series of 20 pilots across 18 countries (15 EU countries). Involving 60 partners, DEMETER adopts a multi-actor approach across the value chain (demand and supply), with 25 deployment sites, 6,000 farmers and over 38,000 devices and sensors being deployed, putting farmers in a position of full control over how pilots are deployed.

Digital technologies can offer opportunities to farming and rural areas. Challenges around rural broadband. Data ownership where companies are forcing farmers to cede ownership of their data. Challenges around economies of scale given heterogeneous needs. Collaboration with other EU agricultural projects. We have 60 partners and plan 20 pilots across 5 sectors.

5.2.2.3 INTERCONNECT

InterConnect is a new H2020 project for management of smart grids that started in October 2019. InterConnect gathers 50 European entities to develop and demonstrate advanced solutions for connecting and converging digital homes and buildings with the electricity sector.
Three open calls will be launched from 2021 to select 42 innovative bottom up projects.

- Large-scale pilots leading to market-driven segments
- Marketplace of integrated digital platforms bridging the gap between IoT and energy
- Establish interoperability framework validating SAREF and semantic interoperability
- User centric energy and non-energy services

The solutions developed within the scope of InterConnect will allow a digitalisation of homes, buildings and electric grids based on an Internet of Things (IoT) architecture.

By including digital technologies (Artificial Intelligence, Blockchain, Cloud and Big Data) based on open standards, such as SAREF, it will guarantee the interoperability between equipment, systems and privacy/cybersecurity of user data.

Who has the opportunity to take advantage of these solutions?

- Energy users in buildings
- Manufacturers
- Distribution grid operators
- Energy Retailers

5.2.2.4 COORDINET

Coordinet started in January 2019 with a focus on electric power grids and distribution systems. The project will demonstrate how Distribution System Operators (DSOs) and Transmission System Operators (TSOs) can act in a coordinated manner and use the same pool of resources to procure grid services in the most reliable and efficient way through the implementation of large scale "TSO-DSO-Consumer" demonstrations, in cooperation with market participants (and end users).

- Enable a smart, secure and more resilient energy system through demonstrating cost-efficient model(s) for electricity network services that (i) can be scaled up to include networks operated by other TSOs and DSOs, (ii) that will be replicable across the EU energy system, and (iii) provide the foundations for new network codes, particularly on demand-response.
- Contribute to opening up significant new revenue streams for consumers to provide grid services and increase the share of RES in the electricity system.
- Some of the aspects to be addressed include load balancing, congestion management, controlled islanding, and voltage control.

Coordinet plans10 pilots across three countries. Support for prosumers (providers + consumers) and will develop a platform for exchange of needs and market results.

5.2.2.5 PlatOne

PlatOne is a new four year H2020 project on smart grids and integrating users including prosumers. The project seeks to define new approaches for increasing the observability of renewable energy resources and of the less predictable loads while exploiting their flexibility. Our consortium of 12 partners from Belgium, Germany, Greece and Italy will develop advanced management platforms to unlock grid flexibility and to realize an open and non-discriminatory market, linking users, aggregators and operators. The solutions developed in the project will be tested in three European demonstration examples and analysed in cooperation with a large research initiative in Canada.

The project will develop a new platform for DSOs featuring block-chains for open markets linking the local system to the transmission system managed by TSOs. This will be an open platform with diversity of communications technologies, open APIs as basis for services, the ability to integrate and secure legacy solutions, and an integration bus for flexible connection.

5.2.2.6 QU4LITY

Qu4lity is a new H2020 project focusing on manufacturing, which started in January 2020 and will last 39 months.

- Qu4lity is the biggest European project dedicated to Autonomous Quality (AQ) and Zero Defect Manufacturing (ZDM) in the Industry 4.0.
- Qu4lity will demonstrate, in a realistic, measurable and replicable way an open, certifiable and highly standardised, SME-friendly and transformative shared data-driven ZDM product and service model for Factory 4.0 through 14 pilot lines.
- Qu4lity will also demonstrate how European industry can build unique and highly tailored ZDM strategies and competitive advantages through an orchestrated open platform ecosystem, ZDM atomized components and digital enablers across all phases of product and process

lifecycle. The main goal is to build an autonomous quality model to meet the Industry 4.0 ZDM challenges.

5.2.2.7 MIDIH

MIDIH is a new H2020 project for the manufacturing industry digital innovation hubs, that seeks realise services to support ICT innovation for manufacturing SMEs.

- MIDIH aims at implementing the fast, dynamic, borderless, disruptive side of the I4MS innovation coin focusing on technological services, business services, skills building services.
- MIDIH is a "one stop shop" of services, providing industry with access to the most advanced digital solutions and the most advanced industrial experiments.
- MIDIH will also supply pools of human and industrial competencies, and access to "ICT for Manufacturing" market and financial opportunities.
- Technological services will be driven by young and dynamic ICT talents virtually meeting older and experienced manufacturing engineers in a one-stop-shop global marketplace.
- Business services will support SMEs, startups, web entrepreneurs as well as corporates in the delivery of innovative products and services, in accessing new markets, in fund-raising.
- Skills building services will not only help SMEs and corporates understand the new technologies, but also provide an operational framework that will stimulate trust, confidence and investments.

5.2.2.8 BD4OPEM

This is a new H2020 project focusing on generation, transition, distribution and consumption.

- Energy power systems face big challenges to cope with grid integration demands of an ever-increasing number of distributed generation and consumption devices in an interconnected world. Technology offers a huge range of opportunities to develop solutions in the uncertain current and upcoming Energy market situation. This proposal considers Open Innovation as a natural solution to create a seamless link and balance between energy stakeholders needs and the solutions to be developed. Nowadays, old metering, operation and control devices are combined with smart systems with a huge amount of data being available yet unused or underused. This data offers a wide range of possibilities to improve existing energy services and creating new ones, all available in an Open Innovation Marketplace, and processed through an Analytic Toolbox.
- BD4OPEM will develop this Analytic Toolbox, based on Big data techniques, providing tools for enabling efficient business processes in the energy sector. By extracting more value from available data, a range of innovative services will be created in the fields of grid monitoring, operation and maintenance, network planning, fraud detection, smart houses/buildings/industries energy management, blockchain transactions and flexibility aggregation for demand-response.
- The Open Innovation Marketplace will ensure secure data flows from data providers to solution providers, always compliant with GDPR requirements, so that asset management is enhanced, consumer participation in energy balancing is promoted and new data-driven business models are created through innovative energy services. The project will demonstrate the above features in four large scale pilots with diverse distributed energy sources (e.g. PV, wind, hydro, EV, storage…), while promoting the competitiveness and synergies of Sustainable innovations and IT Ecosystems in Europe.

5.2.2.9 SYNERGY

SYNERGY is a European project (February 2016 - January 2019) that focused on data analytics for big energy. The project addressed three core objectives:

- Improve JSI excellence and unleash its research and innovation potential through training in parallelisation and surrogate modelling, and aiding organisation of workshops that will foster discovery of new ways of combining the two methods.
- Raise the research profile of JSI staff and broaden its recognition through networking that will result in knowledge transfer, joint publications and future research projects.
- Increase the overall research and innovation potential of Slovenia by disseminating the acquired knowledge to other Slovenian research organisations and deploying it in future applied projects.

We had 24 partners from 9 EU countries and deployed 21 use cases across 5 sites. We developed a cloud-based AI enhanced big data analytics marketplace for data consumers and providers. Our aim is to support end to end coordination, enhance network stability and resilience, and enable collective intelligence.

5.3 Session 2 - Large-Scale Pilots Showcase

This session featured 4 parallel streams with the intention for people to rotate between them. In practice, most people stayed in the same stream, since as a good discussion has started and people preferred to continue rather than breaking off.

5.3.1 Stream 1 - Building an ecosystem, leverage open calls

The session was moderated by Olavi Luotonen (EC DG Connect, Unit E4).

The goal of the session was to assess some deliverables, methodologies and tools that have been developed within the frame the IoT LSPs, in particular around the Open Call Package used by ACTIVAGE, IoF2020 and SynchroniCity. Another aspect for discussion was the idea of a club of SMEs.

The key pitches have been made by ACTIVAGE and SynchroniCity.

5.3.1.1 The experience of ACTIVAGE

A presentation was done by Martin Serrano who has highlighted some points for the assessment.

- The ACTIVAGE Open Calls have used the “cascading funding” process defined by the EC which has to be carefully followed. The notion of “challenges” has been very useful for the filtering and selection of candidates.
- Four information supports were available for the applicants:
  - Technical Information
  - Guide for the Applicants
  - Templates and budget forms
  - Guide for the Reviewers
- Most of the applicants for ACTIVAGE were SMEs.
- ACTIVAGE has developed a web portal on the European-iot-pilot.eu web site to keep track of the Open Calls analytics. The portal could be reused for new projects with Open Calls and transferred from CREATE-IoT to a new CSA, if possible.

5.3.1.2 The experience of SynchroniCity

A presentation was done by Martin Brynskov who has recalled the experience around the Open Call methodology:

- A first attempt has been done with the Open Call in OrganiCity. The lessons learned have been very useful for setting up the Open Call framework of SynchroniCity.

- SynchroniCity has made a huge work to set-up their own Open Call model with a strong insistence on the assurance that they could be safe from a liability point of view, in particular regarding the selection of successful candidates and the re-scoping of the accepted projects.
- For all the 133 applicants, the procedure to follow has been made under the form of a contract. For all the 16 selected projects (which have all finished their work), a similar contractual approach has been followed for the "pilot agreement" and for the "data sharing agreement" (at deployment time).
- The major lesson learned is that legal aspects are the main barrier with a recommendation to treat them as the main priority.

More can be found in the SynchroniCity Guide that is on the CREATE-IoT USB key.

5.3.2 Stream 2 - Ways to share document, promote huge numbers of use cases

The session was moderated by Rolf Riemenschneider (EC DG Connect, Unit E4).

The goal of the session was to assess the way some promotion deliverables have been produced and identify lessons learned. The elements for discussion were the promotion booklets (e.g., IoF2020, AUTOPILOT), the communication strategy and the showcasing strategy adopted for IoT Week.

5.3.3 Stream 3 - IoT Interoperability architectures, AIOTI, standardisation organisations

The session was moderated by Franck Boissière (EC DG Connect, Unit E4)

The goal of the session was to assess some key achievements (in particular the Minimum Points of Interoperability (MIMs), the work with ETSI CIM or the ITU-T SG20) and investigate which can lessons be learned.

After an introduction by Franck Boissière (EC DG Connect, Unit E4), the key pitches have been made by SynchroniCity and OpenDEI.

5.3.3.1 A view from the EC

CREATE-IoT and U4IoT have covered 5 LSPs. Many more IoT related projects are launched and this requires clustering. Hence the creation of OpenDEI with a scope quite similar to the one of CREATE-IoT.

CREATE-IoT used a template to collect information from across the LSPs. The Activity Groups have been launched to reduce the burden of communication across the projects. The role of the LSP Activity Group on "Standardisation, architecture and interoperability" has been to address commonalities, consolidation, influence and dissemination. It has worked on the Interoperability Framework with reference architectures, interoperability points and mechanisms, platforms and technologies, standards and pre-normative activities.

EU is unique in bridging industry and academia. This is a challenge and an opportunity.

5.3.3.2 Achievements: MIMs

The work of SynchroniCity is closely related to Open & Agile Smart Cities (OASC) which is on the demand side and consolidates the vision and requirement of 140 members in 27 countries.

The standards work in Synchronicity was made in the context of fragmentation of standards and SDOs. Given that convergence will be slow, interoperability is crucial. The focus has been put on the Minimal Interoperability Mechanisms (MIMs). They are expected to provide benefits to cities,

businesses and to citizens. There are 5 MIMs, the first three are realized in Synchronicity and MIM1 and MIM2 are accepted by cities

- MIM1 - Context integration management
- MIM2 - Shared data models
- MIM3 - Ecosystem Transaction
- MIM 4: Personal Data Management
- MIM 5: Fair AI
- Bridging legacy systems

Synchronicity has stimulated standards work on context information management (e.g., JSON-LD).

There is some planned work on personal data.

5.3.3.3 Achievements: Data Modelling

Franck Boissière (EC DG Connect, Unit E4) mentions one important topic: API for CIM

- Have a very quick work done in ETSI and have quickly a common base to work
  - NGSI_LD interface is done in ISG CIM, based on the FIWARE NGSI
- First have technical interoperability and then do the data interoperability
- Chose the right tools at the right moment
- Data strategy and Data marketplaces are important
- Standards will be needed (data format, and as well more layers will be needed)
- How to move from a common agreement that can be done nationally to global one (ISO and IEC)? Handling both is an interesting challenge

Some remarks from the floor:

- ACTIVAGE had a semantic interoperability layer; MIMs came to develop a common integration concept
- What about MIMs in manufacturing domain? This might come in Boost 4.0.
- CIM moved in oneM2M and in ITU
- Associate FIWARE and International Data Space Association (IDSA has hubs in different countries across Europe). IDSA connectors
- W3C is seeking to address the fragmentation via an abstraction layer for digital twins (the web of things) that simplifies services very considerably.
- Companies are slowly shifting towards greater interest in common standards, see the Amazon, Apple, Google and ZigBee alliance announcement on defining common standard for using existing transport protocols.
- We need to convince business of the benefits of migrating towards common standards and committing to drive these standards, but regulatory frameworks can help by creating a common open marketplace
- Difficulties with proliferation of IoT technologies, data models and formats. We need more than common data formats.
- Importance of describing and dissemination of use cases, and the relation to interoperability and architecture.

5.3.3.4 OpenDEI

Sergio Gusmeroli (Politechnico of Milano) has introduced OpenDEI and highlighted that it has similarities to what CREATE-IoT has done for the first 5 LSPs

- OpenDEI focuses on 4 domains: Healthcare, Manufacturing, Agriculture, Energy

- OpenDEI comes with a new set of projects (26 projects at least) and therefore will have to work in a different manner than what CREATE-IoT did for the 5 LSPs
- A challenge is to create a community across the 4 domains. To this extent:
  - Representatives are appointed
  - Knowledge exchange (one expert from each domain)
  - Cross virtualization from one domain to another domain is organised
  - Four ambassadors are experts for each domain: when a cross-domain issue occurs, all the 4 ambassadors will be involved
  - Digital twins born in manufacturing and used in other domains

The EC supports the approach:

- It provides the ability to think on the same topics, e.g., Interoperability, Semantics, Architecture
- Each project can identify one individual as the contact person who knows the project and can contribute to
  - General architecture
  - Domain specific and cross-domain together
  - Common goals to verify cross-domain enablement

5.3.3.5 Conclusions

Franck (EC DG Connect, Unit E4) not that there are now many projects and it is difficult to expect full agreement across them, but nonetheless, progress can come from looking for commonalities.

The experience of the LSPs is that they had a big impact on European policy.

All projects can learn from previous CSAs such as CREATE-IoT. Each project needs to identify people who have the time to act as a bridge / ambassador for knowledge exchanges across projects.

Similarly, it is possible to improve the Activity Groups as a coordination and information sharing mechanism across projects.

5.3.4 Stream 4 - Innovation support: Create-IoT - Brochures, market support

The session was moderated by Jan Komarek (EC DG Connect, Unit E4).

The goal of the session was to review topics such as the White Paper on GDPR, the IERC Cluster Books, the Security approach, the KPIs for the LSPs, the eBook, the IoT Handbook, the IoT Policy Framework, the Wiki and the Use Case mapping.

The key pitches have been made by CREATE-IoT and ACTIVAGE.

5.4 Session 3 - Parallel Sessions

This session was fully dedicated to topics of common interest in order to identify and organise common work teams for the coming year.

Four streams have been organised in parallel:

- IoT Data Space, sharing, conceptual reference-model
- IoT Data Lakes, platforms, economics of data-driven services and marketplaces
- IoT Security, privacy policy framework
- Navigating the future of IoT Technologies/Applications towards edge computing

They were followed by a plenary session in two parts:

- Reporting from the sessions - take away, Highlights, Short presentations from moderators
- Looking back and aiming forward. Main take away. Future actions.

5.4.1 Introduction

Rolf Riemenschneider (EC DG Connect, Unit E4) has introduced the afternoon's session.

He has recalled the dimensions of EU digital future from February 19th announcement:

- Technology that works for people
- A fair and competitive economy
- An open, democratic and sustainable society

High impact projected on EU Data spaces and high value data sets.

- Digital marketplaces enable economies of scale.
- Examples of data marketplaces: location data, EV charging and parking

"Whoever controls the platform controls the future"

Issues for discussion:

- What is the strategy for European actors, markets, regulators?
- Incentives, standards, safety and Open APIs.
- More than 70% of the value of IoT systems is today in the cloud.
- Important role of analytics and the sizeable security challenges and increased attack surface.

5.4.2 IoT Data Space, sharing, conceptual reference-model

The stream was moderated by Rolf Riemenschneider (EC DG Connect, Unit E4). Participants were coming from current IoT LSPs ecosystem (SynchroniCity and CREATE-IoT) and from OpenDEI projects (Boost 4.0, Qu4lity, MIDIH, Productive 4.0, Smart4Health).

Identified achievements

- Projects focus on Data Formats:
- Domain specific
- Some (standard) components
- First technologies on EDGE

But: is standardization mature?

Marketplaces are fashionable:

- Exploitation based on data services
- Open APIS
- Value of data

But: which governance?

Which way forward:

- Promote a concept/ Framework
- KPIs for Infrastructure // Sandboxing
- Ecosystem for services for data infrastructure; look at governance model;
- Finance: how to use the infrastructure project with sandboxing
- Data Quality on AI
- AI learning in Clouds and edge

Some more details during discussions:

- Challenges
  - Building the IoT ecosystem
  - How to realize analytics and what are the challenges related to data?
  - How to come from application to data?
  - Access layer (reference frameworks) is where the data sharing is defined

- IoT Data sharing and conceptual reference model
- It is important to have a reference data framework fit for digital age. Such a framework should encompass at least 9 building blocks
  - Data Standards and formats
  - Operational Agreements
  - Legal agreements
  - Earnings model
  - Data exchange
  - Governance
  - Metadata
  - Cybersecurity
  - Identification, authentication and authorisation
- Metadata: generic metadata (IDSA) data is described in 6 dimensions, such as:
  - Connectivity
  - Legal agreements unified terms & conditions (liability, …) to use in contracts
  - Operational agreements: how to start the process of data sharing; SLA
  - Governance (be neutral): Someone needs to operate it; decentralized model? Blockchain; central or decentralized
  - Business models and billing:
  - Identification and Authorization

5.4.3 IoT Data Lakes, platforms, economics of data-driven services and marketplaces

The stream was moderated Jan Komarek (EC DG Connect, Unit E4).

It starts with the presentation of several EC projects.

- I3Market - Intelligent, Interoperable, Integrative and deployable open source MARKETplace with trusted and secure software tools for incentivising the industry data economy
  - Started eter
  - uary 2020 for 3 years
  - The i3-MARKET project addresses the growing demand for a single European Data Market Economy by innovating marketplace platforms, demonstrating with industrial implementations that the data economy growth is possible. i3-MARKET proposal provides technologies for trustworthy (secure and reliable), data-driven collaboration and federation of existing and new future marketplace platforms, special attention on industrial data and particularly on sensitive commercial data assets from both SMEs to large industrial corporations is taken.
  - Taking into account that there is no broadly accepted trusted and secure data marketplace, i3-MARKET will develop technologies and solutions for a trusted (secure, self-governing, consensus-based and auditable), interoperable (semantic-driven) and decentralised (scalability) infrastructure, called i3-MARKET Software Framework (aka i3-MARKET Backplane).
  - i3-MARKET focuses on the desired levels of privacy and confidentiality that support both legal and user-desired control and transparency for sharing data among relevant systems and services.
  - The i3-MARKET backplane pays special attention to regulatory aspects around sensitive data assets.

The next two ones, MIDIH and QU4LITY, are engaged in a collaboration around marketplaces.

- MIDIH - Manufacturing Industry Digital Innovation Hubs (see also 5.2.2.7)

- MIDIH is a new H2020 project for the manufacturing industry digital innovation hubs, that seeks realise services to support ICT innovation for manufacturing SMEs.
- Thinks about how the customer, e.g., small companies, can benefit from the data marketplace and develops the mechanisms to create the connections between local regions and local companies.
- The project has 16 hubs, between 20 or 30 SMEs each. They are potential customers for the data marketplace.
- Currently, the data are produced, and they are already useful. But, so far, no digital platform to trade the data.

- QU4LITY – Digital Manufacturing Platforms for Connected Smart Factories (see 5.2.2.6)
  - Qu4lity is a new H2020 project focusing on manufacturing, which started in January 2020 and will last 39 months.
  - Data are related to factories, e.g., quality of the products, maintenance.
  - The way to design the services in the data marketplace is important, and which functions are offered.
    - No single owner of the whole data set.
    - The data sets cannot be open, providers want to retain how the data are used. It is more about open APIS to exchange them.
  - Discussion between factory and providers about the type of data: They are more willing to exchange / share data about 2nd hand or ancillary processes: recycling energy efficiency, remanufacturing. They would not share data about the production process (which is their added value).
    - Format of data exchanged: usually logs, maybe structured files if the context allows.
  - Comparison with agriculture: they start to setup a code of conduct, openPLM, linked with self-assessment, on a voluntary basis. Now PLM vendors (19) have 10% market share after 1 year of existence. Big OEMs and aeronautics are asking whether their providers are complying with this code of conduct.
  - Market place may be open, but applications would be more limited to a small set of missions.
  - Data providers need trust, need assurance how the data is used, attached to a particular application.
  - SMEs are more willing to share their data, but in exchange of a compensation for providing their data: data for data or discount to get access to a particular data set. Big companies are more reluctant.
  - There may be regulations that they have to provide their data. But it has a cost for the providers. So, one of their reaction is that they may find a way to also benefit from these data.

5.4.4 IoT Security, privacy policy framework

The stream was moderated Peter Wintlev-Jensen (EC DG Connect, Unit E4) and Salvatore Scalzo (EC).

Some elements from the discussion:

- GDPR has created jobs in America with companies learning from Europe.
- W3C workshop in Europe this Autumn for a new approach: turning privacy on its head for services that use much richer sources of personal data - pull based business models for privacy - putting the user in control as the owner - delegation of management of privacy preferences - regulatory implications -
- How to give Europe a leadership role for machine to machine data exchange and business transactions.
- Data quality and related metadata, relationship to liability.

- Decentralised identifiers, decentralised models of trust, non-hierarchical models of security for increased resilience and damage limitation as the attack surface expands as we introduce new technologies and much greater connectivity.
- New Horizon Europe calls around new approaches to security.
- Current business models focus on value of hoarding data. Regulatory incentives may be needed to tip this on its head.
- Europe should emphasise new work on AI that can learn from modest datasets and exploit the context. This will tip the balance back from the very large companies who otherwise have an unfair advantage with their deep pockets enabling them to acquire huge datasets.
- How should we deal with legacy data that is weakly protected?
- The European Commission's remit to provide data regulations could be a problem when the remit is currently at national level.

Findings:
- Privacy and privacy by Design was well executed in projects from synchronicity project.
- Risk analysis was well carried out
- Cyber security not taken enough into consideration it was lost with privacy there was no clear separation
- Confusion between Personal data and Privacy aspects
- Assurance is needed across different levels; this should not be limited to assurance in region but should consider global impact as market is bigger.
- Also lack of understanding between Personal data and ethics which all form part of privacy
- Clear understanding of who owns data for responsibility and reliability aspects

Recommendations:
- Privacy and privacy by Design was well executed in projects from synchronicity project.
- Risk analysis was well carried out
- Cyber security not taken enough into consideration it was lost with privacy there was no clear separation
- Confusion between Personal data and Privacy aspects
- Assurance is needed across different levels; this should not be limited to assurance in region but should consider global impact as market is bigger.
- Also lack of understanding between Personal data and ethics which all form part of privacy
- Clear understanding of who owns data for responsibility and reliability aspects

5.4.5 Navigating the future of IoT Technologies/Applications towards edge computing

The stream was moderated by Franck Boissière (EC DG Connect, Unit E4).

Question to the participants: IoT and AI are drivers for transformation. The following talking points have been collected from around the room:
- Sentient Web (web of digital twins + cognitive AI + open marketplaces)
- Decentralised identifiers - verifiable, decentralized, digital identity
- Data security
- Data privacy & role of edge computing
- Data sovereignty
- Coms scalability, reliability, latency; 5G is not cheap, other technologies
- Data exchange, monetisation, data structure and shared ledgers
- Middleware close to the cloud
- Technical Internet of Things
- Intelligent autonomous IoT
- Federation/orchestration, cloud/edge

- AI at the edge
- Privacy-preserving federated machine learning

5.5 Conclusions

5.5.1 Future Tech/apps/edge/DLT achievements

List of recommendations – (see also list above in 5.4.5).

- Ecosystem, marketplaces, GDPR handling
- Performance related
  - Reliability, latency, safety, robustness
- Architecture optimisation
  - Device, edge, cloud off loading
  - Federation and orchestration cloud/edge
  - Intelligent connectivity (wireless, 5G/6G, optical, etc.)
- Data exchange/monetization
  - DLT, shared ledger, decentralised identifiers, smart contracts
  - Data structure and formats
- Analytics, AI and ML
  - Preserving privacy is easier at the edge

5.5.2 Findings/Learnings from LSPs in respect to privacy & security

Findings:

- LSPs addresses these issues overall successfully
- Risk management principles and security/privacy by design generally operated
- Requirements/checklists were produced
- Lack of an assurance path seen as a major problem
- Data protection vs privacy
- Strong multi-stakeholder engagement in the context of the LSPs
- Detected need for multidisciplinary approach in analysing these issues
- Ethics seen as a separate and crucial dimension
- Positive consideration of data privacy as a...

Recommendations:

- Future assurance/certification scheme seen as highly beneficial
- Multidisciplinary/multi-stakeholder approach in addressing these issues seen as essential
- Setting legal responsibilities for actors other than manufacturers to be considered.
- Interaction between data protection and ethics
- Need for model/mechanism to screen and identify project outputs that could be readily exported and moved forward when project ends
- Introduction of requirements for data protection strategy together with exploitation plan
- Links among different projects to be strengthened, notably on privacy/security issues, make best possible use of clusters, including sharing templates
- Educational aspect seen as important, both on demand and supply side
- Need for standardisation in the field with 2 caveats:
  - Global level standardisation,
  - Standardisation is unlikely to cover all aspects
- Considering tools to map aspects to standards/requirements\

5.5.3 IoT Data Space, sharing, conceptual reference model

Nine building blocks:
- Data standards
- Business model
- Governance
- Legal agreements
- Operational agreements
- Metadata
- Authorisation
- Identification and authentication
- Exchange standards

Achievements:

- Projects focused on data formats
  - Domain specific
  - Some standard components
  - First tech on EDGE
  - Standardisation mature?
- Marketplaces, fashionable
  - Exploitation based on data services
  - Open APIs, Governance
  - Value of data

Way forward:
- Promote a conceptual framework
- KPIs for Infrastructure, Sandboxing
- Data quality for AI

More challenges:
- Combining data from different data spaces.
- Federated data spaces and open APIs.
- Decentralised approaches and arbitration

5.5.4 IoT Data lakes, platforms, economics of data-driven services and marketplaces

Core:
- Healthcare
  - Clinical data & ethics
- Agriculture
  - Input & crop data
- Manufacturing
  - machine data
  - Logistics
  - Maintenance

Secondary:
- Well-being data and context
- EE
- Recycling
- Manufacturing
- Some anonymisation, GDPR
- Role of delay for commercially time sensitive info.

- More efficiency and keeping IPR
- Safety
- Business & societal impacts

Challenge: to make sense of large federation of data sets.

Opportunities:

- Reuse of B-to-C data sets
- Case by case approach to data collection and sharing.
- Provider controls data use.

5.5.5 Summing up

Rolf Riemenschneider (EC DG Connect, Unit E4) has brought some conclusions before the networking session.

- Very timely workshop with old and new projects.
- A need for effective communication within and across projects, directorates and sectors.
- Lot of emphasis on technology for the citizens and stakeholders across different sectors. The emergence of vocabularies for this.
- See where things are moving faster and how to identify best practices and to share them around.
- My thanks to the CREATE-IoT team for making this event happen.
- I look forward to seeing you at this year's IoT week in Dublin.

6. AIOTI: BREAKING DOWN THE TECHNOLOGY SILOS

The workshop was kicked off by Georgios Karagiannis, AIOTI WG03.

The workshop is organised in three sessions with the following objectives:

- Session 1: Digital transformation. What are the needs of standardization, regulation and policy for the successful realization of the digital transformation in Europe, considering among others 5G deployments?
- Session 2: IoT-enabled Data marketplaces. Transformative journey from building infrastructure to the local enablement of cross-domain marketplaces is underway across many domains and geographies; What are the standardization, regulation and policy needs associated with these IoT-enabled Data marketplaces?
- Session 3: Breaking down the technology silos and how the AIOTI approach can address the horizontal harmonization. This session will focus on the work that has been done by AIOTI on current gaps in IoT standardisation and will discuss the opportunities and barriers on leveraging technologies like 5G, IoT/IIoT, AI, robotics, cloud and edge computing and as well automation and required standards, governance, policy and rules to address the horizontal harmonization.

6.1 Introduction

Nikolaos Isaris - Head of unit (acting) IoT Unit E4, EC DG Connect.

Nikolaos notes the EC announcement on Wednesday 19th February of its 5 years digital strategy (Shaping Europe's digital future, Brussels, 19.2.2020, COM(2020) 67). Digital is one of the six priorities of the EC. The strategy covers digital transformation, trust, and AI.

The associated AI White Paper (On Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020, COM(2020) 65) is trying to mobilise the community at large. There is a 12 weeks' open consultation on the White Paper. One can reply to questions and possibly send a paper with longer comments.

The European data strategy (The European Data Strategy – Shaping Europe's Digital Future, February 2020) is acknowledging the huge explosion in the amount of data and aims at making data available via the creation of a single market for data by Europeans for Europeans.

There are plans to roll-out data spaces for different sectors, e.g. agriculture, manufacturing, health, etc.

This data strategy is a very important component for engaging the research community and has three pillars:

- Open access to data.
- The infrastructure to run processes that act on data.
- Specific sectorial actions on creating data spaces.

The intention is to bring together data, AI and IoT.

6.2 Session 1: Digital Transformation

This session was moderated by Antonio Conte, EC DG Grow

The session focused on digital transformation and, more precisely, what are the standardisation, regulation and policy needs for a successful realisation of digital transformation in Europe, considering among other things 5G deployment.

6.2.1 Panellists positions

Antonio invited the panellists to the stage and briefly introduce themselves, before they made quick statements.

Table 8: Session 1 – Comments and position

Panellist	Comments and position
Johannes Nitschke, 5G ACIA, Siemens	I am based in Brussels and work for Siemens on government affairs. I am also here on behalf of our membership of 5G ACIA. 5G addresses 3 application scenarios, but there is no one size fits all approach: enhanced mobile broadband (eMBB), massive machine type communication (mMTC), and ultra-reliable low-latency communications (URLLC). The possible 5G deployment scenarios are public; semi-public; and local, private deployment. This includes bandwidth provision for industrial site wide rollout. Industrial private wireless networks need private spectrum! The advantage of the wireless network ownership by the OT (operation technologies) are e.g., spectrum self-management bringing flexibility, quality of service, 24x7 support and maximum data privacy and security (data staying on premises; protection of trade secrets, production data and patents). Hence, a lot of excitement around industrial 5G! To make this happen, needed focus on industrial AI, security, trust and transparency and support of industrial protocols (PROFINET, OPC UA).
Ana García, BDVA/AI-PPP	The key challenges for BVDA: • EU public-private investment environment; Policy and Regulation; Digital Single Market • Skills and know-How; strong Research landscape • Access to AI / Data Infrastructure and test environments • Standards • Societal/Business Trust The required way forward for Digital Transformation (and the new AI-PPP focus on AI, data and robotics): a holistic view on how AI can create value; fast and secure deployment environments; sustainable and interoperable ecosystems based on standards; collaboration, openness and inclusiveness and a joint strategy across Europe.
François Fischer, AIOTI WG Smart Mobility	The challenge is to move away from big data silos and encourage collecting and sharing data. We need a common vision of IoT to address the ICT and policy environment. • Standards ecosystem for IoT architecture and data models • Commonly agreed policies for use with GDPR • Service level agreements for data marketplaces We want to support new business models and ensure acceptance of the whole value chain. Open issues remain such as: • Lack of commitment for companies to adopt open data access strategy. • Value chain controlled by (automotive) OEMs but evolving towards more open collaboration models. • Well established industry and service practices that hinder progress. • Increased competition, etc. Digital transformation will impact mobility sector significantly. There is a need to ensure that ICT and service platforms are managed by EU organisations using standardised architectures and data models. And to encouraging innovation by new, small and more local players. IoT as a key catalyst. The IoT LSPs have identified and partially addressed the challenges. AUTOPILOT has used the oneM2M device management and is feeding into new work on 5G.
Marco Carugi, Huawei,	I also work with ITU-T expert focus group Network 2030.

representing the Telecom supply side	IoT applications show the importance of enhancing network capabilities with respect to bandwidth, latency, multi-streams synchronization, jitter, large scale deterministic networking, security and reliability. The network also needs to support holographic type communications; Tactile Internet for remote operations; Industrial IoT with cloudification; and seamless co-existence of heterogeneous network infrastructures (non-IP networks, etc.). Other new capabilities required include time engineered services (high precision communications with in-time, on-time, coordinated guarantees); qualitative communication allowing applications to specify different priorities for different data; support for Compound Services. ITU-T is working on a global framework for "New IP"-based networks. The supporters of New IP highlight that "New IP" is not only a novel Internet Protocol, but rather a new architecture with associated signalling, control, management and transport capabilities together with intrinsic security, user customisability, etc. Some prototypes have been already presented in public and some operators/service providers have shown strong interest.
Peter Thoene, John Deere, representing the Vertical Industry demand side	Working for John Deere, I focus on EU driven standards. Digital transformation impacts production processes and products. A combination of security, innovation and digital policy is a game changer. EU standards and the European legislation provide the framework for the technology to be used in Europe but also beyond this region. Regarding data exchange, an example is on-board diagnostics for farm machinery involving John Deere, service providers and third parties, in respect to extended agriculture functions. Another agriculture example is tractors with ISO bus for data exchange, open cloud to cloud data exchange, including machine position over time, fuel tank levels, current status and speed. For the near future, standardisation is a strategic level, and creates market opportunities and boosts industrial competitiveness. Standardisation is an industry driven bottom up approach but can be a top down regulatory driven approach when it comes to safety. Why to design top down regulatory approach to address safety? • Member States in Europe are responsible for ensuring the health and safety on their territory of workers, consumers, animals and goods in relation to the risks arising out of the use of connected machinery. • The industry needs to analyse the essential data processing requirements in terms of trust, security and effective conformity assessment when they put on the market a machinery. • The industry needs to explain how a single registry at the cloud level can be used by the OEM to provide trust to organizations, and operators when hardware, and software are deployed on the connected machinery.
Riccardo Vitorino – Ubiwhere, representing the Industry supply side	How can we help cities to become smart, helping us all get stronger, more resilient, more connected, more active and freer? By designing cities in a way that values everyone's experience, by deciding who our cities are for, and by believing that they can change. How can cities become truly smart? By placing changes and being able to measure them; following the good practices on Smart Cities implementation; avoiding vendor lock-in and isolated solutions with no-integration; investing in data harmonization; allowing a proper analysis and data correlation/integration. Vision of city as a single system of systems, avoiding isolated silos and enabling real-time awareness of city status. Use cases for Smart City: real time status of the city (information from several verticals in a single map; general overview of short-term historical data capability to take decisions on real-time); KPIs Analysis (dynamic, contextual insights about the city ecosystem to foster smooth operations); sustainability (well-defined metrics to help cities benchmark their progress towards the UN's Sustainable Development Goals).

6.2.2 Q&A and discussion

Congratulations in the audience to Germany for allocating spectrum to industrial 5G.

Table 9: Session 1 – Questions and answers

Questions	Answers
Working on alignment of architectures to foster digital transformation, can we harmonise engineering transformation as well as digital transformation?	Johannes: harmonisation is a goal for standardisation. Ana: need to address in AI-PPP partnership- How to do system integration Francois: Standardization is needed
How would you see trends for global and local networks? Related to Campus of 5G and IIoT cloudification, global cloud and local clouds will be needed and how can they be supported?	Marco: we may have local scenarios which act as islands for a given vertical. As we grow the scale, we need to support end-to-end characteristics. Johannes: importance of data ownership and business models Georgios: in large scale networks, and when you need to support private domains, then you need to support end to end aspects.
About data and standardization and fast deployment, how to make more agile the standardization system to become more agile?	Peter: this is a question that usually manufacturers have towards policy makers; ISO is to have a common architecture Ana: there are many standards; from a Big Data perspective, things come too late. VDE representative: campus networks and other spectrum is in contradiction and bring experience of networks; providing privacy and liability are not a contradiction.

6.3 Session 2: IoT-Enabled data marketplaces

This session was introduced and moderated by Franck Boissière, (EC DG Connect, Unit E4).

The session focused on IoT-enabled data marketplaces: the transformative journey from building infrastructure to the local enablement of cross-domain marketplaces is underway across many domains and geographies. What are the needs for standardisation, regulation and policy associated with these IoT-enabled Data marketplaces?

6.3.1 Panellists positions

Franck Boissière (EC DG Connect, Unit E4) invited the panellists to the stage and briefly introduce themselves, before they made quick statements.

Table 10: Session 2 – Comments and position

Panellist	Comments and position
Sergio Gusmeroli, Politechnico di Milano	The EC 2020 European Strategy for Data: Industrial Data Space Common European industrial (manufacturing) data space Europe has a strong industrial base, and manufacturing in particular is an area where the generation of and use of data can make a significant difference to the performance and competitiveness of European industry.

	In order to unleash this potential, the Commission will: • Address issues related to the usage rights on co generated industrial data (IoT data created in industrial settings), as part of a wider Data Act (Q4 2021). • Gather key players from the manufacturing sector to agree in a manner compliant with competition rules as well as principles of fair contracts the conditions under which they would be ready to share their data Manufacturers are increasingly providing services that complement their physical products. This is referred to as "servitisation". Companies originally thought that they couldn't monetize their data, but this view is changing. The EC is now talking about business to business data sharing. • Open data approach where data is made available with few restrictions • Data monetisation via a marketplace • Data exchange via a closed platform, i.e. between limited entities with explicit agreements Open data vision as exemplified by "didactic" factories, i.e. physical factories in a laboratory for educational purposes. Open data models, use of different networking technologies (including OPC-UA. MQTT, etc.). B2B data sharing in a trusted network along with contractual obligations. The idea of access sovereignty, i.e. controlling who can access your data. An example is the Boost 4.0 project in which data from manufacturing machines is used to improve reliability via predictive maintenance. The tool maker commits to isolating data for tools deployed in different companies. The challenges for Data/Service Sharing Spaces: • Open data. This is operational in other domains, but Manufacturing Industry Managers and Decision Makers need to understand the value of Open Innovation. • Dynamic and SME oriented data marketplaces supporting new business models (e.g., servitisation). • Trusted data networks. They are often dominated by Large Platform Economy and multi stakeholders Innovation Models
Chris Decubber, EFFRA, vertical industry, manufacturing	Key enablers and cross-cutting factors for the Factories of the Future: skills and engineering tools; skills for operation of technologies; added value / optimisation focus; business models / financial investment; interoperability / standards; security; technology - building blocks. One of the main challenges is linking data islands across the enterprise and the importance of standards for this. A lot of attention to examples as a means to encourage interest in factories of the future: • FAREDG3 (Factory Automation Edge Computing Operating System Reference Implementation) addressing the overall concern about keeping data in the factory rather than having it leaking out; • eFactory: European Connected Factory Platform for Agile Manufacturing with the idea of a data spine to bridge different systems.; • Connected Factories: Service development (collaborative product services factories).

Tom de Block, AIOTI	Tom represents the AIOTI WG on distributed ledger technology (DLT). Different AIOTI Work Groups (Smart Cities, DLTs and Smart Energy) have developed a model of Market Drivers and High-Level Architecture for IoT-enabled Data Marketplaces. It involves managed data lakes (e.g., utility, smart city), data buyer (consumer), data enricher (algorithms), data aggregator (operates marketplace on behalf of data providers and data sellers (producers with an IoT infrastructure). Tom has presented a concrete example in which payments are directly transferred between buyers and sellers. A proportion is retained by the aggregator to fund the marketplace along with its discovery and auditing systems.
Silvia Castellví IDSA, GAIA-X	Data is an economic asset. There is a major requirement for vendor independent platform that is open to all, has proven data provenance, audit-proof, and based upon European values. Open issues include governance for data sharing, defining usage constraints and trusted manipulation of data. IDS has more than 100 members and 50 plus industry driven projects in 20 countries. GAIA-X is a new initiative for enabling digital ecosystems.

6.3.2 Q&A and discussion

Table 11: Session 2 – Questions and answers

Questions	Answers
Are there other models that don't involve the central aggregator as a third party in data exchange?	Tom: the aggregator needs to offer value e.g. data formatting, discovery, etc. Chris: the vision was there for a while, including interest in more peer to peer approaches. Smart contracts and DLT are an enabler. Tom: certification is another service the aggregator can offer. Sergio: many companies are uploading data to the Siemens MindSphere cloud platform. This needs to support data sovereignty to support data exchange. Silvia shows a diagram illustrating how IDS enables data sharing. Antonio: we must consider the business models, strategies and policies. We need the platform architects to enable policies to be expressed in a flexible way. Sergio: we are working on that in the OpenDEI project Tom: we are working on distributed governance.
Can we agree on a reference architecture architects to specify your decisions in a flexible way and consider business models and clean room?	Answer Sergio: Open DEI is Working at level of data. The idea is to involve champion projects to develop the model and support the vision that was addressed. To break the silos, we need to find ways to work together and move from technical IoT architectures

Europe is perceived as inward looking. What is the competitive position we can grow in Europe? Do we need to invest in infrastructure to support this?	Chris: we don't have big cloud storage providers as European companies as yet. Silvia: in Italy, we plan to federate cloud storage infrastructure and will present this at the Hannover Messe as an alternative to providers like Amazon. Georgios: it is important to support platforms like GAIA-X, but data may already in held in existing data lakes, and we need to support those. Franck: important questions include where my data is and who is using it.
We need to help our members to make a data economy - just opening the data is not the only way. Small companies fear being "eaten up" if they open up. This means trusting the framework to give them sovereignty over their data.	Tom: security is a major topic and we need to convince people that the risk is manageable. Sergio: education is important, and in my opinion, is missing at the moment. Martin: regarding architectures and federated platforms, marketplaces and verticals, guidance or reference should be created for integration of the marketplaces. Franck: we should distinguish business models and reference implementations and ensure that what we are proposing supports the range of business models that companies are interested in. Marco: there is a need to look at governance models and standardisation to enforce some guidelines and principles. Dave: two points. First W3C's standards for data catalogues (DCAT) is very relevant to data markets. Second: as data is easily copied, trust must be founded on the means to audit compliance with T&Cs for sharing data, along with strong regulatory teeth for dealing with abuses. The location of where data is held is secondary and subject to heterogeneous requirements. Martin: supports Dave in the importance of DCAT. The value of data may be much higher than the hardware.

Franck Boissière (EC DG Connect, Unit E4) sums up and encourages everyone to collaborate and share ideas and come towards a more converged position before the end of the year.

6.4 Session 3: Horizontal harmonization

This session has been moderated by Wael Omar El Hassan el Rifai, AIOTI

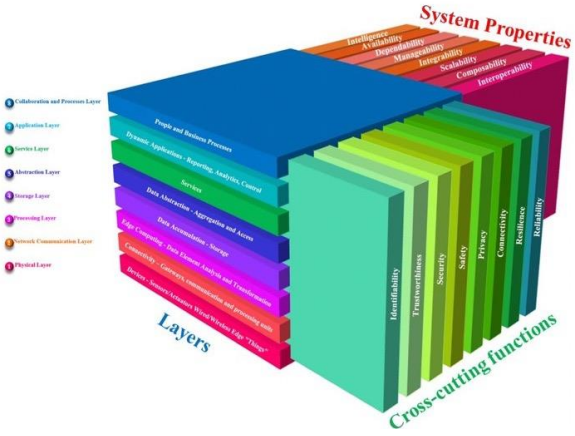
The session focused on breaking down the technology silos and how the AIOTI approach can address the horizontal harmonisation: the work done on current gaps in IoT standardisation, and how opportunities and barriers to leveraging technologies such as 5G, IoT/IIoT, AI, robotics, cloud and edge computing, as well as automation and required standards, governance, policy and rules to address horizontal harmonisation.

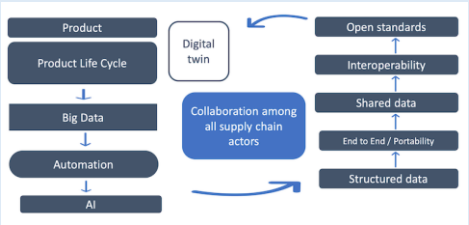
Table 12: Session 3 – Comments and position

Panellist	Comments and position
Dave Raggett, W3C/ERCIM, IoT semantic interoperability	Semantics is the study of meaning – explicit agreement on semantics is vital to the success of IoT, hence the focus on semantic interoperability – ensuring that the providers and consumers of services have a shared understanding of the meaning of

	data. An example is enabling clients to know that a given data value is the temperature of a given room in degrees Celsius. The IoT today has heterogeneity, data silos and tight coupling. Tomorrow's IoT will feature sharing of information, federation across silos and dynamic use of sources. It is not enough to collect data from multiple sources, we also need to know what the data signifies. The layers for interoperability: technical, syntactic, semantic and organisational. Today the technology is available but is limited to a relatively small community. There is misconception that semantic interoperability and semantic technologies is academic, difficult and for experts only. We want to spread the word, make it easier for all stakeholders, and to promote best practices. AIOTI WG03 has prepared a series of white papers that have been published on Research Gate then jointly announced by AIOTI, EC, oneM2M, W3C, ISO/IEC JTC1 and IEEE-SA • Initial white paper: DOI: 10.13140/RG.2.2.25758.13122 • Semantic IoT solutions, a developer perspective: DOI: 10.13140/RG.2.2.16339.53286 • Towards semantic interoperability standards based upon ontologies: DOI: 10.13140/RG.2.2.26825.29282 Ontologies provide a formal specification of a shared conceptualization, by formally defining relevant concepts, their attributes and the relationships between these concepts (Gruber 1993). This can be applied to model data and metadata for a working interaction between the supplier and consumer of data. Domain specific ontologies can be bridged by cross domain ontologies. There is a rift between RDF (W3C's resource description framework) and work on labelled property graphs (LPG), with industry showing interest in LPG as something allegedly easier to work with. However, LPG is weak on interoperability. ISO is attempting to address with extensions to SQL and new work on the GQL query language. Industry also seems to favour a more pragmatic focus on graph manipulation in contrast with the emphasis on formal semantics and logical proof in the Semantic Web. There is a need for improved standards for mapping data between different ontologies, as different communities may have different requirements that resists adoption of a shared ontology. The solutions may involve context dependent mappings analogous to terms in human languages where related concepts are described by different taxonomies in different languages. Mappings can be peer to peer or via a shared "upper" ontology with definitions of base concepts. W3C's Easier RDF initiative seeks to make RDF easier for the average developer, and hence to win over industry with a strong interoperability story. Looking further out, Dave believes that semantic technologies will be subsumed by cognitive technologies. He talked about "chunks" as an amalgam of RDF and LPG inspired by advances in the cognitive sciences. This seeks to address real world uncertainty, incompleteness and inconsistency: • Combining graphs and statistics • Reducing the cost of data cleansing • Enabling further kinds of reasoning, e.g. abduction • Machine Learning from few examples in contrast to Deep Learning • Federated processing for Big Data with distributed cognitive databases This is pointing the way to realising artificial general intelligence (AGI), and the opportunity for Europe to lead the world for human-AI collaborative solutions. For more details, see the W3C Cognitive AI Community Group.
Michelle Wetterwald, AIOTI, standardisation gaps	The high priority IoT standardisation gaps and the relevant standards development organisations have been addressed in the recent years, in particular in the 2017 ETSI SmartM2M: TR 103 375 on IoT standards, and future evolutions, and TR 103 376 on IoT use cases and standards gaps. This work has been fed into AIOTI work in 2018 on high priority IoT standardisation gaps and relevant SDOs, which also considered

	the gaps perceived by the Large Scale IoT Pilots and include a preliminary analysis for resolving these gaps. In respect to semantic interoperability, AIOTI WG03 concludes that: • Semantic interoperability is being addressed in different SDOs, which deliver ontology and semantics standards • but gaps remain and indeed, multiple approaches are increasing the fragmentation and confusion in the number of options. • Further coordination between various groups would be needed to avoid a fragmented offer for IoT semantics Other identified gaps include standards relating to safety. The second version of the AIOTI analysis published in January 2020 enumerates a list of gaps and suggestions for their resolution. It covers • an up-to-date analysis of previously identified standardisation gaps, • as well as tools to obtain an overview of standardisation activities and specifications related to IoT The main outcome from the standardisation viewpoint: • Technical topics are well understood • Interoperability is making its way • Market enablers are starting to raise attention Deployment and societal topics need further focus in standardisation.
Marco Carugi, AIOTI High level architecture	Marco presented a status report for the AIOTI work on a high-level architecture (HLA) for IoT platforms. The latest version dates back to 2018. Further discussion is needed with respect to IoT architectural concerns: Privacy, Virtualization, Big Data-IoT architectural integration, Artificial Intelligence for IoT, Autonomous Systems and IoT, API cloud-based platform-to-platform interoperability. Three areas have been progressed: security, interoperability among platforms, and device virtualisation. The discussion at the end of 2019 addressed the potential for HLA extensions and the potential for new studies: • New clause/Reference architecture for Data Market Place ("data lake" being one approach), including consideration of IDS • 3D architecture (decentralized, cloud-edge coordination) – including integration with HLA • Meta data architecture • Next generation of data How the data will flow (Business IoT Consumer IoT; Industrial IoT, Tactile IoT, NG IoT) • Convergence of technologies • Intelligent connectivity • IIoT Edge capabilities • Capabilities that data is collected • Tactile edge capabilities. **Emilio Davila Gonzalez** (EC DG Connect - Head of ICT Standardisation Sector – Digital Innovation and Blockchain Unit) mentioned that the 2019 ICT Rolling plan for standardization has been released and thanked the AIOTI for the provided contributions: https://ec.europa.eu/growth/content/2019-rolling-plan-ict-standardisation-released_en
Ovidiu Vermesan, AIOTI IoT research	Ovidiu talked about research priorities for IoT. He lists: AI, Distributed Ledger Technologies, edge computing, network slicing and virtualisation, and the role of digital twins. The next generation IoT is expected to support massive density of devices and high data rates for industrial applications. We will see ultra-reliable, very low latency, static and mobile networks that stimulate the growth of new kinds of services. Changes to what kinds of data are collected. Sometimes data is only needed in real-time, in other cases, it has long lasting value. Ovidiu expects a trend from centralised

	to decentralised, distributed systems, with a greater emphasis on edge processing including embedded AI. He presented the CREATE-IoT 3D reference IoT architecture with layers, cross-cutting functions and system properties as the three axes.  This was designed to cover all of the function aspects, in particular, cross cutting layers, and more than just the functional aspects. The goal was to provide a model that can be used to frame a discussion of a range of existing IoT architectures. Suggested IoT research priorities: • IoT - DLTs Heterogeneous Platforms and Interoperability • IoT and AI Methods and Techniques • IoT and Distributed Ledger Technologies • IoT Privacy, Safety, Security, and Trust • Tactile and Industrial-Tactile IoT • Digital Twins for IoT • Integration of information and operational technologies • Standardisation
Franck Boissière, EC DG Connect, IoT standardisation activities overview	Two things are important to understand. We here in relation to the annual ICT Rolling Plan. On Monday, an update to this plan will be announced. The plan identifies priorities for different areas. This workshop omitted the topic of standards for cybersecurity. 5G and IoT are important areas for standards, as are Block Chains, and AI. We have to go further and find a way to go beyond the established constituencies. The PPP's like BVDA and AIOTI are very important. We expect to have announcements towards the end of the year in respect to standardisation respecting European values.
Emmanuel Darmois, ETSI	IoT is a very complex problem domains and issues, relating to brand new systems: IoT is pervasive with a very complex Standardisation landscape. IoT is a major priority for ETSI (with a large part of the work done in SmartM2M TC) and, on top of oneM2M, AIOTI is a very important channel for the ETSI results. There is a lot of new requirements emerging from cross sector applications. A vast number of standards, e.g. for smart cities some ten thousand standards. Collaboration is essential to successful development and deployment of standards. Hone very important question is how solutions developed in one SDO can become global. In this perspective, SDO collaboration increasingly important, as can be demonstrated by the example of oneM2M. Another example is the IoT LSP 3D Reference Architecture model developed in the IoT LSP Activity Group 02, where a third dimension was added to account for additional viewpoints. A new approach is the provision of guidelines towards the largest possible range of stakeholders, not just the standardisation ecosystem. A first example is ETSI STF 547 which has provided guidelines for the definition, design and development of IoT systems on security, privacy, semantic interoperability and platform interoperability. Another example is ETSI STF 561 which focuses on improving the role of citizens in smart cities standardisation and provides guidelines in this respect.

Francesca Poggiali, GS1	 How to avoid data silos? Need for a common language for ecosystem interoperability. GS1 as a precedent. GS1 has strict rules for involving full range of stakeholders. GS1 believes in global data models (video). GS1 standards for supply chains: Identify: globally recognized unique identification of products, assets, locations and more; Capture: real-time accurate and automatic capture of data; Share: efficient sharing of information from trusted and authentic sources We see a lot of value for the digital twin concept, and to its relation to product lifecycle.  The importance of regulations for driving change: the EU green deal, focus on circular economy, the EU strategy for data, and the fight against illicit trade. The importance of metadata: What's inside? Where does it come from? How was it produced and manufactured? Is it safe? Putting interoperability first. • Identify the data required to meet the business objectives • Clearly define the data sharing issues that need to be accessed • Consider the existing product identifiers and data sharing business processes and assess the changes needed • Identify and assess the necessary trading partner governance strategy • Enable an open data approach based on global, open standards for product authentication

6.4.1 Q&A and discussion

Table 13: Session 3 – Questions and Answers

Questions	Answers
Standardisation bodies also form an ecosystem, and this includes some competition, is this an issue?	Marco: certainly, there is some competition, but in many SDOs we are missing the voice of the citizens. In many cases collaboration is needed and sought. Antonio: each SDO has its sphere of expertise Wael Omar: fragmentation of standards is to a big extent driven by vendor lock-in. Emmanuel: for a given topic, the vast number of SDOs are likely to be irrelevant. One may have a very good specification but will lack the involvement and support of the important actors in the ecosystem. Ovidiu: previously banks built their own silos, but they realised that collaboration is better for security and now they see opportunities to innovate on top of of the common infrastructure using common standards and approaches (e.g. security and information/transactions exchange). IoT is similar. Franck: the ICT Rolling Plan provides a relatively exhaustive list of things for each domain. We try to put interoperability high up in priority. We've included standardisation in the projects, with mixed results. In successful

	projects, we often see early agreement on what technology solutions to focus on. We need to focus on how to boost European standards. We want to involve different SDOs to add speed and value. Each sector tends to have their own group of SDOs. We try to our best and will continue to do so. Michelle: it is valuable to provide guidance around how to use standards. Small industry alliances can be very fast in the appropriate circumstances, and a good way to build momentum. Ovidiu: pre-normative standardisation activities can help to reduce fragmentation. An example is where alliances have merged, e.g. fog computing and Industrial Internet Consortium. Marco: fully agree with importance of pre-normative work.
How do you assess which standards are still relevant?	Emmanuel: no straightforward answer. Relevance is a question of the level of impact on ecosystems. However, business conditions are often unclear and quite fluid. We need a mix of standardisation and regulation.
For GDPR, we may gain something if we can protect data in real life. Data sharing between companies has been held back on account of fears of losing competitive edge. Comments?	Ovidiu: incentives play an important role for adoption, e.g. as we have seen for adoption of electric vehicles. Franck: the rules of the game need to be much clearer; we have some experience of this in the energy sector. One incentive is to lower the entry barrier, e.g. to define common data formats. Examples of successful practice can help to alleviate fears of opening up for sharing.

6.5 Conclusions

Rolf Riemenschneider (EC DG Connect, Unit E4) provides a summary of the major takeaways from the workshop.

We need to find an accommodation between global and local perspectives. We may see some changes in the partnerships, and to review the standardisation approach, to identify gaps and react to market trends.

The majority of value for the IoT is from cloud. We need to balance the interest to preserve proprietary approaches and open approaches. We have more stakeholders to talk to. More automation at the edge. A larger playground.

We urgently need standards at the metadata level and not just the data level. We need a mix of private and public money.

Please stay in touch and stay tuned to announcements and developments.

Rolf Riemenschneider (EC DG Connect, Unit E4) thanks all the organisers, speakers and participants!

7. CONCLUSIONS AND FUTURE STEPS

7.1 Contribution to overall picture

The Workshop has addressed, in a very broad panorama, all the current questions under analysis within the IoT technical community, those addressed by the first generation of LSPs (within the 5 LSPs and the Activity Group 02 on "IoT Interoperability, Architectures and Standardisation") as well as those identified in the work program of the new LSPs grouped in OpenDEI. All issues under discussion have an impact well beyond the IoT standardisation community, in particular on the IoT research one.

Firstly, the contribution of the first generation of LSPs – as described by CREATE-IoT in the "IoT LSP Interoperability Framework" - has been consolidated and recalled during the workshop. A large part of these contributions has been going to IoT standardisation and some examples are listed below:

- The collaborative development by LSPs of a 3D Reference Architecture model.
- The Minimum Interoperability Points (MIMs) specified by ACTIVAGE, IoT 2020 and SynchroniCity.
- The MONICA requirements for a new standard for time-critical data links for IoT sensors.
- The LSPs contributions to SAREF (Smart Appliances REFerence ontology).
- AUTOPILOT contributions to oneM2M
- The contributions of SynchroniCity to the ITU Study Group 20 on IoT and Smart Cities.

In addition, some others have been developed as tools in support of the efficient implementation and deployment of the LSP Use Cases and may possibly become more standardised elements to be used by the second generation of the LSPs, such as the ones listed below:

- The IoT Catalogue that collects components that can be used and reused in implementation projects.
- The methodology for launching Open Calls and following their implementation.

These developments are significant results of the work done around the LSP Interoperability Framework. It is important that these achievements be carried out even after the end of the first generation of LSPs. In some cases, this will be the case, in particular for the on-going developments in standardisation. The work done in the context of the LSPs can contribute to the advancement of the new Digital Strategy and to the revision of the GDPR that the Commission in undergoing. The experience gained could also contributed to shape the European approach to global and national standardization initiatives.

7.2 Future Directions

The very large breadth of the discussions during the Workshop has confirmed that the innovation in the IoT field is by no means showing any sign of slowing down. Some topics have been clearly identified as priorities by several projects of the second generation of LSPs. A short list of these topics is the following:

- Supporting the efficient adoption of new technologies such as Distributed Ledger Technologies or Artificial Intelligence, across all parts of the IoT systems from physical to business layers, in support of cross-cutting functions such as security, privacy or safety.
- Developing solutions (including the necessary infrastructure) for secure data management in support Open Access to data and the creation of generic or sector-specific data spaces.
- Addressing the challenges of industrial adoption for semantic interoperability together with improving the efficiency of organisational interoperability solutions.

- Strengthening the provision of privacy and security for resilient services.
- Taking full benefits of communications scalability, reliability, latency (e.g., 5G).
- Boosting the efficiency of edge solutions (data privacy, federation, AI, etc.).
- Proposing robust solutions for privacy-preserving federated machine learning.
- Fostering the emergence of the Intelligent autonomous IoT.
- Defining the Sentient Web (web of digital twins, cognitive AI and open marketplaces).
- Fostering the development of common visions (e.g., through White Papers) across the largest possible number of relevant actors in the field of standardisation.
- Promoting recommendations for collaborations across PPPs, SDOs and other alliances.

These topics will be further developed in the coming 3 years where a larger number of LSPs in a larger set of sectors will address them under a variety of complementary angles. Some of these topics will be characterised and briefly analysed in the CREATE-IoT Deliverable D06.06 (Final report on IoT standardisation activities) due at the end of April 2020.

Altogether, the workshop has also very much insisted on the need of collaboration, exchange of information and identifying common approaches and best practices. On first level, collaboration must take place across the new LSPs in order to create common solutions likely to have an impact on the global scene. More largely, these new common developments should be brought, as with the first generation of LSPs, in the field of IoT standardisation. From this standpoint, it is important that the "IoT LSP Interoperability Framework" be maintained and expanded in the new coordination structures put in place, such as through the ambassadors that OpenDEI has nominated for the handling of cross-projects issues.

8. REFERENCES

[1] Navigating IoT Architectures and Standards Days, online at: https://european-iot-pilots.eu/2020-february-brussels/
[2] IoT Europen Large-Scale Pilots Programme, online at: https://european-iot-pilots.eu/
[3] "Privacy study report – Standards Landscape and best practices", ETSI TR 103 591, 2019
[4] "Security study report – Standards Landscape and best practice", ETSI TR 103 533, 2019
[5] "Teaching material – Part 1: IoT Security and Teaching material", ETSI TR 103 534-1, 2019
[6] "Teaching material – Part 2: IoT Privacy and Teaching material", ETSI TR 103 534-2, 2019
[7] "Guidelines for using semantic interoperability in the industry", ETSI TR 103 535, 2019
[8] "Strategic/technical approach on how to achieve interoperability /interworking of existing standardized IoT Platforms", ETSI TR 103 536, 2020
[9] "Plugtests preparation on Semantic Interoperability", ETSI TR 103 537, 2019
[10] "Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach", ETSI SR 003 680, 2020
[11] "Personal data protection for IoT deployments - lessons learned from the European large-scale pilots for the IoT", Common Report of IoT LSP, CREATE-IoT and U4IoT, 2020.
[12] "Cyber Security for Consumer Internet of Things", ETSI TS 103 645, 2019.
[13] "Semantic Interoperability for the Web of Things", AIOTI WG03, 2016.
[14] "Semantic IoT Solutions: A Developer Perspective", AIOTI WG03, Oct. 2019.
[15] "Towards Semantic Interoperability Standards based on Ontologies", AIOTI WG03, Oct. 2019.