D3.3 OPPORTUNITIES AND BARRIERS IN THE PRESENT REGULATORY SITUATION FOR SYSTEM DEVELOPMENT

WP 3

IoF2020 has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 731884. Visit iof2020.eu for more information about the project.

DOCUMENT IDENTIFICATION

Project Acronym	**IoF2020**
Project Full Title	Internet of Food and Farm 2020
Project Number	731884
Starting Date	January 1st, 2017
Duration	4 years
H2020 Call ID & Topic	IOT-01-2016
Website	www.iof2020.eu
File Name	D3.3
Date	May 29th, 2018
Version	1.2
Status	Final
Dissemination level	PU: Public
Author	José Manuel Cantera, Joud Sayed Issa (FIWARE Foundation), Peter van der Vlugt (AEF), Sabine Klaeser, Tim Bartram (GS1), Ayalew Kassahun (WU), Isabel Neira (365FarmNet), Thierry Milin (Orange)
Contact details of the coordinator	George Beers george.beers@wur.nl

PROJECT SUMMARY

The internet of things (IoT) has a revolutionary potential. A smart web of sensors, actuators, cameras, robots, drones and other connected devices allows for an unprecedented level of control and automated decision-making. The project Internet of Food & Farm 2020 (IoF2020) explores the potential of IoT-technologies for the European food and farming industry.

The goal is ambitious: to make precision farming a reality and to take a vital step towards a more sustainable food value chain. With the help of IoT technologies higher yields and better-quality produce are within reach. Pesticide and fertilizer use will drop and overall efficiency is optimized. IoT technologies also enable better traceability of food, leading to increased food safety.

Nineteen use-cases organized around five trials (arable, dairy, fruits, meat and vegetables) develop, test and demonstrate IoT technologies in an operational farm environment all over Europe, with the first results expected in the first quarter of 2018.

IoF2020 uses a lean multi-actor approach focusing on user acceptability, stakeholder engagement and the development of sustainable business models. IoF2020 aims to increase the economic viability and market share of developed technologies, while bringing end-users' and farmers' adoption of these technological solutions to the next stage. The aim of IoF2020 is to build a lasting innovation ecosystem that fosters the uptake of IoT technologies. Therefore, key stakeholders along the food value chain are involved in IoF2020, together with technology service providers, software companies and academic research institutions.

Led by the Wageningen University and Research (WUR), the 70+ members consortium includes partners from agriculture and ICT sectors and uses open source technology provided by other initiatives (e.g. FIWARE). IoF2020 is part of Horizon2020 Industrial Leadership and is supported by the European Commission with a budget of €30 million.

Executive summary

This report is intended to facilitate an understanding by different stakeholders (particularly use case owners and developers) how IoT and related technologies can be applied to the domain of Agrifood, with a view to creating interoperable and portable solutions. In addition, it is intended to help stakeholders from other business domains to identify potential cross-sector synergies. The final aim is allowing for the building of an IoT ecosystem around the IoF2020 project and ultimately around Smart Farming in Europe.

The technologies and associated standards considered by this document address different layers that have to be tackled when deploying a Smart Food and Farming solution, as depicted by the figure below. To this aim the main layers that have been identified are:

- *Physical Device Layer*. This layer is composed by different IoT devices and agricultural machinery deployed in the field.
- *Connectivity Layer*. This layer enables the bidirectional transmission of data produced by devices or machinery.
- *IoT Service Layer*. It exposes the raw data generated from IoT Devices and, possibly, actuation commands through different application-level transport protocols.
- *Mediation Layer.* It transforms the raw data coming from devices or other external services, into curated, harmonized and possibly aggregated data.
- *Information Management Layer*. This layer serves mainly as a data hub which enables the publication, consumption, subscription and processing of all the information relevant to a food and farming solution.
- *Application Layer.* In this layer resides all the different applications such as those related to decision support (DSS), farm management (FMIS), dashboards or enterprise resource planning (ERPs).
- A cross-cutting layer on *Security and Privacy* aimed at guaranteeing secure access to information and devices, while respecting the privacy of consumers, farmers and exploitations.

In addition, other external entities play a relevant role, namely:

- *Open Data providers and Public Geo-Services*. For instance, public databases offering data in the agricultural domain, geo-services publishing weather or spatial data or even satellite data/image platforms.
- *Harmonized information models.* They define the structure and representation of the information to be managed, with a view to enabling interoperability and portability of solutions in a wider ecosystem.

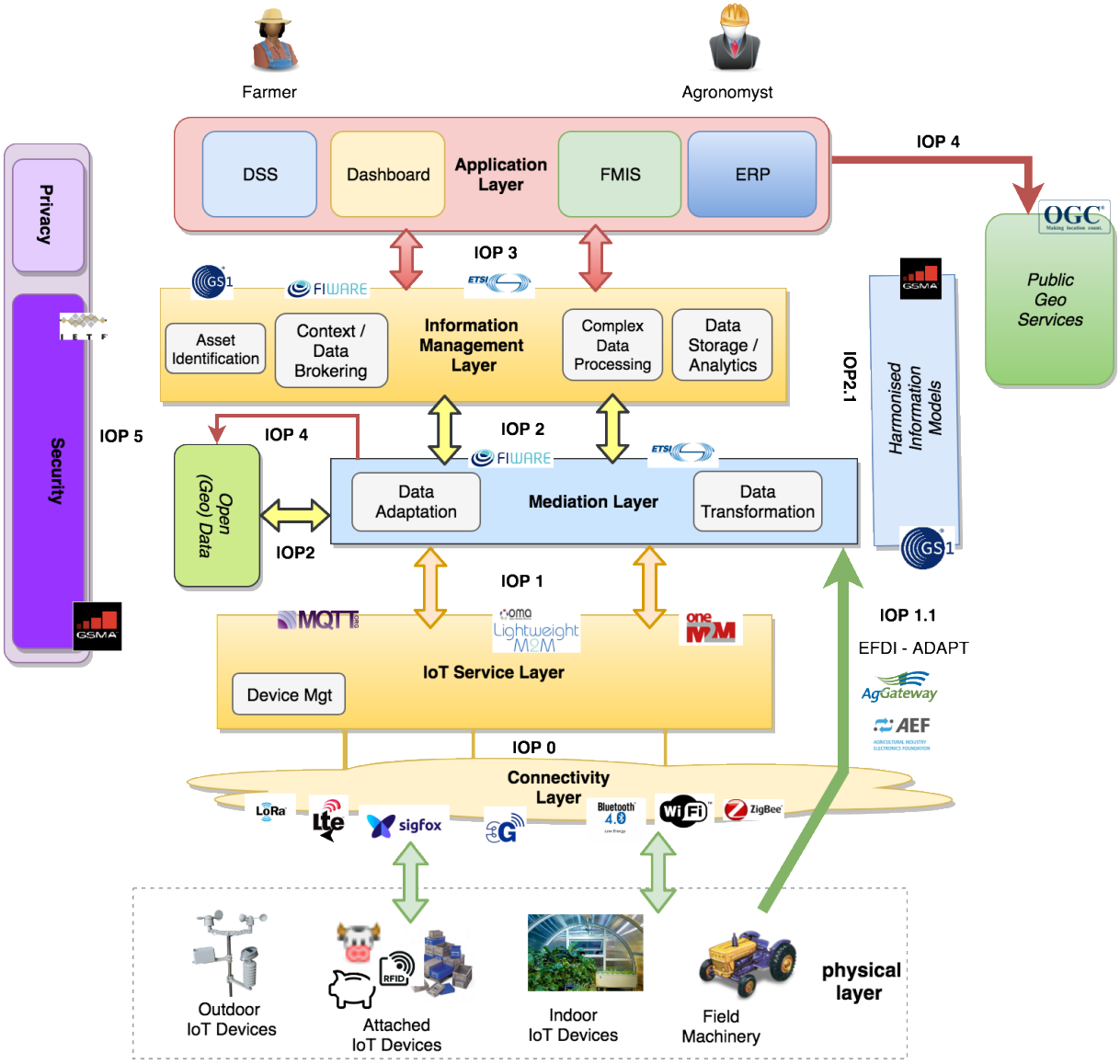


Figure 1: Overview of IoF2020 Use Cases and its relationship to standards

The interoperability points identified and depicted by the referred figure are the following:

- *Interoperability Point 0*: It is realized as a connectivity enabler for IoT Devices and agricultural machinery. Low Power Wide Area Wireless Technology (**LPWA)** networks are described more in depth by this document, as they are currently one of the most suitable communications technology for the farming domain. The main drawback is the connectivity limitation. In fact, even though more than 90% of the world population today is connected via cell phone-based technologies, only 30% of the rural landscape is covered by cellular radio and even less with 3G or above [63]. Most of the agricultural used areas come with a low bandwidth or no cellular coverage at all.

- *Interoperability Point 1*: It is situated in between the IoT Service Layer and the Mediation Layer, enabling the exposition of the data and services offered by IoT Devices through well-known programmatic interfaces. **MQTT(-SN), CoAP**, **LWM2M** and **oneM2M** are analysed as the main technology enablers. The latter is the proposed worldwide standard unified platform (interworking with the former ones) for the IoT Service Layer.
- *Interoperability Point 1.1*: It makes it possible the bi-directional transmission of data between the agricultural machinery and the upper layers. **ISOBUS** and **ADAPT** are key enabling and emerging technologies described by the present document. ISOBUS is a complex standard and as a result it has led to different implementations by manufacturers of agricultural equipment. This have resulted in incompatible tractor and implement combinations for the farmer or contractor, thus leading to a lot of frustration. The ADAPT framework is precisely aimed at reducing misunderstandings between actors and consumers of agricultural data when it comes to exchange information from different sources and formats.
- *Interoperability Points 2, 2.1 and 3*: It is crucial that the set of data exchange principles is standardized throughout the Agrifood Industry. In other words, the industry has to go for just one type of interface protocol between devices/machinery and cloud services, and from cloud services to External API's. To that aim it is needed a set of standardized cloud-cloud interfaces and data models. **FIWARE NGSI** and its evolution to an ETSI standard, **NGSI-LD**, provide a solution to information management and data exchange, enabling the transformation, aggregation, harmonization and publication, as context information, of harmonized data coming from IoT Devices, agricultural machinery or other sources of information. Accompanying NGSI-LD, the work developed by the **GSMA** IoT Big Data Project on data harmonization (data models) plays a relevant role to achieve data portability, together with **GS-1** standards and the aforementioned ADAPT Data Model.
- *Interoperability Point 4*: It enables the Application and Mediation Layers to consume public Geo-Services, enriching the smart farming applications with geospatial data and off-the-shelf visualizations. OGC **WFS** and **WMS** play a relevant role as the main standards to be considered.
- *Interoperability Point 5 (IOP5)*: It is a cross-cutting interoperability point that facilitates the secure interchange of information between the different layers and actors. The **GSMA IoT Security Guidelines** and the traditional security technology stacks (TLS, DTLS, PKI, …) or protocols (particularly **OAuth2**) are under the scope of this interoperability point.

Interoperability Points are the cornerstone for the development of the use cases tackled by the IoF2020 project. As a consequence, this document also analyses the link between those use cases (grouped by trial for brevity purposes) and several technology enablers for interoperability. The final aim is to help use case stakeholders, product owners and developers to identify and harmonize a set of common technology enablers, software components, open platforms and related architectures that guarantee the

creation of a sustainable ecosystem of portable solutions for the Farm and Food sector. In the end, that will foster

- the flourishment of a marketplace composed by different vertical solutions capable of interoperating and integrating into a broader system of farm management,
- the identification and development of IoT reusable components and reference configurations and compositions in the framework of a common architecture,
- finally, this IoT marketplace, enabled and empowered by standard technologies, will turn into the ideal space for collaboration and incubation of further innovations in the Agrifood sector.

Table of Contents

LIST OF ACRONYMS

ADAPT	AgData Application Programming Tool
AEF	Agricultural Industry Electronics Foundation
AgData	Agricultural Data (Weather Data, Crop Data, Machine Data, etc. related with Precision Farming)
Agrifood	The business of producing food Agriculturally
CIM	Context Information Management
DSS	Decision Support System
EFDI	Extended FMIS Data Interface
EPC	Electronic Product Code
ETSI	European Telecommunications Standards Institute
FMIS	Farm Management Information System
GSMA	Global System for Mobile Communications Association
HTTP	Hypertext Transfer Protocol
ICT	Information and communication technology
IoT	Internet of Things
ISG	Industry Specification Group
ISM	Industrial Scientific Medical
ISO	International Standards Organization
JSON	JavaScript Object Notation
LPWA	Low-Power Wide-Area Wireless Technology
M2M	Machine to Machine
MAC	Media Access Layer
MQTT(-SN)	Message Queuing Telemetry Transport (- Sensor Network)
NGSI	Next Generation Service Interface
OEM	Original Equipment Manufacturer
OGC	Open Geospatial Consortium
OMA LWM2M	OMA Lightweight Machine to Machine protocol
REST	Representational State Transfer
SDO	Standard Development Organization
SPADE	Standardized Precision Ag Data Exchange
UCs	Use Cases
UDP	User Datagram Protocol
URI	Unified Resource Identifier
WFS	Web Feature Service
WMS	Web Map Service

1. INTRODUCTION

One of the main objectives of the IoF2020 project is to create a reference architecture and an open platform for interoperable and replicable solutions that deliver added-value functionalities to various stakeholders in the food and farms domain. To meet such an ambitious objective, WP3 has been working on identifying the key and common interoperability points that apply to the different use cases and trials, allowing secure and controlled exchange of information and capabilities across heterogeneous components. Interoperability points shall be realized by reusable open platforms and components that implement widely adopted standards (published by SDOs or de-facto ones) suitable for the Agrifood domain.

This document identifies and summarizes the main **relevant standards** that have to be considered by the technological solutions proposed to implement the different use cases, so that **interoperability** and **replicability** are achieved, allowing for the building of an Internet of Things (IoT) ecosystem around the IoF2020 project and ultimately around Smart Farming in Europe. In other words, to make use case developers aware of related opportunities and barriers, to facilitate and trigger collaboration and synergies and as input for collaboration with external stakeholders.

The technologies and associated standards considered by this document address different layers that have to be tackled when deploying a Smart Food and Farming solution.

It is noteworthy that the objective of this document is not to analyze thoroughly the general status of the current IoT standardization, fragmentation and related issues. There are other sources, for instance [ETSI TR 103 375 V1.1.1], published by ETSI, where readers can find a detailed summary of the status of the current IoT standardization efforts; the degree of industry and vertical market fragmentation; and pointers towards actions that can increase the effectiveness of IoT standardization.

To better understand the context around this deliverable, it is encouraged to read **D3.2** which contains the technological analysis and the architecture of the different solutions proposed to address the IoF2020 use cases. The recommendations made by this deliverable should serve as input for *Task 3.3, Open Platforms*. In fact, it should guide the definition and selection of platforms and components during the upcoming implementation of the use cases to be developed.

The analysis performed by this report provides a “common ground” to establish IoT-based innovations in the upcoming phases of the project, both within each use case, spawning across multiple use cases or even beyond the traditional limits of the Agrifood and farming sector.

Chapter 2 presents the approach and methodology, including an architectural view that could be applied to the different IoF2020 use cases. The main outcome of such chapter are the architectural layers and the interoperability points (IOPs). For each IOP one or more relevant standard technologies are identified.

Chapter 3 focuses on the IoT Network Layer identifying the main IoT network technologies, including, but not limited to LPWA networks. Chapter 4 describes the IoT Service Layer technologies, namely LWM2M, MQTT or oneM2M. Chapter 5 reviews the state of the art concerning standards for the digitization of agricultural machinery and their relationship with IoT technologies. Chapter 6 summarizes the main technologies revolving around the Information Management and Mediation Layers, including OGC and ETSI standards. Chapter 7 tackles a very important aspect in terms of interoperability, the harmonization of data, where the GS-1, ADAPT, FIWARE and GSMA initiatives are key for meeting the IoF2020 objectives. Chapter 8 addresses, succinctly, all the challenges that have to with security and privacy in the Food and Farming domain. Finally, the main conclusions, including an action plan, and a complete bibliography is included.

2. APPROACH & METHODOLOGY

2.1. INTRODUCTION

One of the main concepts behind IoF2020 is the maximization of synergies across multiple use case systems, so that real large scale deployments take up in the Agrifood sector. As a consequence, much attention is paid to ensuring the interoperability of multiple use case systems and the reuse of IoT components across them. The figure below shows the proposed approach to achieve this during design, development, implementation and deployment.

To enable reuse of components, IoF2020 will provide a catalogue of reusable system components, which can be integrated in the IoT systems of multiple use cases of the project. It is expected to include as much as possible existing components from previous and running projects and (open source) initiatives, including FIWARE, FIspace, etc.

Within the main goal of achieving interoperability, it is of paramount importance the identification of the different Interoperability Points (IOPs) and enabling standard technologies. To that aim, first of all, an analysis of the different trials and use cases has been conducted, identifying and generalizing the main architectural layers and interoperability points. Afterwards, they have been associated with one or more open standard technologies that are supported by an official or de-facto standard. Such technologies are later described and analyzed identifying gaps and barriers for adoption.

The final result of the analysis will allow other tasks in WP3 to make informed decisions, for the benefit of use case owners, developers, stakeholders and the farm and food domain.

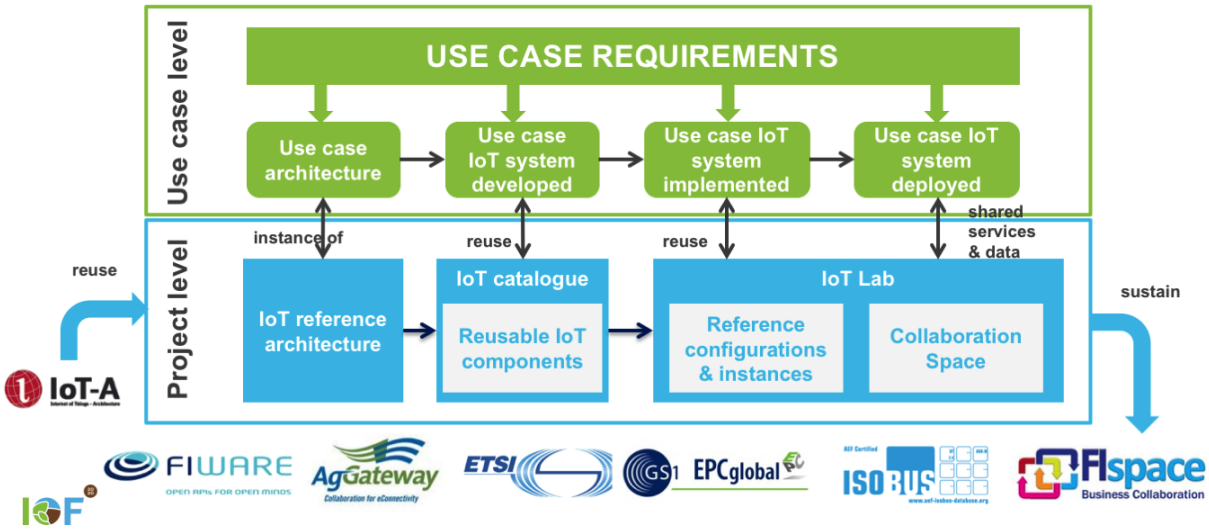


Figure 2: IoF2020 Large Scale Pilot approach

2.2. IOF2020 TECHNICAL SOLUTIONS AND STANDARDS

Building on the experience being generated on the field, **D3.2** has established a common architectural view, for each of the UCs, which can be used as a "common ground" to establish IoT- enabled synergies and new added-value services, together with the technologies which can act as the common enablers for the different interoperability points.

The figure below shows an attempt, leveraging the IoT-A Architectural Reference Model, to provide a generalized architecture (from a functional point of view) of the IoF2020 solutions and the main standards that enable each interoperability point.

The main layers that have been identified are:

- *Physical Device Layer*. This layer is composed by different IoT devices and agricultural machinery deployed in the field, that are capable of sensing their environment and generating data of interest for smart farming applications.
- *Connectivity Layer*. This layer enables the transmission of the data produced by devices to upper layers, and vice versa.
- *IoT Service Layer*. The IoT Service Layer exposes the raw data generated from IoT Devices to upper layers in the architecture through different application-level transport protocols based on different paradigms (publish / subscribe, request / response, etc.). In addition, it offers interfaces that allow to communicate with devices for management or actuation purposes.
- *Mediation Layer.* The Mediation Layer transforms the raw data coming from devices or other external services, into curated, harmonized and possibly aggregated data that can be exposed to data processing algorithms or analytics. In addition, this layer is also capable of sending

actuation commands to the IoT Service Layer. The IoT-A Reference Model subsumes this layer into the “Virtual Entity” and “IoT Services and Resources” layers.

- *Information Management Layer*. The main component of this layer is usually a data hub (which could be incarnated by a context broker) which enables the publication, consumption and subscription of all the information relevant to a smart farming solution. The information present at this layer, which can be current or historical, may have been aggregated from different sources, not only IoT. In addition, this layer may offer complex event processing, storage or analytics services, which can generate insights, prescriptions or predictions. The IoT-A Reference Architecture names this layer as “Virtual Entity and Information”.
- *Application Layer.* In this layer resides all the different smart farming applications that could be used by stakeholders, particularly farming professionals. They include, but are not limited to, systems related to decision support (DSS systems), farm management (FMIS systems), dashboards or enterprise resource planning (ERP systems).
- A cross-cutting layer on *Security and Privacy* aimed at guaranteeing secure access to information and devices, while respecting the privacy of farmers and exploitations.

In addition, other external entities play a relevant role, namely:

- *Open Data providers*. These could be incarnated, for instance, by databases offering open data in the agricultural domain (pests, disease, weather historical data, ...) or services publishing certain contextual data such as weather forecasts, weather alerts or weather observations. Satellite data/image publication platforms or geo-services which provide geospatial data are also under this scope.
- *Harmonized information models.* They define the structure and representation of the information to be managed. The final aim is that the different smart farming trials share common information models with a view to enabling interoperability and portability of solutions in a wider ecosystem.
- *Public GeoServices.* They offer public geospatial data related to agricultural assets (for instance parcels), frequently coming from geo-information systems owned by the public authorities.

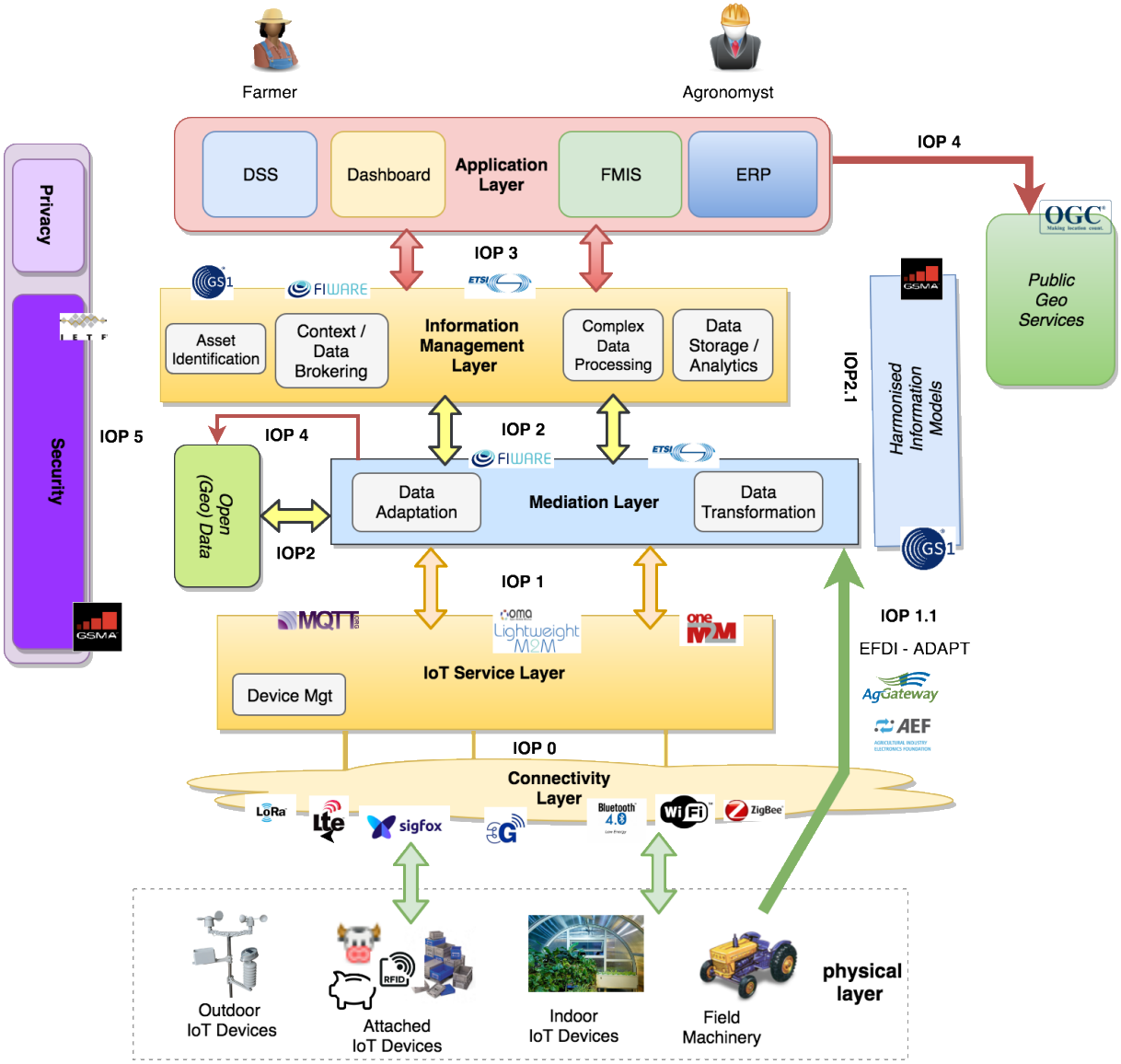


Figure 3: Overview of IoF2020 Use Cases and its relationship to standards

2.3. MAIN IOF2020 INTEROPERABILITY POINTS

The interoperability points identified and depicted by the figure above are the following:

- *Interoperability Point 0 (IOP 0)*: It is realized as a connectivity enabler for IoT Devices and agricultural machinery. Multiple communications technologies can be considered as its basis, including traditional wireless short range (WiFi, Bluetooth, IEEE 802.15.4, ...), Machine to Machine (M2M) powered by global telco networks (3G/4G/5G) or long range IoT networks specifically designed for the IoT (**LPWA**).
- *Interoperability Point 1 (IOP 1)*: It is situated in between the IoT Service Layer and the Mediation Layer, enabling the exposition of the data and services offered by IoT Devices through well-

known programmatic interfaces. The present document describes **MQTT**, **OMA LWM2M** and **oneM2M** as main technology enablers available in the industry today.

- *Interoperability Point 1.1 (IOP 1.1)*: It is situated in between the physical machinery (tractors, etc.) and the Mediation Layer, making it possible the bi-directional transmission of data between the agricultural machinery and the upper layers that deal with information management. **ISOBUS**, **ADAPT** and **EFDI** are key enabling and emerging technologies described by this document.
- *Interoperability Point 2 (IOP 2)*: It is situated in between the Information Management Layer and the Mediation Layer. On the one hand it enables the transformation, aggregation, harmonization and publication, as context information, of harmonized data coming from IoT Devices, agricultural machinery or other sources of information (open data portals, web services providing contextual data, etc.). On the other hand, it exposes a unified way to send commands and to mediate with IoT Devices or agricultural machinery, regardless the interface exposed by the IoT Service Layer or the Physical Machinery. **FIWARE NGSI**, **ETSI ISG CIM** and **GS-1** are key enabling technologies when it comes to IOP2.
- *Interoperability Point 2.1 (IOP 2.1)*: The main enablers of this interoperability point are *Harmonized Information Models* that allow to publish smart farming information following the same meta-model, data representation formats and conventions (units of measurement, etc.). IOP2.1 is key when it comes to portability of solutions at the data layer. **GSMA Harmonized Data Models** and **GS-1** are two specifications of common information models described by this document.
- *Interoperability Point 3 (IOP 3)*: It is situated in between the Application Layer and the Information Management Layer. It is intended to provide access to all the data of interest to smart farming applications, including, but not limited to, real or right time data, historical data or analytics results. In addition, it allows the subscription to data changes and to publish new data coming from the application layer. **FIWARE NGSI**, **ETSI ISG CIM** and **GS-1** are under the scope of IOP3.
- *Interoperability Point 4 (IOP 4)*: This interoperability point enables the Application and Mediation Layers to consume public Geo-Services, enriching the smart farming applications with geospatial data and off-the-shelf visualizations. OGC **WFS** and **WMS** play a relevant role with regards to IOP4.
- *Interoperability Point 5 (IOP 5)*: It is a cross-cutting interoperability point that facilitates the secure interchange of information between the different layers and actors. The **GSMA IoT Security Guidelines** and the traditional security technology stacks (TLS, DTLS, PKI, …) or protocols (particularly **OAuth2**) are under the scope of this interoperability point.

Apart from Interoperability Points, Privacy Guidelines are an important asset to be taken into account. European Agricultural Associations such as Copa-Cogeca, are starting to define some Privacy Guidelines. This document also summarizes them but further information is provided by D1.4.

2.4. INTEGRATION OF INTEROPERABLE VERTICAL SOLUTIONS

The sections above have presented the proposed architectural view and interoperability points of single, vertical solutions intended to solve specific problems, as those posed by the different IoF2020 use case and trials. However, it is envisaged that no single company will be able to provide the best solution for all the challenges faced. Furthermore, the smart Agrifood domain is very broad, specialized and diverse. In fact, it is usually needed to count with different solution developers to tackle each farmer's user story, which may involve multiple applications working at the same time. For instance, the technology, devices and applications needed for silo monitoring (sensors based in 3D cameras), is very different than those required for livestock control (collars worn by animals). Also, the graphical user interfaces to be devised are quite different. The latter needs maps and other intensive geospatial data, whereas the former needs a compelling graphical representation of silos and their filling levels.

Therefore, it is envisaged that no single company will be able provide the best solution for all Agrifood challenges. Furthermore, there is an opportunity to integrate innovative solutions coming from different parties. It will be based on the integration of information generated by different solutions to build a holistic picture of what is going on the farm. As a consequence, farm management information systems will be able to provide users an integrated view, encompassing information from different verticals and mashing-up the best of breed user interfaces. In the end, Context Information associated to a farm will be enriched with the contributions coming from different vertical solutions (system of systems), all of them able to share data between each other and enabling a further optimization of processes, saving time, money and resources.

The figure below shows a picture of the envisaged architecture of integrated (system of systems) smart farm solutions, sharing a common (Context) Information Management Layer. At the bottom of the picture there are different smart Agrifood vertical solutions devoted to solve specific problems and which, individually, may have built using an architecture similar to the one it was depicted by figure 1.

There is also the possibility that vertical solutions could have been developed using proprietary approaches, i.e. custom APIs and data models. In that case an adaptor in the Mediation Layer would be needed. Such an adaptor will serve as a bridge between harmonized Information Management APIs and data models of IoF2020 and vertical-specific, proprietary artefacts.

The main layer in the referred picture is the Context Information Management Layer, enabled by NGSI-LD and Harmonized Data Models. It will expose (partially or totally) to the farm management information system all the different Entities, Properties and Relationships that capture what is going on in the farm

concerning the different verticals involved. Furthermore, each vertical could benefit from information generated by other integrated verticals, yielding to synergies that can bring new applications or insights to end users (farmers, agronomists, etc.). In the end, end users will get access to an integrated view of farming processes from a single stop-point, the farm information management system. Such system, could offer, globally, different integrated applications, both horizontal or vertical (from the different vertical providers) such as alert management, dashboards, advanced map representations, analytics (prescriptive, predictive or descriptive), KPI monitoring or data mash-ups.

In addition, vertical solutions could also export their data to a Data Marketplace, or even benefit from existing open data present in the marketplace. The open data available could also be exploited directly by farm management information systems. Open data could also be made available through standard Geo-services, adapted and mashed-up as Context Information or being consumed directly by ad-hoc adaptors.

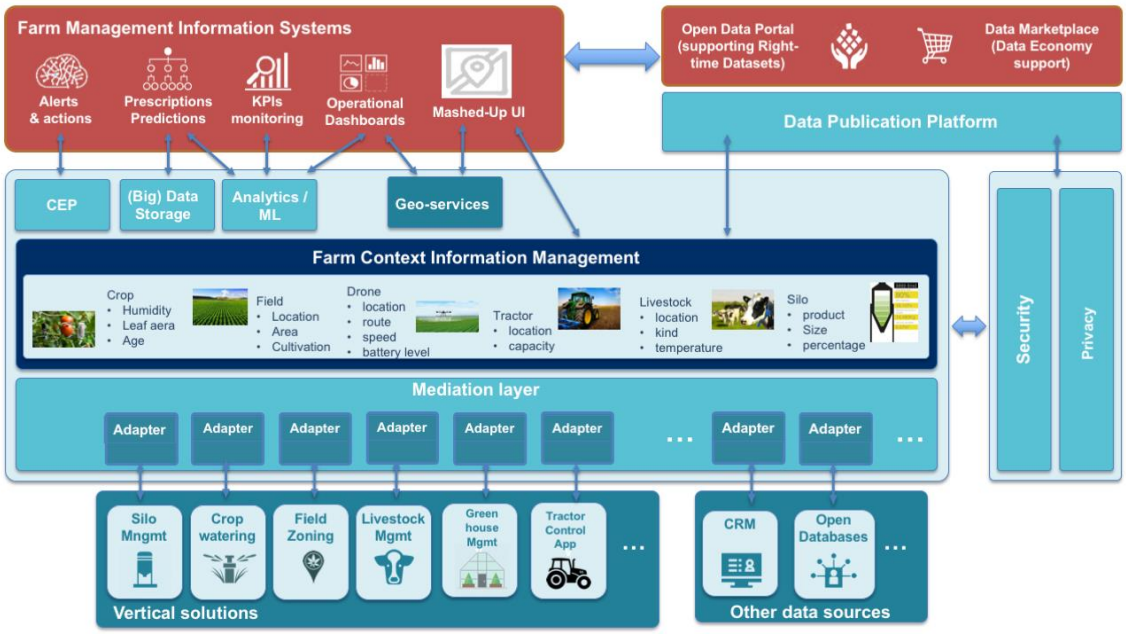


Figure 4: System of systems view for IoF2020 integrated smart Agrifood solutions

2.5. LINK TO USE CASES AND TRIALS

Once identified and described the role of the technologies that enable each interoperability point for the IoF2020 solutions, and Smart Farming in general, an analysis and description is provided, so that solution developers, customers, use case promoters and other stakeholders can understand each technology and its main areas of application. Finally, for each relevant technology, standardization and evolution an outlook is provided, together with the main drawbacks and barriers of adoption.

Interoperability Points are the cornerstone for the development of the use cases tackled by the IoF2020 project. As a consequence, this document also analyses the link between those use cases (grouped by trial for brevitiy) and several technology enablers for interoperability. The final aim is to help use case stakeholders (product owners and developers) to identify and harmonize a set of common technology enablers, software components, open platforms and related architectures that guarantee the creation of a sustainable ecosystem of portable and integrable solutions for the Farm and Food sector.

In the end, that will foster

- the flourishment of a marketplace composed by different vertical solutions capable of interoperating and integrating into a broader system,
- the identification and development of IoT reusable components and reference configurations and compositions in the framework of a common architecture,
- finally, this IoT marketplace, enabled and empowered by standard technologies, will turn into the ideal space for collaboration and incubation of further innovations in the Agrifood sector.

3. IOT CONNECTIVITY LAYER

3.1. INTRODUCTION

The IoT Connectivity Layer is intended to enable the communication between IoT devices or agricultural machines (physical device layer) and data gathering platforms. More specifically, it enables, on one hand, the transmission of data from devices (uplink), and on the other hand, the reception of actuation commands or task plans by devices (downlink).

In essence, there are three different enabling technologies for the IoT Connectivity Layer:

- Short Range Communications, including both general purpose technologies (WiFi, Bluetooth, etc.) and those intended to support wireless sensor networks, fundamentally IEEE 802.15.4 (Zigbee).
- Cellular, telco-operated networks exploiting 3G, 4G or even 5G technologies.
- Long range, low power, low bandwidth technologies (LPWA).

With regards to *Short Range Communications*, there are well established standards for wireless indoor communications based on local area networks. WiFi and Bluetooth in its different flavors (BLE, etc.) are the most significant ones. There are solutions for outdoor facilities as well, for instance, Zigbee (IEEE 802.15.4) gives support to wireless sensor networks operating in small areas. When it comes to the

particularities of smart farming (remote locations, large field areas, animals involved, rural environments, etc.)., the referred technologies are limited in terms of device battery life, coverage, network provisioning and operation costs.

Cellular networks allow data transmission at high speed, long range, with high reliability and with a great degree of autonomy. They have been used for years as an enabler of the traditional M2M business. In terms of the requirements posed by smart farming, their main drawbacks are universal coverage, battery lifetime and device cost. This is motivated by the particularities of smart farming exploitation areas which could have a considerable extension, could be located in rural areas with low connectivity and involve a big number of assets to be monitored, for instance, individual animals.

Low Power Wide Area Network (LPWAN) technologies complement existing cellular mobile network and short-range technologies, with lower costs and better power consumption characteristics. In fact, LPWAN provides battery efficient (years on a battery, not days or weeks), ubiquitous wide-area connectivity, that is professionally managed [1]. LPWA technologies are intended to serve a diverse range of vertical industries, applications and deployment scenarios. As LPWA networks are designed for IoT applications that have low data rates, they will be easy to deploy across a number of different verticals such as utilities, smart cities, logistics, farming, manufacturing, and wearables [2].

Particularly, LPWA networks are very well suited for smart farming as they provide long range communications and a low-cost proposition for devices, together with long battery life. Initially, they have been designed to operate in unlicensed (ISM) parts of the spectrum, more concretely, the sub-GHz frequency bands between 500MHz and 1GHz which are optimal for long range communication and the physical size and efficiency of antennas. LoraWAN and SigFox are the two key technologies that this document deals with, as they count with wide support from the industry and development communities.

Nonetheless, recently, a convergence between LPWA and cellular networks has been proposed by telecommunications operators, industry associations (GSMA) and standards bodies (3GPP). The idea is to take the best from LPWA and cellular, mobile, telco-operated networks. The result is a cellular network technology, named as *Mobile IoT*, capable of providing LPWA capabilities but with a higher degree of reliability, as they operate in the licensed bands of the spectrum (also in the sub-GHz frequency bands). NB-IoT and LTE-M are two of the most promising technologies, and, as the time of writing, they are in process of being deployed by mobile network operators in several countries.

The remainder of this chapter focuses principally on LPWA technologies (both licensed and unlicensed), as described by table 1. They are most suitable for smart farming and particularly for the trials and use cases addressed by the IoF2020 project. Zigbee is also described at the end of the document as another alternative.

3.2. SIGFOX

Sigfox is a LPWA cellular network specially dedicated to connected things. It offers a strong connectivity (direct access to the internet), allowing very tiny data packages to be sent, while keeping power consumption low. Sigfox employs a proprietary technology that enables communication using the Industrial, Scientific and Medical (ISM) radio band. Actually, it utilizes a wide-reaching signal that passes freely through solid objects, called "ultra-narrowband" and requires little energy.

The network is based on one-hop star topology (a network topology where typically a number of sensor nodes and one coordinator are organized) and requires a mobile operator to carry the generated traffic [3]. The signal can also be used to easily cover large areas and to reach underground objects [4].

Sigfox operates on the 868-MHz frequency band, with the spectrum divided into 400 channels of 100 Hz. Each end-device can send up to 140 messages per day, with a payload size of 12 octets, at a data rate up to 100 bps. Sigfox claims that each access point can handle up to a million end-devices, with a coverage area of 30–50 km in rural areas and 3–10 km in urban areas [5].

The Sigfox protocol stack is the software used by connected devices modem to generate radio frames and thus transmit Sigfox messages. It covers layers one to four of the Open Systems Interconnection model, a conceptual model that characterizes and standardizes the communication functions, and is composed of Frame, medium access control (MAC), and physical layer. The Sigfox protocol is located between the connected devices and the Sigfox network. It is embedded in connected devices to enable the radio frame modulation and its mission is to transmit messages [6].

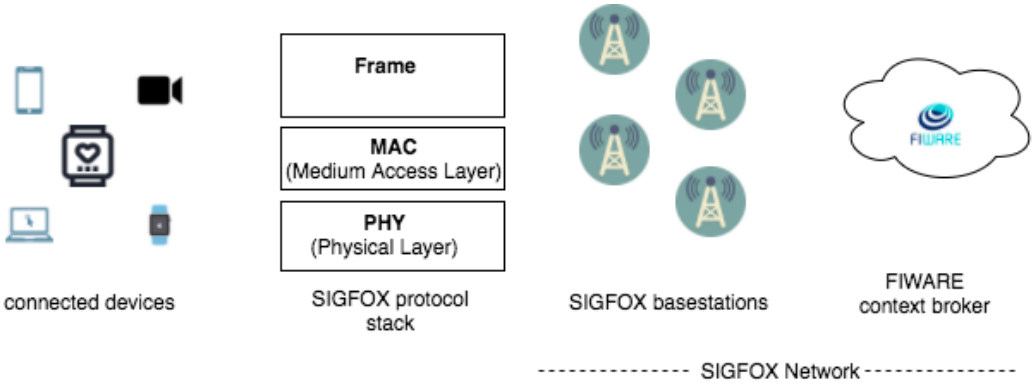


Figure 5: Integration of SIGFOX with an IoT Platform (FIWARE)

Some use cases in the agricultural domain have been produced using Sigfox (such as UC2.1: Grazing cow monitor and UC3.4: Intelligent Fruit Logistic) . Livestock monitoring applications help in knowing where livestock is, how active are animals, how many hours animals reside on pasture, etc. Another use case is wireless monitoring of soil moisture to make it easy to use precision watering of crops.

3.3. LORA

LoRa (Low Power, Long Range) is a LPWA technology intended for wireless battery-operated things in a regional, national or global network. LoRaWAN targets key requirements of IoT such as secure bi-directional communication, mobility and localization services. This communication system aims at being usable in long-lived battery-powered devices, where energy consumption is of great importance. LoRa can commonly refer to two distinct layers:

- a physical layer using the Chirp Spread Spectrum (CSS) radio modulation technique;
- a MAC layer protocol (LoRaWAN), although the LoRa communications system also implies a specific access network architecture. [7]

Typical LoRa network is “a star-of-stars topology”, which includes three different types of devices, as shown in the figure:

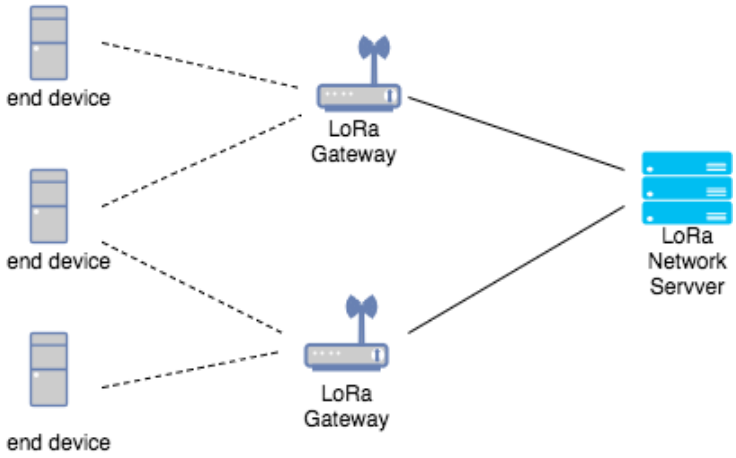


Figure 6: LoRa Network Architecture

The basic architecture of a LoRaWAN network is as follows: end-devices communicate with gateways using LoRa with LoRaWAN. Gateways forward raw LoRaWAN frames from devices to a network server over a backhaul interface with a higher throughput, typically Ethernet or 3G. Consequently, gateways are only bidirectional relays, or protocol converters, with the network server being responsible for decoding the packets sent by the devices and generating the packets that should be sent back to the devices. There are three classes (Class A, Class B and Class C) of LoRa end-devices, which differ only with regards to the downlink scheduling [5].

The data rate and maximum packet size roughly depend on the distance to the nearest gateway and the type of data to be sent and are also defined in the specification for each region. Like for the European 863-870MHz band, the application packet size varies between 51 bytes for the slowest data rate, and

222 bytes for faster rates. At most 10 downlink messages per day, including the ACKs for confirmed uplinks [8]

LoRaWAN technology can enable detection, monitoring and control over very long distance (over 15 km) of a wide variety of key agricultural data like soil temperature and moisture, weather, rainfall and water quality, airborne pollution, crop growth, livestock position, condition and feed levels. Smart connected harvesters and irrigation equipment, fire, theft and flood detection, etc. [9].

3.4. NARROWBAND IOT (NB-IOT)

NB-IoT is a Low Power Wide Area Network radio technology standard developed to enable a wide range of devices and services to be connected using cellular telecommunications bands. It is especially designed for IoT and is one of a range of Mobile IoT (MIoT) technologies standardized by the 3rd Generation Partnership Project (3GPP) as a part of Release 13, and it is integrated into the Long Term Evolution (LTE) standard [10]. NB-IoT focuses specifically on indoor coverage, low cost, reliability, long battery life, and enabling a large number of connected devices.

NB-IoT can be deployed in three ways: In-band deployment, In-Guard-band deployment and Standalone deployment. In-band deployment means that the narrowband is multiplexed within normal LTE carrier. In Guard-band deployment the narrowband uses the unused resource blocks between two adjacent LTE carriers. Finally, Standalone deployment is where the narrowband can be located alone in dedicated spectrum, which makes it possible, for example, to restructure the GSM carrier at 850/900 MHz for NB-IoT [11].

The protocol architecture of NB-IoT and LTE is separated into control plane and user plane [1]. The protocol stack for NB-IoT is the general fundamental protocol stack of LTE, which is reduced to the minimum and enhanced for re-using and preventing NB-IoT from overhead of unused LTE [12].

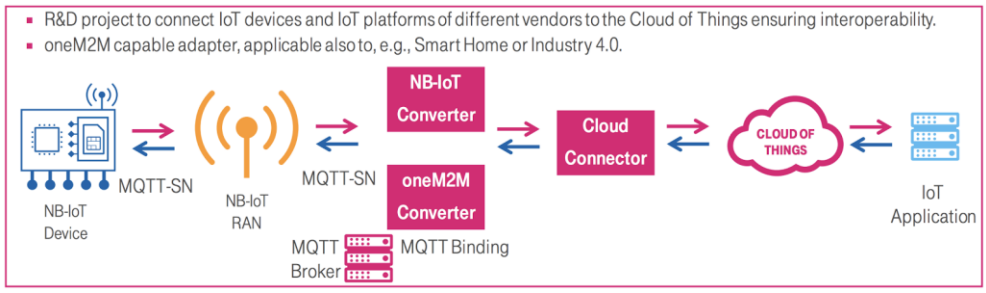


Figure 7: NB-IoT scenario (Deutsche Telekom [13])

NB-IoT technology can be also easily integrated in open platforms such as FIWARE. Particularly, it is needed an IoT Agent and the Context Broker. The role of the cloud connector will be performed via the referred IoT Agent, whereas the role of the cloud of things will be performed via the Context Broker as shown in the following figure:

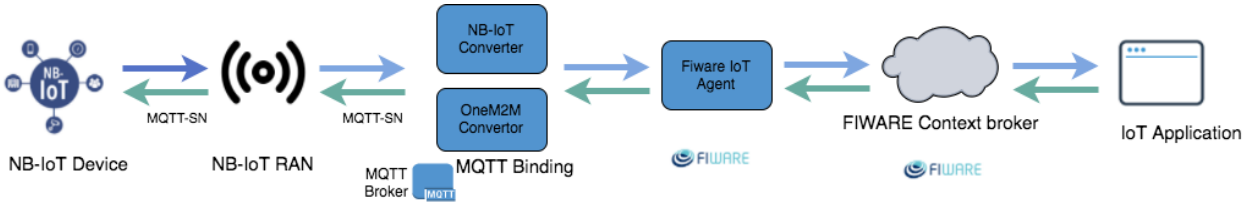


Figure 8: Example FIWARE integration with NB-IoT

NB-IoT can be used in precision farming to improve productivity and reduce risks. New services can be easily deployed. Irrigation systems can be monitored using a sensor on water sprinklers that register the position using GPS, tank levels, tipping alerts in case of falling pressure and provides the operating status of the irrigation system at intervals of time [14]

3.5. LONG TERM EVOLUTION FOR MACHINES (LTE-M)

LTE-M is a Licensed LPWA technology and one of the Mobile IoT solutions based on **3GGP** specifications (release 12/13). LTE-M combines several RAN (Radio Access Network) and CN (Core Network) features to optimize LTE Networks for IoT needs and support of new category of LTE devices (Cat M1).

The main characteristics of LTE-M Networks are:

- data rate from 200kbps to **1Mbps**
- battery lifetime evaluated to 10 years with a metering use case
- long range < 11 kilometers
- enhanced coverage with +15/20dB over existing LTE/GPRS

- support SIM security (later eSIM)
- latency from 110ms to 10 secs depending on coverage

LTE-M is sharing resources with other services (Mobile Broadband, Voice Over LTE) from an existing LTE carrier. LTE-M responds to a wide variety of use cases in different domains smart territories and industry (smart metering, critical trackers), Automotive and logistics (fleet management, onboard telemetry).

3.6. SUMMARY OF LPWA TECHNOLOGIES

The following table summarizes the characteristics of the IoT networks discussed in this chapter.

Technology	Msg Size	Maximum Number of Messages	Transmission Speed	Range	Band usage
NB-IoT	MTU: 1600 B	unlimited	Downlink: 60 Kbps Uplink: 30 Kbps	– Rural: long range (10-35 km)	regulated band 850 /900 MHz
Sigfox	≈ 12 bytes	140 Messages /day	100 bits per second	30–50 km in rural areas	license free ISM bands 868 MHz (Europe) 902 MHz (USA)
LoraWAN	≈ 50 - 222 bytes	Some networks may impose restrictions (Fair Access Policies)	18 bits/s - 37.5 kb/s	15 km	license free ISM bands 863-870 MHz in Europe
LTE-M	unlimited	unlimited	Up to 1 Mbps	< 11 kilometers	regulated band 850 /900 MHz

Table 1: LPWA Technology summary

3.7. OTHER TECHNOLOGIES

3.7.1. ZigBee Technology in Agriculture

The IEEE 802.15.4 standard supports low data rate connectivity among relatively simple devices that consume minimal power and connect short distances. ZigBee adds to IEEE 802.15.4 standard the network, security and application software. Owing to its low power consumption and simple networking configuration, ZigBee is one of the most remarkable technologies when it comes to wireless sensors networks.

Zigbee supports three device types: ZigBee Coordinator, ZigBee Router, and ZigBee End Device. Each device type implements varying levels of functionality with associated cost impacts. Thus, equipment manufacturers and system developers may implement network topology and tradeoff functionality with overall cost.

Table 2 shows a comparison between Wi-Fi, Bluetooth and ZigBee.

Feature	**Wi-FI (IEEE 802.11 b)**	**Bluetooth (IEEE 802.15.1)**	**ZigBee (IEEE 802.15.4)**
Radio	DSSS[1]	FHSS[2]	DSSS
Date rate	11 Mbps	1 Mbps	250 kbps
Data Type	Video, audio, graphics, pictures, files	audio, graphics, pictures, files	Small data packet
Range (m)	100	10	70
Battery life	Hours	1 week	>1year

Table 2: Comparison between Wireless LAN, Bluetooth and Zigbee

A solution based on wireless sensor networks for precision agriculture based on ZigBee is proposed in [16]. The system allows sensing several environmental properties (such as data of climatologically where for example weather conditions averaged over a period of time) in real time, and to make decisions based on their evolution.

Some of the requirements that are expected to be satisfied in producing effective agricultural monitoring are: system level issues and final user needs [16]. System level issues would be aspects like maximum network lifetime and end user needs could include robustness and user friendliness. Other important properties are scalability and adaptability of the network's topology. Two network topologies for such system were proposed. In the first one, each sensor node is placed at the corner of each grid and server node is located in the middle of the area. In the second scenario, server nodes are placed at out of the area. For other similar recent papers, you can refer to references [49] to [57] in the reference table at the end of this document.

3.8. GAPS AND ADOPTION BARRIERS

It is clear that radio-based machine-to-machine communication is the next step towards digital revolution in food and farming. Compared to other IoT markets (smart city, industry, automotive, …), usage of IoT devices in areas with low population density and therefore bad cellular coverage are boundary conditions for such machine-to-machine radio interface. Even though more than 90% of the world population today is connected via cell phone-based technologies, only 30% of the rural landscape is covered by cellular radio and even less with 3G or above. Most of the agricultural used areas come with a low bandwidth or no cellular coverage at all. Technologies like LoraWAN or ZigBee can potentially overcome the lack of connectivity, but there is always the handicap of the cost of management and operation, especially in remote and rural areas.

In addition to this, the mix of different brands of agricultural machines is a restraint for backend-based cellular communication services. Due to these facts, there is a general demand for the standardization of a wireless direct machine-to-machine communication for agricultural machinery in field usage. AEF has started initial talks and workshops to explore the connectivity developments in the Automotive and Truck/Bus Industry. It is the goal to reuse existing standards or standards under development.

tSeamless connectivity can only be reached by industry cooperation and by acceptance and implementation of Industry Standards for communication and data exchange.

3.9. LINK TO USE CASES AND TRIALS

Below it can be found an analysis of the suitability of each connectivity technology to the different functionalities addressed by the IoF2020 use cases, grouped by trial. Further analysis of the synergies between the different use cases can be found on **D3.7**.

An "X" indicates that the corresponding use case / trial is planning to use it. A "P" indicates that the technology could be potentially used, provided there is network coverage in the field areas.

	Sigfox	LoRa	NB-IoT	LTE-M	Zigbee
Trial 1: The Internet of Arable Farming					
Accurate Geo Location of different assets		X		P	
Machine Control (Fertilization, irrigation and harvest machinery)		X	P	P	
Quality control (crop quality)		X	P	P	
Weed control		X	P	P	
Weather Monitoring (weather stations, climate sensors)		P	P		
Soil Monitoring (Soil moisture, Vris soil scanner, soil temperature)	P	X	P		
Trial 2: The Internet of Dairy Farming					
Manage animal feeding process (measuring roughage and grass intake of individual cow)		X	P	P	
Control Cow's life span (monitor the oestrus)		X	P	P	
tracing and tracking (cow identity, location service for cow, monitor grazing cow)	X	P	P	P	
Trial 3: The Internet of Fruit					
fruit crops development (Climatic and soil moisture data for Irrigation scheduling and fertigation purposes, measure maturity level for Selective harvesting)	X	X	P		

	Sigfox	LoRa	NB-IoT	LTE-M	Zigbee
Water application automation (Measure Pressure gauges and flow meters to automate the water application)		X	P		
Optimize Fertilization process (apply variable Rate Fertilization doses)		X	P	P	
Labor monitoring (Schedule for workers and route planning) (GPS)				P	
Disease Management (infestation alert, applying variable rate spraying doses according to site-specific crop)		X	P	P	
Risk Management (maximum shelf time period and product quality) (weather stations, multi spectral cameras, thermal cameras)		X		P	
Trial 4: The Internet of Vegetables					
Resource efficiency management (Camera information from weeding machines)				P	X
Monitor vegetable growth (control artificial lightning for green houses)	X	P	P		X
Optimize Fruit production (Quality monitor and Trace vegetable transport process)	X		P	P	
Trial 5: The Internet of Meat					
Maintaining the health and welfare status (taking measures related to growing phase of animal, anomalies detection in animals' behavior, weight	P	X		P	

	Sigfox	LoRa	NB-IoT	LTE-M	Zigbee
parameter, measure/monitor drinking water consumed, presence, animal behavior or)					
Monitor environmental condition (temperature, CO2 level, humidity, ammonia)	P	X	P		
Disease Control (Feed intake, water intake, transfer action to meat process once a disease has been detected)	P	X	P		

Table 3: correlation between the different connectivity technologies and the different functionalities addressed by the IoF2020 use cases

4. IOT SERVICE LAYER

4.1. INTRODUCTION

The IoT Service Layer exposes the raw data generated from IoT Devices through different application-level transport protocols based on different paradigms (publish / subscribe, request / response, etc.). In addition, it offers interfaces that allow to communicate with devices for management or actuation purposes. This layer sits in between the physical devices and the mediation layer. The standard technologies described by this chapter enable the IOP 1, and include MQTT, OMA LWM2M and oneM2M, as the most relevant ones for the farming and food domain.

4.2. MQTT

MQTT stands for “MQ Telemetry Transport”. “A lightweight event and message-oriented protocol allowing devices to asynchronously communicate efficiently across constrained networks to remote systems” [25]. Some of the main design goals around MQTT are [25]

- To make it easier to connect the IoT (physical) world to the traditional IT world without being bound to any particular domain of application.
- Cater for frequent network disruption – built for low bandwidth, high latency, unreliable, high cost networks.

- Support client applications that may have very limited resources available (for instance 8-bit controller, 256KB RAM)
- Provide loose coupling to support dynamic system environments with high volumes of messages coming from large numbers of devices.
- Provide multiple message delivery options to reflect trade-offs between bandwidth, availability, and delivery guarantees.
- Simple for application developers and implementers of the protocol.

Figure 9 below shows how MQTT works. It is a publish/subscribe messaging protocol capable of delivering messages from one publisher to multiple subscribers through a topic as follows:

- A producer sends (publishes) a message (publication) on a topic (subject)
- A consumer subscribes (makes a subscription) for messages on a topic (subject)
- A message server / broker matches publications to subscriptions
- If there are no matches the message is discarded
- If there are one or more matches the message is delivered to each matching subscriber/consumer

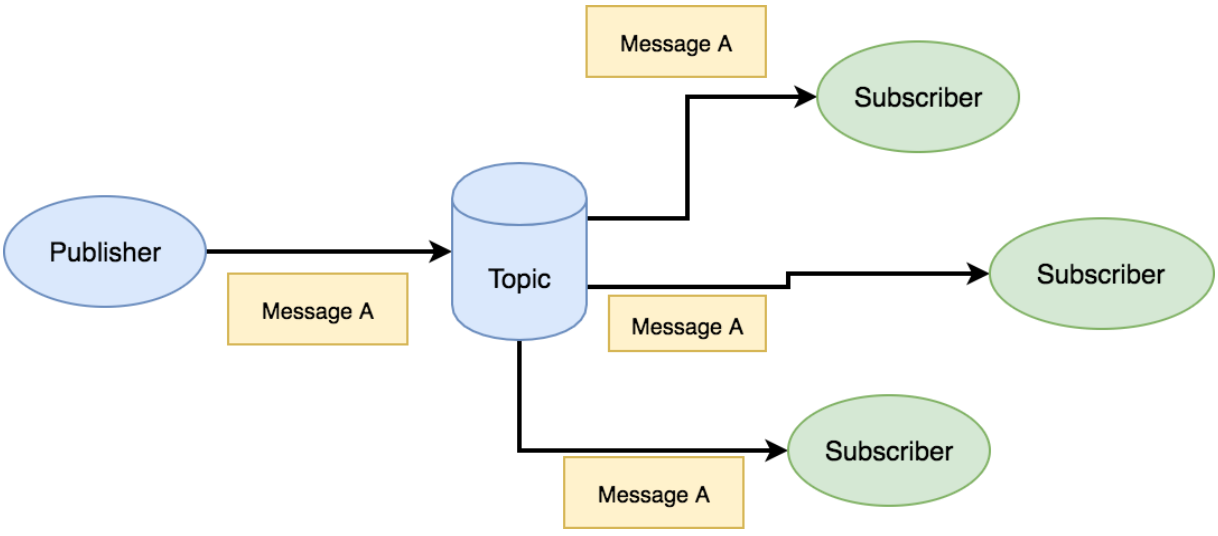


Figure 9: MQTT message delivery flow

Topics are structured hierarchically with each “sub topic” separated by a /. For instance, a greenhouse can publish information about itself on:

<country>/<region>/<town>/<postcode>/<greenhouse>/energyConsumption

<country>/<region>/<town>/<postcode>/<greenhouse>/solarEnergy

<country>/<region>/<town>/<postcode>/<greenhouse>/alarmState

And subscribes for control commands:

<country>/<region>/<town>/<postcode>/<greenhouse>/thermostat/setTemperature

A subscriber can subscribe to an absolute topic or can use wildcards. A subscription can be durable or non-durable. Once a durable subscription is in place a broker will forward matching messages to the subscriber immediately if the subscriber is connected. If the subscriber is not connected messages are stored on the server/broker until the next time the subscriber connects.

For non-durable subscriptions, the subscription lifetime is the same as the time the subscriber is connected to the server / broker. A publication may be retained i.e. the broker / server remembers the last known good message of a retained topic and as a result the broker / server gives the last known good message to new subscribers, i.e. the new subscriber does not have to wait for a publisher to publish a message in order to receive its first message.

The MQTT protocol is compressed into bit-wise headers of variable length fields. It supports asynchronous bidirectional “push” delivery of messages to applications without the need of polling. It supports always-connected and sometimes-connected communications which can be session oriented. The transport layer is typically based on TCP.

MQTT is being standardized by the **OASIS** consortium. Furthermore, version 3.1.1 of MQTT has been approved for release by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and given the designation **'ISO/IEC 20922**'.

There are multiple MQTT open source implementations [28] and client libraries [28]. MQTT has been applied successfully to the smart farming domain. [26] [27] are two examples to name just a few.

OASIS is currently developing a new version of MQTT, MQTT version 5 [29] summarizes the new features offered.

4.3. MQTT-SN

MQTT-SN [30] can be considered as a version of MQTT which has been further adapted to the peculiarities of a wireless communication environment. Wirelesss radio links have in general higher failure rates than wired ones, due to their susceptibility to fading and interference disturbances. They have also a lower transmission rate. For example, Wireless sensor Networks (WSNs) based on the IEEE 802.15.4 standard provide a maximum bandwidth of 250 kbit/s in the 2.4 GHz band [31]. MQTT-SN is also optimized for the implementation on low-cost, battery-operated devices with limited

processing and storage resources. MQTT-SN is designed in such a way that it is agnostic of the underlying networking services.

Compared to MQTT, MQTT-SN is characterized by the following differences:

- The topic name is replaced by a short, two-byte long “topic id”.
- “Pre-defined” topic ids and “short” topic names are introduced, for which no registration is required. They are known in advance by both the client’s application and the gateway/server.
- Multiple gateways may be present at the same time within a single wireless network and can cooperate in a load-sharing or stand-by mode.
- A new offline keep-alive procedure is defined for the support of sleeping clients. With this procedure, battery-operated devices can go to a sleeping state during which all messages destined to them are buffered at the server/gateway and delivered later to them when they wake up.

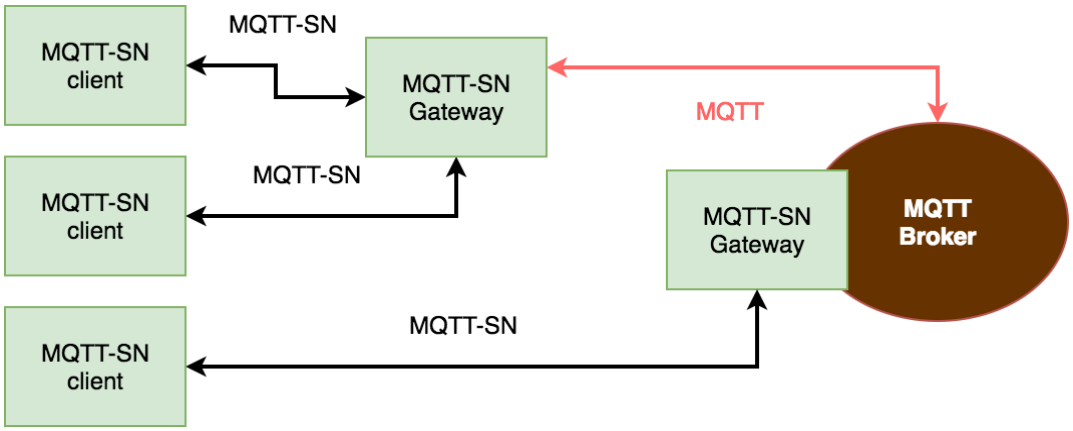


Figure 10: MQTT-SN Architecture

The architecture of MQTT-SN is shown in Figure 10 MQTT-SN clients connect themselves to a MQTT server via a MQTT-SN gateway using the MQTT-SN protocol. A MQTT-SN gateway may or may not be integrated with a MQTT server. In case of a stand-alone gateway the MQTT protocol is used between the MQTT server and the MQTT-SN gateway. Its main function is the translation between MQTT and MQTT-SN. Depending on how a gateway performs the protocol translation between MQTT and MQTT-SN, it can be differentiated between two types of gateways, namely transparent and aggregating gateways, see figure below.

A *transparent gateway* will setup and maintain a dedicated MQTT connection to the MQTT server per connected MQTT-SN client. The transparent gateway will perform a “syntax” translation between the two protocols. The main drawback of this approach is that some MQTT server implementations might impose a limitation on the number of concurrent connections that they support.

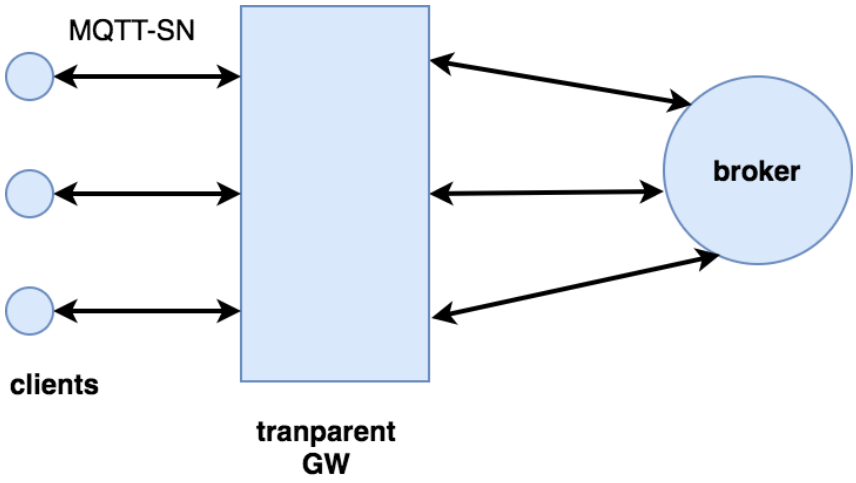


Figure 11: Transparent gateway

An aggregating gateway will have only one MQTT connection to the server. All message exchanges between a MQTT-SN client and an aggregating gateway end at the gateway. Although its implementation is more complex than the one of a transparent gateway, an aggregating GW may be helpful in case of sensor networks with very large number of devices because it reduces the number of MQTT connections that the server has to support concurrently.

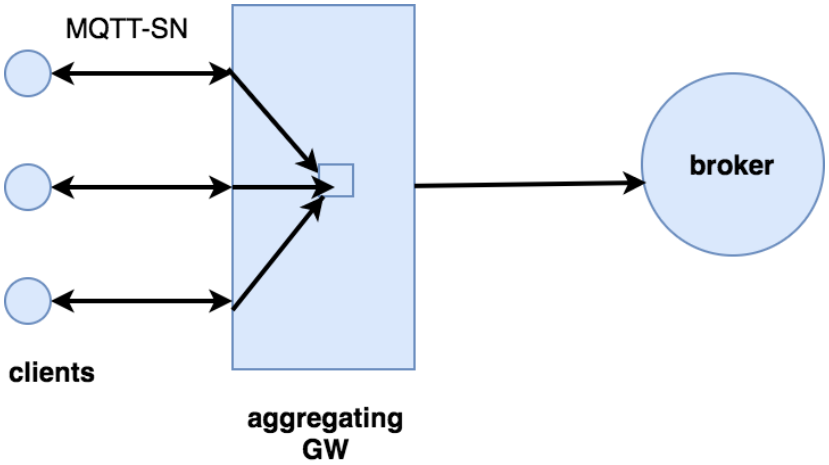


Figure 12: Aggregation Gateway

There are different open source implementations of MQTT-SN [31]

4.4. OMA LWM2M

4.4.1. Introduction

Lightweight M2M defines the application layer communication protocol between a LWM2M Server and a LWM2M Client, which is located in a LWM2M Device. The OMA Lightweight M2M enabler includes device management and service enablement for LWM2M Devices. The target LWM2M Devices for this technology are mainly resource constrained devices. Therefore, LWM2M makes use of a light and compact protocol as well as an efficient resource data model. As a result, it is frequently used with the Constrained Application Protocol (CoAP).

4.4.2. COAP

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things. The protocol is designed for machine-to-machine (M2M) applications such as smart energy, building automation [17] or smart farming. CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with Hypertext Transfer Protocol HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments [18]. CoAP can run over IPv4 or IPv6. However, it is recommended that the message fit within a single IP packet and User Datagram Protocol (UDP) payload to avoid fragmentation. For IPv6, with the default Maximum Transmission Unit (MTU) size being 1280 bytes and allowing for no fragmentation across nodes, the maximum CoAP message size could be up to 1152 bytes, including 1024 bytes for the payload.

As illustrated in the below figure, communications across an IoT infrastructure can take various paths. Connections can be between devices located on the same or different constrained networks or between devices and generic Internet or cloud servers, all operating over IP.

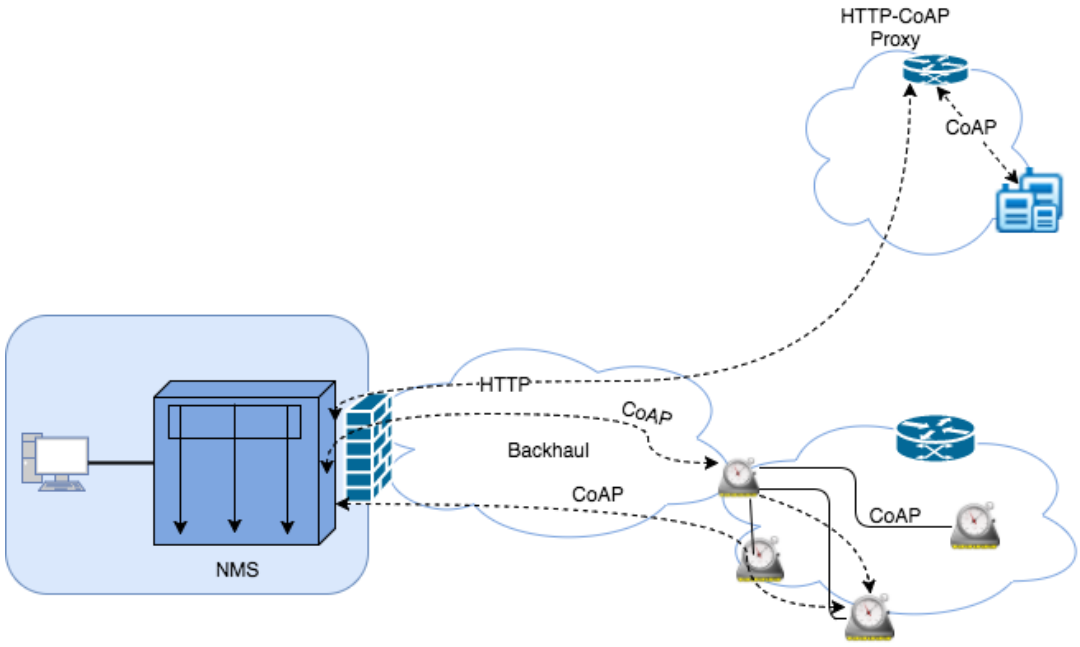


Figure 13: CoAP Communication in IoT Infrastructure

Just like HTTP, CoAP is based on the Representational State Transfer (REST) architecture, but with a “thing” acting as both the client and the server. Through the exchange of asynchronous messages, a client requests an action via a method code on a server resource. A uniform resource identifier (URI) localized on the server identifies this resource. The server responds with a response code that may include a resource representation. The CoAP request/response semantics include the methods GET, POST, PUT, and DELETE.

An Example would be:

coap-URI = "coap:" "//" host [":" port] path-abempty ["?" query]

In this CoAP URI format we can notice that “coap” is a URI Schema similar to “http” or “https”. A CoAp URI identifies a resource, including host information and UDP port, as indicated by the host and port parameters in the URI [19]

4.4.3. OMA LWM2M

OMA Lightweight M2M is designed to:

- Provide Device Management functionality over sensor or cellular networks
- Transfer service data from the network to devices
- Extend to meet the requirements of most any application [20]

The need for device management is an intrinsic part of the IoT, millions of devices need to be configured, provisioned, monitored, maintained, updated and repaired ideally from a remote location [21] . The

solution for this is the standardized OMA LWM2M protocol that can be used for remote management of M2M devices. The architecture of the protocol is client-server, the client software on the M2M device establishing a connection with the server software.

The main features of the protocol are the following:

- has a modern architectural design based on REST
- is highly extensible (defined resource and data model)
- is designed considering high memory and computation constraints of M2M devices
- reuses and builds on an efficient secure data transfer (CoAP).

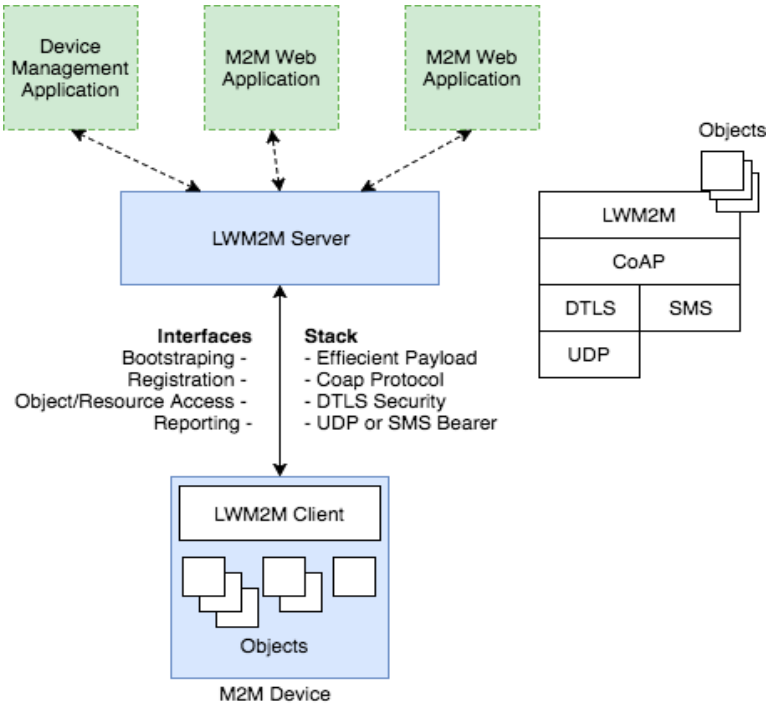


Figure 14: LWM2M architecture [22]

The OMA Lightweight M2M Enabler, consisting of a LWM2M Client (M2M device) and a LWM2M Server (M2M service/platform/application), employs a client-server architecture plus CoAP with UDP/SMS transport bindings as shown in the above figure. The enabler is targeted, in particular, at constrained devices, e.g. devices with low-power microcontrollers and small amounts of Flash and RAM over networks requiring efficient bandwidth usage. At the same time, LWM2M can also be utilized with more powerful embedded devices that benefit from efficient communication.

The LWM2M Server is typically located in a private or public data center and can be hosted by the M2M Service Provider, Network Service Provider or Application Service Provider. The LWM2M Client resides on the device and is typically integrated as a software library or a built-in function of a module or device.

Following four logical interfaces are defined between the server and client:

1. Bootstrap: allows LWM2M Bootstrap Server to manage the keying, access control and configuration of a device to enroll with a LWM2M Server.
2. Device Discovery and Registration: allows an LWM2M Client device let the LWM2M Server know its existence and register its capability.
3. Device Management and Service Enablement: allows the LWM2M Server to perform device management and M2M service enablement by sending operations to the Client and to get corresponding responses from the LWM2M Client.
4. Information Reporting: allows the LWM2M Client to report resource information to the LWM2M Server; can be triggered periodically or by events.

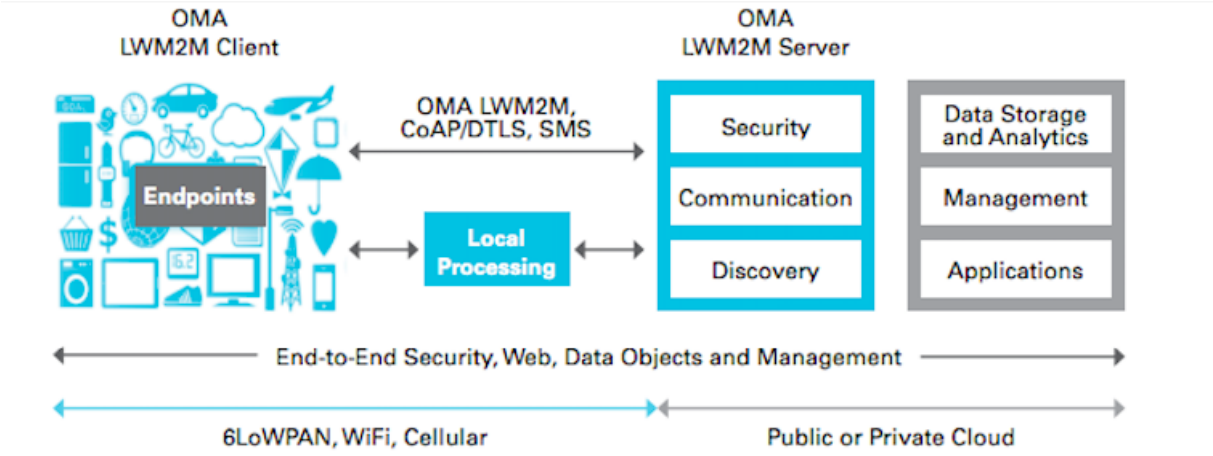


Figure 15: Deployment Scenario [23]

The LWM2M communication model is based on simple COAP methods we mentioned in the previous section such as GET, PUT, POST, and DELETE with bindings over UDP or SMS as transport layer. The binary encoded message overheads will only be a few bytes and the flat, simple objects with uniform URI across devices makes the protocol best suited for constrained device connectivity and easy management. The LWM2M Enabler defines a simple resource model where each piece of information made available by the LWM2M Client is a Resource. The Resources are further logically organized into Objects. The LWM2M Client can have any number of Resources, each of which belongs to an Object. For example, the Firmware Object contains all the Resources used for firmware update purposes [24].

4.5. ONEM2M

OneM2M [9] is the global partnership project formed by worldwide standard development organizations (i.e. ATIS, TIA9, ETSI, TSDSI, CCSA, TTA, TTC and ARIB) to bring a horizontal IoT/M2M middleware platform. The horizontal platform provides common services functions of different vertical service

domains so that developers can focus on application logics since oneM2M provides abstracted and common APIs. A oneM2M based IoT system can be consisted of both non-oneM2M devices and oneM2M devices together.

oneM2M layered architecture model consists of three layers and each layer has associated logical entities:

- **Application Entity (AE)** is an entity in the application layer that implements an M2M application service logic. Each application service logic can be resident in a number of M2M nodes and/or more than once on a single M2M node. Each execution instance of an application service logic is termed an "Application Entity" (AE) and is identified with a unique AE-ID. Examples of the AEs include an instance of a fleet tracking application, a soil moisture monitoring application, a power metering application, etc.
- A **Common Services Entity (CSE)** represents an instantiation of a set of "Common Service Functions" of the M2M environments. Such service functions are exposed to other entities through the Mca and Mcc reference points. Reference point Mcn is used for accessing underlying Network Service Entities. Each Common Service Entity is identified with a unique CSE-ID.
- Underlying **Network Services Entity (NSE):** A Network Services Entity provides services from the underlying network to the CSEs. Examples of such services include device management, location services and device triggering. No particular organization of the NSEs is assumed.

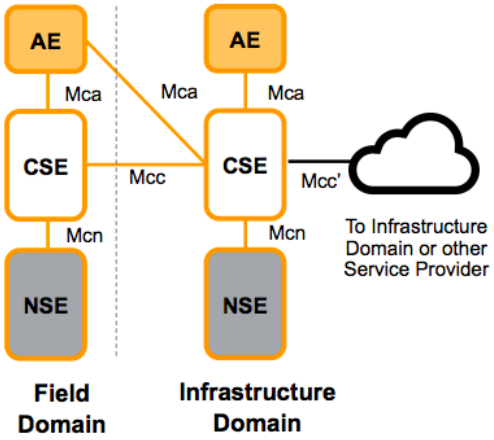


Figure 16: oneM2M architecture overview

Services provided by the Common Services Layer in the M2M/IoT System reside within a CSE and are referred to as Common Services Functions (CSFs). The CSFs provide services to the AEs via the Mca reference point and to other CSEs via the Mcc reference point. CSEs interact with the NSE via the Mcn reference point. An instantiation of a CSE in a Node comprises a subset of the CSFs.

oneM2M Infrastructure Node (IN) communicates with the other oneM2M nodes (i.e. MN, ASN and ADN) in the field domain using the APIs provided by CSFs over Mcc and Mca reference points. oneM2M protocols are bound to CoAP, HTTP, MQTT and WebSocket for protocols (TS-0008, TS-0009, TS-0010 and TS-0020, respectively). The other IoT/M2M systems such as LwM2M, AllJoyn, OCF are interworked with oneM2M system as defined in the corresponding interworking specifications (TS-0014, TS-0021 and TS-0024, respectively). oneM2M also provides generic interworking for legacy protocols (e.g. ZigBee) in M2M Area Network using Interworking Proxy Entity (IPE) (TS-0030).

It is up to application to use relevant functionalities of the platform such as storing/sharing data (e.g. *container* and *content Instance* resource type), announcement and group management. As common services, CSFs includes Data Management and Repository (DMR). Device Management (DMG), Discovery (DIS), and Group Management (GMG).

oneM2M REST APIs over Mca reference points are northbound from oneM2M platform (i.e. Common Services Entity) to applications (i.e. Application Entity). Once the AE is successfully registered (i.e. AE registration), by access control mechanism, it can get access to data and functionalities that platform provides.

oneM2M defines its Base Ontology which can be extended for domain specific ontologies. This can be used for legacy device interworking in area networks to represent their services and functionalities. Not only for legacy devices but also for oneM2M native devices, resource types that contains IoT/M2M data (e.g. *container* resource type) can have semantic annotation (i.e. *semantic Descriptor* resource type) while referring an ontology which can be external.

As well as the commercial implementations (e.g. InterDigital, HPE, ntels), some of oneM2M members manage their own open source implementations:

- KETI leads the OCEAN which provides the different oneM2M node type implementations based on Spring and Node.js frameworks. [44]
- LAAS-CNRS leads the OM2M open source projects in eclipse based on OSGi framework. [45]
- Cisco leads the IoTDM project which provides open source for SDN environment. [46]

4.6. GAPS AND ADOPTION BARRIERS

The main adoption barrier in the IoT Service Layer is the absence of a single standard technology. In fact, different SDOs are promoting different technology stacks. OASIS endorses MQTT. IETF is working with CoAP whereas ETSI is betting on oneM2M. Each technology stack is based on different message exchange paradigms (request/response, publish/subscribe), different protocols (CoAP, plain TCP/IP) and data encoding formats.

In practice it means that IoF2020 use case implementers will have different technological options when it comes to implement their solutions. Furthermore, device manufacturers for the Agrifood domain have to choose which IoT service protocol to use for their devices. In addition, there is no standardization in the format of messages or in the data types or units used by devices. For instance, if an IOF2020 use case is monitoring weather conditions using a device or station provided by one manufacturer, if the station is substituted by another one supplied by a different manufacturer, then it is very likely that the application code would have to be changed to adapt to a new format, protocol or measurement units.

It would be highly desirable to have a unified service layer for IoT, harmonizing interfaces, message exchange protocols or data types. oneM2M was born precisely to provide a complete technology stack (encompassing other existing) to unify the architecture and technologies (through interworking) of the IoT Service Layer. However, despite the amount of resources employed, and the thorough technical specifications produced, its adoption and traction is still low. The main challenge for oneM2M has been to convince the developers community about its advantages. And for doing so, in our opinion, oneM2M would need to be simplified and democratized, evolving from a classical telco standard to a more IT-oriented technology stack, which can get the attention from the IoT start-up community.

In the meantime, other SDOs have started working on alternative approaches to a unified IoT Service Layer. In our opinion, one of the most promising is the Web of Things (WoT) initiative, aimed at exposing IoT devices as Web resources, regardless IoT protocols, leveraging the possibilities offered by Open Linked Data. To this aim, WoT defines a discoverable Thing Descriptor (encoded using JSON-LD) which includes key metadata to interact with a device. Such metadata shall be provided by device manufacturers, and IoT solutions could, in principle, automatically adapt to new devices, provided there is runtime support. Nonetheless, WoT has not released any final specification yet, although there are some working prototypes demonstrating the feasibility of the approach.

4.7. LINK TO USE CASES AND TRIALS

As it has been stated before, there is no a dominating technology in the IoT Service Layer. In practice this means that the IoT Service Layer in IoF2020 use cases would depend on the specific technologies offered by the device manufacturers for each use case. As a consequence, the best strategy to be followed is to provide generic IoT components ready to be used by the different use cases, depending on their needs and in accordance with the devices chosen for implementations. In practice it means the, for the time being, the best solution to the heterogeneity in the IoT Service Layer is to delegate to a Mediation Layer that adapts to multiple protocols and data representations.

There are different IoT libraries and components that can fit the bill of a mediation layer between the IoT Service Layer and upper layers (the Information Management layer). One example of a useful suite is the FIWARE IoT Agent suite which allows to connect devices using different IoT protocols (MQTT, LWM2M, etc.) to the Context Information Management layer of FIWARE. As a result, data from devices

provided by different manufacturers could be exposed using a harmonized API (NGSI-LD) and data models, overcoming the IoT Service Layer issues.

Last but not least, we recommend that under the IoF2020 project, the Web of Things technology is explored as a way to improve interoperability at the IoT Service layer. A liaison between one or more use cases, a device manufacturer and the WP3 team could be desirable, so that to materialize an initial proof of concept that applies WoT technologies to the Agrifood sector.

5. AGRICULTURAL MACHINERY COMMS LAYER

5.1. INTRODUCTION

This chapter outlines the Agricultural Equipment Industry and its communication standards that are very commonly used in the industry to achieve compatibility between different brands of equipment and software systems. This layer sits in between the agricultural machinery (tractors, implements, etc.) and the Mediation Layer and allows to publish relevant data generated from machinery to the cloud. The concerned interoperability point is IOP 1.1.

The Agricultural Industry has a long history of collaboration in standards for electronics and data exchange between machines (e.g. tractor – implement) and between machine and software systems, such as Farm Management Information Systems (FMIS). In particular the developed standard **ISO-11783** (also commonly known as ISOBUS, including its *ISO-XML Data exchange interface*) is the de-facto standard for decades, now between tractors and has been implemented by different manufacturers.

5.2. ISOBUS

The ISOBUS standard (ISO-11783) governs electronics and data exchange between different farm machines (e.g. tractor – farm implement).

The figure below shows a typical ISOBUS system as it is sold into the worldwide markets today. A local communication bus-system based on CAN bus connects the Tractor and the Implement and various components such as a Terminal or an auxiliary joystick. In addition, external interfaces are added for M2M communications to Farm Management Systems and/or Manufacturer Cloud Portals.

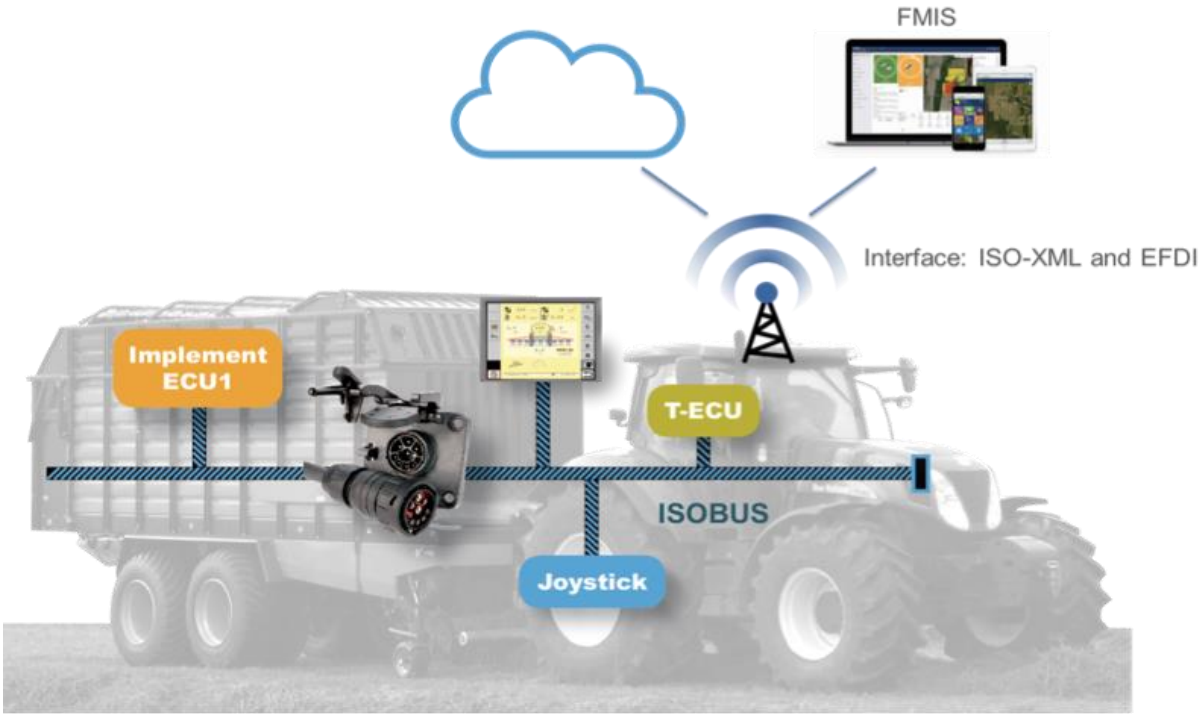
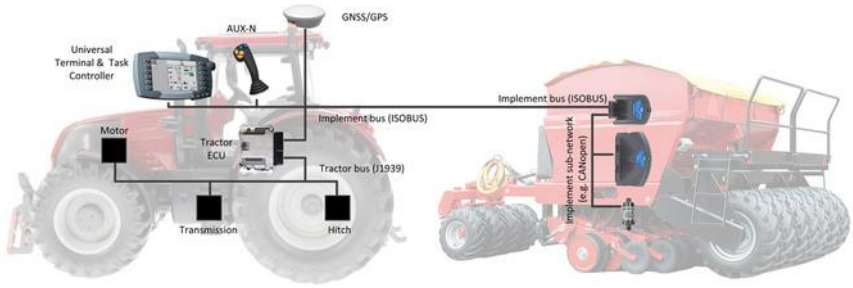


Figure 17: Typical ISOBUS System where the tractor ECU is the tractor's "job calculator". This provides information, such as speed, power take-off RPM, etc.



5.3. DATA INTERCHANGE

Data Management interfaces facilitate the exchange of data with the mobile equipment in the field. Through this functionality the user gets his data into a management system for registration purposes and further future planning. Newly planned data can be generated by such systems (e.g. decision support management systems) and taken back into the farming equipment for planned field tasks and operations through, for example, a wireless service or Telematics portal of the manufacturer.

The data exchange standards between mobile farm equipment and farm management systems (or data management systems) are standardized in ISO-11783, Parts 10 & 11. AEF is working on guidelines

which define clear interfaces by using ISO-XML and the new extended FMIS data interface referred as “EFDI”.

Part 10 of ISO-11783 describes the XML file format with about 60 potential elements for content like, client, farm, part field, polygon, worker or device. This file format enables a FMIS to send an order to a mobile information control system (MICS), a task controller can understand the job and can command a device. While the job is running, a task controller can log all the activities and can send back a finished task to the FMIS with all totals and information. All the required values in this process (e.g. fertilizer in mass per area, yield, fuel…) are standardized in Part 11 of ISO-11783, currently about 525 public entries.

5.4. DATA PROCESS FLOW

The data transport process has changed over the last few years. To have a USB stick with data at the end of the day is no longer adequate because of:

1. Machines are working for long periods in the fields and no longer returning to the farm at the end of the day. No data would be available to check tasks and values in between in this case.
2. Sometimes it is necessary to send new orders to the working machines in the field: Consequence: Not possible.
3. In addition, the farmers need the current field and machine status which is also not possible currently.

In all these examples, and there are more, the task data file set via USB stick is no longer useful in the near future. In addition the complexity of the data and workload has to be taken into account: several machines with different drivers that do not have the whole overview on all available data are doing different tasks, so directly wireless communication between machines and FMIS will prevent a great deal of manual and error prone labor. Therefore, communications between devices directly wireless to a server or a cloud system in real time is necessary and has to be standardized.

With this understanding of the current needs in the market, the AEF started the development of a new data transmission system, called Extended FMIS Data Interface (EFDI). The AEF is working on a new standard which can send a fragment of the log file every second or a whole task set of the day as well, without any data media.

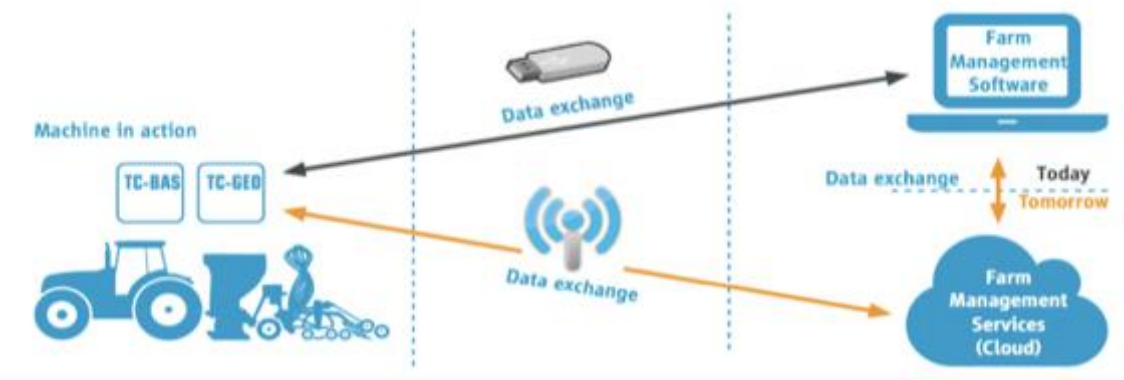


Figure 18: Data exchange between machines and Software/Services

5.5. STANDARDIZATION OUTLOOK

AEF has also joined forces with AgGateway to define the protocols and data elements for data exchange, making it future-proof and adapting it to the needs of Digital Farming. Apart from the fact that both AEF and AgGateway are active in developing sector specific standards and guidelines, the value of collaboration lies in pooling different areas of expertise and knowledge. This allows both to cover the entire landscape of Digital Farming.

The figure below shows an outline of the many different interfaces that currently exists, all the way from the Agricultural Equipment, through Telematics portals, Farm Management Systems to Service Providers (SP in the figure) and Suppliers / Traders.

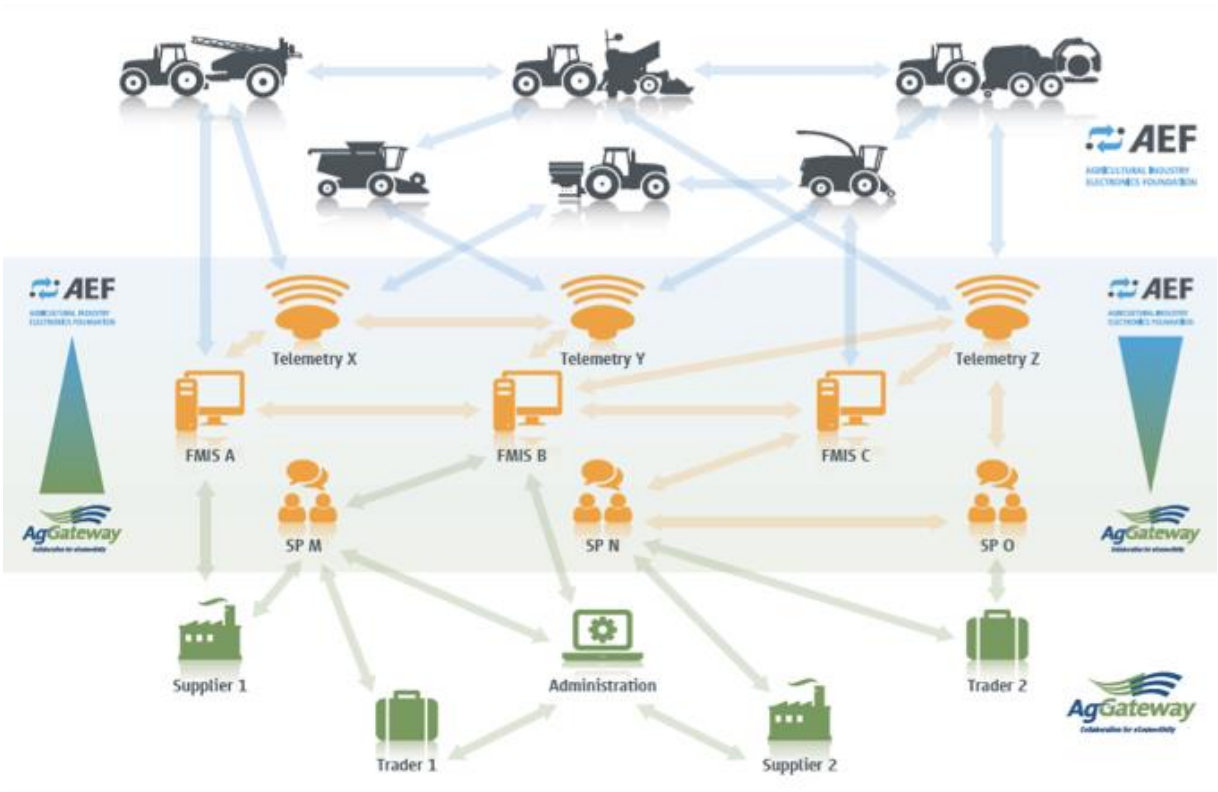


Figure 19: AEF and AgGateway scope and collaboration areas

5.5.1. AgGateway

Besides the exchange of agricultural specific data concerning field and crop operations, there also is a need for standardizing more transaction related data exchange with other actors in the supply chain. AgGateway is the recognized international organization that uses the concept of industry collaboration to expand the use of e-Business standards and guidelines globally and as such enabling the use of information and communication systems.

AgGateway Global Network carefully considers regional operating practices, to be in balance with opportunities for standardization. The intent is to share “what has worked” in various regions of the world, to promote global e-business, and to collaborate on necessary standards where specific needs exist. So AgGateway brings together agricultural companies to agree on what standards for a specific area should be leading. If there is not yet a standard available for exchanging specific data, AgGateway takes the initiative to develop, in cooperation with existing standardization boards, these missing standards. Using AgGateway standards globally reduces the chance that conflicting standards will be developed and implemented in other regions. In locations where conflicting e-Business standards already exist, this plan will provide a good opportunity to resolve those differences in a collaborative effort.

For standardized data exchange of order, invoice, and dispatch data the UN/CEFACT, GS1 or UBL standards are leading. For exchanging e.g. laboratory analysis results and crop related data for compliance purposes, new standard UN/CEFACT messages are developed over the recent years. For data exchange, the unique identification of farmers, crop fields, inputs, etc. is very important. GS1 provides a set of worldwide implemented standards for unique identification: Global Location number (GLN), Global Trade Item Number (GTIN), Global Product Classification (GPC).

5.5.2. The Role of ISO

It is clear that The International Organization for Standards (ISO) is the one and only worldwide standards organization responsible for drafting and publishing the final ISO standards. AEF as such is not writing ISO standards, but creates Implementation Guidelines and supporting products to facilitate the implementation of International Standards for its members, such as the Implementation Guidelines, or the AEF Conformance Test or the AEF ISOBUS database.

The AEF addresses new technical areas and prepares guidelines through new Project Teams, from which work these guidelines can eventually go into the ISO standardization process. As an example; When the FMIS project team has finalized and released the EFDI guideline within AEF, this document will then also form the basis of the start of a New Work Item Proposal (NWIP) in the ISO Working Groups. EFDI may then become another standard besides ISO-11783 or will be added as a new part to ISO-11783 (currently there are 14 parts).

5.6. GAPS AND ADOPTION BARRIERS

Initially, the main focus of the AEF was the implementation and further development of the ISOBUS standard (ISO-11783) which governs electronics and data exchange between different farm machines (e.g. tractor – farm implement). With the digital revolution in farming unfolding, the AEF's scope of work is no longer limited to ISOBUS only, but has been expanded to cover additional areas of critical importance for Digital Farming such as: Farm Management Information Systems (FMIS), Wireless in-field communication, High-Speed ISOBUS, Electric drives, and Camera systems. This chapter has provided a short overview of the possibilities for data exchange with the different interfaces and describes the activities of AEF and AgGateway. In conclusion, it has been shown what has to be done to fulfil customer needs and how to manage the EU expectations.

Implementation of complex electronic standards, such as for example ISO-11783, may lead to different interpretations and thus different implementations by manufacturers of agricultural equipment. In the field this may for example result in incompatible tractor and implement combinations for the farmer or contractor, thus leading to a lot of frustration. These problems can be very broad; e.g an implement not communicating properly with a tractor terminal, but it can also be at the level of data exchange for the tractor-implement combination to external Farm Management systems.

In the past decades, uncoordinated introduction in the field of such standards has proven to be problematic and undesirable, and therefore the Agricultural Industry recognized the need to cooperate in a new worldwide organization. This resulted in the founding of the Agricultural Industry Electronics Foundation (AEF) organization, and actions taken by the industry to get a coordinated introduction of new standards and functionalities into the field with focus on existing standards, but also future focus for new upcoming technologies and standards.

Over the last few years AEF has also teamed up with the AgGateway organization to collaborate further on the Data Exchange standards.

It is crucial that the set of data exchange principles is standardized throughout the Ag Industry, in other words the industry has to go for just one type of interface protocol between its machines and the telematics service, and from the telematics service to External API's through a set of standardized cloud-cloud interfaces with clear and standardized data structures.

In the cases where interfaces to the outside world are needed, AEF has teamed up and established cooperation with other International Bodies and Standards Organizations, such as ISO, AgGateway and ETSI. Also identifying existing standards and technologies that can be reused and applied for the Ag Industry are important for AEF.

5.7. LINK TO USE CASES AND TRIALS

Obviously, there is a direct relationship between the Arable Trial and the technology described in the present chapter. Particularly with those use cases, such as 1.4, which involve monitoring agricultural machinery in the field and integration with FMIS. The recommendation, from WP3, is to collaborate with AEF and AgGateway, so that the latest technology developments, namely EFDI, are used when developing those use cases (at least in a proof of concept basis). The results obtained from the IoF2020 use cases could serve as a very valuable input to the further standardization processes conducted. Collaboration with formal standards bodies like ETSI is also recommended, particularly in the framework of Specialist Task Forces.

6. MEDIATION AND INFORMATION MANAGEMENT LAYER

6.1. INTRODUCTION

The final aim of the *Mediation and the Information Management* Layers is to offer the right information to the right application at the right time. In other words, they are in charge of transforming raw data into information relevant and ready to be consumed by applications, so that smart behaviors are exhibited, enabling the optimization of Agrifood processes. It is noteworthy that the data involved at this stage could not only come from IoT but also from other different data sources (open databases, linked data, existing systems, public Geo-Services, etc.).

On one hand, the *Mediation Layer*, situated in between the IoT Service Layer and the Information Management Layer (IOP 2), is responsible for gathering the raw data coming from devices or other external services, and curate, harmonize and possibly aggregate it, so that it can be published as context information, or supplied to upstream data processing algorithms or analytics. In addition, this layer is also capable of sending actuation commands to the IoT Service Layer. In other words, one of the main functions of the Mediation Layer is to hide the complexity and diversity of the IoT Service Layer. In addition, the Mediation Layer may also be capable of gathering data from other data sources such as agricultural machinery (see chapter 5, IOP 1.1) or public geo-services (IOP 4).

On the other hand, the *Information Management Layer*, situated in between the Mediation Layer and the Application Layer, serves mainly as a data hub (usually incarnated by a context broker) which enables the publication, consumption and subscription of all the information relevant to an application. Such information it is modelled in terms of Entities, Entity Types, Properties and Relationships (see below). As it was said before, the information present at this layer, which can be current or historical, may have been aggregated from different sources, not only IoT.

In addition, this layer may offer complex event processing, storage or analytics services, which can generate insights, prescriptions or predictions, offered later to applications as additional information. However, this document does not cover formal or de-facto standard technologies covering the referred functionalities.

The main technology enabler for the referred layers is FIWARE NGSI and its linked data extension, named, NGSI-LD, recently published by ETSI as an ISG Group Specification. Such standard is composed by a Context Information Management API and an accompanying Core Meta-model, which prescribes how to represent information. Some of the following sections of this document are devoted to describe it.

Other technology enablers related to this layer are OGC Geo-Services, namely WMS and WFS (see IOP 4). They are technologies that allow to offer geospatial data by means of standardized interfaces. They are of importance, as many public administrations in Europe offer Agrifood-related data using them. For instance, in Spain the SIGPAC [57] system offers information about agricultural parcels through WMS and WFS. There are also satellite agencies that offer their data using these standards. It is noteworthy that Context Information could be mashed-up with geo-spatial information, for the benefit of applications, which can harness all the potential of IoT-generated data with public data of high quality. In fact, some of the formats endorsed by NGSI are also used by the OGC standards, namely GeoJSON [58].

6.2. FIWARE NGSI

6.2.1. Introduction

Before introducing the Context information management theme, it is necessary to explain the notion of what the Context of an entity is. The Context of an entity consists of:

- a set of characteristics that describe it, including its (dynamic) state
- other entities with which it has defined relationships, and the nature of those relationships.

A shift in context corresponds to a change in one or more of the aforementioned enumerated aspects.

Context Information can be defined as the informational representation of a context as defined above. A property can be defined as a description instance which associates a value, to either an entity, a relationship or another property. For instance, “speed”, “soilTemperature”, “windDirection”. A relationship describes the conceptual connection from one entity to another entity, in a context, for example, "adjacent to", "owned by", "created by".

Context information management (CIM) can be referred to a platform or system (usually named Context Broker) which provides the following services: *context information registry, discovery, publication, mediation, modification or notification*. Cross-cutting context information management provides CIM between independent target domains (yet obviously can also handle same or similar domains).

A CIM system collects information from user-driven applications, platforms managing end-devices and other sources and provides it to applications via a CIM API. The CIM system enables use-cases which link together disparate but related information. It is thought that IoT services will be enriched when applications have access to a full set of context information. A CIM system potentially enriches services by bringing together information from a wider set of service-relevant sources than would otherwise be available.

In the Smart Agrifood domain Context information can be composed by the state of entities such as tractors, parcels, greenhouses, drones, etc. See figure below. In addition, other Context information might be relevant, for instance weather forecasts, pests or diseases historical information, etc. However, the latter can be offered by specialized services or databases.

The Context / Data Broker middleware offers application interfaces for CIM so that, a real time view of what is happening can be obtained. The sections below describe what standard application interfaces are available for CIM and related implementations.

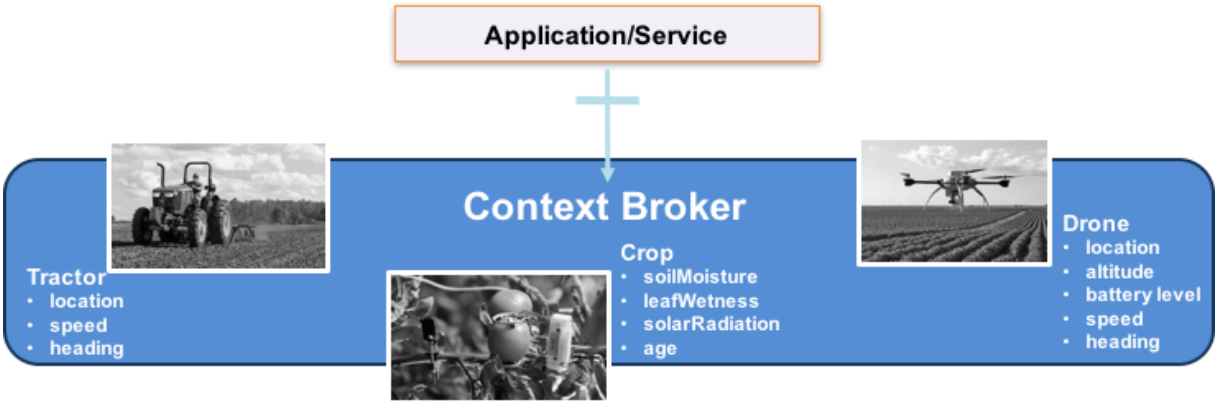


Figure 20: Context Information Management in the Agri Domain. De facto standards: FIWARE NGSI

FIWARE NGSI is an instantiation (binding) of the OMA NGSI-9 and NGSI-10 [32] abstract interfaces for Context Information Management. The version of 2 of the FIWARE binding (*FIWARE NGSIv2*) is based on HTTP/REST and JavaScript Object Notation (JSON), following the usual, de-facto industry standards. Such API binding for CIM has been recommended by the GSMA for IoT and Big Data Projects [33].

NGSI supports a powerful, yet simple, well-known approach to represent Context information, with a meta-model based on entities, attributes and extra attribute's metadata (see figure below). Attributes can represent the properties of an entity or can point to (using a priori defined conventions) other entities. Experience demonstrates that instantiations of this meta-model can be easily mapped / implemented using a wide variety of data stores including NoSQL, SQL or even Graph Databases. Furthermore, the NGSI information meta-model is quite close to other meta-models widely used in the industry, namely schema.org, thus enabling interoperability and reusability.

6.2.2. The NGSI meta-model

The figure below represents the NGSI meta-model.

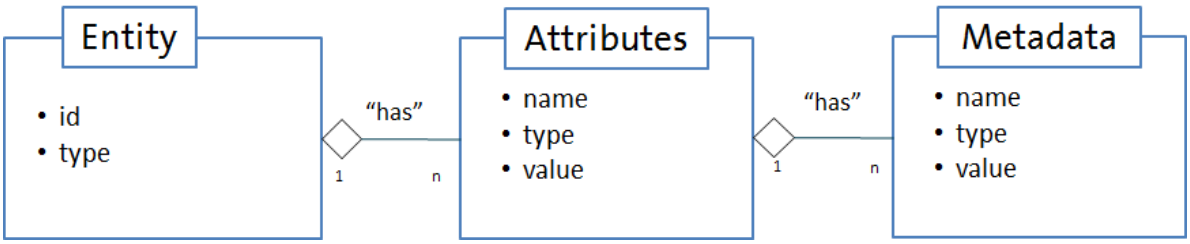


Figure 21: The NGSI meta-model

Entities are the center of gravity in the NGSI information model. Each Entity has an Entity Id. The type system of NGSI enables entities to have an Entity Type. Entity Types are semantic types; they are intended to describe the type of thing represented by the entity. For example, a context entity with id "tractor-365" could have the type "Tractor". Each entity is uniquely identified by the combination of its id and type. It is noteworthy that these elements are always mandatory when the meta-model is instantiated.

Attributes are properties of context entities. For example, the current speed of a tractor could be modelled as attribute "speed" of entity "tractor-104". In the NGSI data model, attributes have an attribute name, an attribute type, an attribute value and metadata. The attribute name describes what kind of property the attribute value represents of the entity, for example "speed". The attribute type represents the NGSI value type of the attribute value, which is usually similar or equivalent to the JSON data type. The attribute value, finally, contains the actual data and optional metadata describing properties of the attribute value like e.g. accuracy, provider, or an observation timestamp.

Metadata is used as an optional part of the attribute value as described above. Similar to attributes, each piece of metadata has a metadata name, describing the role of the metadata in the place where it occurs; for example, the metadata name "accuracy" indicates that the metadata value describes how accurate a given attribute value is; a metadata type, describing the NGSI value type of the metadata value; a metadata value containing the actual metadata.

6.2.3. The JSON Representation of NGSI

Instantiations of the NGSI information meta-model can be encoded using simple JSON structures (key-value structures), so that application developers or other parties can consume data easily. At https://gist.github.com/GSMADeveloper/c02633ceaab7f18afd489b559d2ab0f4 there is an example of encoding an entity of type "AgriCrop" as per the GSMA IoT Big Data Harmonised Data Model [1] As the NGSI information model does not support natively the concept of relationships, they are conveyed using a special name pattern for attributes (ref<related Entity Type>). For instance, the "refAgriFertilizer" attribute refers to the fertilizers (which are also entities of type "AgriFertilizer") suitable for such "AgriCrop".

As JSON is used, definitions of information models to be used with NGSI can benefit from the usage of JSON Schema [43]. JSON Schema is a JSON media type for defining the structure of JSON data. JSON Schema is intended to define validation, documentation, hyperlink navigation, and interaction control of JSON data. Another advantage of adopting JSON-Schema is that other tools, such as Swagger (https://swagger.io/), will be enabled, allowing developers to create specific REST APIs on top of the existing NGSI APIs.

The geospatial properties of an entity can be represented by means of regular attributes. The provision of geospatial properties enables the resolution of geographical queries. The format adopted by FIWARE NGSI is GeoJSON. GeoJSON is a geospatial data interchange format based on JSON. GeoJSON provides greater flexibility allowing the representation of point altitudes or even more complex geospatial shapes, for instance multi geometries.

6.2.4. FIWARE NGSIv2 API Overview

The FIWARE NGISv2 API [40] supports the generic capabilities to allow arbitrary Context information, in terms of 'entities', to be stored within a generalized data repository. Once stored they can be retrieved, updated, deleted and searched (queried). NGSIv2 also supports the ability to create 'subscriptions' whereby a subscribing application can receive updates from the NGSIv2 compliant repository when information is updated relevant to the subscription criteria. Subscriptions can of course be deleted.

In summary, at the highest level the NGSIv2 API supports, through an HTTP-REST interface, the following groups of functional capabilities:

- Context Information Provision: Entity creation, modification (with attribute-level granularity), deletion through standard HTTP methods (POST, PATCH, DELETE).
- Context Information Consumption: Query entity using attribute filtering criteria and geospatial relationships, HTTP GET method.
- Context Information Subscription: Subscription to the changes happening in entities and configuration of the notification messages to be delivered.
- Registration of new sources of Context information (NGSI-9). For instance, external systems or open data sources can be registered as additional sources of Context information, provided that the proper adaptors are available.

A more detailed enumeration of the operations offered by the API is provided below:

- Create an entity including one or more attributes;
- Retrieve entity (/specified attributes) by entity identifier;
- Update one or more attributes of an existing identity;

- Remove an entity;
- Get an attribute value;
- Update an attribute value;
- Remove an attribute of an entity;
- List entities matching specified criteria;
- List known entity types;
- Retrieve entity type information;
- Create a subscription;
- List subscriptions;
- Retrieve details of a subscription;
- Update details of a subscription;
- Delete a subscription;
- Register a new context source (NGSI 9)
- Unregister a context source
- Update details of a context source registration
- Batch update;
- Batch query

6.2.5. FIWARE NGSI Implementations

The most popular implementation of FIWARE NGSI is the Orion Context Broker [40] which uses MongoDB as its underlying data store. The figure below shows an overview of the architecture and functional interfaces supported by this component. It can be deployed using Docker in the most popular platforms.

The Orion Context Broker allows to publish, consume and subscribe to data coming from multiple devices and data sources. In fact, it allows applications to get access to (harmonised) data entities, regardless data sources. The broker may store data in the short to medium term using a data store. The expected use of this is:

- Retention of current instances of harmonized data entities processed from IoT devices and external sources (context data);

- Storage of a window of short term historical harmonized data entities that may be queried directly via a third party application.
- Storage of any results of Analytics and Intelligence results which become additional context data that can be queried or mashed up with other IoT data or external data sources.

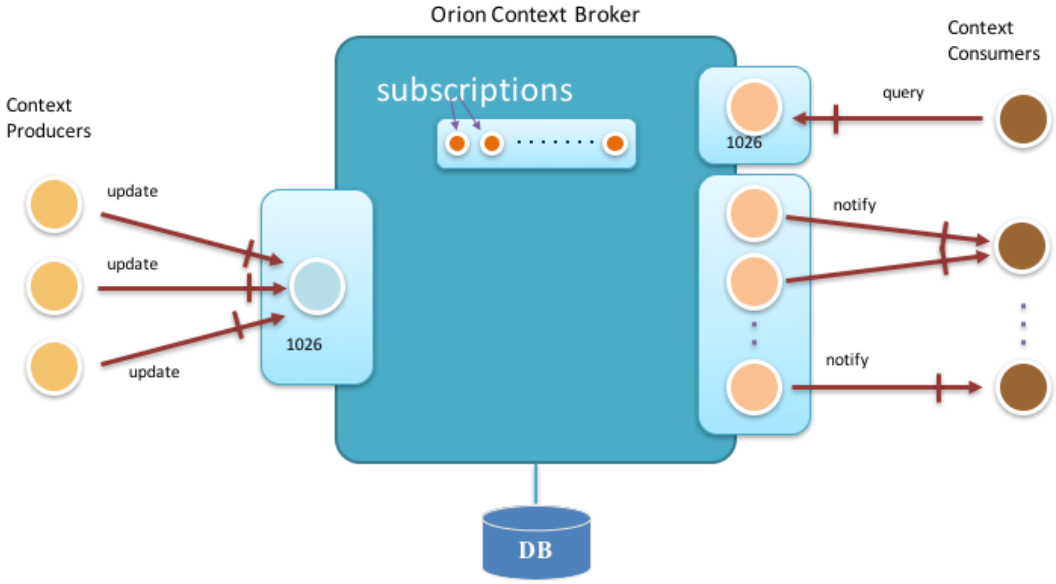


Figure 22: Orion Context Broker architecture and overview

6.3. EMERGING STANDARDS: NGSI-LD

The OMA NGSI information model is currently being evolved to better support linked data (entity's relationships), property graphs and semantics (exploiting the capabilities offered by JSON-LD). This work is being conducted under the ETSI ISG CIM initiative [42] and it is going to be branded as NGSI-LD.

It is noteworthy that the ETSI ISG CIM information model is a generalization of the existing OMA NGSI information model. As a result, it is expected a good level of compatibility and a clear migration path between both information models.

Although at the time of writing it is unknown when implementations will start supporting this new information model, it is worth devoting some words to it, so that the IoF2020 stakeholders know the new possibilities offered and have a clearer view of the roadmap.

6.3.1. ETSI ISG CIM Information Model

The figure below shows a UML diagram which describes the ETSI ISG CIM information model. The main constructs are NGSI-LD Entity, NGSI-LD Property and NGSI-LD Relationship. NGSI-LD Entities

(instances) can be the subject of NGSI-LD Properties or NGSI-LD Relationships. In terms of the traditional NGSI data model, NGSI-LD Properties can be seen as the combination of an attribute (property) and its value. NGSI-LD Relationships allow programmers to establish relationships between instances using linked data. In practice, they are an NGSI attribute, but with a special value which happens to be a URI which points to another entity (internally or externally). They are similar to the "ref" attributes already mentioned.

NGSI-LD Properties and NGSI-LD Relationships can be the subject of other NGSI-LD Properties or NGSI-LD Relationships. Thus, in the ETSI ISG CIM information model there are no attribute's metadata but just "properties of properties". It is not expected to have infinite graphs and in practice only one or two levels of property or relationship "chaining" will happen. Usually, there will be one, equivalent to the NGSI metadata abstraction.

NGSI-LD Entities are represented using JSON-LD, a JSON-based serialization format for Linked Data. The main advantage of JSON-LD, apart from the ability of representing linked data, is that it offers the capability of expanding JSON terms to URIs so that vocabularies can define terms unambiguously.

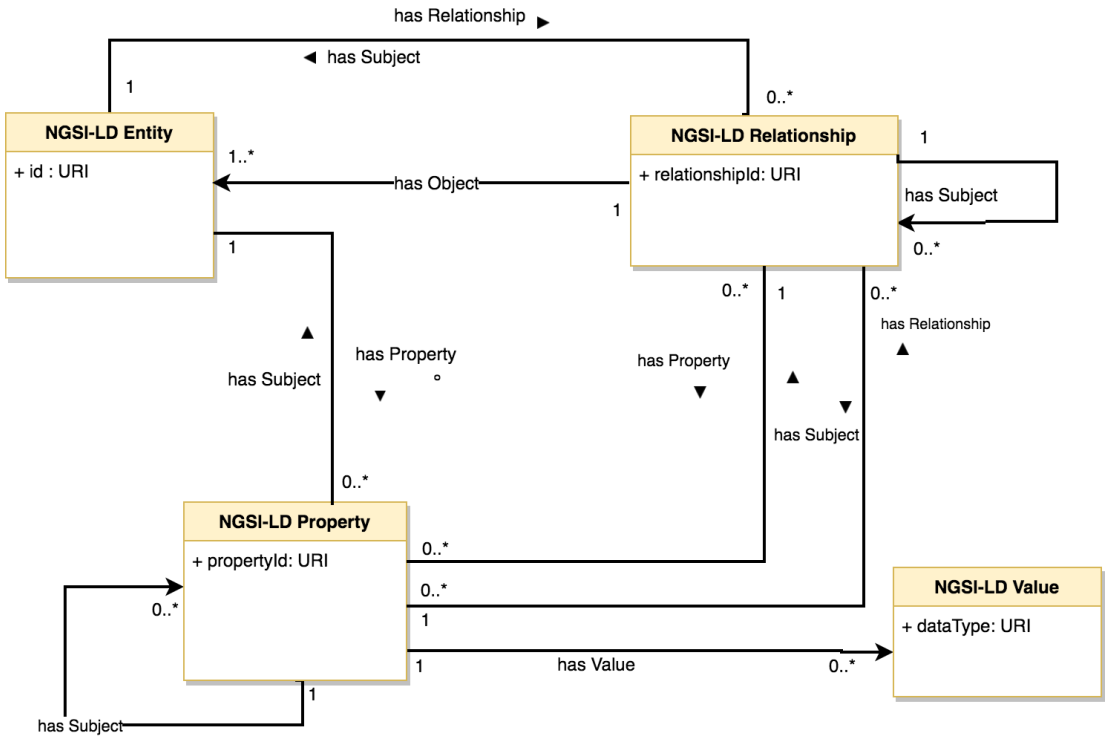


Figure 23: ETSI ISG CIM Information model represented using UML

The following figure shows an instantiation example of this information model. It conveys that there is an instance of an entity of type "Tractor" which current driver is a person (entity type "Person"). The tractor is performing a task in a parcel (entity type "AgriParcel"). Different properties about those entities

are provided (“speed, “brandName”, “temperature”, etc.) and additional properties of properties (for instance, an accuracy level) or properties of relationships (“startedAt”) are described.

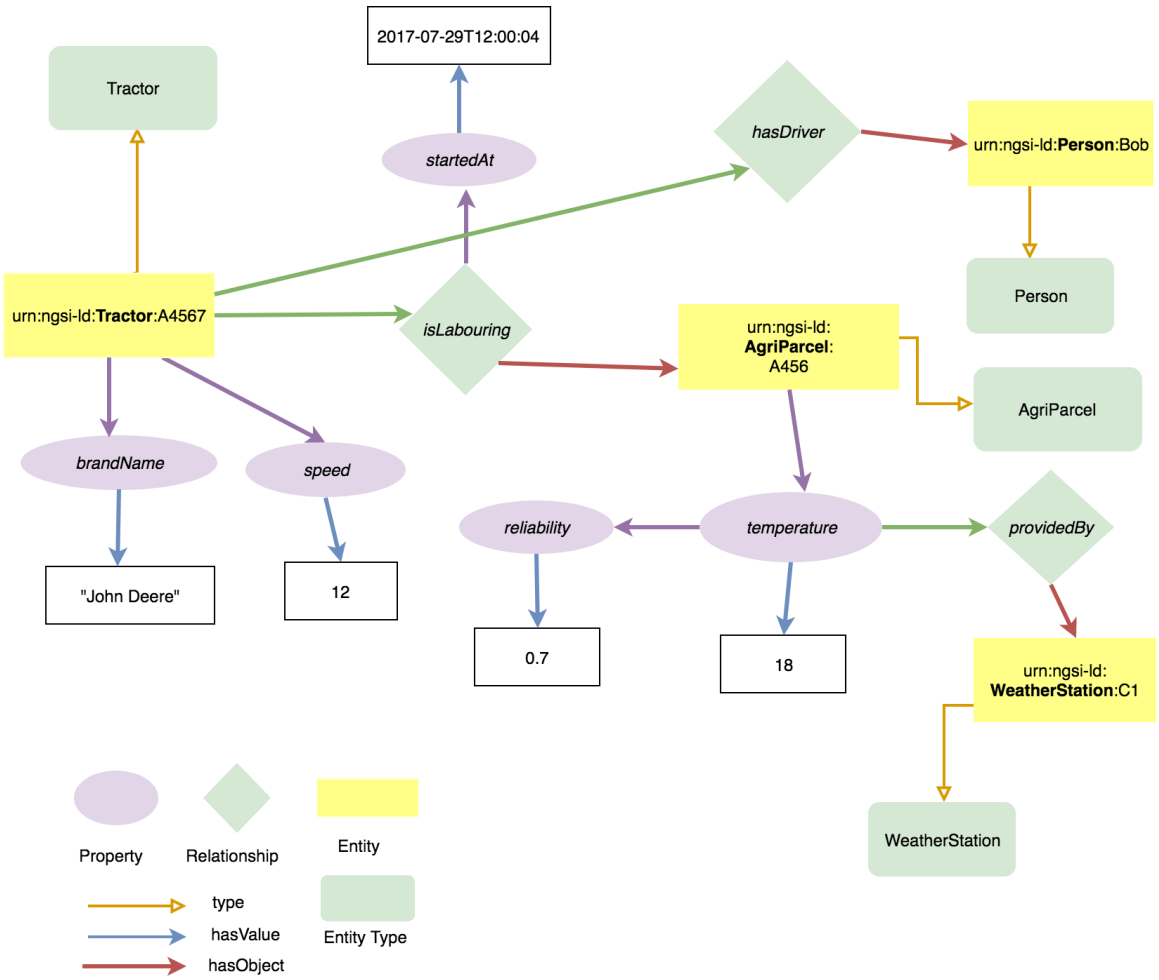


Figure 24: Instantiation Example of the ETSI ISG CIM Information Model

Finally, below there is an example of the JSON-LD serialization corresponding to some of the ‘entities’ represented above. NGSI-LD Entities are represented as JSON-LD objects. JSON-LD objects are regular JSON objects that incorporate a special tagged member (named “@context”), which value provides (or points to) the mapping between terms (short-hand strings) and fully qualified names (URIs), so that every term in the JSON object is unambiguously identified.

```
{
  "id": "urn:ngsi-ld:Tractor:A4567",
  "type": "Tractor",
  "brandName": {
    "type": "Property",
    "value": "John Deere"
```

```
  },
  "isLabouring": {
    "type": "Relationship",
    "object": "urn:ngsi-ld:AgriParcel:A456”,
    “startedAt”: {
      “type”: “Property”,
      “value”: “2017-07-29T12:00:04”,
    }
  },
  “hasDriver”: {
    “type”: “Relationship”,
    “object”: “urn:ngsi-ld:Person:Bob”
  },
  “@context”: “http://example.org/agri/iof2020/context.jsonld”
}

{
  "id": "urn:ngsi-ld:AgriParcel:A456",
  "type": "AgriParcel",
  "temperature": {
    "type": "Property",
    "value": 18,
    "reliability": {
      "type": "Property",
      "value": 0.7
  },
  "providedBy": {
      "type": "Relationship",
      "object": "urn:ngsi-ld:WeatherStation:C1"
  },
  “@context”: “http://example.org/agri/iof2020/context.jsonld”
}
```

6.4. GEOSERVICES – WFS

The Web Feature Service (WFS) is an interface specified by the Open GIS Consortium (OGC) that allows for the exchange of geographic data across the Web. It defines the rules for requesting and retrieving geographic information using the Hyper Text Transmission Protocol (HTTP). The interface describes the data manipulation operations on geographic features. Extensible Markup Language (XML)-based Geographic Markup Language (GML) is used for exchange of information. It should be noted that WFS supports the vector data model.

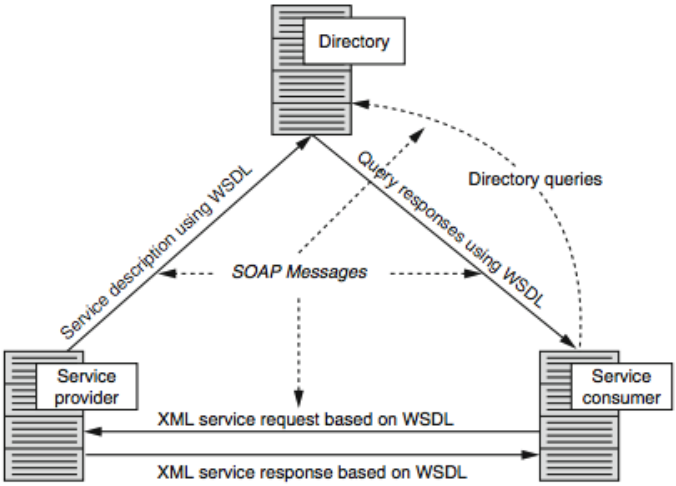


Figure 25: Web service and its service-oriented [37]

WFS provides interfaces for describing data manipulation operations on geographic features. Data manipulation includes creating a new feature instance, deleting a feature instance, updating a feature instance and getting or querying features based on spatial and non-spatial constraint.

The operations that support transaction and query processing are described as follows:

- GetCapabilities
- DescribeFeatureType
- GetFeature
- Transaction
- GetGMLFeature

Types of Web Feature Services: It is not necessary that a Web Feature Service provide support for all the above operations. Accordingly, Web Feature Services can come in three flavors: **Basic WFS, XLink WFS and Transactional WFS** [34]**.**

- Basic WFS : A basic WFS only allows querying and retrieval of features. That is, it supports the GetCapabilities, GetFeatureType and GetFeature type of requests. Since such a kind of web feature service supports reading of data only, it is also known as a 'read-only' server.
- XLink WFS : In addition to supporting all the operations of a basic web service, an XLink WFS also provides the GetGmlObject operation.
- Transaction WFS : A transactional WFS supports all the operations of a basic web server and in addition, it also implements the Transaction operation. A transactional WFS may, optionally, support the GetGmlObject operation as well.

The Geographic Markup Language (GML) is used for encoding the information that passed between a client and a server. Thus, it is required that both the client and the server support and understand GML [34].

There are some important requirements that a server must satisfy before it can claim to be a Web feature server.

- The interfaces must be defined in XML.
- The server must be able to encode the geographic information using the Geographic Markup Language (GML).
- The client should not be required to have knowledge of the data store used to store the geographic features. The client's only view of the data should be through the WFS interface.
- The predicate or filter language must be defined in XML and be derived for the Common Query Language (CQL) as defined in the OpenGIS Catalogue Interface Implementation Specification [34].
- A Web Feature Service must also be able to describe the structure of each feature type defined by it.
- It must be possible for a client to specify which feature properties to fetch and to do so using spatial and non-spatial constraints.

When performing the GetFeature operation on the GeoServer a WFS returns the GML data associated with the features specified in this request. This is the request that is used by a client to get the geodata associated with features supported by the web feature server. WFS returns features and feature information in a number of formats. The syntax for specifying an output format is:

outputFormat=<format>

when we specify the format as "application/json" then it returns a GeoJSON or a JSON output. Here is an example of a simple GeoJSON file:

{**"type"**: "Feature",

```
  "geometry": {
    "type": "Point",
    "coordinates": [125.6, 10.1]
  },
  "properties": {
    "name": "Dinagat Islands"
  }
}
```


6.5. GEOSERVICES – WMS

Web Map Service (WMS) is a specification which outlines communication mechanisms allowing disjoint software products to request and provide preassembled map imagery (“compiled” map images, which may contain both vector and raster data) to a requesting client [35].

Although WFS is closely related to the Web Map Service (WMS), there are significant differences. With WMS, the machine that requests some other machine for information gets a completely rendered map in return for its request. The requesting machine does not get raw data. It gets a readymade map which it merely displays.

WMS specifies a number of different request types, two of which are required by any WMS server:

- GetCapabilities
- GetMap

Request types that WMS providers may optionally support include:

- GetFeatureInfo
- DescribeLayer
- GetLegendGraphic

In WMS, the key communications are performed using XML documents which list the available data on a server (the GetCapabilities request), which provide details on a given dataset (the DescribeLayer request), or which request a map image (the GetMap request).

A WMS server usually serves the map in a bitmap format, e.g. PNG, GIF or JPEG. In addition, vector graphics can be included: such as points, lines, curves and text, expressed in SVG or WebCGM format.

The software package implementing WFS and WMS is MapServer and GeoServer. This package acts as both a client and server for WFS and WMS data, meaning that it can serve data in these formats as

well as consume this data from other servers. Other applications that can consume WFS and WMS data include OpenEV, ArcExplorer, MapWindow GIS and uDig, among others [35].

In the European Data Portal there are many registered WMS and WFS services, one example that has been offered through WFS/WMS is the “2016 SIGPAC plots”, but it is also provides a viewer application where we can query information about different parcels. The WFS service has info about the polygons for each parcel an it is distinguished via identification number. When query any specified polygon id by clicking on the specified region in the province a full described information will appear at the end of the page in a tabular form. Such information would be (id of the polygon, x and y coordinate, area size, category of earnings, fruit trees, etc ..)

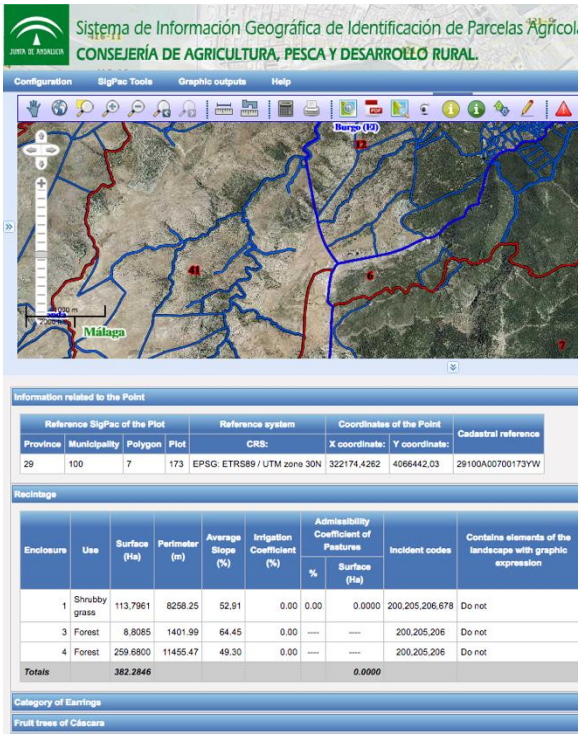


Figure 26: WMS service application example [36]

This kind of services can provide this type of information, in the previous example, it is a static information, but in future work these parcels would be provided with sensors in order to combine the static open data that are coming from these services with the dynamic data coming from different sensors like soil temperature or humidity and aggregate these information in an application to provide all the information.

6.6. GAPS AND ADOPTION BARRIERS

The main adoption barrier in the Mediation and Information Management Layer is the proliferation of proprietary APIs and incompatible data models. Those APIs are usually exposed (through REST, for

instance) on top of backend services supported by a document-oriented, NoSQL database, typically mongoDB. Such approach leads to isolated information silos, without the capability of interworking with other systems. As we stated previously, integral farm management should involve multiple Agrifood solutions from different vendors, working seamlessly to achieve a common process optimization goal through data sharing. And the only option to achieve such a goal is to expose a common information management layer, based on harmonized APIs and data models.

Another adoption barrier is the proliferation of multiple vocabularies and data models developed by different organizations with different levels of detail, and often too general and complex. Usually, solution developers do not have time to understand those sophisticated models and decide to develop their own simple solution, which finally does not scale or adapt to increasing problem complexities.

6.7. LINK TO USE CASES AND TRIALS

All the use cases from the different trials, without exception, can benefit from the usage of the context information management and geospatial technologies described by this chapter. In fact, it is of paramount importance for the success of the IoF2020 project the development of solutions that can interoperate and exploit the inherent synergies of data sharing. These solutions can be seen as lego building blocks which yield to integral farm management systems, where different use case solutions, inter and intra trial, could meet and harness all their collective potential.

7. DATA HARMONIZATION AND VOCABULARIES

7.1. INTRODUCTION

Interoperability in the Agrifood sector is not only a matter of harmonized APIs, such as NGSI-LD or WFS. The former are a necessary but not sufficient condition. In order to achieve full interoperability Smart Agrifood solutions shall use common and harmonized domain-specific data models, capable of modelling (as Entities, Properties and Relationships) the different concepts that are relevant and which intervene in the different applications. As a result, solutions could be easily replicated and, furthermore, they could be integrated into a larger ecosystem of farm management systems and other complementary Smart Agrifood solutions.

Harmonized Data Models are precisely highlighted as one of the interoperability points for IoF2020, IOP 2.1. There are different data harmonization initiatives that might be relevant for IoF2020 and it would be long to describe all of them here. For the sake of simplicity, the focus will be put on two initiatives directly

supported by the partners of the IoF2020 project. The GSMA IoT Big Data Harmonized Data Model, the ADAPT Framework and Data Model, and the GS-1 Core Business Vocabulary family. The rest of the chapter is devoted to outline them.

7.2. GSMA IOT BIG DATA HARMONIZED DATA MODEL

The GSMA Internet of Things program is an initiative to help operators add value and accelerate the delivery of new connected devices and services in the IoT. This is to be achieved by industry collaboration, appropriate regulation, optimizing networks as well as developing key enablers to support the growth of the IoT in the longer term. Inside this program, the GSMA is working with the mobile industry to follow a common technical approach in order to define a generalized architecture for delivery IoT Big Data services as well as to specify harmonized data models. The aim of this working group is to address the technical barrier of data interoperability and build a common IoT Big Data Ecosystem.

The first result of this activity is the publication of several official documents including the document "CLP.26-IoT Big Data Harmonized Data Model" (Version 3.0, 24 October 2017). This normative document describes some harmonized data entities used in different IoT Domains as Agriculture, Environment, Smart City. The definition of the different entity types is based on JSON and the FIWARE NGSIv2 information model, while reusing some parts of schema.org. Each entity is described using an agreed set of harmonized attributes in a uniform and consistent way:

- common mandatory attributes are always presented first and by definition are included in all entities (<Entity Name><Generic Attributes>)
- followed by entity specific mandatory attributes and entity specific optional attributes (<Entity Name><Entity Specific Attributes>)

Regarding Smart Agriculture, several entities have been defined (not exhaustive):

- **AgriCrop**, this entity contains a harmonized description of a generic crop
- **AgriGreenHouse** this entity contains a harmonized description of the conditions recorded within a generic greenhouse, a type of AgriParcel
- **AgriParcel**, this entity contains a harmonized description of a generic parcel of land
- **AgriParcelOperation**, this entity contains a harmonized description of a generic operations performed on a parcel of land.
- **AgriParcelRecord**, this entity contains a harmonized description of the conditions recorded on a generic parcel of land
- **AgriPest**, this entity contains a harmonized description of a generic agricultural pest
- **AgriProduct**, this entity contains a harmonized description of a generic agricultural product
- **AgriProductType**, this entity contains a harmonized description of a generic agricultural product type

- **AgriSoil**, this entity contains a harmonized description of soil

7.2.1. About GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors. (http://www.gsma.com/)

7.3. THE ADAPT FRAMEWORK

The ADAPT framework comes from a previous AG-Gateway project called SPADE. The main goal of the SPADE-project was reduced misunderstandings between actors and consumers of agricultural data, when they want to exchange information from different sources and formats. The objective was achieved through the consolidation of a common reference data model for the documentation of precision farming field operations. As result of the work, in particular as regard to interoperability, laid the foundations of a set of Reference Data APIs (e.g. Equipment, Product and Context Item) and the ADAPT framework.

ADAPT has three core elements: the ADAPT data model (ADM), a plugin manager and the set of plugins. Essentially the ADM collects the data elements defined within the SPADE that are needed in the wide variety of field operations. The plugin manager defines how plugins are managed and how the data is actually passed through the tool. Finally, the plugins are a collection of software licensed libraries, which define on how a partner's data system maps into the ADM. Currently there are two open source plugins available under the ADAPT-framework:

- ADM-plugin used for testing as well as to transfer from one system supporting ADAPT to another without having to first convert to a different format
- ISOXML-plugin developed by the AG-Gateway ADAPT that is AEF conformance tested for compatibility with the ISO11783 standard

The real potential of the approach lies not in the technology itself, but in the business, it facilitates with its way of work. The ADAPT-Framework involves the development of a proprietary plugin, which maps the own system's model into the ADM model and serializes the information into a container to share it with the partner or service provider. The receiver deserializes the container using its own plugin and extracting the relevant information for its system. The data flow back through the same process.

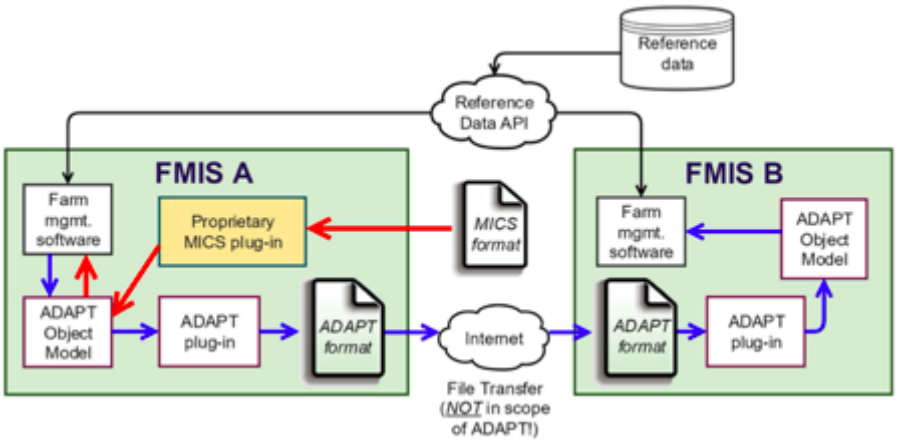


Figure 27: ADAPT Overview, schematized. Blue flow: FMIS-FMIS, Red flow: MICS-FMIS. Source: AgGateway Global Network

The ADAPT's major goal is facilitate the translation of agricultural data into different formats improving their business value for the farmers. In detail, the work is focused on maintenance common controlled vocabularies to ensure every party has the same interpretation of data elements for the exchange of documents within the framework. Due the dynamic nature of the agricultural business and its regulations, the vocabulary requires to be easy extensible and be relevant to the farmers.

From the point of view of the farmers and growers, the exchange take place in form of core documents during the process (crop plan, recommendations, work orders, work records, observations and measurements). Considering that the farmers are who decide what kind of information will be shared and whom share it with, the documents are the user's form to send and receive information. The user easily can establish value from his/her data through a structured documentation process. In other words, the farmers profit benefits from a clear documentation for everyone.

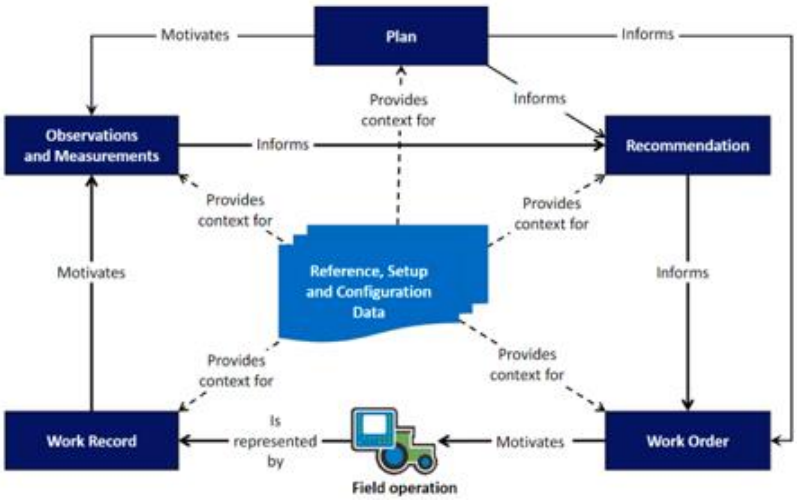


Figure 28: Documentation during the crop production. Source: AgGateway Global Network

7.3.1. ADAPT and ISO11783: Complementary

When the ISOBUS was standardized and the ISOXML was defined as format for the data exchange between machines, it was not expected that the amount and complexity of the Agricultural Data could grow so fast, or that the cloud computing could have a relevant role within the farm technologies. Currently, the data are becoming more important to consumers and at the same time there are a lot of harmonized data sources.

The basis of the interoperability within the ADAPT framework is the ISO11783, because the majority of transactions between machine-implement and FMIS are based on ISOXML. As stated above, the ISO11783 and especially the ISOXML has to deal with the introduction of new digital technologies in farming outside of machines and implements and needs to be extended considering them. Although this is a challenge, the ADAPT Project is not intended to replace ISOXML as standard format. ADAPT is intended to fulfill the gaps between FMIS and OEMs improving FMIS interoperability.

In the agricultural case, very few farmers run a fleet of one brand but would like all data in one place. The machines could be compatible with each other, but not necessarily with an FMIS. ADAPT plugins will ensure FMIS are compatible with equipment manufacturer file formats and ensure data from machines are compatible with the farmers FMIS of choice. That means independence on the data source and freedom of action.

New generations of farmers are realizing their data have value and difficulty in managing data from a machine brand or software system will become a factor in purchasing decisions. Provide an easier way to use and analyze data for customers will drive future adoption of additional precision technology products and services.

7.4. GS1 CORE BUSINESS VOCABULARY (CBV)

7.4.1. Introduction to GS1

The international GS1 community is the neutral competence and service center for cross-company business processes along the value chain in a global economy. It is regarded as mover for the development and implementation of automatic identification, communication and process standards that can be used in all industries and in addition offers platforms for cooperation, networks and know-how sharing for companies across industries – from supermarkets to the agricultural domain.

111 Member Organisations

GS1 standards represent the “global language of business” with 111 Member Organisations comprising 1.300.000 member companies and 150 countries served. Briefly, GS1 is

- neutral and not-profit oriented
- user-driven and governed
- global and local
- inclusive and collaborative

GS1 standards help to make business processes efficient by ensuring important information is accessible, accurate and easy to understand. They are classified in four categories:

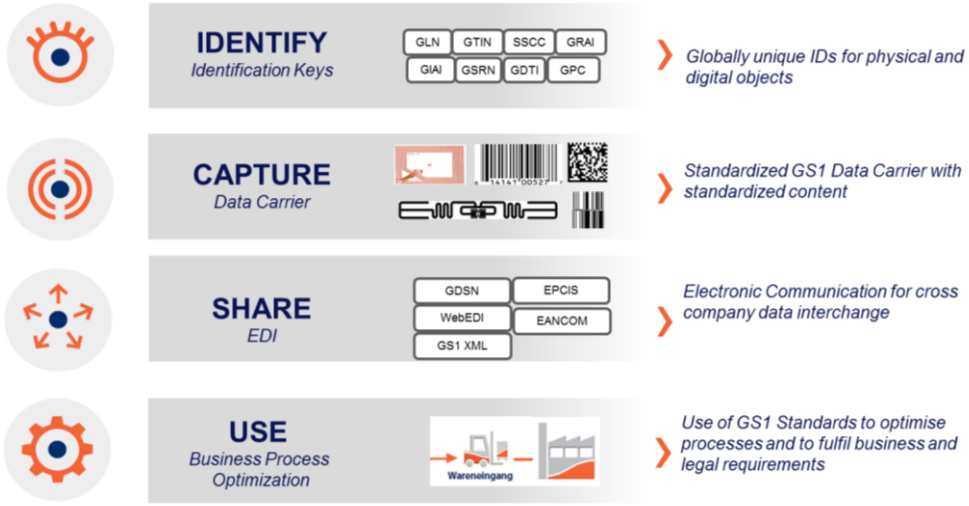


Figure 29: categories of GS1 Standards

Identify – GS1 identification standards include standards that define unique identification codes (called GS1 identification keys) which may be used to refer unambiguously to physical or digital entities such as a trade items, logistics units, physical locations or documents.

Capture – GS1 data capture standards currently include definitions of barcode and radio-frequency identification (EPC/RFID) data carriers which allow GS1 identification keys and supplementary data to

be affixed directly to a physical object. The most famous GS1 Code is the EAN/UPC Code with the GTIN encoded and used on nearly every consumer package.

Share – GS1 standards for information sharing include data standards for master data, business transaction data, and physical event data (EPCIS).

Use – Businesses can also combine various GS1 standards to streamline business processes such as traceability.

7.4.2. Core Business Vocabulary

This GS1 standard defines the Core Business Vocabulary (CBV) – published October 2010. The goal of this standard is to specify various vocabulary elements and their values for use in conjunction with the EPCIS standard [EPCIS1.2].

When it comes to data sharing, **EPCIS** (Electronic Product Code Information Service) plays an important role in IoT contexts. EPCIS is an interface standard of GS1 for capturing and sharing of event data. Defining data format, capture and query interfaces, EPCIS can be used independently from any data carrier. It only requires identification of an EPC with serial or lot number. Designed for data sharing within a company and across companies, it improves control and documentation of processes and increases transparency (What happened when, where and why?) or event-driven process optimization. The **CBV** (Core Business Vocabulary) is the data standard used within EPCIS. It defines vocabulary elements and their values e.g. for business step identifiers, disposition identifiers, business transactions/ business transaction types as well as source/ destination identifiers/types.

This standard is intended to provide a basic capability that meets the above goal. In particular, this standard is designed to define vocabularies that are core to the EPCIS abstract data model and are applicable to a broad set of business scenarios common to many industries that have a desire or requirement to share data. This standard intends to provide a useful set of values and definitions that can be consistently understood by each party in the supply chain.

Additional end user requirements may be addressed by augmenting the vocabulary elements herein with additional vocabulary elements defined for a particular industry or a set of users or a single user. Additional values for the standard vocabulary types defined in this standard may be included in follow-on versions of this standard.

This standard includes identifier syntax and specific vocabulary element values with their definitions for these Standard Vocabularies:

- Business step identifiers
- Disposition identifiers

- Business transaction types
- Source/Destination types
- Error reason identifiers

This standard provides identifier syntax options for these User Vocabularies:

- Objects
- Locations
- Business transactions
- Source/Destination identifiers
- Transformation identifiers
- Event identifiers

This standard provides Master Data Attributes and Values for describing Physical Locations including:

- Site Location
- Sub-Site Type
- Sub-Site Attributes
- Sub-Site Detail

Additional detailed master data regarding locations (addresses, etc.) are not defined in this standard.

7.4.3. Vocabulary Kinds

Vocabularies are used extensively within EPCIS to model conceptual, physical, and digital entities that exist in the real world. Examples of vocabularies defined in the EPCIS standard are business steps, dispositions, location identifiers, physical or digital object identifiers, business transaction type names, and business transaction identifiers. In each case, a vocabulary represents a finite (though open-ended) set of alternatives that may appear in specific fields of events. It is useful to distinguish two kinds of vocabularies, which follow different patterns in the way they are defined and extended over time. These concepts are explained in more detail below:

- Standard Vocabulary: A Standard Vocabulary is a set of Vocabulary Elements whose definition and meaning must be agreed to in advance by trading partners who will exchange events using the vocabulary.
- User Vocabulary: A User Vocabulary is a set of Vocabulary Elements whose definition and meaning are under the control of a single organization.

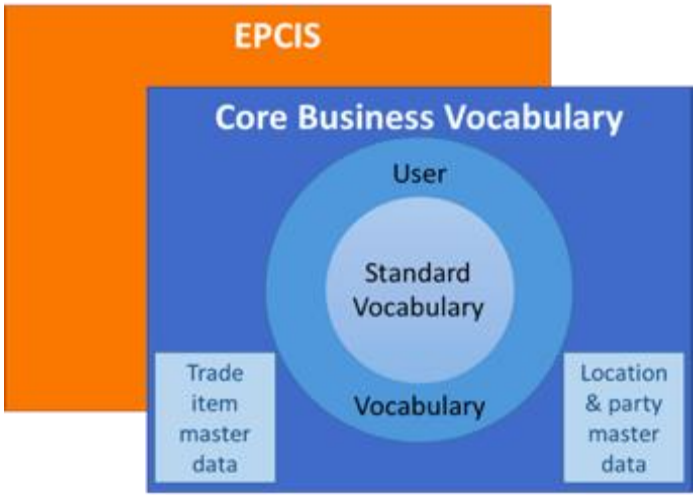


Figure 30: Vocabulary Kinds

7.4.4. Standard Vocabulary

A Standard Vocabulary is a set of Vocabulary Elements whose definition and meaning must be agreed to in advance by trading partners who will exchange events using the vocabulary. For example, the EPCIS standard defines a vocabulary called “business step,” whose elements are identifiers denoting such things as “shipping,” “receiving,” and so on. One trading partner may generate an event having a business step of “shipping,” and another partner receiving that event through a query can interpret it because of a prior agreement as to what “shipping” means.

Standard Vocabulary elements tend to be defined by organizations of multiple end users, such as GS1, industry consortia outside GS1, private trading partner groups, and so on. The master data associated with Standard Vocabulary elements, if any master data is defined at all, are defined by those same organizations, and tend to be distributed to users as part of a standard or by some similar means. New vocabulary elements within a given Standard Vocabulary tend to be introduced through a very deliberate and occasional process, such as the ratification of a new version of a standard or through a vote of an industry group.

The Standard Vocabularies specified in the Core Business Vocabulary standard are: business steps, dispositions, business transaction types, and source and destination types. The elements and definitions are agreed to by parties prior to exchanging data, and there is general agreement on their meaning.

Example: the following is a business step identifier

urn:epcglobal:cbv:bizstep:receiving

This identifier is defined by the GS1 Core Business Vocabulary standard, and its meaning is known and accepted by those who implement the standard.

While an individual end user organization acting alone may introduce a new Standard Vocabulary element, such an element would have limited use in a data exchange setting, and would probably only be used within an organization's four walls. On the other hand, an industry consortium or other group of trading partners may define and agree on standard vocabulary elements beyond those defined by the Core Business Vocabulary, and these may be usefully used within that trading group.

7.4.5. User Vocabulary

A User Vocabulary is a set of Vocabulary Elements whose definition and meaning are under the control of a single organisation. For example, the EPCIS standard defines a vocabulary called "business location," whose elements are identifiers denoting such things as "Acme Corp. Distribution Centre #3." The location identifier and any associated master data is assigned by the user. Acme Corp may generate an event whose business location field contains the identifier that denotes "Acme Corp. Distribution Centre #3," and another partner receiving that event through a query can interpret it either because the partner recognises the identifier as being identical to the identifier received in other events that took place in the same location, or because the partner consults master data attributes associated with the location identifier, or both.

Example:

urn:epc:id:sgln:0614141.12345.400 285

This identifier is assigned by the End User who owns the GS1 Company Prefix 0614141, and the meaning of the identifier (that is, what location it denotes) is determined exclusively by that end user. Another End User can understand the meaning of this identifier by consulting associated master data.

User Vocabulary elements are primarily defined by individual end user organisations acting independently. The master data associated with User Vocabulary elements are typically defined by those same organisations, and are usually distributed to trading partners through the EPCIS Query Interface or other data exchange / data synchronisation mechanisms. New vocabulary elements within a given User Vocabulary are introduced at the sole discretion of an end user, and trading partners must be prepared to respond accordingly.

While the Core Business Vocabulary standard does not specify particular user vocabulary elements, the Core Business Vocabulary does provide syntax templates that are recommended for use by End Users in constructing their own user vocabulary elements. The user vocabularies for which templates are specified in this standard are: physical or digital objects, locations which include both read points and business locations, business transaction identifiers, source/destination identifiers, and transformation identifiers. Unlike the standard vocabularies, a vocabulary element in a User Vocabulary is created by an End User. For example, an End User who creates a new business location such as a new warehouse may create a business location identifier to refer to that location in EPCIS events. The specific identifier

string is defined by the End User, and its meaning may be described to trading partners via master data exchange, or via some other mechanism outside of the EPCIS Query Interface.

Further information on EPCIS and CBV (standards, artifacts, application standards and implementation guidelines) can be obtained under www.gs1.org/epcis

7.4.6. Outlook for Standardization

Regarding the agro sector CBV allows providing further creation of user vocabulary or extensions as well as application standards and implementation guidelines. Future developments and requirements of stakeholders are taken into account in a user-driven process. With regard to the above mentioned two releases of CBV (1.1 and 1.2) on the one hand it is therefore likely to have new features or attributes in one of the coming releases of CBV, e.g. for stakeholders of the agro sector. On the other hand, a cross-domain approach of a new release might be a bigger step ahead, incorporating related supply chains to the existing ones in agriculture but also to technological and legal enterprise software.

7.5. ASSET IDENTIFICATION USING GS1

The GS1 Global Company Prefix is a unique string of four to twelve digits used to issue GS1 identification keys. It guarantees uniqueness and associability. It is indicated in GEPIR (Global Electronic Party Information Registry; http://gepir.gs1.org/) that gives access to basic contact information for companies that use GS1's globally unique identification system. By simply typing a GS1 key or a company name you can find relevant contact details respectively the GCP. As an Example, GEPIR contains the following information about GS1 Germany.

Figure 31: GS1 Example

The **EPC** permits the automatic and unambiguous identification of objects. The EPC can be encoded in GS1 data carrier or in EPC/RFID technology. With the EPC, the flow of goods and information can be managed efficiently across sectors and globally.

EPCIS used in supply chains with dispersed read points like in the agricultural sector may lead to a high degree of transparency and safety when traceability for example of food stuff is registered granularly

according to the four information bricks: what – GTIN + lot or serial; when – date/time-stamp; where – GLN and why – business vocabulary.

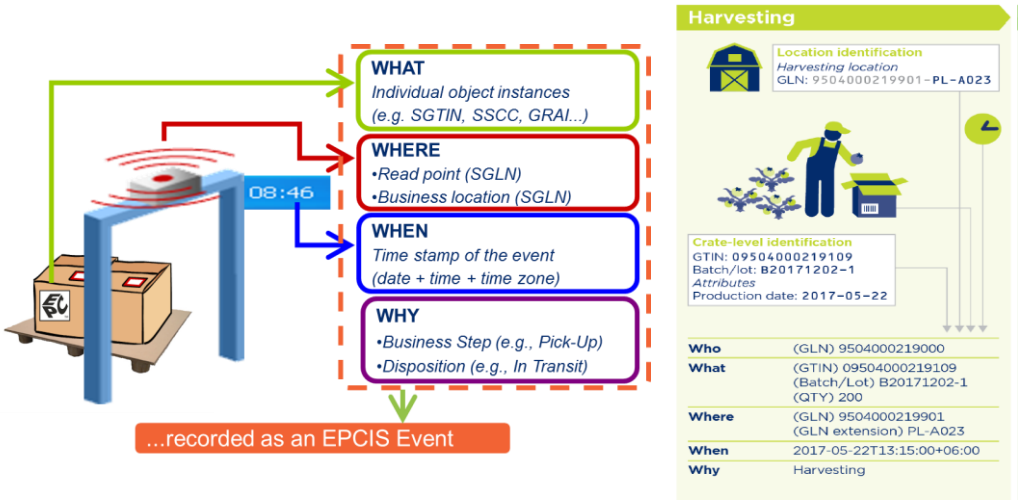


Figure 32: How EPCIS used in supply chain

7.6. HOW CAN GS1 STANDARDS SUPPORT THE IOF2020 USE CASES?

As depicted above GS1 standards are open and designed to support every industry across the entire supply chain. Especially in the agricultural domain traceability with unique GS1 identifiers for locations and products as well as EPCIS help to make process chains transparent, as described in the GS1 Traceability Standard.

7.6.1. Event data from devices and sensors and the Internet of Things

While IoT is inevitable to upcoming farm management, it is transformational to systems, devices, technologies and applications — across industry and around the world — and driven by:

- an expectation by businesses and consumers that all things will be connected,
- increasing capabilities and lower cost of microcontroller and communications technologies,
- the explosion of cloud-based data gathering, processing and sharing platforms.

GS1's "Global Language of Business" connects the physical and digital world. Identification of objects, assets, locations, etc. and automatic data capture are supported by GS1 barcodes and EPC/RFID. GS1 standards for data sharing enable interoperable, trusted and transparent data that are foundational to unleashing IoT capabilities.

GS1 has started to engage in IoT-related standardization initiatives, in particular when it comes to the use of identifiers, the interpretation (semantics) and fusion (adding business context) of event data from devices and sensors. Sensors passively record changes in the state of the physical world and the

objects contained within it, such as a temperature sensor in a food truck recording events outside an acceptable temperature range. Event data from actuators record a history of intentional changes, such as the opening of a valve for a water reservoir or gas pipeline or the locking/unlocking of a door.

Event data from devices and sensors are expected to be very similar in nature to visibility event data. The data will be enriched with business context -including the five dimensions that define the who, what, when, where and why- and shared using networked or decentralized choreographies

7.6.2. Relevance for the Agricultural-Sector

Currently only few companies collect data according to their own rules or the GS1 standards developed for processes along the value chain that simplify the identification of goods, their collection and the communication of systems and departments. The complete flexibility in choosing the right GS1 ID keys is one key factor for entrepreneurs in the agricultural sector, e.g.:

- foundation of a common language
- globally-recognized numbers
- accurately defining anything in the supply chain
- uniquely identifying products, pallets, assets or locations sub-allocated by users
- provide access to information - often master data - held in databases
- include the GS1 Company prefix assigned to every user company by GS1
- the process determines the technology

7.6.3. EPCIS in Agricultural Processes

Aspects in the agricultural domain with relevance for processors, retailers and consumers can be rearing, antibiotics treatment, special treatment, animal welfare, date of harvest, provenance and other aspects. The picture below depicts details for the pork supply chain.

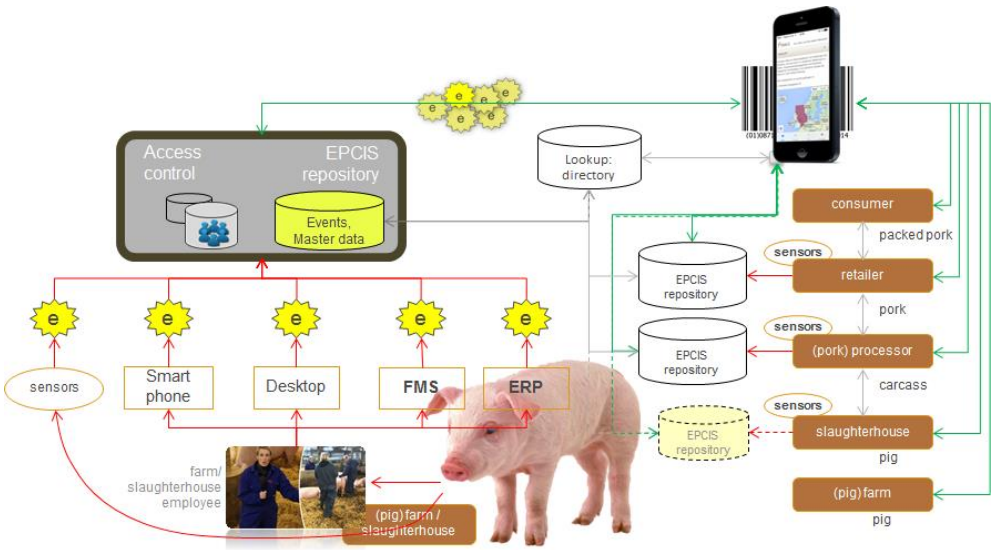


Figure 33: How does it work? for IoF2020, Source: Ayalew Kassahun

7.6.4. Relevant GS1 Keys for IoF2020

As depicted in the agricultural supply chain below there are many keys applicable in the agricultural supply chain

Figure 34: Agricultural supply chain

The **GLN** (Global Location Number) for example can be used to identify e. g. their locations like fields and barns or feeding areas. It is related to the “who” and “where” of an EPCIS event.

The **GTIN** (Global Trade Item Number) can be used to identify e.g. medicine, feeding, any product or even a (living type of). Together with a batch or serial number it is very often related to the “what” of an EPCIS event.

The **GRAI** (Global Returnable Asset Identifier) identifies every returnable container or packaging Returnable transport items (RTI) are reused for multiple deliveries, e.g. crates, trays and pallets. A GRAI is encoded in a barcode or EPC/RFID tag. Thereby the GRAI helps companies to more easily track and manage their valuable returnable assets. In an EPCIS aggregation event a product (GTIN) can be associated to a GRAI.

Figure 35: GRAI barcode or EPC/RFID tag

GIAI (Global Individual Asset Identifier) identifies any asset throughout its lifetime. This can be a vehicle, machine, computer or spare part. Also, a sensor may be identified with GIAI in an IoT scenario. A typical EPCIS event depicts the movement of a tractor within a determined location.

The SSCC (Serial Shipping Container Code) can be used by companies to identify a logistic unit, which can be any combination of trade items packaged together for storage and/ or transport purposes; for example, a case, pallet or parcel. In case of an EPCIS shipping event the SSCC can act as the “what” category.

7.6.5. Interoperability

Whereas several IoF2020 use case partners have (internal) systems at their disposal it is crucial to guarantee interoperability between systems. A system that is implemented to meet internal traceability requirements may not be able to interoperate with systems of other parties in the supply chain. In order to ensure an appropriate level of interoperability, organizations will need to ensure that their systems are all built on a common set of standards. This does not mean that all actors in the supply chain need to use the exactly the same systems, but their systems will need to be able to support standardized data. With regard to this GS1 supports with unique identification schemes (GLN, GTIN, …), data formats (CBV) and the interface standard EPCIS.

7.6.6. Further Information

- System of GS1 Standards: http://www.gs1.org/standards
- GS1 Traceability Standard: https://www.gs1.org/traceability/traceability/2-0
- GS1 Identification Keys: http://www.gs1.org/id-keys
- S1/EPCIS and CBV Standard: http://www.gs1.org/epcis
- Fruit & Vegetable Master Data Attribute Implementation Guide. https://www.gs1.org/docs/freshfood/Fruit_Vegetable__Master_Data_Attribute-ImpGuide.pd
- Case study: Traceability in Fresh Foods: https://www.gs1.org/sites/default/files/docs/casestudies/traceability_case_study_egypt.pdf
- GS1 and Internet of Things: http://www.gs1.org/standards/internet-of-things

- A Global Farm Registry for the United Nations: https://www.gs1.org/sites/default/files/docs/retail/gln-for-farms.pdf

7.7. GAPS AND ADOPTION BARRIERS

As we stated in previous chapters, is the proliferation of multiple vocabularies and data models developed by different organizations with different levels of detail, and often too general and complex. Sometimes, solution developers do not have time to understand those sophisticated models and decide to develop their own simple solution, which finally does not scale or adapt to increasing problem complexities.

Integral farm management should involve multiple Agrifood solutions from different vendors, working seamlessly to achieve a common process optimization goal through data sharing. And the only option to achieve such a goal is to expose a common information management layer, based on harmonized APIs and data models. ADAPT, GS-1 and GSMA IoT Big Data are good starting points to fill the current gaps and help to eliminate the adoption barriers. For achieving such goal is of paramount importance outreaching the developers community, evangelising on the advantages of following a common and interoperable approach which leads to replicable and composable solutions.

7.8. LINK TO USE CASES AND TRIALS

All the use cases from the different trials, without exception, can benefit from the usage of different harmonized data models described by this chapter. In the particular case of ADAPT, its applicability, in principle, is only under the scope of the arable trial, and particularly UC 1.4, farm machine interoperability. GS-1 can fill the bill of meat transparency (trial 5) and traceability of fruit logistics (UC 3.4).

8. SECURITY AND PRIVACY

8.1. INTRODUCTION

The digitalization of the Agrifood industry to enhance the farming process implies that data is being generated and exchanged throughout the production process. The collection of agricultural data includes, among others, livestock data, land and agronomic data, climate data, machine data, financial data and compliance data. Such increasing exchange of data is a major challenge for the EU Agrifood sector. It poses questions about privacy, data protection, intellectual property, data attribution (ownership), relationships of trust/power, storage, conservation, usability and security.

Furthermore, gathering, evaluating and consuming information in the same IoT platform requires the system to deal with numerous attacks such as cross-site scripting, privilege escalation, account enumeration, man in the middle, side-channels and other vulnerabilities that may result in security problems and data leakage. Therefore, smart farming solutions must adopt serious measures to ensure the privacy and security of data. All systems should be resistant against cyber-attacks, particularly the critical infrastructure like agricultural machinery. As a result, for successful implementation of IoT, smart farming should place privacy and security as a top priority.

Other work in IoF2020 is being done concerning security and privacy. In particular in WP1, WP4 and WP6 (see D1.4, D6.1). There are deliverables that describe in more detail what is presented in this Chapter except for the technical aspects of security and privacy, on which this deliverable is more focused.

8.2. REQUIREMENTS

The essential requirements in terms of security for smart farming IoF2020 solutions include, but not limited to, the ones enumerated below:

- An IoF2020 solution should be able to properly react to data violations (e.g. data are accessed by unauthorized entities or other data breach) with defined procedures.
- An IoF2020 solution should incorporate capabilities in order to secure the platform which is going to support the smart farming services, by providing support for confidentiality, integrity, authentication, authorization, immutability, trust and non-repudiation when needed.

The IoF2020 project has defined a set of IoT Security Guidelines that is recommended to be followed when implementing the use cases and trials.

The nature of agricultural data is highly specific but very diverse. Some of these data can be considered as personal data or can include highly sensitive and protected information of the many agro-business providing services/equipment for farm activities. It is essential that the necessary safeguards are built in. Therefore, the essential requirements in terms of privacy for smart farming IoF2020 solutions include, but not limited to, the ones enumerated below:

- An IoF2020 solution shall provide procedures and guidelines in order to ensure compliance with respect to data protection rules.
- The system has to provide data anonymization/aggregation functions in order to delete personal or restricted information coming from the data sources. It is necessary to have this type of functionalities in order to (re)use and publish data coming from different sources being compliant with privacy and data protection regulations.

- The system has to provide functionalities to allow the end user to control his own personal data defining who and how can access to it. End-user should have full control of his personal data, including the right of erasure.

8.3. TACKLING SECURITY AND PRIVACY IN AGRIFOOD

The regulation, associated standards and technologies for tackling security and privacy in Agrifood are not very different than those used in other domains of the IoT Large Scale Pilot Program, particularly smart cities. At this respect, the deliverable on the Architecture of SynchroniCity, D2.1, provides a good overview and recommendations, and some of them are summarized in the Synchronicity project's website [48].

8.3.1. Privacy Regulation and Guidelines

The General Data Protection Regulation (GDPR) [39], a single pan-European law on data protection, requires all the companies dealing with European consumers to:

1) increase transparency

2) provide user's granular control on data access and sharing

3) guarantee a set of fundamental individual digital rights (including right to rectification, erasure, data portability, and restrict processing). Moreover, accountability should be also provided to demonstrate the compliance with privacy and data protection principles (or legal requirements) which requires clear responsibilities, internal and external auditing and controlling of all data processing.

More specifically, the "EU code of conduct on agricultural on data sharing" which it's copyright reserved to Copa-Cogeca, CEMA, Fertilizers Europe, CEETTAR, CEJA, ECPA, EFFAB, FEFAC, ESA, Coceral [147] provided by is an ongoing development that will look at general principles for sharing agricultural data within the Agrifood chain related to farm products or farm operations and represents a joint effort of the signatory organizations to shed greater light on contractual relations and provide guidance on the use of agricultural data. Below there is a summary of the main security and privacy issues tackled by such code of conduct and the recommendations made:

- **Data Protection**, the data user commits to protect the data received from the data originator, against loss, theft, unauthorized access and alteration by non-authorized persons. In addition, sensitive agricultural data considered must be able to benefit from a special regime with regard to the rights of access, use or sharing as well as any security enhancements (e.g. encryption, authentication, secure internet flow, etc.) as defined in the contract between the farmer and the data provider or user.

- **Data Ownership**. Data cannot be owned in the same way as physical assets. It is therefore crucial to set some key principles on for access to agricultural data and usage rights. The parties should establish a contract clearly setting the conditions for data collection and data sharing, according to the needs of the contracting parties.

- **Data access and control**. Data originator must give permission for their data to be used and shared with the third parties. Information should only be given to third parties as aggregated or anonymized data, unless required for delivering the requested service and/or otherwise in the conditions specified in a contract. The data sets should only be kept for as long as is strictly necessary for the relevant analyses to be carried out. There must be the option to remove, destroy (e.g. right to be forgotten) or return all original data (e.g farm data) at the data originator's request.

8.3.2. Data Protection

From an architecture perspective, privacy by design approach demands privacy to be embedded into design as a preventive and proactive measure, whereas privacy enhancing technologies can help to minimize or avoid risks to privacy and data protection. Technologies that can contribute to enhance privacy and data protection are searchable encryption, verifiable secret sharing and multi-party computation.

There are several techniques to ensure data protection on a storage level. On-the-fly encryption (OTFE) is a method to automatically encrypt data as it is saved. Data masking is the process of obscuring specific data ensuring that data security is maintained and sensitive information is not exposed to unauthorized personnel. Data erasure is a method of software-based overwriting that completely destroys all electronic data residing on a hard drive or other digital media to ensure that no sensitive data is leaked when an asset is retired or reused.

Multi-party computation (MPC) is a privacy-preserving technique which allows to perform computation among parties without revealing any input to each other. MPC was first introduced by Andrew C. Yao with the motivation of the "millionaire problem": two millionaires wish to compute which one is richer, but without revealing to each other how much money they have.

When it comes to data protection, oneM2M provides Secure Storage service to AEs and CSEs with access to the secure storage capability of the Secure Environment (SE). Data securely stored by the AE or CSE shall only be accessible through the Security API and by authorized entities. Stored data shall be under the control of the stakeholder owning the data independently from the other stakeholders. The Secure Environment component is a logical entity that provides Sensitive Functions operating on Sensitive Data, Secure Storage and other resources/functions.

8.3.3. Data Access

Authentication and authorization capabilities are critical aspects to support Smart Farming services and applications. An access control policy is defined as sets of conditions that define whether users have access granted to a protected resource. The authorization function can support different mechanisms, such as Access Control List (ACL), Role Based Access Control (RBAC), Attribute Based Access Control (ABAC), etc. Among the authentication and authorization standard solutions we can mention Security Assertion Markup Language (SAML), eXtensible Access Control Markup Language (XACML), JSON Web Token (JWT), OAuth and OpenID.

OneM2M advises the use of a personal data management framework based on the user's privacy preferences, such a framework could be used to create access control policies from the user's privacy preference and protects the user's Personally Identifiable Information (PII) from unauthorized parties. It may be operated by a Service Provider or another stakeholder acting as trusted third party. If the Service Provider or other stakeholder provides the user's Personally Identifiable Information to third party, the Service Provider or other stakeholder needs the user's acceptance. In case that the user accepted a privacy policy which indicates provision to third party, the Service Provider may provide the Personally Identifiable Information to third party. However, if the privacy policy does not include provision to third party, the Service Provider needs to update the privacy policy and get the user's consent to it.

8.3.4. Security on IoT Infrastructure

The huge heterogeneity in the IoT devices capability (in terms of memory, computational, or energy requirements) plays against the identification of a “unique” or “common” security solution set, whereas they call for a large spectrum of security level versus resource consumption trade-offs. Some protocols such as CoAP, XMPP, Bluetooth mandate for confidentiality and authentication services by means of end-to-end encryption and digital signatures while others such as LoRa, MQTT and Zigbee focus on more lightweight security solutions, thus leaving the task to provide higher security level protection to the transport or application layer.

When it comes to authentication, oneM2M provides mutual authentication schemes. To prevent reading and copying of credentials, a secure environment within the Security CSF provides protection against tampering of those credentials and related processed information. A general mutual authentication protocol is applied to both symmetric and asymmetric key based schemes. Precise protocol messages and parameters depend on the chosen scheme and the security parameters selected.

Concerning authorization, oneM2M authorizes services and specific operations (e.g. Retrieve, Update) on resources to identified and authenticated entities, according to provisioned access control policies and assigned roles. This functionality is mandatory when any services relying on authorization and access control are present. Among other usages, the services of this functionality may be applied to personal information as a means to preserve privacy.

With regards to accounting**,** oneM2M provides service layer charging policies and configuration capturing service layer chargeable events, generating charging records and charging information. The IN-CSE can interwork with charging systems in the Underlying Network (e.g. 3GPP network).

8.3.5. Security on Platform

Applications and services deployed in the farms and food domain can have different security requirements based on their scope, including confidentiality, integrity, authentication, authorisation, immutability, trust and non-repudiation. From a security perspective, best practices mandate for a security in depth approach.

Measures to address these capabilities are deployment of physical protection, access control, alarms and surveillance, implementation of an information security policy, creation of activity logs, regular auditing, and maintenance of backups. More specifically, applications and services can be targeted by tampering and accessing information from different surfaces, thus different protection measures to address this threat must be tailored to the target. Such defenses range from: physical measures to prevent access to restricted areas and the use of tamper-proof designs; measures to make tampering/alteration easier to detect, such as measures to mitigate the in transit manipulation of messages travelling between systems or actors; digital measures to prevent access such as firewalls and authentication systems.

8.4. GAPS AND ADOPTION BARRIERS

Security and privacy are two interrelated issues that have to be tackled. The GDPR compliance introduces new challenges in terms of data protection, sharing or control. The traditional security issues like encryption, authentication, authorization and none repudiation are as well on the table. Security has to be ensured at all the communication levels of the IoT stack. In fact, there is existing prior work and standards available, in the different layers of the IoT stack, that can help to overcome these issues (particularly some of the recommendations made by oneM2M [59]).

To the best of our knowledge, the main adoption barrier is the lack of simple and clear guidelines or recipes to outreach developers in the best practices to be followed concerning security and privacy. The IoF2020 Security Guidelines and the STRIDE analysis made for use cases (Deliverable 3.2) can overcome that situation. In fact, they are definitively helping to position the IoF2020 project, in order to showcase how a smart farming solution should be deployed to be compliant with the latest security and privacy regulations.

8.5. LINK TO USE CASES AND TRIALS

All use cases of the different trials are subject to the security and privacy considerations made during this chapter. Special care has to be taken to respect privacy especially when farmers' or consumers' data is being managed.

9. CONCLUSIONS

In the *IoT Connectivity Layer* emphasis is put on **LPWA** networks, as they meet very well the particular requirements of smart food and farming, i.e. low cost, low data rate usage, long battery lives and operation in remote and hard to reach locations. In the *IoT Service Layer* some of the most popular protocols in the domain are tackled, **MQTT(-SN)** and **LWM2M**, together with **oneM2M,** proposed by a partnership led by eight ICT standards bodies around the world (including ETSI). When it comes to bidirectional communication with agricultural machines, **ISOBUS** and **ADAPT** are analyzed.

For Information Management, **FIWARE NGSI** and its evolution as a European Telecommunications Standards Institute (ETSI) standard, **NGSI-LD** (developed by the ETSI ISG CIM). Accompanying NGSI-LD, the work developed by **GSMA** on data harmonization plays a relevant role to achieve data portability, together with **GS-1** standards. OGC standards, **WMS**, **WFS**, are to be taken into account, particularly when they are supported by public services that offer data and visualization about agricultural assets. A discussion on security and privacy issues is summarized as well.

This document has focused on communication technology and standards for the different layers for IoT applications in farming. Technology enablers and associated standards that can be applied to the smart farming domain in general, and to the IoF2020 use cases in particular have been analysed. Those technologies are core for the development of portable, interoperable and integrable solutions. Such solutions are aimed at creating a rich marketplace and ecosystem for smart Food and Farming, representing an unprecedented opportunity to produce value and create business opportunities, by applying data-driven solutions:

- To improve resource efficiency, productivity, environmental processes and provide tools to mitigate climate change;
- To adapt business plans, respond to dynamic markets and consumer expectations;
- To decrease administrative and bureaucracy costs and enable science-based policies;
- To provide better and more prosperous living conditions for rural communities;

The interoperability points identified by this document are similar to the ones present in other domains, even though, the digital farming domain has its own particularities, for instance the usage of field machinery, or the role of animals in production processes. Nonetheless, the opportunities for collaboration and synergies between domains are feasible and promising, particularly with Smart City and Industrie 4.0.

There are, however, many challenges, in the smart farming domain, posed by the current state of the art of the technology. With regards to connectivity, the coverage in rural areas is still an issue and it seems that privately operated networks will have to coexist with public telco-operated networks. With regards to the IoT Service Layer, there are well known technology enablers and standards (MQTT, CoaP, LWM2M) that have been in widespread use in smart farming along the years. However, a greater level of harmonization could be achieved by the adoption of more holistic approaches such as the one proposed by oneM2M. In this respect, to the best of our knowledge, oneM2M has not been used in a significant manner in the smart farming domain and it is still facing many adoption challenges. Web of Things is another emerging standard that may have its chance in Smart Farming, and it is recommended that IoF2020 starts exploring its applicability to some use cases.

Concerning interoperability points in the upper layers of the architecture, particularly the Context Information Management Layer, FIWARE NGSI and the emerging NGSI-LD specification (NGSI extended with linked data capabilities) are well positioned to be the technological standards needed for offering a consolidated view of information that is high quality and actionable, and which origin can be IoT devices or other sources of information, such as open data portals or external services. However, there is still a challenge in the massive adoption of these technologies and concept, as there are many smart farming solutions that still use their own cloud-based solutions relying on proprietary APIs and data models. To overcome this issue, it is of paramount importance, to promote the adoption of a common information management layer, especially for the sake of interoperability and integrability between smart farming solutions and, future-wise, for the development of multi-sided markets, where different smart domains cooperate by sharing and exchanging data towards a common goal.

Having a standard API for dealing with context information is a necessary but not sufficient condition to achieve interoperability at the information management side. That is the reason for introducing well-known, harmonised data models for the Agrifood domain. The work formerly done by GSMA can be complemented with additional industry initiatives such as GS-1, ISO-XML or the ADAPT Data Model. The suggested strategy is to reuse existing information models by mapping them to the meta-model defined by FIWARE NGSI and, in the near future, to NGSI-LD, instead of reinventing the wheel with new information models.

Another important aspect in the smart farming domain is the availability of open data. Particularly for geospatial data, OGC interfaces and services, WMS and WFS play an important role and they have wide adoption especially by public authorities that usually expose public data about agricultural parcels

using these technologies. Also, satellite observations often are exposed through this kind of services. Last but not least, other sources of agricultural data would have to be exposed through specific adaptors in the mediation layer that translate or map existing data models or APIs to NGSI(-LD).

With regards to communication with field machinery, using existing infrastructure and defined interfaces like ISO-XML (or ADAPT) and the new EFDI protocol is the basis to manage interoperability. Data interaction from machine-to-machine or from machine-to-cloud based solutions have to be further organized and standardized. The AEF and its project teams have a vision of how to manage this challenge. EFDI to transfer data during machine operability is on the way, new wireless communication channels to transfer data from machine-to-machine as well. Initiatives like IoT are a challenge for the Ag industry but can be managed by using existing and new standards. Together with its member companies, the AEF is willing to manage the challenges of this digital revolution.

Security and privacy are two interrelated issues that have to be tackled. The GDPR compliance introduces new challenges in terms of data protection, sharing or control. The traditional security issues like encryption, authentication, authorization and none repudiation are as well on the table. Security has to be ensured at all the communication levels of the IoT stack. In fact, there is existing prior work and standards available, in the different layers of the IoT stack, that can help to overcome these issues (particularly some of the recommendations made by oneM2M). The IoF2020 Security Guidelines and the STRIDE analysis made for use cases (Deliverable 3.2), are definitively helping to position the IoF2020 project, in order to showcase how a smart farming solution should be deployed to be compliant with the latest security and privacy regulations.

To summarize, the Agricultural industry has to integrate many different and “new” technologies based on these standards to allow “interconnectivity” between the different actors. The IoF2020 project collaboration is the perfect playground to try out the different use cases and show that the data interchange between the different manufacturers, domains and information silos is really working. To achieve such an ambitious objective a call for action is needed:

- Aligning use cases towards common IoT Service Layers and explore the suitability of emerging technologies to avoid vendor lock-in and further interoperability at IoT level, particularly Web of Things. Develop a proof of concept with Web of Things technology.
- Aligning use cases towards common Context Information Management approaches based on harmonized APIs and data models, avoiding the proprietary cloud trap.
- Stimulate the development of adaptors or mappings between Agrifood traditional vocabularies (ADAPT, ISOBUS, etc.) and NGSI-LD.
- Foster the integration of different Smart Agrifood IoF2020 verticals into the infrastructure offered by farm management information systems. Develop a proof of concept including two or three use cases and a farm management information system.

- Curate a set of IoT Components, Recipes and associated configurations that make life easier to use case developers and to the broader IoF2020 ecosystem. Outreach other developers and evangelize the benefits of harmonization and integration.
- Promote the usage of open platforms and open source software as a way to avoid vendor lock-in and to accelerate implementation and go to market.

10. BIBLIOGRAPHY

[1] “What Is LPWA?: - Ingenu,” 19-Jan-2018. [Online]. Available: https://www.ingenu.com/technology/rpma/lpwa/. [Accessed: 19-Jan-2018].

[2] “GSMA Mobile IoT Initiatives | Licensed Low Power Wide Area Technology,” 19-Jan-2018. [Online]. Available: https://www.gsma.com/iot/mobile-iot/. [Accessed: 19-Jan-2018].

[3] G. Dregvaite and R. Damasevicius, Eds., Information and Software Technologies. Springer International Publishing, 2016.

[4] “Introduction to Mobile and Networks,” in Mobile and Wireless Networks, John Wiley & Sons, Inc., 2016, pp. 1–13.

[5] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, “A Study of LoRa: Long Range & Low Power Networks for the Internet of Things.,” Sensors, vol. 16, no. 9, Sep. 2016.

[6] "What Is the Sigfox Protocol Stack?" SIGFOX, 8 Feb 2017. [Online]. Available: https://www.youtube.com/watch?v=tGmFgaxKPRU. [Accessed 2018].

[7] A. Berni and W. Gregg, “On the Utility of Chirp Modulation for Digital Signaling,” IEEE Trans. Commun., vol. 21, no. 6, Jun. 1973.

[8] “Limitations: data rate, packet size, 30 seconds uplink and 10 messages downlink per day Fair Access Policy - End Devices (Nodes) - The Things Network.”

[9] “Actility | IoT Solutions - Agriculture | Improve your productivity.”

[10] “NarrowBand IOT - Wikipedia,” 19-Jan-2018. [Online]. Available: https://en.wikipedia.org/wiki/NarrowBand_IOT. [Accessed: 19-Jan-2018].

[11] U. Raza, P. Kulkarni, and M. Sooriyabandara, “Low Power Wide Area Networks: An Overview,” IEEE Commun. Surv. & Tutorials, vol. 19, no. 2.

[12] A. D. Zayas and P. Merino, “The 3GPP NB-IoT system architecture for the Internet of Things,” in 2017 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 277–282.

[13] NB-IoT Services – From the Concept to the Roll-out [Online]. Available: https://docbox.etsi.org/Workshop/2017/201710_IoTWEEK/WORKSHOP/S04_CONNECTING_IoT/DEUTSCHETELEKOM_KESSLER.pdf. [Accessed: 19-Jan-2018].

[14] "NarrowBand IoT (NB-IOT)," Deutsche Telekom, 2016. [Online]. Available: https://m2m.telekom.com/de/telekom-m2m/einblicke/narrowband-iot-nb-iot/. [Accessed 2018].

[15] A. El-Hoiydi, J. Decotignie, C. Enz, and E. Le Roux, “WiseMAC, an Ultra-Low Power MAC Protocol for the WiseNET Wireless Sensor Network.” pp. 244–251.

[16] M. Keshtgari and A. Deljoo, “A Wireless Sensor Network Solution for Precision Agriculture Based on Zigbee Technology.” Scientific Research, 01-Jan-2012.

[17] “CoAP — Constrained Application Protocol | Overview,” 13-Feb-2018. [Online]. Available: http://coap.technology/. [Accessed: 13-Feb-2018].

[18] Z. Shelby, K. Hartke, and C. Bormann, “The Constrained Application Protocol (CoAP),” RFC Editor, Jun. 2014.

[19] “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things > Introduction > How This Book Is Organized: Safari Books Online,” 13-Feb-2018. [Online]. Available: https://proquest-safaribooksonline-com.ezproxy.lib.vt.edu/book/networking/9780134307091/introduction/pref09lev1sec2_html. [Accessed: 13-Feb-2018].

[20] “OMA LWM2M - Wikipedia,” 24-Jan-2018. [Online]. Available: https://en.wikipedia.org/wiki/OMA_LWM2M. [Accessed: 24-Jan-2018].

[21] G. K. Vodafone, F. R. Vodafone, and Z. Shel, “White Paper ‘Lightweight M2M’: Enabling Device Management and Applications for the Internet of Things (2014).”

[22] “IEEE Xplore Full-Text PDF,” 09-Jan-2018. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1017644. [Accessed: 09-Jan-2018].

[23] G. (Vodafone) Klas, F. (Vodafone) Rodermund, S. (Ericsson) Akhouri, Z. (ARM) Shelby, and J. (Ericsson) Höller, “” Lightweight M2M”: Enabling Device Management and Applications for the Internet of Thing.” 01-Mar-2014.

[24] S. Rao, D. Chendanda, C. Deshpande, C. Deshpande, and V. Lakkundi, “Implementing LWM2M in Constrained IoT Devices,” in IEEE Conference on Wireless Sensors, 2015.

[25] D. Locke, „MQTT-OASIS-WEBINAR,” 15 May 2013. [Online]. Available: https://www.oasis-open.org/committees/download.php/49205/MQTT-OASIS-Webinar.pdf. [opened 2018].

[26] S. A. Jaishetty en R. Patil, „IOT SENSOR NETWORK BASED APPROACH FOR AGRICULTURAL FIELD MONITORING AND CONTROL,” IJRET: International Journal of Research in Engineering and Technology, vol. 05, nr. 06, Jun 2016.

[27] J. Bauer en N. Aschenbruck, „Measuring and Adapting MQTT in Cellular Networks for Collaborative Smart Farming,” in 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, 2017.

[28] Eclipse, „Mosquito,” Github, [Online]. Available: https://github.com/eclipse/mosquitto. [Opened Feb 2018].

[29] „MQTT Version 3.1.1,” Oasis, 29 October 2014. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf. [Opened Feb 2018].

[30] A. Stanford-Clark en H. L. Truong, „Protocol Specification: MQTT For Sensor Networks (MQTT-SN), Version 1.2,” 13 November 2013. [Online]. Available: https://mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf. [Opened Feb 2018].

[31] „ty4tw/MQTT-SN: MQTT-SN over UDP and XBee,” Github, [Online]. Available: https://github.com/ty4tw/MQTT-SN. [Opened 2018].

[32] „lightweight-m2m-lwm2m,” OMA, 2017. [Online]. Available: http://openmobilealliance.org/iot/lightweight-m2m-lwm2m. [Opened 2018].

[33] „The guide to integration: IoT Zone,” DZONE, 23 Aug 2017. [Online]. Available: https://dzone.com/articles/mqtt-v5-what-is-on-the-way. [opened Feb 2018].

[34] S. S. en Z. X. Xiong H, „Web Feature Serice and Web Map Service,” in Encyclopedia of GIS, Springer, Charm, 2017.

[35] „WIkipedia: Web Map Service,” 15 Mar 2006. [Online]. Available: https://en.wikipedia.org/wiki/Web_Map_Service. [opened Feb 2018].

[36] „agriculturaypesca: Page of SigPac,” juntadeandalucia, [Online]. Available: http://ws128.juntadeandalucia.es/agriculturaypesca/sigpac/index.xhtml. [opened Feb 2018].

[37] X. H. Zhou X., S. S. en S. A., „Web Feature Service,” in Encyclopedia of GIS, Springer, Charm, 2017.

[38] M. T, Web Mapping Illustrated, O'Reilly series., 2005.

[39] „Home: EU GDPR Portal,” Trunomi, [Online]. Available: https://www.eugdpr.org/. [opened Feb 2018].

[40] „Tutorial: FIWARE NGSI APIv2,” [Online]. Available: http://fiware-orion.readthedocs.io/en/develop/user/walkthrough_apiv2/. [opened Feb 2018].

[41] „Tutorial: Geolocation capabilities (using NGSIv2),” FIWARE, [Online]. Available: http://fiware-orion.readthedocs.io/en/master/user/geolocation/index.html. [opened Feb 2018].

[42] S. Antipolis, „News: ETSI launches new group on Context Information Management for smart city interoperability,” ETSI, 11 January 2017. [Online]. Available: http://www.etsi.org/news-events/news/1152-2017-01-news-etsi-launches-new-group-on-context-information-management-for-smart-city-interoperability. [opened Feb 2018].

[43] „GSMADeveloper,” Github, [Online]. Available: https://gist.github.com/GSMADeveloper. [opened Feb 2018].

[44] „About Us: What is OCEAN,” OCEAN, 2010. [Online]. Available: http://www.iotocean.org/about/. opened 26 02 2018].

[45] „Software: LAAS-CNRS,” [Online]. Available: https://homepages.laas.fr/monteil/drupal/node/36. [opened 26 02 2018].

[46] „Tutorial: IoTDM: Main,” Cisco, [Online]. Available: https://wiki.opendaylight.org/view/IoTDM:Main. [opend 26 02 2018].

[47] "„EU code of conduct on agricultural data sharing,” Copa - Cogeca | European Agri-cooperatives.

[48] European Union's Horizon, „Synchronicity,” 26 02 2018. [Online]. Available: https://synchronicity-iot.eu/.

[49] Weiting ZHANG Hongye YANG Wentao FENG Rui WANG, "Application Study of Greenhouse Environment Monitoring System Based on ZigBee Technology," 亚洲农业研究：英文版, vol. 9, (2), pp. 39-43, 2017.

[50] Fuping WANG Panpan FENG, "Design of Intelligent Irrigation Monitoring System Based on GPRS and Zigbee," 亚洲农业研究：英文版, vol. 7, (6), pp. 97-100, 2015.

[51] Z. Zhang et al, "Remote monitoring system for agricultural information based on wireless sensor network," Journal of the Chinese Institute of Engineers, vol. 40, (1), pp. 75-81, 2017.

[52] S. P. Goyal and D. A. Bhise, "Zigbee Based Real - Time Monitoring System of Agricultural Environment," International Journal of Engineering Research and Applications, vol. 4, (2), pp. 06-09, 2014.

[53] X. Ming, "Research and Design of Intelligent Agricultural Management System Based on Zigbee," Applied Mechanics and Materials, vol. 644-650, pp. 1372, 2014.

[54] Q. G. Yao and Y. L. Liu, "Design of General Agricultural Wireless Monitoring System Based on ZigBee," Applied Mechanics and Materials, vol. 380-384, pp. 811, 2013.

[56] L. Ma, H. L. Yu and L. Y. Cao, "Agricultural Information Remote Collection System Based on Zigbee Research," Applied Mechanics and Materials, vol. 651-653, pp. 1515, 2014.

[57] „Geographical Information System for Agricultural Plots - SIGPAC,” Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente , [Online]. Available: http://www.mapama.gob.es/es/agricultura/temas/sistema-de-informacion-geografica-de-parcelas-agricolas-sigpac-/default.aspx. [opened May 2018].

[58] H. Butler, M. Daly, A. Doyle, S. Gillies, S. Hagen en T. Schaub, „The GeoJSON Format,” Internet Engineering Task Force (IETF), August 2016. [Online]. Available: https://tools.ietf.org/html/rfc7946. [opened May 2018].

[59] „Documentation: Getting Started,” oneM2M, [Online]. Available: http://www.onem2m.org/developers-corner/documentation/getting-started. [opened May 2018].

[60] W. Joachim, „Internet-of-Things Architecture IoTA Project Deliverable D1.2 - Initial Architectural Reference Model for IoT,” 05 2018. [Online]. Available: https://www.researchgate.net/profile/Walewski_Joachim/publication/247935429_Internet-of-Things_Architecture_IoTA_Project_Deliverable_D12_-_Initial_Architectural_Reference_Model_for_IoT/links/54ef2e0d0cf25238f93bdad4/Internet-of-Things-Architecture-IoTA-Pr.

[61] W3C, „Web of Things Description,” May 2018. [Online]. Available: https://w3c.github.io/wot-thing-description/. [opened May 2018].

[62] FIWARE, „Architecture: IoT Agent,” [Online]. Available: http://fiware-iot-stack.readthedocs.io/en/latest/device_gateway/. [opened May 2018].

[63] "Extending Mobile Networks into Rural Areas via Satellite," Gilat, MAY 2015. [Online]. Available: https://www.gilat.com/wp-content/uploads/2017/02/Gilat-White-Paper-Cellular-Extending-Mobile-Networks-into-Rural-Areas-via-Satellite.pdf. [Accessed 2018]