CEMA

Full deployment of agricultural machinery data-sharing: technical challenges & solutions

CEMA's contribution to deliver on a profitable sustainable agriculture

5 February 2020

EXECUTIVE SUMMARY

A key element to reach the full potential of digital farming is easy, protected, automated data sharing. This data sharing is realised by allowing automatic communication between digital platforms. This document explains how the agricultural machinery industry is planning to tackle all remaining technical hurdles whilst staying in line with the Code of conduct on data sharing by contractual agreement.

It starts with the general principle of restricting the data sharing to workable sets of value data only. The necessary filtering and classification happens to the maximum extent already at machine and machine cloud level. The OEM cloud must be the first access point for retrieving the data and not the machine level. It ensures the safety and security at machine level without tampering with the data rights of the farmer. The number of data formats must be restricted so they can be used by all platforms.

A maximum of innovation freedom should be retained at data platform level. Therefore the data sharing and cloud2cloud communication is realised through standardised Application Program Interfaces APIs. It allows a full system of systems approach where a farmer can get all information and all services in one central point – his preferred farm management and farm information management system.

Standardised data access and secured data flow, by means of certification, should significantly increase the level of trust of farmers and cloud manufacturers for data sharing.

And a dedicated agricultural data governance scheme will allow sharing of different types of data, e.g. highly protected data to farmers only, certified data for proof of compliance and open data for a general public, if the farmer agrees to do so.

Allowing also data transfer between systems by automatic consent, rather than between persons, will in future reduce the burden for users even further.

With these developments the full data potential can be exploited for a profitable sustainable agriculture.

Contents

1. Introduction

Agriculture 4.0, in analogy to Industry 4.0, stands for the integrated internal and external networking of farming operations. This means that information in digital form exists for all farm sectors and processes; communication with external partners such as suppliers and end customers is likewise carried out electronically; and data transmission, processing and analysis can be automated under the control of the farmer. The use of Internet-based portals can facilitate the handling of large volumes of data, as well as networking within the farm and with external partners.

There are many questions circulating on the out roll of agricultural 4.0. Main problem is that for a proper working of digital agriculture a number of big hurdles, as also raised in ICT-AGRI, still need to be taken:

- To obtain an integrated approach to agriculture and food that enhances the vitality of rural communities and protects the environment
- adapting the current business models to suit better a digital and smart agri-food landscape.
- To use data more effectively to optimise consumption
- To use data to empower consumers in deciding knowledgeably what to buy and why
- To use data more effectively to optimise sustainable production
- To ensure that data also empowers farmers in producing more aligned with the consumers' wishes, market trends and in building networks
- To provide traceability of the crop/animal from production to sales according to potential prescriptions.

All these hurdles are linked to 'data sharing'. Much data available could generate much more added value when it was shared, up the chain and down the chain. The role of each actor in the data chain must be clear and there must be assurance that added value is also shared. *The Code of Conduct on data-sharing by contractual agreement* is a first commitment by stakeholders in the agricultural production chain that creates such rules. But sharing with a digital profile rather than a physical person requires new rules, hence new attitudes. The Code of Conduct contains the lead principles that need to be integrated in technical solutions. **Yet, there are many remaining technical barriers that need to be eliminated to obtain easy, protected, automated data sharing and thus before there can be a true adoption of digital agriculture.**

With this document CEMA explains how the agricultural machinery industry is committed to provide support in eliminating the remaining technical barriers, whilst integrating the legacy developments, and in optimising the use of data. The result must be well informed and empowered farmers who can increase their profit margins whilst delivering on a sustainable agriculture.

2. Technical challenges to tackle in order to achieve a full deployment of data-sharing in agriculture

2.1. Introduction

When we use our phones and our laptops we take it for granted that the data that is exchanged can be read by so many apps. However for agricultural machinery to be connected to the world, many hurdles remain, which are listed here and explained in the next chapters:

- Define a limited set of value data to justify the development of a data eco-system in agriculture
- Have suitable data standards: These are standards which describe the format (semantics) and meaning (meta data) of data used in information systems by the food and agriculture sector. With these standards one can construct computer systems which (in theory) should make them compatible with each other, but also enable the publication and sharing of data for other purposes. For event data modelling another type of standards will be needed.
- Proper data categorization preserving the legacy inherited from 15 years of standard definitions (ISOBUS, AEF – Agricultural Industry Electronics Foundation). It is critical that compliant products today remain valid for more than 10 years, which is the average system change over period for agricultural machinery.
- Effective interoperability between existing data models/standards network infrastructure (hardware) to ensure full data sharing capabilities
- Ensure the security of the data streams (cybersecurity)
- Automated consent transfer for cloud2cloud data transfer with smart contracts

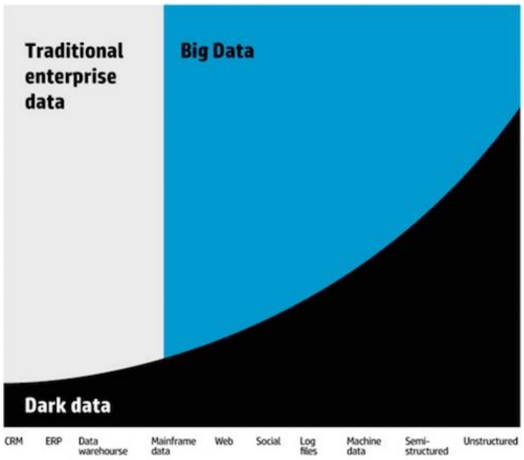
Besides, there are also more general problems to be solved:

- Use of suitable communication technologies and long-range frequency bands
- Privacy, trust, safety and security of machines in a connected world

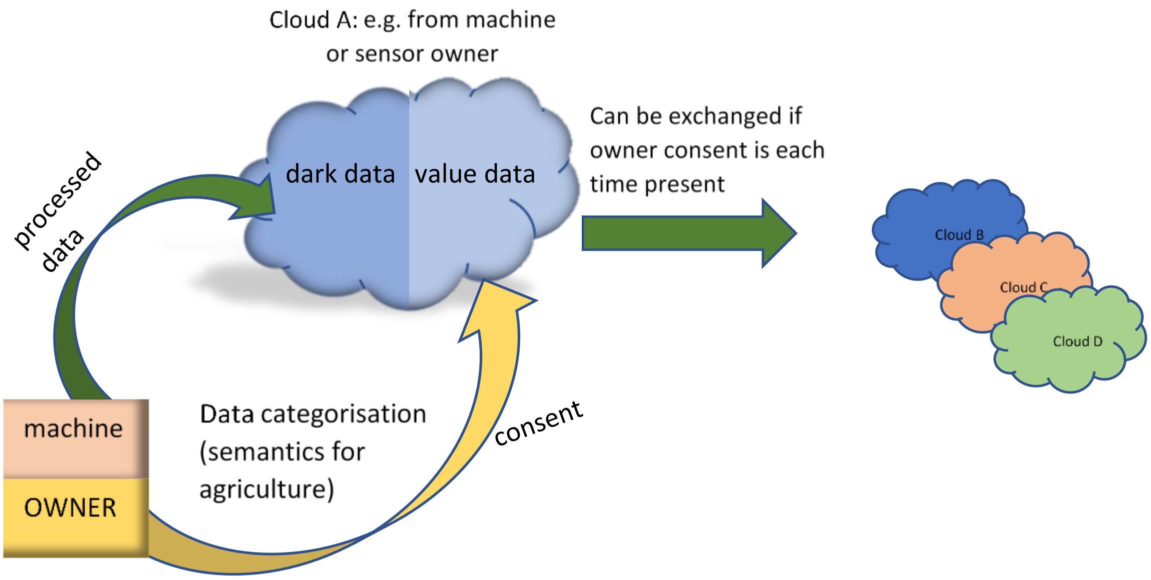
2.2. Agricultural value data through categorisation and filtering

Data categorisation and filtering is considered essential to get a workable set of value data and needs to be solved at OEM infrastructure level, whether at machine or cloud level, for proper data sharing.

Big data consists for 90% out of “dark data” (data which is acquired through various computer network operations but not used in any manner to derive insights or for decision making – the ability of an organization to collect data can exceed the throughput at which it can analyse the data) which is currently not good enough to make proper correlation, and to offer additional services.



Therefore a major portion of the big data (data sets that are so voluminous and complex that traditional data-processing application software are inadequate to deal with them) does not justify the development of a data eco-system (shared global data space). By a standardized process of alignment and harmonization of data from in-house information collection systems, data with value can be retrieved (named **'value data'**) for further sharing.


Cloud A: e.g. from machine or sensor owner
dark data
value data
Can be exchanged if owner consent is each time present
processed data
Cloud B
Cloud C
Cloud D
machine
OWNER
Data categorisation (semantics for agriculture)
consent

Picture: prefiltering to value data and value data sharing from the OEM cloud

It is recognised that much data of the field is gathered by agricultural machinery during the different farm operations. With better, more affordable sensors, the gathered data is increasing. The majority of new machines are equipped with sensors and with smart technology overall.

Therefore, machine manufacturers play a crucial role in the creating of value data.

By limiting the data exchange to "value data" the necessary resources are reduced for doing the data mapping and build a **high level architecture** allowing easy data exchange between platforms and use of external data in cloud service platforms overall and everywhere.

This High Level Architecture (HLA) is a family of related standards that together describe a unified approach and common architecture to constructing interoperable simulation systems. Besides data categorisation/filtering the other architecture elements identified are:

- **Interoperable processing rules:** to interpret the data in an identical manner across heterogeneous platforms
- **Standardised access** to data from machines through cloud to cloud.
- **Automated consent transfer** to move data from cloud to cloud without repeating the demand for consent.

2.3. The right data standards to make systems understand each other

Unfortunately there is no 'one-size-fits-all' solution. Software and data formats are developed for specific environments, functionalities. Historically different data and service providers have developed their own choice of architecture, language, data formats for their platforms. It means that proprietary data from machines are sent to proprietary service platforms from which it is difficult to exchange data to other platforms. The many different ontologies and semantics developed by research institutes in the past did not help so far to harmonise the situation. Due to their different background and point of view, each one had a specific idea about the data definition required for the reviewed topic/situation. This makes the data reconciliation almost impossible without a consistent data definition.

It could be argued why not make one single platform with one data format. However, it is expected that this would put a brake on innovation and in general the specificities of certain situations requires flexibility to develop new services. It is expected that most data and service platforms will allow access of other service providers for app integration and data to be exchanged easily. Therefore, it is critical that devices, systems and resources can receive and send but also understand the information coming from other devices, systems and resources. For that reason some concepts are clarified here:

Identification (of devices, systems and resources[1]): It serves to find and connect to a device or resource on the network, regardless of physical communication method (cellular, wi-fi, internet, …). The user should not be bothered with changing settings and servers. E.g.

- ❖ I have a tractor with VIN ZYX-123ABC-4567DEFG or PIN ZYX-123ABC-4567DEFG. How can I communicate with it in a secure way?
- ❖ I need data from a field with coordinates DD 51.1315281, 3.1600765000000592. Where can I find it?

[1] *Clarification on terms devices/systems/resources:*

*A system resource, or simply **resource**, is any physical or virtual component of limited availability within a computer system. Every device connected to a computer system is a resource. Every internal system component is a resource.*

*An input device sends information to a computer system for processing, and an output device reproduces or displays the results of that processing. Most **devices** are only input devices or output devices, as they can only accept data input from a user or output data generated by a computer.*

*The main software component is itself an **operating system** that manages and provides services to other programs that can be run in the computer while A computer is an electronic device that manipulates information, or data. A "**computer system**" is how engineers refer to the inner-workings of the computer. **Overall a system can receive, manipulate and send out information.***

Authentication (of people or systems): A way for people to verify their identity when accessing the network. This should also be extended to systems. E.g.

- In Belgium citizens can use a digital identity service called “itsme” (www.itsme.be) to authenticate with online systems. Itsme avoids having to use and remember different log-ins and passwords. Itsme is funded by the big banks and telecom companies.

Authorisation: This is the main function of data governance (see further). It defines which person can access what data or execute what function. It will be important to streamline authorisation, as access rights will need to be carried over across systems.

Semantics: Is the definition of data elements used in the communication. It can be considered an extended dictionary. E.g.

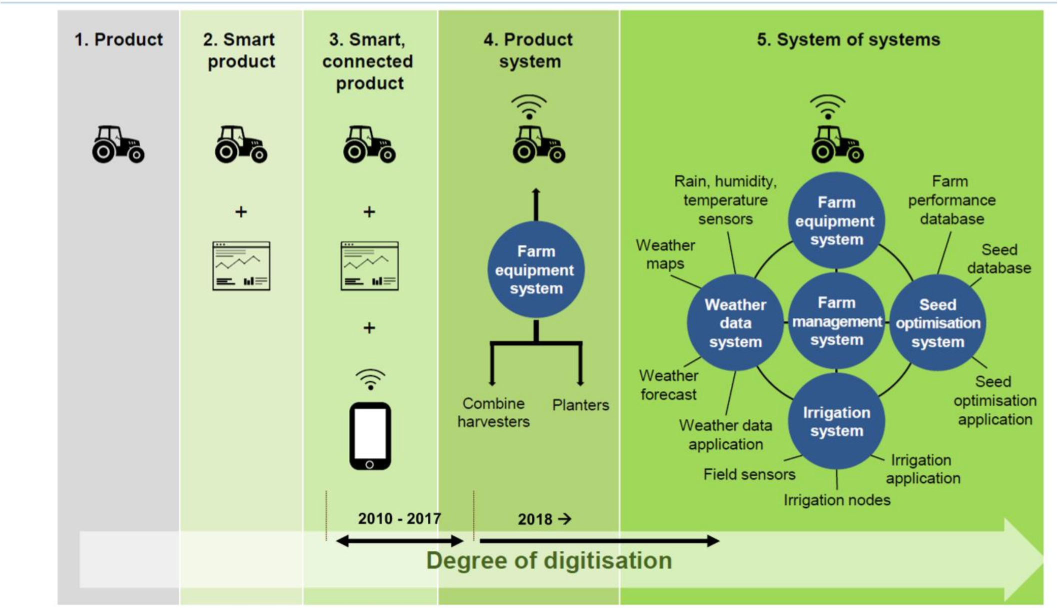
- Schema.org is a collaborative, community activity with a mission to create, maintain, and promote schemas for structured data on the Internet.

Ontologies and taxonomy: Defines what a resource is and what it can do, and how it relates to other resources.

Some work is already done in **data standards**. In the agrifood sector the most widely used and best known examples of standards are the ISOBUS (ISO11783) standard for agricultural machinery data, the GS1 EPCIS standard for product data encoded in barcodes and RFIDs, and the AGROVOC vocabulary for the annotation of agrifood research. GS1 XML are messaging standards compliant with the EDIFACT standard. EDIFACT is the international EDI standard developed under the UN for Electronic Data Interchange.

2.4. Effective interoperability between systems to ensure full data sharing capabilities

Lots of data is still in proprietary data formats. They are created in proprietary systems that can receive, manipulate and send out information between the elements (vehicles, FMIS…) of that system. However these different systems cannot communicate with each other. The full **system of systems** approach where a farmer can get all information and all services in one central point, is not yet fully achieved.



Picture: Source Harvard Business Review 11/20014; PA Consulting 2015

The key is to define all elements to **make the infrastructure as backbone of an operational system of systems** and this as key condition to fully deploy farming 4.0.

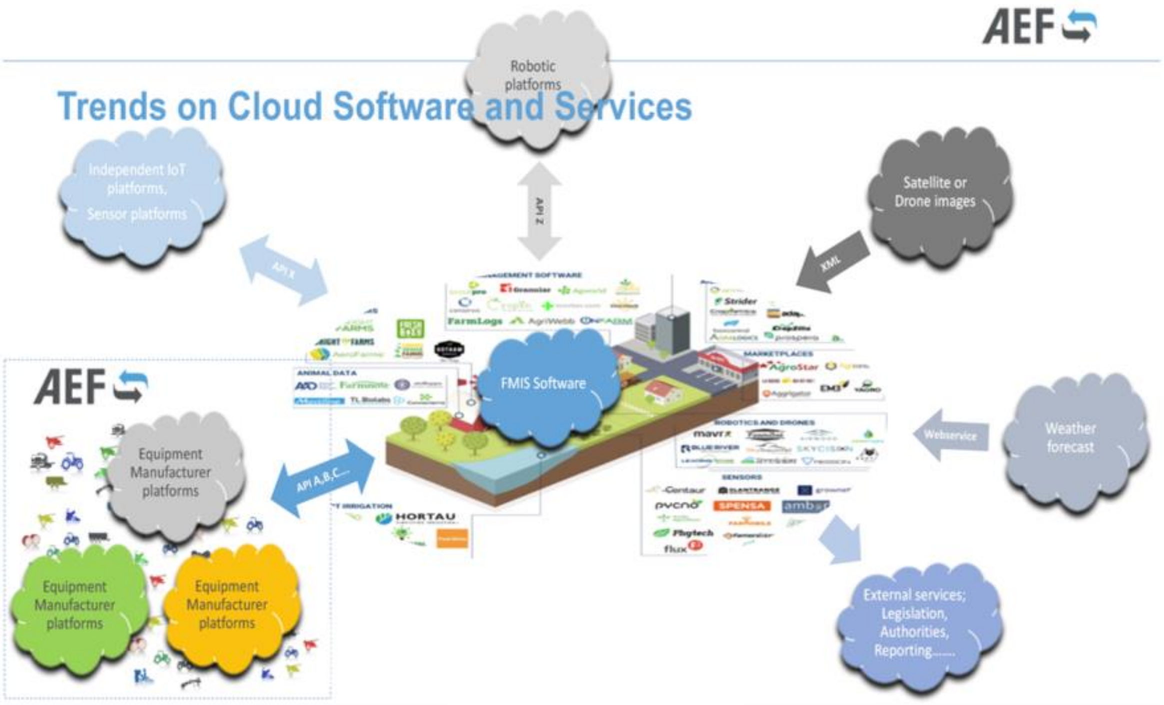
The **architecture of this data eco-system** (shared global data space) should rely on cross-industry standards for **interoperability** between systems. Many solutions are out there and many claim to be the best and only solution. However it is not so easy, and as often is the case a combination of solutions will be needed.

CEMA experts concluded that the most logical and suitable solution are **customized APIs (Application Program Interfaces)** for each service – as defined in standards. It does not ask for an alteration of existing cloud service platforms, only adding **an interface to exchange data** to the outside world.

Such **standardized API service layer** will help to allow access to good quality machine data by third parties when there is consent from the data rights owner (often the farmer towards e.g. advisors, independent repairers, insurance companies…).

For data originators like farmers the FMIS will be the digital tool to have an overview of all data sets and possible cloud service platforms. The aim is to give the farmer the freedom of choice by providing the technical means.

The industry, teamed up in the global organisation AEF - the Agricultural Industry Electronics Foundation, will work on this open source interface within the EU project ATLAS[2].


AEF
Trends on Cloud Software and Services
Robotic platforms
API Z
Independent IoT platforms, Sensor platforms
API X
Satellite or Drone images
XML
MARKETPLACES
ANIMAL DATA
FMIS Software
ROBOTICS AND DRONES
SENSORS
HORTAU
AEF
Equipment Manufacturer platforms
API A,B,C...
Webservice
Weather forecast
Equipment Manufacturer platforms
Equipment Manufacturer platforms
External services; Legislation, Authorities, Reporting.......

Picture: Courtesy of AEF 2018

[2] Atlas Project - The EU-funded ATLAS project aims to develop an open platform and create a sustainable environment for innovative agriculture. The project will address the lack of data interoperability in agriculture by combining the use of agricultural equipment with sensor systems and data analysis. https://cordis.europa.eu/project/id/857125

2.5. Safety and security of machines in a connected world: exchange of data from the OEM cloud.

It is considered beneficial that this data sharing process is done at the cloud level and not at the sensor level due to the pre-filtering and due to the flexibility at the cloud level, while the sensor level and the machine level can only be updated and be protected to a certain extent.

When connecting systems there is an information/task messages flowing in both directions. By installing a portal to access the vehicle wirelessly, there is the possibility that third parties can use that portal without consent of the owner. The vehicle is the source of much intel, from agronomic data of the farmers' fields to sensitive machine data that could reveal company intellectual property and secrets. Also does a vehicle act as a system of systems. Tampering with one system could impact the behaviour, lifetime and crucial safety functions of the entire vehicle. So shielding the information flow is of interest to both the owner and the manufacturer. With more and more autonomous functions on-board and full autonomous driving well underway it is a crucial aspect.

There are two ways to achieve this: through shielding of the individual vehicle or through the OEM cloud. The latter is preferred by the agricultural machinery industry as it ensures that there is a centrally guarded point where all requests for data arrive.

This does not change anything on the rights of people to get access to the vehicle data or vehicle parameters. So the farmer is entitled to receive the agronomic data, that he generated within his vehicle and everybody that has consent from the farmer to access the vehicle, e.g. for repair and maintenance, will receive that access. Through the OEM cloud, the information of the farmer can then be transferred and processed on the storage and/or service platform - FMIS of his/her choice.

2.6. Securing of the data streams (cybersecurity)

Securing the wireless data stream is key to generate trust between brands of systems exchanging data, not only for info messaging but also for task messaging. Therefore, how does the vehicle knows with 100% certainty it is the OEM cloud connecting? It is similar to V2V communication in agricultural tractor-implement combinations, even if it is not wireless. In 2019 AEF launched TIM (tractor-implement-management). This system does not only allow the exchange of information messages, to show things on the monitor of the tractor and allow the operator to give tasks to the implement through this monitor, but also to allow, on an autonomous basis, for task messages to be sent from the implement to the tractor. The goal is to optimise the performance of the implement. Therefore the latter can ask the tractor to change speed, give more power, adapt its trajectory, etc. The tractor within its boundaries will try to comply to these tasks without the intervention of the tractor driver/operator. The challenge is that it concerns vehicles of different brands.

That problem is solved with a PKI (public key infrastructure) which gives a key to the company, to different phases in the product process and to the individual vehicle. Without these keys, vehicles will not connect. It is the same principle built in smart phones to allow you to do transactions with your bank. The transaction will only be accepted if the key of the smartphone is verified and you have put in your code. AEF has developed an infrastructure that enables secure communication based on proven standards, such as mentioned above. This standardized solution – in conjunction with digital certificates – is necessary so that the implement can control certain tractor functions and can actively carry out the work process without the influence of the driver. Both machines trust each other so that the farmer can work more efficiently.

2.7. Data governance: rules on who get what data under which conditions.

It is crucial to have the technical means to allow seamless, secure data flow from platform to platform.

However, there is no “one-size-fits-all’ solution in terms of:

- What data can be shared,
- How well the data transfer and cloud handling of data should be protected,
- To whom the data can be shared,
- How to ensure the data quality in the chain.

There is a need for a pragmatic and fit for purpose approach.

On micro level, like company level, there exist the principles of data governance. The key focus areas of data governance include availability, usability, consistency, data integrity and data security and includes establishing processes to ensure effective data management throughout the enterprise such as accountability for the adverse effects of poor data quality and ensuring that the data which an enterprise has can be used by the entire organization. Often they work with a data steward that ensures that data governance processes are followed and that guidelines enforced, as well as recommending improvements to data governance processes. (source: Wikipedia)

Similar data governance rules could be set for cloud 2 cloud communication (manufacturer to manufacture data exchange) on value data coming from agricultural machinery. This standardised data access will be part of the process of building trust.

Some interesting principles to be worked out:

- The principles of the Code of Conduct on data sharing by contractual agreement’ should be further incorporated. It remains the basis document. But depending on the type of data there can be differences in the principles to be used or the level of implementation
- Data exchange should be bi-directional if that could create added value
- Access to data should be equally granted by platforms (no exclusivity – the set conditions by the platform apply to all interested parties)
- Main focus is on agronomic data
- Data will always be taken from the primary source to ensure the traceability and the data quality
- Data will not be used for reversed engineering.

The first outcome could be integrated in this Code of Conduct on cloud 2 cloud communication/connectivity in agriculture, containing the essential requirements, to be further worked out into technical standards that are the basis for trust for data sharing between clouds. Industry Cloud certification systems could be worked out that guarantee the necessary level playing field for access to data for platforms and ensure the necessary data quality. As an open system, further data aggregation in the chain could build on the existing certifications.

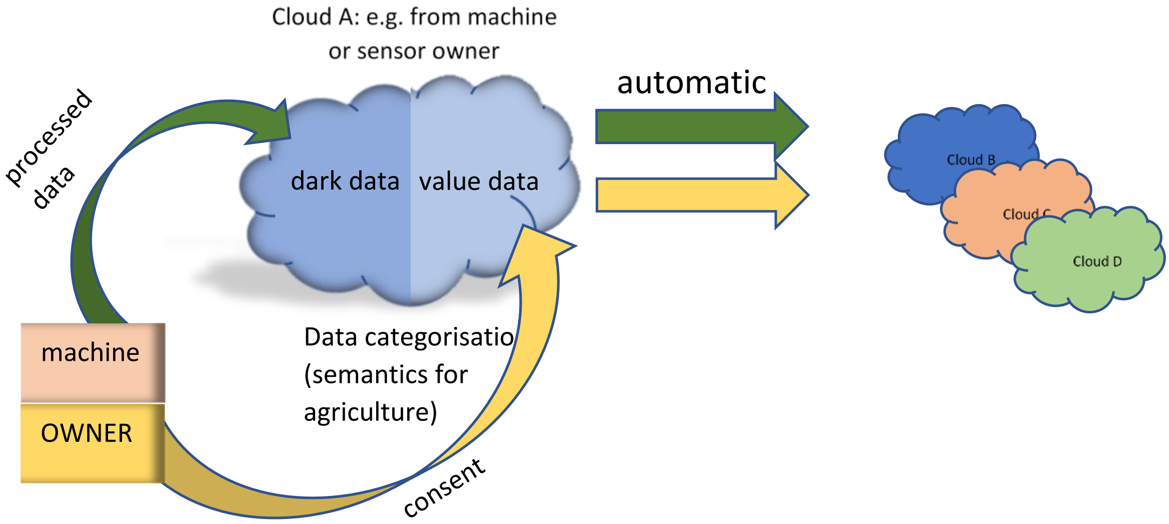
This way there could be highly restrictive data for the farmer only, certified data for proof of compliance, and open data for the research community, for service providers and for the general public.

In a first phase there should be a short list of value data from a specific agricultural area, considered fit for sharing, on which there can be investigated to whom to share and under which conditions both in relation to the data itself and in relation to the beneficiary. This list can grow over time and be extended to several areas of agriculture.

2.8. Automatic consent for data transfer

Within the code of conduct there is general agreement that the data originator, often the farmer (the one that performed or ordered the field/farm operations that generated the data), has the rights on the data. So he decides if the data is released and to whom.

If consensus is given directly from the machine/sensor/data owner to one cloud system/platform there is no issue. If a data originator shares data to anyone when certain conditions are met it would be burden that he/she would have to give its consent for each interested platform. The idea is that consent could also be transferred from platform to platform, This can be arranged by having a certification scheme for platforms applying API cloud based standardization. As a result clouds can pass on this consent to each other without requesting a consent again from the data rights owner.



Picture: automatic consent transfer

With data categorisation taking place before any analysis, the majority of dark data is turned into useful value data. Furthermore, with automatic consent, transfer through compliance with the standard (certification) for the different cloud systems, **a cascade of consents** is possible. This will also open the door for the use of **automated data analysis** (e.g. based on AI) **on anonymised (non-personal) data**.

2.9. Use of suitable communication technologies and long-range frequency bands

For proper data sharing, the data must get into the cloud. But getting signal in rural areas is a real issue. And it is not about the villages in rural areas. Connecting households in rural areas to broadband internet is a first priority of many national and regional governments. But that does not mean that a farmer who lives remotely gets connected, let alone that his fields are covered. Providing 4G full coverage everywhere would already be a major step forward. In doing so focus must be on the lower bandwidths 700 (5G), 800 (4G) 900 (3G) MHz. These signals can cover larger areas (up to 15-20 km) which makes that less hardware is required. Partnerships could be set up between telecom and other agricultural industries like the agricultural machinery industry to complete the network of antennas.

In terms of alternatives there are commercial initiatives to build low power wide area networks (LPWAN) with wireless communication technologies like NB-IoT, LoRA and Sigfox. They do not need a cellular connection. These are perfect for standalone sensors that remain e.g. in the soil for years. With the low power needed to send signals over large distances, the battery life is extended. It is expected that 5G will shake up the entire LPWAN landscape. It promises low-latency, low-power, and high data transfer rates—a previously unattainable combination. Problem with these LPWAN technologies is that the information transfer is slow but in many applications that is not necessary.

The agricultural machinery industry, by means of AEF, has chosen for application for wireless Infield communication by using the IEEE802.11p standard, also called WLANP. It builds on the standard for WIFI that we all use at home, but the range is bigger (up till 1.5 km) and the connection faster. A part of the automotive industry, joint in the CAR2CAR consortium, is still planning to roll out vehicle2vehicle (V2V) communication using WLANP, called ITS-G5.

Also for agriculture the WLANP will serve for V2V but also to transfer data to the farm. It will ensure that information but also tasks are transferred seamlessly allowing better coordination and organisation of the work in the field and transfer of data to the closest cellular hub or fibre network for it to be uploaded to the cloud.

3. The role of agricultural machinery manufacturers in data sharing

3.1. Willingness to share data

Much debate has been spent on the question of data sharing and whether legal obligations should be in place. The main point of the discussion is whether persons and businesses are willing to share data without it.

To clarify the point we can refer to the report of the Commission on data sharing[3]. Questions of data supply and data sharing for re-use need to be addressed in two situations: business-to-business (B2B) and business-to-government/public sector (B2G). Focussing on B2B the Commission identified a number of principles as also outlined in the ‘Code of conduct on data sharing under contractual agreement’:

a) Transparency
b) Shared value creation
c) Respect for each other's commercial interests

[3] Study on data sharing between companies in Europe: Everis report for the European Commission 2018 - ISBN 978-92-79-77360-0 doi: 10.2759/354943

d) Ensure undistorted competition
e) Minimised data lock-in by data portability

B2B data sharing and re-use can be generally understood as making data available to or accessing data from other companies for business purposes. Companies share and re-use data among them to enhance their business opportunities and improve internal efficiency.

The main particulars of data sharing B2B:

- Companies that engage in B2B data sharing do not necessarily grant access to their complete datasets. The proportion of data shared by companies usually depends on their business strategy.
- The term ‘sharing’ should not be understood as ‘for free’. Data can be shared against a payment, through the provision of a service, or for free
- Companies ultimately decide with whom they wish to share their data with, and for what purpose. Although there may be legislation in force that regulates access to certain data, companies have autonomy and control over the data they want to share and in relation to the usage conditions they want to set.

B2B data sharing and re-use are expected to significantly grow in a near future. Companies not yet engaged recognise the benefits of these activities and express their intention to start sharing and re-using data in the next five years. The Commission study also found that companies that do not invest a critical amount of money in accessing real-time or positioning data may be missing business opportunities.

The ‘companies’ mentioned can be the farmers and the mobile machinery producers.

It is in everybody’s interest that data is shared. In the particular case of agricultural machinery data, machinery manufacturers recognise the right of farmers on protecting/sharing the data generated by the machines as outlined in the Code of conduct. Above all manufacturers want to share data with farmers so a maximum profit can be obtained from the smart technologies they buy. Manufacturers also use the machine data and some agronomic data with a view to optimise individual machine efficiency and make improvements to new models. However the farmer’s data will not be used without his consent.

It must be iterated that the main problem is not the willingness to share data but the technical gaps still to be solved to allow the easy, protected exchange of data, brand independent.

3.2. Open and fair data that can be shared from agricultural machinery

The ‘FAIR Guiding Principles for scientific data management and stewardship’ were published in Scientific Data in 2016.

FAIR is an acronym that stands for **Findable, Accessible and Interoperable and Reusable**.

As indicated before a lot of machine data is dark data. Often it concerns communication messages between systems or very specific parameters, sent to systems’ ECUs. Most of that data cannot be shared as it could reveal the company’s engineering secrets. A lot of money is invested in making the different systems of a machine works smoothly together, optimising comfort of use, energy efficiency, etc.

Agronomic data is the kind of data most shared, being extracted from a field, through a dedicated operation like soil cultivation, crop care or harvesting; or livestock through an operation like milking e.g.

But some machine data is of use to farmers like the fuel used and some diagnostic data that can reveal the severity of a warning of malfunction.

When data can be shared there is a difference to be made between open and fair data. FAIR data and open data are different, although there are similarities. The key difference is that open data should be available to everyone to access, use, and share, without licences, copyright, or patents. It is expected that open data at most should be subject to attribution/share-alike licenses.

FAIR data, however, uses the term **"Accessible"** which means accessible by appropriate people, at an appropriate time, in an appropriate way. This means that data can be FAIR when it is private, when it is accessible by a defined group of people, or when it is accessible by everyone (open data). It depends completely on the purpose of the data, where the data currently is in its lifecycle, and the end-usage of the data. For example, new experimental data may only be accessible by the generator and their group to start, then with consortia partners as the findings become refined, and finally with the public upon publication. Personally sensitive data may never be publicly accessible and usable. Commercially sensitive data may be held privately for stretches of time after collection and interpretation. Users are also free to use more restrictive licenses to govern how the data may be reused.

FAIR also explicitly includes other characteristics:

Findable: where data should be able to be found by appropriate people at appropriate times. This can include shared folders, drives, private databases, public databases or more. It really depends on what part of the data life cycle the data is currently in. The data will likely transition through a few of these different options during its lifecycle.

Interoperable/Re-usable: these characteristics refer more to how the data is formatted (e.g. standard formatting), whether the software for interpreting/interrogating/using the data is available (e.g. freely, with a license etc.

In agriculture open data is considered 'open public data', therefore coming from sources that generate data for public use. That can be satellite images, weather data, soil maps, etc. The data from farmers are seen as fair data. Farmers will share the fair data by consent to input manufacturers to retailers or to the government. Field data sharing with government will be increasingly used to comply with the different legislations. Already today governments are in possession of the bulk of agricultural data. In this B2G relationship the conversion of certain fair data into open data will have to be part of a strategy of the government to generate added value for the general public. The compensation of farmers for the value added should be taken into account.

Hence, using knowledge wisely and act accordingly is of course a responsibility for each stakeholder in the chain, but access to data and access to added value created from data like insights in the process (knowledge) will need a higher architecture to ensure that each right is respected in relation to the Code of Conduct. It requires much more in-depth analysis of particular situations.

And this added value from data can be manifold. A manufacturer that uses machine and agronomic data to optimise an individual machine or learns for next updates/models is an accepted current practice. When this manufacturer would use machine and agronomic data to create additional value not related to the machine use but the farm operation/ management, this value must also be shared to farmers in the form of discounts or insights in results and can only be done with his consent.

A clearer high level strategy should outline what data and under which criteria and preconditions for use could be used in a broader setting to give added value to the society. Much data will continue to flow down the food production chain, even all the way to the consumer. Later is willing to pay more if he knows more of the product origin, and the safety precautions and environmental criteria used.

It is therefore crucial to define more clearly the value data. It should be a non-exhaustive but clearly defined list on which further considerations can be made of the principles under which certain data can be shared. Some of that data could then serve as open (public) data after processing and after agreement with public authorities. Some of the data could follow the food chain to the end-customer, again under the right principles of use. Finally it can be questioned whether such data flow should not happen in both directions.

3.3. Defining a legal framework

The preferred end-result of any legal exercise for the agricultural data market is a **Code of Conduct on connectivity** containing essential requirements like the EU includes in the NLF (New Legislative Framework) legislation. Standards can specify the details but manufacturers should not be bound to use the standards. Though highly recommendable and increasing the presumption of conformity, it is important to avoid problems like with the RED (Radio Equipment Directive) where the implementation gave problems as the necessary standards were not finalised on time

A good example is the Machinery Directive when it relates to the safety of machines. Idea is to extract the necessary ESSR (essential safety and security requirements) related to connectivity.

Common technical specifications will be a good base for further actions e.g. on safety of autonomous functions or to elaborate on a new data ecosystem (a shared global data space) in the cloud, ready for the application of AI (Artificial Intelligence). The main tool 'machine to cloud communication', to achieve the latter, is the first step.

This is without prejudice to already applicable legislation like the GDPR.

4. Other considerations for full deployment of data sharing in the food chain

There are some additional aspects that need to be incorporated in a clear political strategy to get a full deployment of data sharing in the food chain and therefore reach the full potential of agriculture 4.0:

Take up of smart technologies: there is much technology already available that gives detailed localised feedback on the agricultural soils, on the crops farmers are growing and on the impact of all their actions and the inputs they apply. Thus, there is also much technology on the market that allows to act accordingly and precisely based on that information. Unfortunately, uptake is slow and overall low. Indeed, there are some crucial problems to be solved on the easy dataflow as depicted above but there is more to it than just some technological barriers such as the need for a proper analysis of the market problems and more in particular on the rigidity/resistance for uptake. Some elements as earlier analysed are trust for data sharing and a lack of certain data.

Investments in smart technologies: it is not only for farmers to be interested in smart technology but also the investment funds to be available to farmers to make the additional investments.

Industry investment: especially SMEs should not miss the boat and invest in engineering that allows their technological solutions to be future proof and provide digital added value to their very specialised equipment.

Monitoring and traceability: there are many goals to be met in agriculture, from suitable field practices including timing of input application, prevention of erosion, prevention of compaction, to environmental goals, CO2 reduction, waste management and circular economy etc. In the past many of these targets had to be met on the agriculture primary production. The result is more administration. It does not necessarily have an impact on the prices for the European products. The link with retailers and consumers was far away. With improved monitoring through sensors and FMIS, and traceability of data flows related to the production process, a complete different approach is possible. As a consequence, the more advanced policies will go for improved monitoring and traceability of all aspects of food production looking at all inputs and outputs, farming practices but also food processing aspects and logistics. Targeting the final product is therefore a better idea to steer buying and eating habits.

This traceability down the chain can be done by blockchain or other suitable technologies to ensure that the date packages from the different sequential and logical steps within the process are traceable and cannot be tampered with.

If this tracing can go from Farm to food, it can also go from food to farm. Certain consumer behaviour can be of interest to farmer to optimise their production, change their production methods, include additional measures like greening or landscaping, and choice of crops. Again details should be worked out on what data could be exchanged and the criteria/preconditions of this data exchange. If consumers want to have the notion that their buying behaviour can change the way agriculture is practiced, this direct link must be established. By using secure channels for traceability it can also automatically secure the rights on data within the chain.

****

For further information, please contact:
Dr Ivo Hostens
CEMA Technical Director
secretariat@cema-agri.org

About CEMA

CEMA (www.cema-agri.org) represents in total 4,500 manufacturers of agricultural equipment consisting of large multinational as well as numerous small and medium-sized enterprises (SMEs). The sector has a total annual turnover of €26 billion and provides employment for 135,000 people directly in the sector and another 125,000 persons indirectly in the distribution and service network.