CONVENTIONS FOR IMPROVED SUSTAINABILITY OF MULTI-VENDOR IOT SOLUTIONS

DEVELOPED BY THE ALEXANDRA INSTITUTE AND AARHUS UNIVERSITY
IN COLLABORATION WITH PARTNERS

Supported by DigitalLead

DigitalLead.

AARHUS UNIVERSITY

ALEXANDRA INSTITUTE

TABLE OF CONTENTS

01	PURPOSE AND TARGET AUDIENCE	page	3
02	BACKGROUND AND PARTNERS	page	4
03	WHAT IS THE PROBLEM? SUSTAINABLE IT	page	5
04	EU IS PAVING THE WAY FOR LONGEVITY OF PRODUCTS	page	6
05	FOCUS AND FOUNDATION OF THE FRAMEWORK	page	8
06	WHAT IS A MULTI-VENDOR IOT SOLUTION?	page	9
07	DIFFERENT MODELS FOR PURCHASING IOT SOLUTIONS	page	10
08	INTERVIEWS WITH MUNICIPALITIES AND UTILITY COMPANIES	page	13
09	IOT-VENDORS' RESPONSES TO THE CLIENTS	page	15
10	BRINGING TOGETHER CLIENTS AND VENDORS	page	17
11	CONTRIBUTION	page	26
12	CONCLUSION	page	27

01 PURPOSE AND TARGET AUDIENCE

TARGET AUDIENCE: CLIENTS PURCHASING IOT SOLUTIONS AND IOT-VENDORS

The framework is building upon existing frameworks and guidelines on sustainability, circularity, repairability, and interchangeability (see more on page 20.

The framework presents a model for defining the important interfaces between different components in multi-vendor IoT solutions, where it is important to ensure modularity and interchangeability to make sure that the full product can be repaired and updated over time. Thus, the framework is specifically building on top of the Danish Standards DS-INF 176:2021 *Guide for Sustainable, Digital Transformation in Denmark*[1] (see more on page 26). In this guide 7 recommendations are outlined and the second one is *Build with Interfaces*. The present framework is specifying this recommendation presenting a model for the modular layers in a multi-vendor IoT-solution.

1 https://www.ds.dk/da/download/guide-til-baeredygtig-digital-omstilling-i-danmark

02 BACKGROUND AND PARTNERS

The present framework is the outcome of an innovation project investigating how multi-vendor IoT solutions can become more sustainable and longer-lasting. IoT solutions too often 'die' prematurely. One key reason for IoT solutions to fail is that, often, multiple vendors deliver different parts of the solution (sensors, network, data analytics, visualisation, etc.). So one of the weak points of the multi-vendor value chain is to ensure that the different parts will continue to work together over time.

Thus, this framework explores the weaknesses and potentialities in multi-vendor solutions. The purpose of the framework is to provide guiding principles, which can improve sustainability and strengthen the longevity of multi-vendor IoT solutions.

The project *Connectivity conventions for improved sustainability of multi-vendor IoT solutions*[1] was funded by DigitalLead. It was conducted in 2022–2023 by the two knowledge institutions – the Alexandra Institute and Aarhus University – in collaboration with partners from industry and municipalities.

1 https://digitallead.dk/innovation/projekter/connectivity-conventions-for-improved-sustainability-of-multi-vendor-iot-solutions/

03 WHAT IS THE PROBLEM? SUSTAINABLE IT

There is no doubt that the ICT sector – and IoT more specifically – contribute positively to the green transition and helps to reduce CO2 emissions in other sectors such as energy, transport, manufacturing, etc. However, while the amount of IT and data is growing exponentially, it is also vital to ensure that the ICT sector itself is also moving towards becoming green and sustainable.

Luckily, there has been quite some focus on the energy consumption of data centres in recent years. The hardware components are becoming increasingly energy-efficient. There is a growing focus on repair and reuse of electronics, and attention is gradually shifting towards the development of energy-efficient software and network technologies. However, the increase in demand by far exceeds the efficiency gains, so more efforts are needed.

We hope this framework will be a tiny contribution. The focus is on multi-vendor IoT solutions and specifically on the problem that too many of these die prematurely, so how can we pave the way for more sustainable and longer lasting multi-vendor IoT solutions?

Environmental impacts of the ICT sector

- **Responsible for 4% of the world's CO2 emissions. This is twice the emissions of the aviation sector.**
- **Consumes as much energy as the world's 3rd largest country (after USA and China).**
- **In 2021 the sector produced 57.4 million tons of electronic waste – more than the weight of the Great Wall of China**

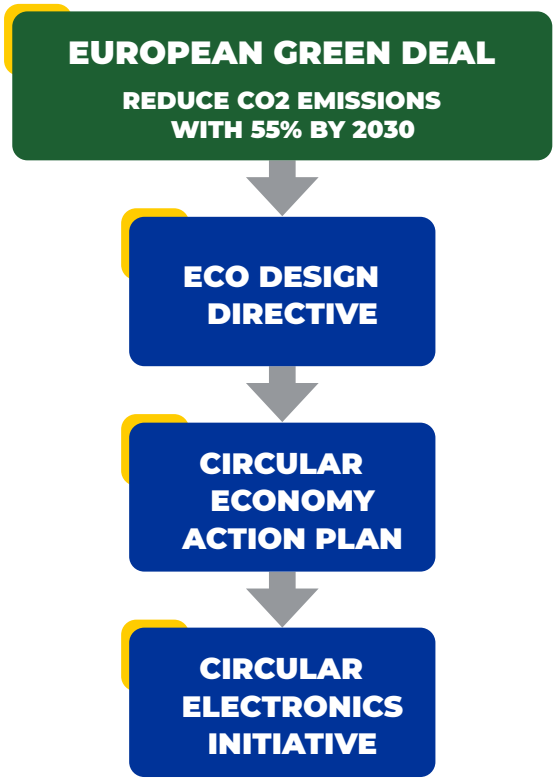
04 EU IS PAVING THE WAY FOR LONGEVITY OF PRODUCTS

In 2009, the EU Commission implemented the *Eco Design Directive* covering 31 product groups. The directive currently only covers energy-related products.

In 2022, a new *Ecodesign for Sustainable Products Regulation (ESPR)*[1] was proposed. It builds on the *Eco Design Directive* but will include many other product categories and have more comprehensive objectives. This will lead to increased requirements on sustainability and environmental impacts that product developers must comply with.

In March 2020, the European Commission presented a new *Circular Economy Action Plan* under the *European Green Deal*, in which it announced a *Circular Electronics Initiative* that aims to address the shortcomings in durability, circular design, presence of hazardous and harmful substances, recycled content, reparability, access to spare parts, upgradability, e-waste prevention, collection, reuse and recycling as well as the issues of early obsolescence.

This means that the electronics industry, and IoT more specifically, already now needs to embrace these coming regulations.



1 https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/sustainable-products/ecodesign-sustainable-products-regulation_en

EU IS PAVING THE WAY FOR LONGEVITY OF PRODUCTS

CIRCULAR ECONOMY ACTION PLAN

- **durability** (e.g., minimum lifetime of products or critical components)
- **reparability** (e.g., availability of spare parts and repair manuals, design for repair)
- **upgradeability**
- **design for disassembly** (e.g., easy removal of certain components)
- information (e.g., marking of plastic parts)
- ease of reuse and recycling (e.g., avoiding incompatible plastics)
- greenhouse gas and other emissions

CIRCULAR ELECTRONICS INITIATIVE

- **regulatory measures for electronics and ICT** including mobile phones, tablets and laptops under the *Ecodesign Directive*
- **implementation of the 'right to repair', including a right to update obsolete software**
- regulatory measures on chargers for mobile phones and similar devices (including the introduction of a common charger)
- **improvement of the collection and treatment of waste electrical and electronic equipment**
- review of EU rules on restrictions of hazardous substances in electrical and electronic equipment

05 FOCUS AND FOUNDATION OF THE FRAMEWORK

HYPOTHESIS

Based on previous experience with multi-vendor IoT solutions, the innovation project was built on the following hypothesis:

Many IoT-projects and solutions die prematurely because the many components (hardware, software, sensors, platforms, connectivity, etc.) in multi-vendor solutions are not designed to be replaced, repaired, and updated when parts of the system are to be changed or no longer work.

RESEARCH QUESTIONS

- What are the most important reasons why IoT solutions in municipalities and utility companies become obsolete over time?
- What are the biggest barriers for IT developers to design for more 'repairability' and 'interchageability'?

EMPIRICAL DATA

In order to investigate this hypothesis, the following empirical field work was conducted:

- 1 literature review
- 7 qualitative interviews with IoT-responsible personnel in:
  5 municipalities
  2 utility companies
- 2 online surveys with IoT vendors
- 1 workshop with IoT vendors
- 1 workshop was held where IoT vendors, municipalities and utility companies met to discuss how to ensure longer-lasting multi-vendor IoT solutions. In the workshop existing frameworks for sustainable product design were tested in order to develop the present design recommendations.

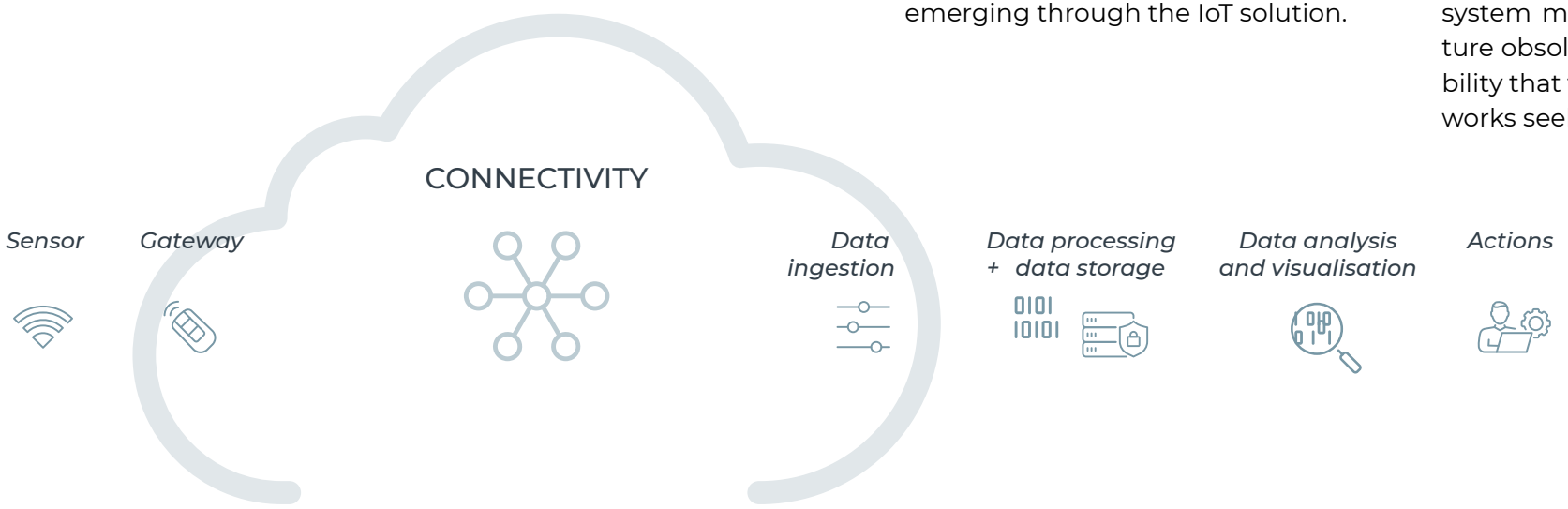
06 WHAT IS A MULTI-VENDOR IOT SOLUTION?

Before getting into the findings from the project, it is essential to understand what a *multi-vendor IoT solution* is.

An IoT solution is always made up of several components. As shown in the figure, an IoT solution can roughly be divided into: sensors, gateways, connectivity, data ingestion, data processing, data storage, data analysis, data visualisation and, lastly, some kind of actions happening based on the information emerging through the IoT solution.

In what is called *end-to-end solutions*, one company delivers the entire solution. However, the *start* and the *end* of the solution are a variable concept. More often, there are two or more vendors. There might also be a number of less visible sub-contractors.

This is what we call a *multi-vendor IoT solution*. In a multi-vendor IoT solution, responsibility for maintaining and updating the system is distributed, which often makes the system more vulnerable to premature obsolescence. It is this vulnerability that the current design frameworks seek to mitigate.



07 DIFFERENT MODELS FOR PURCHASING IOT SOLUTIONS

When municipalities, utility companies, and other customers – from now on collectively referred to as *clients* – submit tender bids and purchase new IoT solutions, they can choose different approaches.

See an overview of the different approaches on page 11.

Some choose to buy a complete end-to-end solution (model 1). Here, the customer will have very little insights into the different components and layers of the solution, and little or no possibility of repairing or replacing any part of the system by themselves (this is not the intention of this model).

The customer can also choose to play a more facilitating role and engage in a dialogue with more suppliers on how the solution should be designed and composed with components from several vendors. This role can either lead to a purchase from one single vendor, who might have subcontractors (model 2), or the customer can choose to buy the components separately and perform the integration on their own (model 3). In the last model 4, the customers more or less build the entire solution themselves. On this spectrum from doing nothing to doing everything, all models have pros and cons (read more on these in the *Guide til Bæredygtig, Digital Omstilling,* page 50) and should be respected for their respective strengths.

It is important to consider which model to choose. In particular, the models require different levels of maturity and internal competencies. Finally, independently of which model is chosen, one of the most important aspects is the quality of the interfaces between the different layers and components of the IoT solution.

For more on different models, the pros and cons, see Danish Standard's *Guide til Bæredygtig, Digital Omstilling, Recommendation 5* and page 50 onwards.[1]

1 https://webshop.ds.dk/standard/M346207/ds-inf-176-2021

COLLABORATION AND MANAGEMENT MODELS FOR PURCHASING IOT SOLUTIONS

SELF-MANAGED PROCESS

- Client purchases end-to-end solution.
- Direct sale or tender.

FACILITATING ROLE

- Client seeks and facilitates collaboration among suppliers.
- Direct sale or tender process with one supplier.

MANAGING ROLE

- Client seeks, facilitates and manages collaboration in the market.
- Manages integration.
- Public-private partnership.
- Split tender process.

IMPLEMENTING ROLE

- Client seeks, facilitates and manages collaboration in the market.
- Implements and integrates parts of or the entire solution.
- Split tender process.

This model is based on the model 'Samarbejds- og styringsmodeller' as presented in ***Guide til bæredygtig, digital omstilling i Danmark****, pp. 50, Dansk Standard 2021*[1]

1 https://www.ds.dk/da/download/guide-til-baeredygtig-digital-omstilling-i-danmark

EMPIRICAL FINDINGS

- Interviews with municipalities and utility companies
- Survey with IoT vendors
- Workshop with IoT vendors
- Workshop facilitating dialogue between customers and IoT vendors

08 INTERVIEWS WITH MUNICIPALITIES AND UTILITY COMPANIES

Based on 7 qualitative interviews with clients, it became apparent that a shift is happening towards taking a more active role in defining and designing IoT solutions. Previously, the clients were more likely to purchase end-to-end-solutions but have had negative experiences with vendor lock-in situations, involving proprietary solutions, each with their own interface and data locked into a single system.

MORE OPEN AND FLEXIBLE SYSTEMS

There is a lack of interoperability between systems, and all the clients want to have more open and flexible systems, allowing them to use data across services and integrated into one another. It is important that the vendors already work with open standards for at least some of the layers, and they want to have more ownership of data.

MORE COLLABORATION AND PARTNERSHIP

Furthermore, the clients express that the challenge with end-to-end and off-the-shelf-solutions is that they often fail to continuously match the clients' current problems. No one solution fits all, and the clients see a need for closer collaboration with the IoT vendors, engaging them actively in processes and in the understanding of the challenges that the IoT solution should solve.

This calls for more active and facilitating management models, where the purchase of an IoT solution is more about collaboration and partnership rather than being a simple customer/supplier relationship. The clients wish to collaborate with vendors who are open to a process, where both problems, use-cases, and solutions can be achieved through a collaborative development process.

WILLINGESS TO PAY MORE

Thus, for the clients, the path to more long-lasting, sustainable and valuable IoT solutions involves more tailored and flexible systems developed in a closer collaboration between vendors and clients.

One very important observation is that the clients are willing to pay more for more flexible, open, and tailored systems, because they are convinced that this will provide more value down the road. One interviewee said that it is important to shift focus from merely looking at the purchase price and, instead, consider *total cost of total ownership* or, even better, *total cost of value creation*. This includes the fact that the municipality assumes the ultimate responsibility if a service does not work anymore due one of the providers' end-of-business.

INTERVIEWS WITH MUNICIPALITIES AND UTILITY COMPANIES

We are done with fixed end-to-end-solutions. We have been locked into proprietary solutions too many times. We don't want 25 different systems where we cannot make value across data. I want to know what makes it attractive for IoT companies to go into close relationship and co-development with the municipalities.

(Municipality)

In the beginning, it was often end-to-end and closed solutions, but within the last couple of years, we see more and more a need for making more modular systems, where we have ownership of the system and direct access to data. This can either be a specification for one vendor, or it can be part of a multi-vendor project, where we take more active part in building the system and in collaborating with more vendors.

(Municipality)

The most important reason why we want to make the systems ourselves is that we believe that this is the only way we can become really good at employing and using IoT and data ourselves.

(Municipality)

We never just have a problem and then make a tender bid. We always engage in dialogue with companies about scoping the problem with us.

(Municipality)

We rarely buy a finished product, but it is always co-development – btw. vendor and municipality – and often also btw. more municipalities together.

(Municipality)

I am done with generic solutions because I do not believe that they can give value to our specific cases.

(Water and district heating utility)

09 IOT-VENDORS' RESPONSES TO THE CLIENTS

The results from the interviews were presented to 11 partnering companies. The companies participating in the workshop represent different types of vendors along the value chain, making up a multi-vendor IoT solution.

CLIENTS DO NOT HAVE THE TECHNICAL EXPERTISE

Some companies were very critical towards clients who did not want to buy existing end-to-end-solutions. All those vendors seemed to question why the clients wanted to tweak or even put together the system by themselves.

As the quotes illustrate, the vendors believed that it would lead to more expensive and worse solutions if the municipalities want to co-design and manage the systems themselves. Those companies did not believe that the clients have the right technical expertise to design, manage and run the systems on their own. Instead, the vendors believed that they should provide the right technology and management to scale up the systems for the clients in the future. The vendors would like to provide the clients with data, implying that the clients should be looking into handling and managing data rather than looking into architecting a hardware system on their own as operational infrastructure. The vendors voiced that there is a large issue of scoping, with the risk of the clients not scoping the problem well enough, leading to project issues.

STANDARDISED SOLUTIONS

During the workshop, it also appeared that most of the vendors were sure that they would make the best solution if they were to provide "the whole value chain". However, upon closer examination of the value chain that various vendors could provide, it became clear that their views of where the value chain for the solution begins and ends differed significantly, depending on the position of each vendor's main product in the value chain.

As opposed to the approach discussed with the clients, several vendors thus believed that the way towards more long-lasting, sustainable and valuable IoT solutions is to employ standardised solutions requiring less active involvement and management from the clients. It should be noted that even in a solution completely designed and operated by a company, the longer-term operation of the solution will face some of the same challenges anyway with e.g. sub-contractors and sourced components.

FACILITATION OF DISCUSSIONS BETWEEN VENDORS AND CLIENTS

Last but not least, an important finding in the workshop was that to help the vendors to scale up, there is a need for facilitating discussions between vendors and clients in order to ensure better tender bids and smoother collaboration processes, where each party has a better understanding of how to set requirements for the different parts of the multi-vendor IoT solutions.

IOT-VENDORS' RESPONSES TO THE CLIENTS

It is stupid of the municipalities to think they can do it all by themselves. They need someone with special competences in order to make a well-functioning and long-lasting system.

Why would the municipalities have a say in all the different elements in the IoT solution – they don't need to care about e.g. the connectivity part.

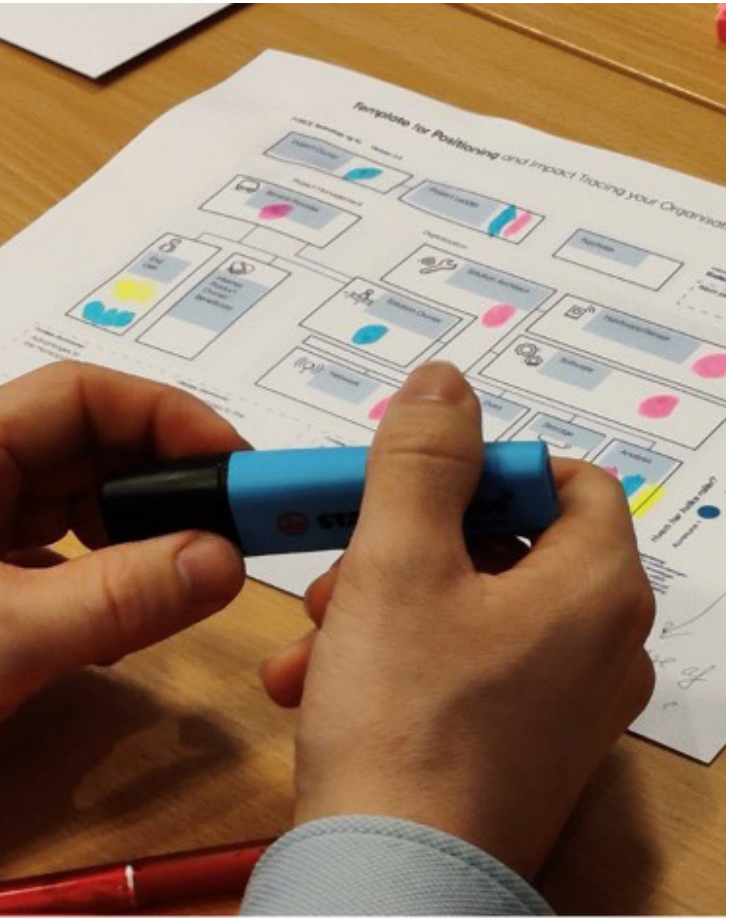
The IoT solutions will be much more robust if the municipalities leave it to a vendor to build, run and maintain the system, because the vendor will have the right knowledge and network to repair, update and exchange parts and pieces when necessary.

The municipalities should rather partner up with a commercial system vendor who can build manage, and maintain their solution.

The municipalities don't need to own the system – they only need to buy data and thus only need to specify the requirements for the data coming in. They don't need to care about how I collect them as long as I deliver.

Tailored solutions become way too expensive, and they do often not run as well.

10 BRINGING TOGETHER CLIENTS AND VENDORS



As described, the interviews and the workshop revealed apparently conflicting perspectives on how the clients and the vendors perceived the means for achieving more sustainable and long-lasting IoT solutions. During the project it became clear, however, that what was needed was a neutral setting, where the clients and vendors could meet and discuss how to create the best models.

Therefore, to validate the approach, a full-day workshop was organised. Two sessions were facilitated – one during which the clients were interviewed about their needs, concerns, and wishes for IoT solutions and one during which the vendors were interviewed about the same. These sessions had the purpose of listening to the other part.

Afterwards, the 20 participants were divided into four groups, where both clients and vendors from different parts of the value chain were included. Each group worked with a specific IoT solution proposed by the client participating in the group, who should now enter a collaboration negotiation with the present vendors.

As a tool, the participants could use *The IoT Actor Map* developed by KL – Local Government Denmark and FORCE Technology (see page 18).

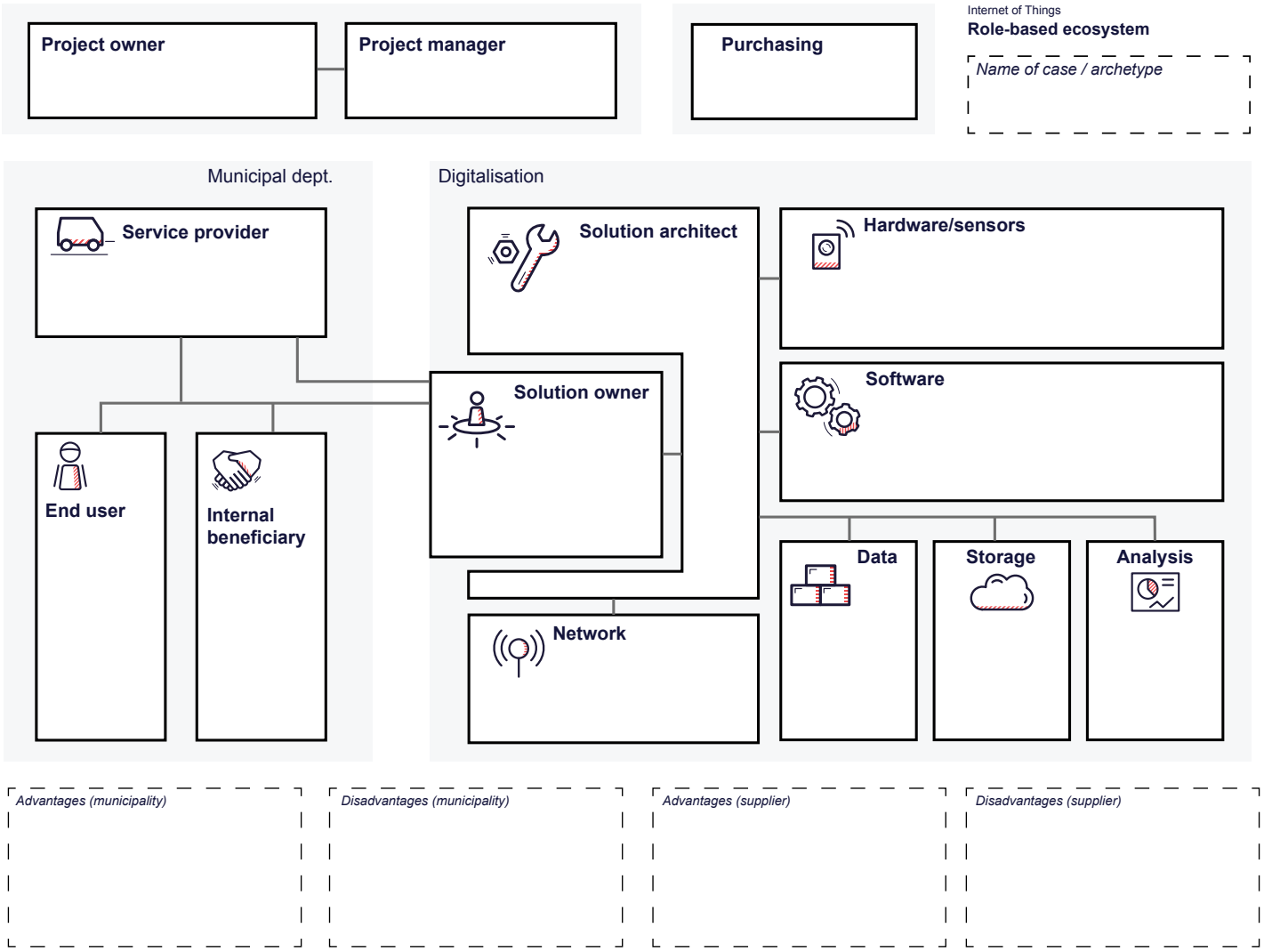
Together they should fill out which parts of the IoT solution each vendor or client was responsible for and thereby make the interfaces between actors and responsibilities clear. The purpose of this exercise was to facilitate a discussion about the different parts of the value chain and to ensure that clients and vendors agree on who delivers and who is responsible for which parts of the IoT solution.

This exercise made apparent how different parts could be made exchangeable or not. More importantly, the outcome is a good first step towards some clear technical interfaces to allow changing the start point of the solution, its endpoint, and allow modifying or replacing some elements over time without impacting the rest of the value chain.

We can recommend such a tool when a client and one or more vendors are entering into collaboration.

IOT: MAP OF ACTORS AND RESPONSIBILITIES

FORCE Technology and KL Version 2.0



The map serves as a tool for establishing consensus on who is responsible for each part of the solution. Colours represent client, developer and others. The participants mark the different areas of responsibility.

Municipality =

Supplier =

Others =

Guide:
1) Show the role distribution by colouring the fields and fill in e.g., names of supplier, department, etc.
2) What advantages/disadvantages do you see in this distribution?

TESTING AND ELABORATING ON TWO EXISTING FRAMEWORKS FOR IMPROVED SUSTAINABILITY FOR IOT PROJECTS

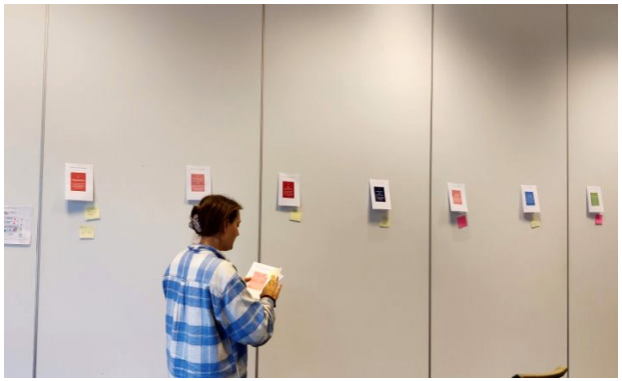
The second part of the group work was testing and elaborating on two existing frameworks that were also developed with the intention of leveraging the longevity, robustness and maturity of products:

IoT Principles Catalogue[1], developed by the Swedish Arkitekturgemenskapen[2], which is an informal network of municipalities and regions in Sweden. The framework is developed with the purpose of promoting good practices increasing the quality of IoT projects, and includes modularity as #1 principle.

Eco Design Directive[3], developed in EU is not specifically developed for IT or IoT but is a framework that will be made applicable in one way or the other to alle product categories. Being able to repair or upgrade parts of the solution is an essential principle in this framework too. See both frameworks on page 20.

The groups were asked to value how important each of the 15 principles from the two frameworks were for the specific IoT solution that they were working on. The groups were asked to pick the 8 most important principles. With post-it notes they explained why they picked the specific principles. They also had to do the same with the 7 principles left out.

This exercise confirmed the complementarity of the essential visions of the different frameworks, together with the layered modularity, which we support in this project, and also confirmed that the participants could operate with those principles.



1 https://inera.atlassian.net/wiki/spaces/AR/pages/2835054990/IoT+principles+catalogue
2 https://www.inera.se/tjanster/gemensam-arkitektur/arkitekturgemenskapen/
3 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02009L0125-20121204&from=EN

USING EXISTING FRAMEWORKS

IoT Principles Catalogue

Developed by Swedish *Arkitekturgemenskapen*

1 . MODULARITY
The IoT system enables the replacement of modules independently of each other.

2. OWNERSHIP AND RIGHT OF USE
Data, information and context-awareness in the IoT system are preserved during module and system changes.

3. INTEROPERABILITY
IoT system information models are built in horizontal overall level and specific vertical levels.

4. TREATMENT AND ENRICHMENT
The IoT system enables the processing and enrichment of information.

5. FLEXIBLE STORAGE
The IoT system supports data storage in different ways based on the nature and usage needs of the information.

6. TRUST AND SECURITY
The IoT system is capable of meeting a defined level of risk and consequence [to achieve the intended information security].

7. HANDLING OF PHYSICAL APPLIANCES
The IoT system can handle digital management of physical IoT devices and their connection to the IoT system.

8. VIRTUAL APPLIANCE MANAGEMENT
IoT system is capable of managing virtual IoT devices.

9. EVENT-DRIVEN ARCHITECTURE
The IoT system enables control and orchestration of event-driven information flows.

10. ACCESS TO DATA AND SERVICES
IoT system information, services and data are available for applications.

Eco Design Directive

1 Design for Upgradeability

2 Design for Disassembly

3 Design for Repairability

4 Design for Durability

5 Design for Digitalization of Product Information

THE POWER OF TECHNICAL LAYERS

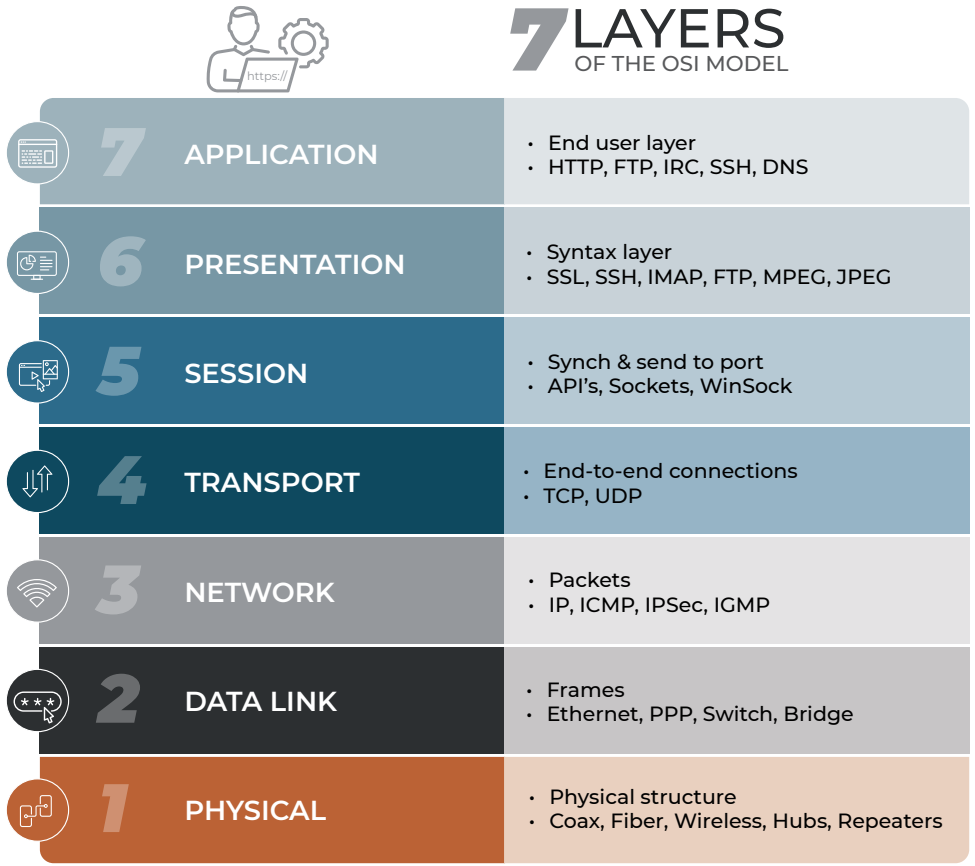
In our project, we have in particular focused on the *modularity principle,* and which conventions to use to achieve it. We have been especially inspired by the main architecture principle used by the Internet – which is also an ecosystem with many actors, many use-cases, and conflicting technical priorities. The success of the Internet is largely thanks to its main architecture principle, namely the Open Systems Interconnection model (OSI model) with its layers.

THE OSI MODEL

The OSI model allows replacing one technical layer by another technical implementation with other characteristics, without having to replace the layers below and above.

- For instance, HTTP, the main Web protocol, has traditionally run over TCP / IP, but HTTP/3 has changed to run over UDP / IP.
- Likewise, the IP layer has evolved from IPv4 to IPv6, to a great extent without having to replace the layers below and above
- From an end-user perspective, those technical changes have been mostly transparent, also for use-cases not anticipated by the technology providers.

While not perfect, this layered approach has been very successful over the years, with a good separation of concerns, modularity, adaptability, maintainability, etc.



STANDARD IOT LAYERS

A few different standards define the main layers of IoT solutions, such as:

- ISO/IEC 30141:2018:
  https://www.iso.org/standard/65695.html
- IoT-A Reference Architecture:
  https://dx.doi.org/10.1007/978-3-642-40403-0
- Industrial Internet Consortium (IIC) Reference Architecture:
  https://www.iiconsortium.org/iira/

Although not identical, and at different levels of complexity, those standards do share some of the same concepts, and the important idea of components and layers

In the future, we might be able to recommend a specific definition of the layers. For now, we recommend ensuring a reasonable amount, as illustrated in the following concreate examples

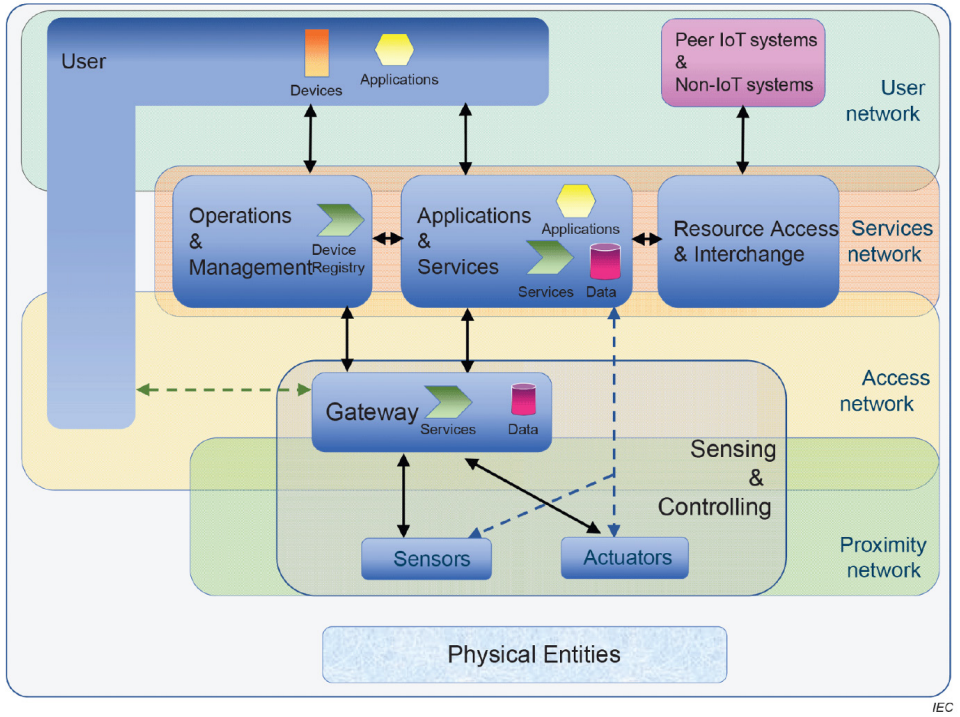


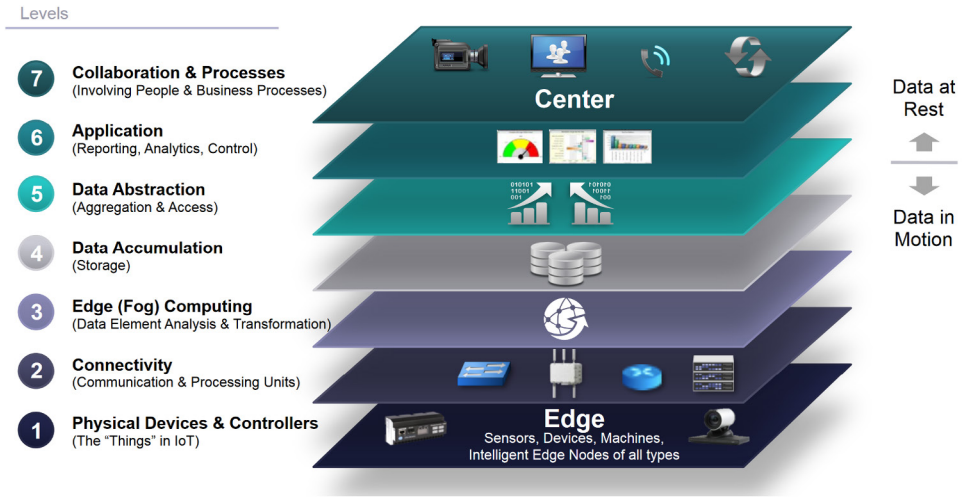
Illustration of networking view from ISO/IEC 30141

EXAMPLES OF COMMERCIAL APPLICATIONS

CISCO

This approach of dividing an IoT solution in layers has already been used for a long time by major commercial actors:

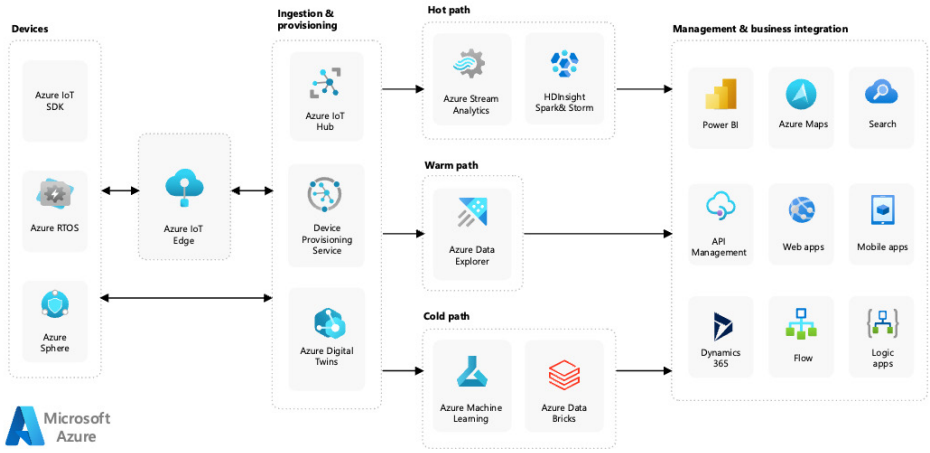
- Example: Cisco's Internet of Things Reference Model, 2014
  https://dl.icdst.org/pdfs/files4/0f1d1327c5195d1922175dd77878b9fb.pdf



MICROSOFT AZURE

Even when vendors are providing end-to-end solutions, we recommend splitting the solution into interchangeable components that end-users can act on individually if necessary.

- For instance, the Microsoft Azure IoT reference architecture uses a similar approach
  https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/iot



List of layers

- Alerts, reaction & control
- Data visualisations & business intelligence
- Data transformation & data analysis
- Data storage
- Data ingestion
- Device provisioning & security
- Connectivity solution
- Gateway
- Edge processing
- IoT sensors
- Hardware components

BETWEEN THE IOT LAYERS

Between each of the layers, it is essential that standard APIs and formats are used, following the current industry conventions.

The connection between the layers should ideally be reconfigurable by the owner of the solution, directly or indirectly.

- For instance, it should be possible to make gateways send data to a new data ingestion endpoint address.
- Reconfigurability offered by already-employed protocols are a good starting point, such as using DNS to connect some of the key layers.
- Ownership and control of those configuration elements should be described and agreed upon in the architecture solution. That includes the various DNS records, security keys, security certificates, and identity & access management.

To the left is the list of layers we used during the workshop. They can be used as a good starting point, complemented by some standards such as ISO/IEC 30141.

DESIGN WITH LAYERS

During the workshop, it was apparent that the participants covered quite well a diversity of roles, with various start-points and end-points for their respective IoT solutions.

The layers split the IoT stack in logical divisions, connected by standard-based APIs and formats.

There was a consensus that the participants could operate under such a model, which we can therefore recommend.

The 7 recommendations

1. Focus on data
2. Build with interfaces
3. Secure a minimum of interoperability
4. Keep an open mind when choosing technology
5. Prioritise partnerships and ecosystems
6. Take maturity and complexity into consideration
7. Start small, think big

11 CONTRIBUTION

This works builds upon – and contributes to solidifying – the first steps formalised in *Danish Standard DS-INF 176:2021*[1].

In particular, we develop the recommendation #2 *Build with interfaces*.

Further development of that standard can be found on the OASC MIMs.

Furthermore, we connect some complementary standards / guidelines together, and mature the principle of 'layers' for modularity of IoT projects, especially in the context of multi-vendor solutions.

The guide should be seen as a first step in establishing a shared framework for understanding and increasing the use of standards in Denmark.

1 https://www.ds.dk/da/download/guide-til-baeredygtig-digital-omstilling-i-danmark

12 CONCLUSION

Suppliers should pay attention to the different interfaces where modular design is necessary. It will foster a healthier project – especially in long-term projects – if the project partners confer with each other, even when users initially do not employ modularity.

Municipalities and other recipients should verify that suppliers have incorporated modularity and interchangeability into the design of the different interfaces.

PUBLISHERS
Alexandra Institute · Aarhus University
DigitalLead
December 2023

EDITORS
Alexandra Alapetite
Lea Schick

DigitalLead.

AARHUS UNIVERSITY

ALEXANDRA INSTITUTE