Internet of Things Architecture

IoT-A

Project Deliverable D6.4 –

Final Validation Report

Project acronym:	IOT-A
Project full title:	The Internet of Things Architecture
Grant agreement no.:	257521
Doc. Ref.:	D6.4
Responsible Beneficiary :	UniWue
Editor(s):	Alexander Salinas Segura (UniWue)
List of contributors:	Martin Bauer (NEC), Martin Fiedler (FhG IML), Markus Hinkelmann (NXP DE), Edward Ho (HSG), Carsten Magerkurth (SAP), Alexander Salinas Segura (UniWue), Norbert Vicari (SAG), Joachim W. Walewski (SAG)
Reviewers:	Alessandro Bassi (HEU)
Contractual Delivery Date:	31.07.2013
Actual Delivery Date:	12.11.2013
Status:	Final

Version and date	Changes	Reviewers / Editors
V01 – 15.05.2013	Table of Contents	Alexander Salinas Segura (UniWue), Norbert Vicari (SAG), Carsten Magerkurth (SAP)
V02 – 29.07.2013	Review & final changes	Carsten Magerkurth (SAP), Alexander Salinas Segura (UniWue), Nobert Vicari (SAG), Alessandro Bassi (HEU), Edward Ho (HSG), Martin Fielder (FhG IML)
V03 – 04.11.2013	Final review & final editing	Alexander Salinas Segura (UniWue)

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)

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

Executive Summary

The deliverable D6.4 represents the final validation report of IoT-A, and gives an overview of the validation activities done by WP6. The main objective of this deliverable is to show the results of the validation approach from a technical, business and socio-economic perspective. Furthermore the document also highlights the collaboration with external stakeholders who showed a keen interest in contributing to the IoT-A project and its main output – the IoT ARM.

The technical validation started early in the project, performing necessary associated activities in order to improve the quality of the IoT ARM from the beginning. This was done internally, as well as externally, involving stakeholders throughout the progress of the project. Therefore, a number of meetings (stakeholder workshops and expert meetings) were set up to obtain external feedback in a structured way. This feedback included recommendations on how to improve the IoT ARM in terms of architecture methodology and utility but also on how to include and to present it to stakeholders. Dissemination activities were also considered in validation as it can act as an indicator to what extent the IoT ARM is accepted by the audience. Traceability of requirements is provided by matching the requirements to the different components of the IoT ARM. Furthermore we performed reverse mappings, i.e. the application of the IoT ARM to existing architectures. These mappings show that an existing system that has been designed without applying the IoT ARM can be redesigned according to the IoT ARM. This exercise revealed how the IoT ARM can be applied to a concrete architecture.

The business validation aims at showing the commercial relevance of the IoT ARM. We started with a qualitative analysis of the potential advantages of using the IoT ARM. This analysis reveals in what way the usage of the IoT ARM can be beneficial for companies. Following this, we adapted Porter's model of the value chain and its extension in health care ([Porter, 2004], [Burns, 2002]) to two concrete use cases of IoT technologies, viz. the WP7 use cases in logistics and health. In order to give a more concrete analysis of how processes and value chains are transformed by IoT-A, we conducted an in-depth business case analysis of two specific use cases. The section about Business Networks reveals the importance of collaboration between partners and the value of the relationships among them.

In the socio-economic validation we performed two activities, namely a Delphi study to investigate the impact of the IoT on the European economy as a whole and a privacy impact assessment to show to what extent the protection of user data is touched by the IoT ARM. The Delphi study as first activity presents results for five different perspectives. Four of them investigate the macroeconomic view, namely political, economic, social and technological. In addition we added the retail industry perspective to examine to what extent the IoT has an impact on the retail industry. The results show that the IoT plays an increasing role in the future, especially in terms of social and technological impacts. Using the example of the retail industry we could also identify a high impact on this industry. In the second activity a privacy impact assessment (PIA) was conducted on a use case scene from WP7. For this purpose, the BSI PIA framework was used following its process [BSI, 2011]. The results show that the PIA is very useful to identify what measures have to be taken to achieve a real implementation respecting full privacy. Furthermore, it has been very obvious during the analysis that the use of the IoT ARM and of the PIA are independent of each other. Thus, IoT ARM does not interfere or hinder the implementation of a secure and private IoT scenario (orthogonal). Even more, they can be seen as two supporting elements to build a private and secure IoT application (parallel).

In summary, the IoT ARM was successfully validated from different perspectives. The technical point of view, ensured that the IoT ARM is sound with respect to requirements and compatible with existing IoT architectures. Feedback from stakeholders and external experts was taken into account to increase acceptance. In addition, the results of the business as well as the socio-economic validation showed the relevance of the IoT ARM in a future IoT world, too.

Table of Content

List of figures

List of tables

List of abbreviations

B	Benefit
BC1	Business Case 1
BC2	Business Case 2
BM	Benefit Model
BN	Business Networks
BSF	Benefit Sensitivity Factor
C	Cost
CA	Calculation
CF	Cash Flow
CCF	Cumulative Cash Flow
CDCF	Cumulative Discounted Cash Flow
COCOMO	Constructive Cost Model
COSYSMO	Constructive Systems Engineering Cost Model
CP	Cockpit
CRF	Critical Risk Factors
DCF	Discounted Cash Flow
DF	Discount Factor
DD	Demand and Delivery
DS	Data Source
EHR	Electronic Health Record
EDI	Electronic Data Interchange
GS1	Global Standards One
HR	Hardware Risk
IC	Input Configuration
ICT	Information and Communication Technology
IoT	Internet of Things
IoT ARM	Internet of Things Architectural Reference Model
IoT DM	Internet of Things Domain Model
IoT-A	Internet of Things Architecture
IP	Investment Plan
IQR	Interquartile Range
IRR	Internal Rate of Return

MR	Miscellaneous Risk
MUNICH	Multi-National Initiative for Cloud Computing in Health Care
NFC	Near Field Communication
NPV	Net Present Value
NRC	Non-recurring Cost
PEST	Political, Economic, Social, and Technological
PIA	Privacy Impact Assessment
PR	Personnel risk
PS	Project Schedule
RAND	Research and Development
RC	Recurring Cost
RFID	Radio Frequency Identification
ROI	Return on Investment
SD	Standard Deviation
SDM	Software Development Model
SFS	Service Fee for System
SITR	Software Implementation Time Risk
SR	Software Risk
SS	Suitable Surgeries
SW	Stakeholder Workshop
UC1	Use Case 1
UC2	Use Case 2
VSCC	Virtual Supply Chain Centre

1 Introduction

The final validation report covers all validation activities within WP6. In addition it provides pointers to further validation activities in other work packages. It explains the activities undertaken and the corresponding results, which had an impact on the evolution of the IoT ARM in WP1. The document is structured in three major chapters, namely the technical, business and socio-economic validation. In the following each of the respective chapters is explained in more detail.

The technical validation aims at assessing the IoT ARM according the criteria listed in section 2.1. The first release of the IoT ARM (v0.9) was published in D1.2 [Walewski, 2011]. This was the first basis on which the validation activities were launched. These activities encompassed mainly project-internal validation, i.e. the technical WPs 2-5 provided feedback to WP1 in terms of their specific background knowledge. As the IoT ARM gained in maturity project-external validation was started in order to make use of the broad IoT community to comment on the IoT ARM and to broaden the feedback to the IoT ARM by project-external opinions. To obtain external feedback different sources were exploited, i.e. the stakeholder core group in stakeholder workshop 2 and 4 (SW2, SW4) and the IERC AC1. For instance, the stakeholder group in SW4 consisted of a mixture of participants with technical as well as business background. This led to a fruitful discussion in which both parties contributed to the results. To obtain specific IoT-related feedback from people with appropriate technical knowledge the IoT-A project engaged itself in the IERC AC1, which is responsible for architecture approaches and models. In both cases, SWs and IERC AC1 meetings, we could get required and successful results which drove the evolution of the IoT ARM significantly. Towards the end of the IoT-A project the IoT ARM was in a very mature state so that the applicability was one important point to examine. Hence, a number of exercises was conducted in which reverse mapping of the IoT ARM onto an existing solution used. Some of the exercises were conducted in the sister project IoT-i, specifically for ETSI M2M, EPCglobal and uID [Carrez, 2013]. In IoT-A we performed this exercise for the MUNICH platform. That way we could show that the concept of IoT ARM is really applicable to an IoT solution which was not built on the basis of the IoT ARM. Although we know that a mapping of only one architecture is not enough we were not able to do such a mapping multiple times due to limited resources. Finally other means of technical validation are presented which refer to the involvement of the requirements from WP6 and standardisation activities.

The business validation aims at revealing the business value of the IoT ARM. We start by describing in a qualitative manner, how the IoT ARM can positively impact various activities related to develop, operate and maintain an IoT system. Secondly, the IoT ARM was investigated using the concept of the value chain from Porter [Porter, 1985]. As this analysis requires domain-specific applications we drew on one hand side on the retail use case developed in WP7 and on the other hand side on the MUNICH platform related to the health domain. The analysis of the value chain shows, the role stakeholders could play in an IoT-A enabled world. Thirdly, we investigate the business value of the IoT ARM to show what processes are changed and what value is generated by the IoT ARM. For this purpose a compelling business case on a quantitative basis was made. Similar to above it concerns the retail use case from WP7 and the MUNICH platform. In both cases we interviewed a couple of experts to identify the potential costs as well as the potential benefits, transformed them into financial figures and finally performed a cost-benefit analysis. As this cost-benefit analysis is based on certain parameters, we supplementary added a sensitivity analysis which takes variations of these parameters into account and provides a range in which the upper and lower bound of the financial impact is indicated. In order to augment the value chain thinking we also considered business networks as of today most probably, if not certainly all companies are directly or indirectly interconnected. As distinguished from value chains, business networks put an emphasis on the relationships between value chains. These relationships are of value to companies involved in business networks and thus we explain how the IoT ARM can support this aspect.

The socio-economic validation has a twofold aim, meaning that we investigated to what extent the IoT has an impact on the economy as a whole and specifically how the IoT ARM provides

mechanisms to protect user data. The former was done by conducting a two-round Delphi study. In total, 15 IoT experts from across Europe participated in the study. As the study was about the macro-environment we applied the so-called PEST analysis, whereas this abbreviation stands for the political, economic, socio and technological perspective. In addition we considered the retail industry as a further perspective aiming at a specific industry. The research objective was to develop qualitative-oriented industry scenarios while maintaining a holistic, retail perspective on the retail industry. The overall result reveals that the experts agreed on the probability of occurrence for 11 projections out of 22 and that for each perspective at least one agreed projection could be identified. The second important activity was the security and privacy impact assessment. By using the PIA framework [BSI, 2011] a standardised and commonly accepted framework was followed in order to ensure valid results. The analysis was performed using a single scene from the healthcare use case developed in WP7. The final result shows that the IoT ARM is suitable for developing privacy-respecting IoT applications.

As already mentioned above not only WP6 performed validation but also other WPs such as WP1 (D1.5) and WP7 (D7.5) to name but a few. While other WPs mainly validated their WP-related work, WP6 followed an overarching approach by interfacing with WP1 and representing a counterpart to the developer group of the IoT ARM.

The remaining part of the document is structured as follows. In chapter 2 the objectives of this document are being discussed. Further the interaction with stakeholders is explained in chapter 3 followed by the three major validation chapters. Chapter 4 deals with the technical validation in which the IoT ARM is examined from a technical point of view. Chapter 5 contains the business validation in which it is shown how the IoT ARM can contribute from a business point of view. Finally, chapter 6 describes the validation activities in the context of the socio-economic perspective.

2 Objectives of the validation

The objective of D6.4 is to report about the validation activities done in the IoT-A project. Based on past validation reports, viz. IR6.1 [Salinas Segura, 2011] and IR6.2 [Salinas Segura, 2012], this document summarises the main and crucial validation activities over the entire project duration.

The focus of the WP6 work is depicted in Figure 1. In the beginning of the project, the requirements collection and analysis had a high priority, as they were the basis for the development of the IoT ARM. The first set of requirements was obtained after stakeholder workshop 1 (SW1) and has been refined successively. With time progressing, the focus of work gradually shifted from requirements towards validation. Both tasks were supported by an extensive stakeholder interaction.

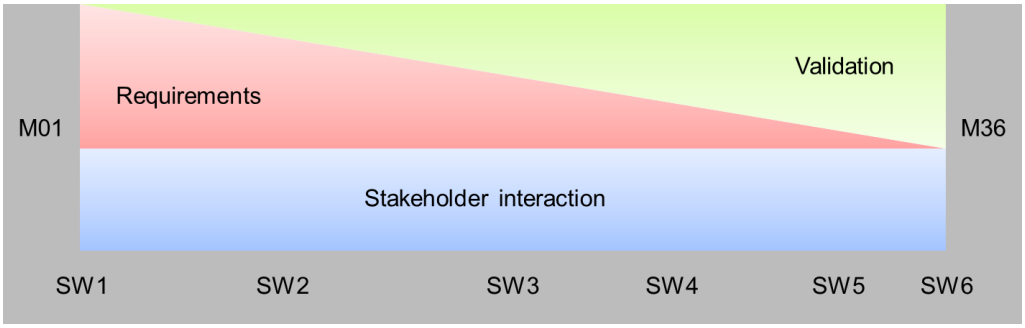

Figure 1: Shift from requirements towards validation

From a formal project point of view, this deliverable covers mainly two objectives from the description of work both of which could be met:

O6.2: Perform validation of the resulting architecture against requirements and stakeholder perceptions.

O6.3: Interaction with a group of stakeholders including knowledge and information transfer.

2.1 Key success factors for validation

Each validation process needs a number of criteria or measures to be checked against. This is also true for the validation work of the IoT-A project. The key success factors for the validation are described according the structure underlying this document.

2.1.1 Technical perspective

The IoT-A project has a strong emphasis on the technical outcome by nature. Accordingly, the technical validation is crucial and we put it in the area of focus due to the evaluation of the core output of the IoT-A project – the IoT ARM. In that respect, we converged the main efforts for validating the IoT ARM in order to comply the following success factors.

Obtain and take into account external feedback on the IoT ARM

In the course of developing the concept of the IoT ARM and its related constituent parts, e.g. the Guidelines and Design Choices, one runs the risk of a biased thinking if denying external opinions on the progress of development and the development itself. Thus, we were continuously seeking for external stakeholders being able to positively contribute to the success of the IoT ARM. This practice ensured reaching consent on the IoT ARM with the project-external community.

Requirements fulfilment

The requirements gathered at the beginning of the project were crucial for the subsequent IoT ARM development process as they build the constituting part. For this reason, it was very important to keep track of the degree of requirement coverage in the IoT ARM to meet the stakeholder aspirations expressed in the beginning of the project. However, the requirements process is not part of this document but accurately described in D6.3.

Applicability to arbitrary IoT systems

One of the primary goals followed by the IoT ARM is its applicability to generate all kinds of IoT systems. Therefore we conducted a reverse mapping from an existing IoT solution, viz. the MUNICH platform, to analyse to what extent the IoT ARM meets the architecture design of a project-independent IoT system and to show that the IoT ARM concepts and components are universally valid for IoT systems. As a consequence, we could identify similarities and disparities that resulted in a further refinement of the IoT ARM. This exercise showed that the IoT ARM contains all essential concepts and components to design a generic IoT system.

2.1.2 Business perspective

The second perspective looks closely at the business. Since the usage of the IoT ARM highly depends on the business value the validation work considered this circumstance as well. Thus, the following success factors refer to justifications for using the IoT ARM.

Applicability of the IoT-ARM in the business context

We adapt Porter's model of the value chain [Porter, 1985] and its extension in health care from [Porter, 2004; Burns, 2002] to two concrete use cases of IoT technologies, viz. the WP7 use cases in logistics and health [Fiedler, 2012]. This establishes, at a general level, who, how and at which stage the key players could contribute to value creation.

Value creation with the IoT ARM

In order to give a more concrete analysis of how processes and value chains are transformed by IoT-A, we conduct an in-depth business case analysis of two specific use cases to show that the IoT ARM can positively contribute in financial terms.

2.1.3 Socio-economic perspective

The socio-economic perspective deals with aspects concerning social and economic effects on a society. Therefore we performed two activities covering social aspects such as privacy as well as economic aspects.

Impact analysis of the IoT on the European economy

To analyse the impact of the IoT on the European economy as a whole we performed a Delphi study. This study was conducted to evaluate in how far the IoT will play a crucial role in the future. This gives some indication of the potential IoT system developments for which the IoT ARM can be deployed.

Privacy impact assessment

The violation of privacy is an important issue related to IoT systems which impacts negatively the adoption of such systems. Thus, a privacy impact assessment of a sensitive scene in the context of healthcare was conducted in order to demonstrate that an IoT application realised on the basis of the IoT ARM preserves privacy of the users.

2.1.4 Outside the scope of validation

The nature of the IoT-A project and its duration limits the applicable validation techniques. Validation techniques such as mathematical proofs or simulations were not feasible to perform.

However, some work packages performed validation for specific components developed in IoT-A by implementation, so that particular instantiations of the IoT ARM are proofed.

In the course of the project duration we were also faced with the request of validating the IoT ARM by application of external industry companies. Even though this is a valid point and would be highly beneficial to get feedback from industry regarding the applicability and utility of the IoT ARM, this approach was not feasible. The IoT ARM was according the project plan in development for almost the whole project duration, undergoing perpetual quality improvements and evolution. The IoT ARM must be seen as a potential candidate for being integrated in future development processes for IoT systems. Similarly, this circumstance can be regarded as the two process steps of product development and product launch. The IoT-A project considers itself as a product developer for the IoT ARM while the second step, the product launch, cannot be done by the project because of the limited project duration. In terms of sustainability the IoT ARM will be maintained by the IoT Forum in which different strategies will be followed to convince industrial partners to make use of the IoT ARM.

2.2 Validation techniques

Validating the IoT ARM in its entirety is a really challenging and difficult task to undertake. This starts with the fact that the IoT ARM consists of the Reference Model and the Reference Architecture which both need a great deal of attention in the context of validation, especially from a technical point of view. It is a given that the IoT ARM is not executable and thus cannot be directly tested in contrast to a piece of software. However, there exist a number of other useful techniques for validating the IoT ARM that vary in cost, complexity, and formality and each is appropriate in different stages of the development process. In order to perform a comprehensive validation of the IoT ARM the following techniques which were used in the IoT-A project are presented.

Presentations

This most widely used technique was the simplest way of doing validation. In essence, the presentations were a general means to make an informal explanation of the proposed IoT ARM, be it the stakeholders at the SWs or at other meetings. As it is impossible to validate the IoT ARM just by presenting it, the presentations were carefully structured to engage the audience. Particularly people with a technical background were greatly interested in thinking deeply about the implications of the candidate IoT ARM. As a result, the subsequent discussions about the IoT ARM often revealed room for improvement which then led to internal activities to address the mentioned points. This technique was almost always used for the stakeholder workshops. This specifically applies to SW4 in which a mature state of parts of the Reference Model and the Reference Architecture was presented and led to important results within the technical validation. In addition, this technique was also used for different expert meetings, e.g. IERC AC1, to take a single example. As an introductory part, and in combination with other validation techniques such as reviews and walkthroughs, presentations supported our work as a communication and selling tool and helped the stakeholders to start thinking about important issues.

Formal reviews and structured walkthroughs

This technique elaborates on the idea of validation in a greater detail as stakeholders are more involved. As an effective way to validate the IoT ARM with stakeholders, it ensured and confirmed an accurate understanding of stakeholders' concerns and allowed us to make considerable improvements in the design of the IoT ARM. The formal review involves stakeholders to go through a document, ideally page by page, raise comments about it, and discuss the concerns in a group meeting as it happened with D1.4 by Prof. Muller. Based on the constructive criticism both parties, Prof. Muller and the representatives of the IoT-A project, could jointly agree on the necessary actions to be taken for further improvement. In the same way the expert meetings with the involved IoT projects from IERC AC1 were set up. The participants of these meetings received the latest versions of the document containing the specification of the IoT ARM to study it before the respective meeting. At the time of the meeting

the IoT experts were able to ask comprehension as well as detailed technical questions in order to drive discussions in the right way. The results of these meetings were manifold. Besides the strong discussions, we got responses via a questionnaire and offered them the opportunity to leave additional comments in our issue-tracking-system Redmine. This technique was mainly applied in combination with presentations and led to valuable results regarding architectural issues. As a summary we can say that even if this technique required some preparation time for the stakeholders, all meetings went well and the results revealed room for improvement for the further development of the IoT ARM.

Evaluation by using scenarios

Using scenarios for evaluation is a very common and proven technique which allows the characteristics of the IoT ARM to be evaluated in specific contexts. Some of the evaluations included in this document followed such an approach. The first to mention is the business case which is on the one hand based on a set of use case scenes from the retail use case of WP7 and on the other hand on the use case in the context of the MUNICH platform. Furthermore the privacy impact assessment was also done by using one particular scene from the healthcare use case of WP7. In summary, the scenario-based approach provided an important means to perform validation and at the same time offered a more explicit understanding for the stakeholders of the implications caused by the IoT ARM within a certain context.

Prototypes and proof-of-concept systems

Prototyping occurs in the early stages of software development and refers to the activity of creating incomplete implementations of a system or model such as the IoT ARM being developed. In the IoT-A project this activity happened in WP1 and WP7. Both use cases of WP7 were realised as a prototype using the IoT ARM which at the same time constitutes a proof-of-concept. Likewise the MUNICH platform acts in the background of its use case of RFID-supported surgeries whereas in this case the proof-of-concept was done by doing a reverse mapping of the architecture of the MUNICH platform onto the IoT ARM. Although prototyping is the most expensive and time-consuming way to demonstrate the applicability of the IoT ARM and to assess it afterwards, it revealed many issues during development by which IoT ARM could be improved. Thus, this technique could be justified due to the important insights while developing a system based on the IoT ARM.

Figure 2 depicts the spiral model containing the different iterations of each cycle – requirements acquisition, development and validation. The validation techniques described above were used in the validation phase in each cycle over the course of the project duration. In the context of validation we mainly worked with presentations in the beginning of the project as we needed the foundation for the IoT ARM, namely the requirements, and the whole concept around the IoT ARM was still evolving. But as mentioned before presentations have a supportive character to be used in almost each case where stakeholders were faced with the IoT ARM. Reviews and walkthroughs started with the first iteration of the requirements since these formed the basis for the eventual IoT ARM. Thus, this validation technique already started right before the development of the IoT ARM and ended with the last expert workshop evaluating the last version of the IoT ARM (v3.0). The scenario-based evaluation was mainly done within validation, thus it began after the first iteration of the IoT ARM as well as the prototyping. As the IoT ARM had its first release the implementation of the prototypes began and lasted until the end of the project duration.

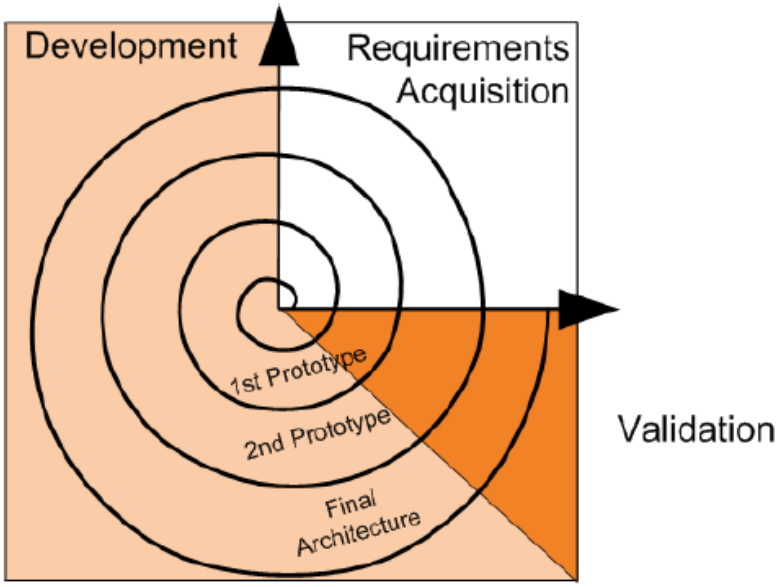

Figure 2: Validation within the spiral model

2.3 Other validation activities within the IoT-A project

Validation work was not only conducted and documented in WP6 but also in the other work packages in the IoT-A project. Table 1 provides an overview of validation activities in other work packages outside of WP6. These activities can be seen as an extension to the technical validation in chapter 4 as all activities were performed to validate the technical outcomes in the respective work packages.

Table 1: Validation activities in each work package

WP	Validation activity	Short description	Reference
WP1	Reverse mapping	The IoT ARM was mapped onto a couple of architectures (e.g. MUNICH platform). This activity revealed how far both architectures were compliant. As a result we could highlight to what extent the IoT ARM is a generalisation of the considered architectures.	D1.5, section 5.6.4
WP1	Requirements mapping	In a first step, the Unified Requirements were mapped to the different Functionality Groups of the IoT Functional Model. Next, clusters of requirements of similar functionality were formed and a Functional Component for these requirements defined.	D1.5, section 4.2.2.1
WP2	Modelling some of the WP7 use cases with the BPMN IoT Extensions	WP2 has developed a modelling environment that validated the BPMN extensions developed in the project by being able to model (and execute) processes based on the WP7 use cases.	D2.4 (entire deliverable)
WP4	Prototype implementation fulfils requirements	The prototype implementations regarding the semantic web-based approach and the semantic-web and federation-based approach fulfil the requirements regarding semantic descriptions of services, virtual entities and associations and semantic discovery based on the semantic	D4.4, section 3.2, section 3.3

		descriptions.	
WP4	Prototype implementation fulfils requirements	The prototype implementations regarding the geographic location based approach, the semantic web-based approach and the semantic-web and federation-based approach fulfil the requirements regarding the support of coordinate-based and logical location descriptions for service areas and virtual entities and the respective discovery according to a respectively specified location.	D4.4, section 3.1, section 3.2, section 3.3
WP4	Prototype implementation fulfils requirements	The prototype implementations regarding the peer-to-peer infrastructure DHT approach fulfils the requirements regarding look-up and resolution of service descriptions and associations respectively.	D4.4, section 3.4
WP4	Prototype implementation fulfils requirements	The prototype implementation of the security components AuthN, AuthZ, KEM & TRA fulfil the security requirements regarding the resolution infrastructure.	D4.4, chapter 4
WP5	Authentication of RFID tags which preserve privacy	A noisy RFID reader coupled with a lightweight cryptographic protocol enables to ensure a safe authentication and also to ensure that only the owner of the tag is able to identify it.	D5.1
WP5	Distance bounding protocol against relay attack in RFID communication	A new type of protocol has been implemented to detect a delay introduce by a relay attack between a legitimate RFID reader and RFID tag.	D5.1
WP7	IoT ARM applicability	The IoT ARM was used to model prior defined use cases of the two domains retail/logistics and health in the IoT domain. The Guidelines were partially followed to come from an application description to the real implementation of a use case scene.	D7.2, chapter 3, chapter 4 D7.5, chapter 3
WP7	Requirements mapping	The IoT ARM was derived from requirements, and as such, one dimension for validating the presence of the IoT ARM in the WP7 use cases is to check to what extent the unified requirements are present.	D7.5, chapter 5

3 Interaction with Stakeholders

It is a well-known fact that effective development of any kind of system requires close collaboration between research disciplines and stakeholders at all levels to strike a balance between different perspectives and objectives. Accordingly the project was set up to involve external stakeholders formed in a core stakeholder group. Appropriate stakeholder selection is a key challenge for participatory research. This approach must be as inclusive as possible to avoid marginalising stakeholder groups, and this is a challenge with the small sample sizes that are usually used to attain depth of understanding in participatory research. Thus, it was more important to have a small group but with a broad knowledge within their domains. The process of electing stakeholders encompassed various steps to get the relevant stakeholders who have a vested interest in the development of an IoT ARM. First, a list of key people was generated to have a first basis to select from. Second, a stakeholder analysis was performed in order to identify those stakeholders who showed a clear interest in supporting the project. This resulted in a core stakeholder group which assisted as a valuable source of feedback from the beginning of the project. These stakeholders represented a broad general public of industry sectors working in the field of IoT, such as Logistics, Healthcare, Technology Integration, Retail, Automotive, Service Integrators, Telecom Operators, Law, Standardization and Veterinary Medicine.

After the definition of the stakeholder group, the first stakeholder workshop (SW1) was held. At this event the initial stakeholder requirements were gathered which in turn laid the foundation for the IoT ARM. In SW2 the stakeholders were confronted the first time with the first iteration of the IoT ARM. As this was the very first release a bunch of comments were raised at that time. These comments were gathered and structured in order to organise the respective activities to improve the IoT ARM. The following SW3 was focused on the requirements and the validation process. The requirements were discussed for the last time with the stakeholders as (1) they were in a very mature state then and (2) we wanted to identify still existing gaps, if there were any. Regarding the validation process we discussed the progress until then. SW4 played a crucial role in the validation process as it will be explained in greater detail in section 4.2.1. In this workshop we could get important technical feedback to drive the further work on the IoT ARM. The second last SW5 had a focus on the privacy issues in IoT and thus we conducted an initial run to get feedback for the privacy impact assessment. The last SW6 had no impact on the validation due to the very late date of this event. Rather it served for disseminating the project results. In order to get feedback from a group of people with technical background, dedicated meetings were set up to discuss certain aspects of the IoT ARM (see section 4.3).

Apart from the stakeholder workshops we seeked feedback and advice from other important sources. For obvious reasons we drew on related IoT projects from the IERC Activity Chain 1 (AC1) as this activity chain deals with architecture approaches and models. The researchers involved in those projects could share their experiences from the challenges within their projects and provide their consequent best practices. Another important expert meeting took place with a multinational engineering and electronics company working in the area of IoT. This meeting was particularly important because of the discussed applicability of the IoT ARM in industry. Similar to the workshop set up before was the workshop with the industry company Alleantia. The results helped us to identify the similarities and differences between the IoT-A approach and industry approaches and to reveal the benefits of using the IoT ARM for those companies. To obtain feedback from an expert in the field of architecture methodology a further workshop has been carried out. Therefore Prof. Muller was invited to provide his opinions about the IoT ARM and the methodology we used to develop it. As an experienced expert he was able to give informative feedback to further drive the development of the IoT ARM. The collaboration with the responsible people of the MUNICH platform gave us the opportunity to include it in the validation process. In this regard we could perform a reverse mapping of the MUNICH platform architecture onto the IoT ARM. Consequently it permitted us to check the approach taken for the MUNICH platform and the IoT ARM against each other to reveal similarities and differences. Hence, we could identify to what extent it would be possible to design the architecture of the MUNICH platform based on the IoT ARM. The final results for validation were not achievable without the support of the stakeholders.

Dissemination can be regarded as validation in that it gives indication about the acceptance of the audience at each event. This is particularly important if potential users of the IoT ARM are in can be addressed by such events and this group ideally gives feedback on the work. Table 2 summarises the most important dissemination events in the course of the project duration.

Table 2: Dissemination events

Date	Location	Event
29th of September 2010	Brussels	ICT 2010
29th of November 2010	Tokyo	IoT2010
16th of June 2011	Shanghai	IoT Conference
6th – 9th of June 2011	Barcelona	IoT Week #1
18th – 22nd of June 2012	Venice	IoT Week #2
10th of September 2012	Brussels	IERC AC1 Meeting
22nd of November 2012	Regensdorf	IERC AC1 Meeting
7th of February 2013	Delft	IERC AC1 Meeting
16th – 20th of June 2013	Helsinki	IoT Week #3
19th of June 2013	Helsinki	Stakeholder Workshop 6

As already mentioned above we invited experts to specific expert meetings in order to discuss certain topics with them. This was particularly useful to obtain feedback on details in the development of the IoT ARM as well as recommendations for future work. Table 3 summarises the expert meetings.

Table 3: Expert meetings

Date	Location	Event
17th of January 2013	Dortmund	Expert meeting with Prof. Muller
13th of March 2013	Stuttgart	Meeting with industrial company
23rd of March 2013	Pisa	Meeting with industrial company
15th – 16th of April 2013	Heidelberg	IERC AC1 Expert Meeting
8th of May 2013	Dublin	FIA Dublin 2013

Finally we also did validation within the stakeholder workshops. This started with SW2 as at this event the first version of the IoT ARM was presented. From that point on we included in each of the following stakeholder workshops validation activities taking into account that SW6 had no impact on validation as it was conducted after the validation work. Table 4 summarises all stakeholder workshops which contained validation activities.

Table 4: Validation meetings

Date	Location	Event
6th – 7th of June 2011	Barcelona	Stakeholder Workshop 2
22nd of November 2011	Berlin	Stakeholder Workshop 3
20th of June 2012	Venice	Stakeholder Workshop 4
26th of November 2012	Bled	Stakeholder Workshop 5

4 Technological validation

This chapter gives an overview of the various trails of activity that the project conducted in order to perform the technological validation of the project results, most notably the IoT ARM. To do justice to the different perspectives of technological validation, we have applied various, rather different methods. We have started with an internal validation during the course of the project in which the technological experts from the different technical work packages gave feedback to the IoT ARM as it was developed in work package 1. We have also sought feedback from the different stakeholders such as our own IoT-A stakeholder groups or the related IoT projects from IERC AC1. As these can be regarded as similar to IoT-A in terms of being research projects from the same cluster, we have also sought contact with real industrial stakeholders that are not part of any EC project and therefore were able to give meaningful feedback from an industry perspective. Finally, we have also met with experts from the field of software and systems architecture and have performed a mapping of the IoT ARM to a real and deployed architecture in order to evaluate the utility of the IoT ARM. Parts of these activities are already reported in other deliverables, whenever this is the case, we will point out the original deliverable that contains more detailed information than what is discussed here.

4.1 Internal Validation: Cross-WP IoT ARM Feedback Process

This section discusses the IoT-A-internal feedback process from the perspective of technological validation by considering the input of the individual work packages. Already in 2011, the second year of the project, there was a lot of feedback, propositions and interest from the individual technical IoT-A work packages to the IoT ARM that was just being developed. These comments were collected using an excel document, which in the meantime collected more than 300 feedback entries. Each IoT-A work package has a very specific technical view on the IoT ARM and could thus include its perspective to the validation process (e.g. WP2 provides the perspective of services and business processes of the Future Internet). By the organized nature of following up with feedback items one individual feedback comment could directly affect the next version of the IoT ARM.

For each response it was recorded which IoT-A WP has provided the feedback, what the original context of the post is, who the responsible owner of the post is, as well as the type of contribution, the proposed change and the final solution to the problem. Accordingly, each post was indicated with a suitable colour code. For instance, the colour green was used if the comment could be resolved successfully, yellow was used if the owner could lastly agree on the already existing solution, and red was used if the solution is still in discussion, grey was used for duplicate entries, and no colour was used if there was still no answer of the respective owner. Figure 3 gives an overview of the status of the individual comments received for each work package and for all work packages consolidated.

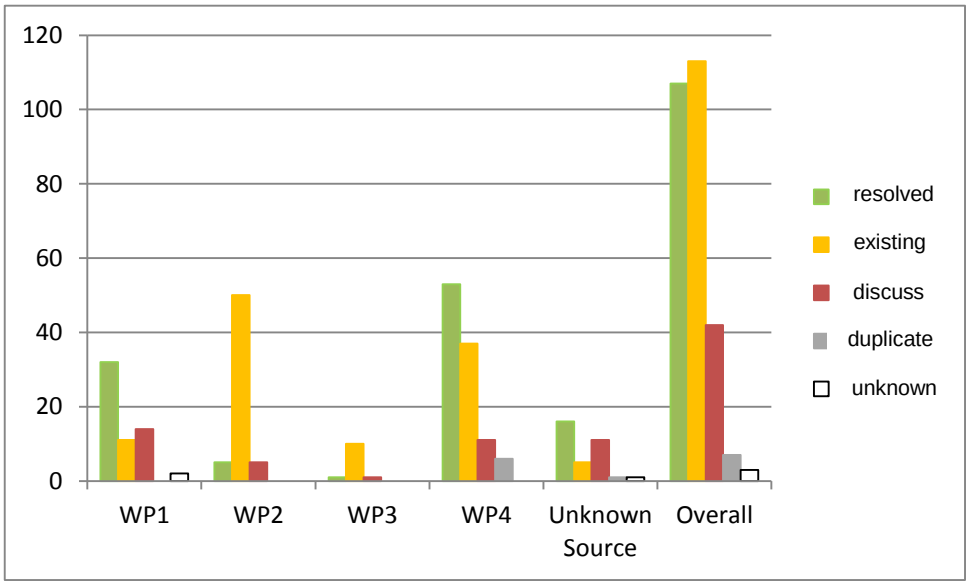

Figure 3: States of the individual comments received per each IoT-A work package

The following section summarizes the amount and types of feedback posts from each of the technical IoT-A WPs, WP1 included.

WP1 itself mainly addresses individual comments from IoT experts within the consortium. These comments arose partly through their own critical specialist feedback and partly from scientific discussions with other IoT experts (e.g. Gerd Völkens of Siemens as an expert for IoT-aware complex event processing or Prof. Jacques Pasquier-Rocha as an experienced professor of software engineering and expert on IoT and Web of Things meta-modelling). Overall, 59 responses from WP1 were received and documented. While 32 comments were completely resolved, 11 comment owners could finally agree on the existing IoT ARM solution, while 14 comments are still in the discussion and 2 further comments were not marked, since no feedback from the respective owner has been received. The content of the feedback can be mainly split into the two categories general and editorial.

From WP2, in total 60 responses were obtained, which consist of general feedback and comments provided by the document IR2.2. While 5 of the comments could be completely resolved, agreement on the existing IoT ARM solution was reached on 50 of the comments, while 5 comments are still in the discussion. No comments have been grouped as duplicates or are currently open, so that no comment remained untreated. The content of the comments includes almost all feedback types. Thus, general, technical, editorial, and additional content type entries were provided for validation purposes since the WP2 partners cover a broad application domain of the Future Internet research area.

In comparison to the further technical IoT-A work packages, with a number of 12 posts received, there was very little feedback from WP3. These entries can be split into generally obtained WP feedback and feedback provided by the document IR3.2. Thus, only one comment could be completely dissolved, while for further 10 feedback posts the existing solution could finally be agreed upon and one post is still under discussion. The feedback to the IoT ARM covers the types “general” and “technical” comments.

WP4 offered with 107 statements the most numerous responses of the technical work packages, which can also be divided into general feedback and entries provided by the internal IoT-A document IR4.2. Here, 53 responses were resolved completely and thus incorporated in the IoT ARM, The authors of 37 comments finally agreed on the existing IoT ARM solution, 11 comments are currently still in discussion and 2 further comments were grouped as a duplicate. All content types are covered by the WP4 feedback. Thus, the provided entries could finally lead

to new and attached content of the IoT ARM, further content issues and additional information could be addressed and general, technical as well as editorial feedback were offered. WP5 did not provide dedicated comments due to the somewhat “low level” nature of the work package.

There is also a smaller number of 34 feedback entries addressing mixed issues, whose source is not known, but which were nevertheless taken into account for the IoT ARM validation.

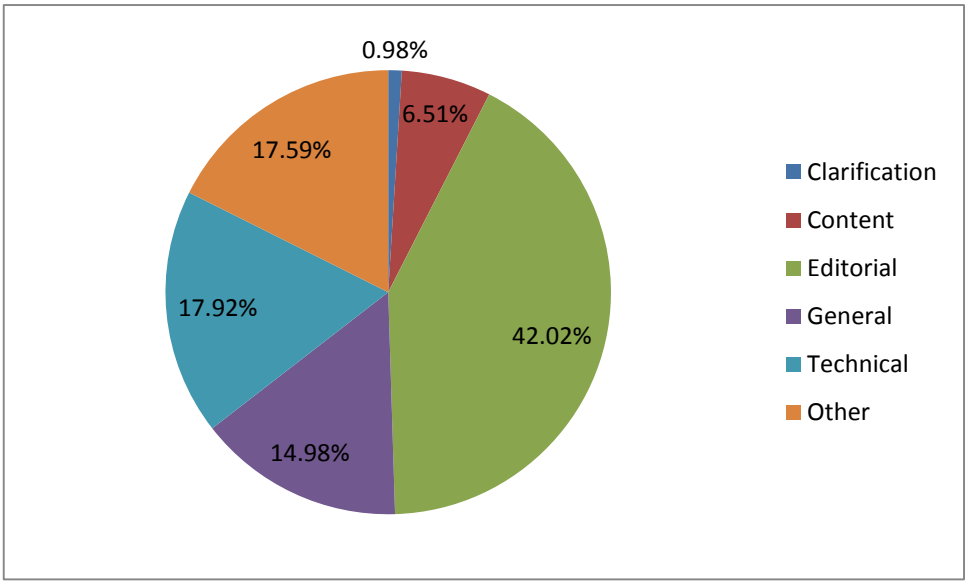

Figure 4: Percentage distribution of IoT-A internal feedback types

In general it can be summarized that project internally the IoT ARM development led to numerous discussions, interest and participations from the consortium partners, but also from externals. A total number of 307 project-internal responses were recorded and continuously taken into account in the development of the different IoT ARM versions. Accordingly, the IoT ARM could be validated internally by the help of the IoT-A technical work packages WP2-WP4 in addition to the external IoT-A validation with stakeholders and other IoT research projects. Figure 4 shows the percentage broken down into the different types of feedback comment in which the internal feedback has been divided. Furthermore, it can be summarized that the majority of comments could either be directly included in one of the IoT ARM versions (39.34%), or could finally match with the existing IoT ARM version (41.54%). At a lower portion of the entries, the project partners are still in discussion (15.44%) and a very small portion of entries could be identified as a duplicate (2.57%). Due to changing project partners and project participants in the consortium there are 1.1% of the total entries that are no longer pursued, since the corresponding owner was no longer available for IoT-A purposes.

It can be concluded that the internal technological validation process of IoT-A was massive and certainly unusual for typical EC integrated projects. A three digit number of comments received from project internal experts directly changed the IoT ARM during the development, which is certainly an impressive number.

4.2 Stakeholder Domain Model Validation

Although the internal feedback process was certainly very valuable, it bears the danger of groupthink which potentially causes bias, i.e. the internal feedback reflects the backgrounds and expertise of the project partners, but not necessarily those of experts and other stakeholders outside the project. As the IoT-A project was planned to have a dedicated stakeholder group right from the start, it naturally makes sense to utilize the stakeholder group in order to gain technical feedback from them. Stakeholder workshop 4 (SW4), held at IoT Week 2012, was an excellent occasion to gather the stakeholders and perform a validation with them, as the IoT ARM was just reaching its milestone D1.3 release [Magerkurth 2012] that includes significant

improvements over the previous release. The other stakeholder workshops did focus on other issues such as requirements gatherings or economic validations and were thus less suited for an intensive technical validation, although comments from SW2 and the related IoT week, as well as SW3 were also taken into account.

Accordingly, this section reveals the validation results of SW4 validation activities. Based on SW4 feedback, extensive results could be obtained for technological validation.

The technological validation conducted at SW4 consisted of five distinct components. We did focus on the IoT Domain Model as the single most important part of the IoT ARM that is easy enough to grasp and work with without a dedicated period of learning.

1. A briefing package focusing on the Domain Model, including modelling exercise of a real world scenario from the stakeholders domain that should be modelled with the notation and concepts of the IoT Domain Model. This package was sent to the stakeholders in advance in order to prepare them for the technological validation session at SW4.

2. An introductory talk about the IoT ARM in general given as an introduction to the technological validation session at SW4. The aim of this part was to provide a context for the subsequent presentation of the IoT Domain Model and to give an overall idea of the goals of the IoT-A project.

3. A presentation of the IoT Domain Model including an introduction of how to apply the related concepts and a rationale for several design decisions, such as why resources and services are modelled as distinct components instead of a single and coherent component, as resources are only exposed through services.

4. An open discussion about the concepts of the IoT Domain Model and about the IoT ARM in general. The results of this discussion, i.e. the main feedback gathered from the discussion, are presented in the next section.

5. Finally, a dedicated questionnaire targeting the IoT Domain Model was handed to the participants of SW4 and was filled out at the end of the technological validation session at SW4. The results of the questionnaire are also presented and discussed later in this chapter.

The results of the open discussion as well as of the dedicated questionnaire will be discussed in the next two sections.

4.2.1 Feedback from the Stakeholder Workshop 4

The discussion round at SW4 was opened after presenting the IoT Domain Model, so that most of the feedback addressed the IoT Domain Model, although certain statements also apply to the entire IoT ARM, such as the first one in the following list.

The following issues are also put in the annex of the D1.4 document [Magerkurth, 2012] in order to ensure that they do not get lost, if interested external parties focus on the WP1 deliverables without taking WP6 output into account. The respective responses come from the IoT Domain Model Task Force in WP1 that analysed the feedback from SW4 after the workshop.

The items specifically addressing the IoT Domain Model are discussed in D1.4, but the following list includes both those items from D1.4 and those that are not specific to the IoT Domain Model, including the project's initial responses:

There are different standardized ways of documenting software architectures such as e.g. ISO 4071. It is suggested to adopt one such framework.

This feedback relates more to the architecture methodology than the IoT Domain Model as such. Nevertheless, it must be noted that it is not the intention of the IoT-A project to provide

concrete software architectures, but a reference architecture from which concrete architectures can be derived, so that the adoption of one concrete standard does not seem to be appropriate.

The term „user“ is commonly referred to humans, but the IoT Domain Model also uses it for machines. A suggestion can be to find a new term, such as e.g. “purposeful actor“

This is indeed a valid point. The IoT Domain Model uses the term “user” for anything that makes use of the system, including machines. In order to identify human users, the derived term “human user” is used. This can indeed be counter-intuitive. We are thus evaluating different terms. The term “actor” however is also ambiguous in the context of IoT due to the phonetic similarity to “actuator” which is in itself a core IoT concept.

Services are commonly described in terms of producer and consumer outside IoT-A.

The IoT Domain Model has a different focus than most other service models so that the term “consumption” in particular is less central. As the IoT ARM deals with the real world where actuation services are a central aspect, the focus on service consumption is less appropriate, because actuating services often do not produce results that can be “consumed” by other services or users.

The „thing“ is missing as a concept in the IoT Domain Model.

It is true that in the context of other related research initiatives (such as e.g. FI-WARE) the term “thing” is being used instead of other terms. Initially, the IoT Domain Model also used the term “thing” to include the various kinds of real-world objects. However, as the model matured, we realized that this term would need to be sharpened in order to differentiate between e.g. “entities” (things one is interested in) and “devices” (pieces of hardware that host resources that might be used to obtain information about entities). In that respect, we believe that our omission of “things” is an evolutionary step towards a clearer and sharply defined IoT Domain Model instead of a disadvantage of the model.

The concept of a Tag is overemphasized in the IoT Domain Model.

The rationale behind this criticism is that a tag is just used for identifying physical entities and might therefore be modelled by simple relationships instead of a dedicated modelling concept. This is somewhat true and the concept could be left out. However, our IoT Domain Model comes from the domain of RFID and we do make assumptions about certain central concepts in order to not become too general and thereby lose expressive power.

The IoT Domain Model is used both for a conceptual model and for software artefacts, although certain concepts fit better to software architectures than others.

While this observation is certainly true, it is the nature of IoT to integrate physical aspects with software artefacts. Insofar the Domain Model concepts need to address both physical and software artefacts, as e.g. in order to model typical IoT mediated interactions in addition to traditional direct interactions, both hardware and software aspects of the domain are required to be defined.

A Youtube video explaining the IoT Domain Model should be provided in order to facilitate an understanding of the IoT ARM.

This item is of course most valid. While we do believe that a live workshop such as the stakeholder workshops conducted so far are the best way to convey the key elements of the IoT ARM due to their interactive nature, this approach naturally does not scale well. Insofar, we have looked into producing an introductory video, but during the course of the project we have not yet created one. This might be an activity to be picked up by the IoT Forum.

In order to explain the IoT Domain Model, a concrete use case should be provided

This item has been picked up and a “red thread” example is now a central part of the upcoming D1.5 document.

A multi-level use case is difficult to be modelled with the IoT Domain Model

While this feedback item can be true, we have no indication that difficulties stem from the IoT Domain Model as such, and not from the complexity of the use case. Without a concrete example, this item is difficult to assess.

The modelling of a "User as a Device" is unclear

This criticism relates to the issue of how human users that provide information into the system can be modelled. Currently, it is necessary to model the user as a device, since devices provide information into the system. While, depending on their roles, humans can also be correctly modelled as users and entities, they are not really devices, as they are no pieces of hardware. It could be an option to augment devices in order to include human devices that are made of technical hardware. However, this would have questionable implications towards the boundaries to actuators, so that this issue is currently not resolved.

There seem to be too many degrees of freedom in the IoT Domain Model

This issue relates to the appropriate level of abstraction that is usually some kind of compromise between different views. The question of too many or too few degrees of freedom is therefore to some degree subjective. It is clear, however, that reference models need to have more degrees of freedoms than concretizations. For instance, in the IoT domain, many different kinds of sensors can be imagined, like e.g. cameras, instead of only tags, which necessarily leads to a higher level of abstraction and therefore to more degrees of freedom. In general, the IoT domain is rather broad due to the complexity of the real world and therefore Domain Models tend to have more degrees of freedom than in other domains.

As we can see from the discussion above, most of the issues raised by the stakeholders at SW4 were either integrated into the further development of the IoT ARM or were not valid after a respective analysis.

4.2.2 Results of the SW4 Questionnaire

In addition to the feedback we received "live" at the event, we also handed a questionnaire over to the participants to get additional feedback.

The questionnaire was insofar very important, as it provided the first means of quantitative feedback to the concepts of the IoT Domain Model.

In the aggregate, there had been 11 participants in SW4 who took part in the feedback survey. Among these participants, 2 also attended SW1, 3 attended SW2 and further 4 also attended SW3. While all 11 interviewees hold a university degree, 8% are currently working in the area of Information Management, 23% in either Computer Science, Business Management, or Management & Economy and further 46% in other fields. Moreover, 45% have stated to be familiar with UML diagrams.

Please find detailed information about the interviewee's opinions about both the IoT Domain Model and the technical validation session below. The entirety of items of the questionnaire can be found in Annex A.2.

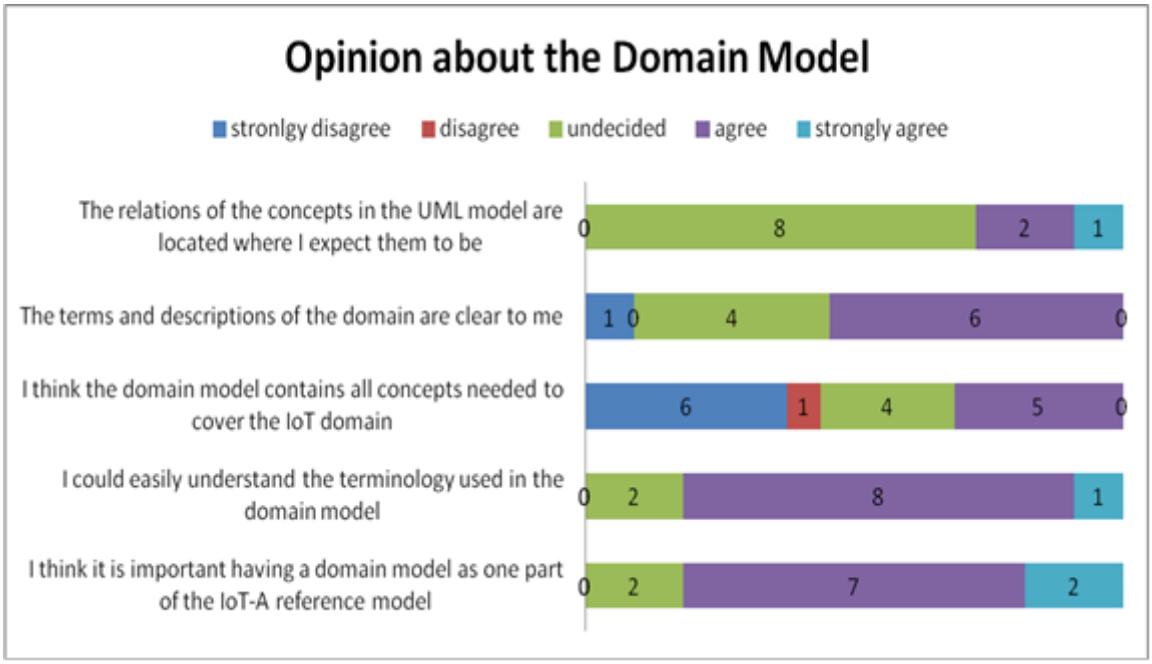

Figure 5: Opinion about the IoT Domain Model

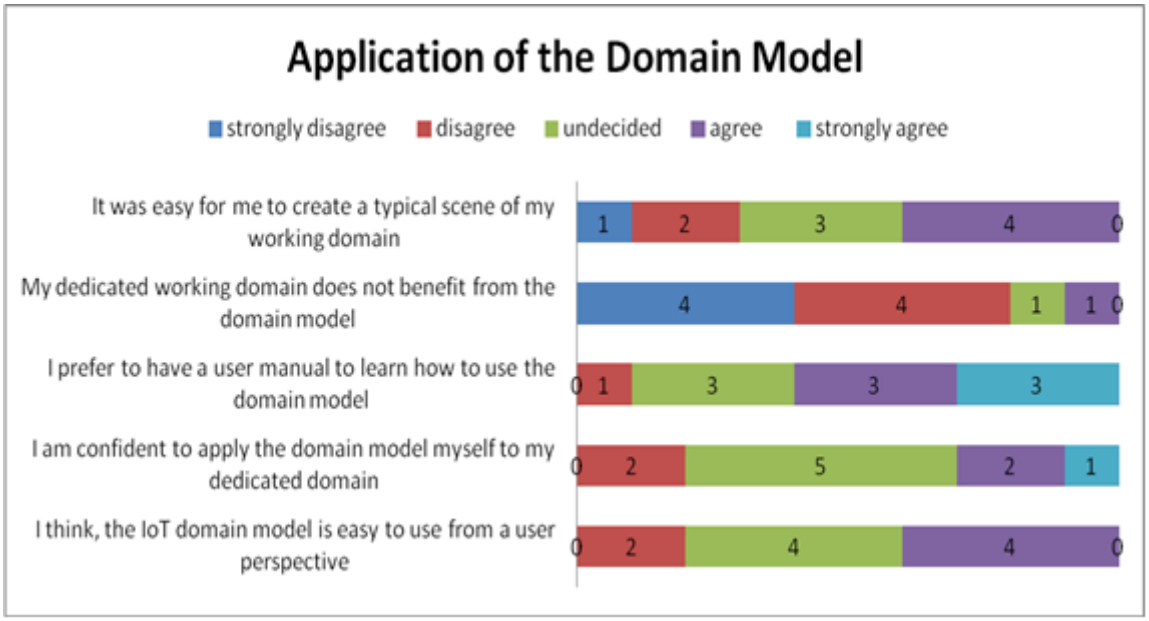

Figure 6: Application of the IoT Domain Model

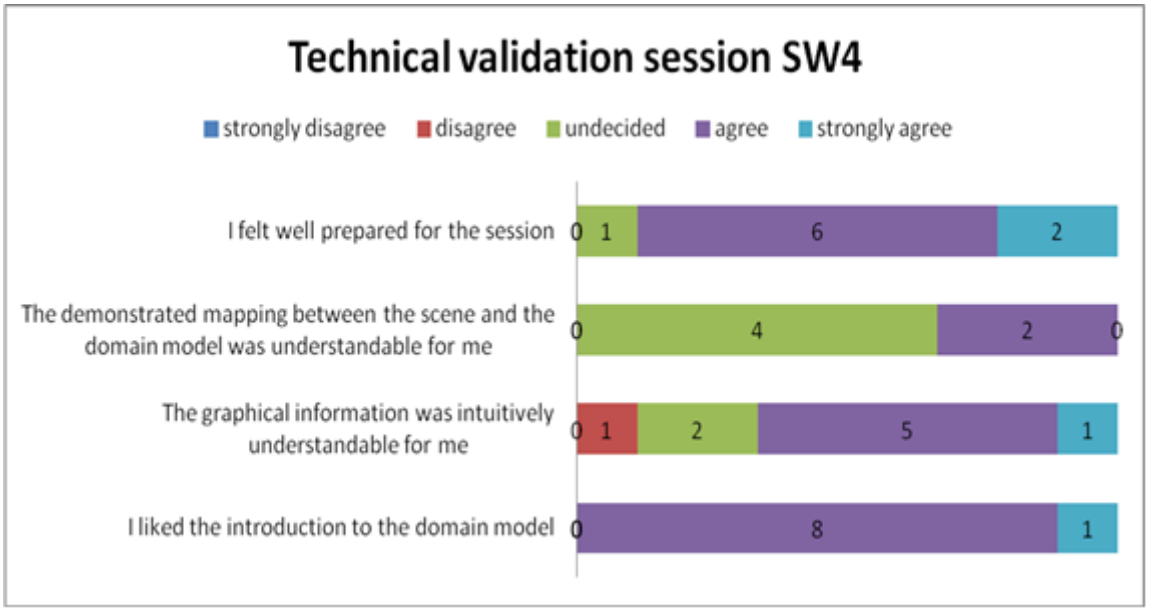

Figure 7: Technical validation session

In addition to that, there had been several further remarks concerning the IoT Domain Model provided as free text on the questionnaire sheets. These are provided here as a transcript from the handwritten notes:

Missing concepts in the IoT Domain Model:

- Provisioning sensor self discovery (device)
- User profile => the user as a resource
- Connection to existing IT systems
- Active digital entity?
- Time
- A static vision of IoT is a limited vision of IoT
- Relations (predefined but also emerging, not preconfigured at design time)
- Relationship between physical entities
- Name “user” different: new term for “purposeful subject” (human/ machine)
- Connection of a device to a human body, e.g. sensor in human body
- The stakeholder to provide a service cannot be modelled

Disagree with concepts in the IoT Domain Model:

- The concept of Virtual Device, Virtual and Physical Entity is not entirely clear. Can humans interact with Physical Devices or Physical Entities?
- Unsure about all relationships
- Nesting
- User (Actor? Needer? *[sensu Demander]*)
- No need for “tags”. Its identity is an attribute of “user” and “physical entity”

Disagree with relations in the IoT Domain Model:

- Is not the device enabling a physical entity to be also a virtual one? Where is the relation between Device and Virtual Entity? What is the difference between Virtual Entity, Digital Entity and Augmented Entity? Can this be simplified?

Difficulties applying the IoT Domain Model to your domain:

- I tried to apply it to a more complex use case than the flower example I received in the email. This introduced many questions. The model is so flexible that it leaves too many degrees of freedom
- The concept of Physical Entity needs to be précised
- Problem: linearity of the architecture (e.g. Id first and THEN service)… in a dynamic world (please remember Weick's call 4ScRAP computing, situated, unplanned…). Is the architecture flexible and evaluable? I think an entry point here is to reflect on the notion of resource

Additional comments:

- Some graphs (even the ones on paper) were very compact/ small
- Introduction to the IoT Domain Model too fast sometimes
- Use cases and demo examples are too simple + You need ones that won't work without IoT!"

Most of the points raised by the comments given as free text were also discussed during the open discussion session and have been reflected upon above. In general, it seems that the IoT Domain Model cannot yet be picked up by all of the stakeholders, although they felt that the concepts in general are clear and that both the preparation for the stakeholder workshop and the introduction given at the workshop worked sufficiently well. This means that the project has so far succeeded in getting the information about the IoT Domain Model across to the respective stakeholders, but there seems to be a gap between understanding and following the presentation of the IoT Domain Model, and applying it in the context of the work of the stakeholders. In other words: the IoT Domain Model can be understood, but not easily applied within the context of the stakeholder's own domain of work. Obviously, there seem to be concepts missing in the IoT Domain Model that some of the stakeholders appear to need, and there might be a general lack of experience in applying domain models, which is not surprising given the diverse nature of the stakeholder group. In order to cope with the latter, the IoT-A consortium had decided to conduct technical workshops with an audience that comes from very technical and software architectural fields. The results are discussed in the next section. Regarding the former issue, it might be worth noting that the IoT Domain Model only includes concepts of the Internet of things. Many real-world applications that the stakeholders might have in mind also include other aspects of e.g. enterprise or domain applications that fall out of the scope of the IoT Domain Model. In that respect, the IoT Domain Model is complete as a domain model for IoT, but what needs to be done on the side of the IoT-A project, however, is to provide more information and guidance on applying the IoT Domain Model in the context of applications that go beyond pure IoT systems.

4.3 Expert Validations of the IoT ARM

4.3.1 End-User Validation: Industry Workshop

In order to perform a technological validation with a technical audience from industry, we held an "Internet of Things Architecture Workshop" with a multinational engineering and electronics company headquartered near Stuttgart, Germany, in the beginning of 2013. The workshop participants and results are confidential, as the industrial company disclosed parts of their architectures. Therefore, we will only report high-level findings. The eleven participants met on March 13th, 2013 at the premises of the industrial company. The basic agenda was as follows:

- General introduction and goals of IoT Architectural Reference Model (IoT ARM)
- General introduction of the industrial company and about their architecture work and processes
- IoT ARM: Reference Model
- IoT ARM: Reference Architecture

- Discussion of how applicable the IoT ARM is for the industrial company

Regarding the IoT Reference Model, many questions were discussed. For example, the difference between Resources and Services: In the IoT Domain Model the physical world and its digital representation is modelled in one instance. This can be confusing for software engineers, because in Software Engineering it is not uncommon to model the real world in the domain models and implement software (i.e. digital representations) based on this.

Another question was brought up regarding the Tag and why it is part of the IoT Domain Model, what the difference to other AutoID-technologies: Instead of reading an RFID tag, one could also read a barcode or recognise an object/person using a video camera. These questions were discussed in detail and there are arguments to not treat RFIDs differently than other identification technologies (be it barcodes or face recognition as examples). However, RFID has played and is playing an important part in the Internet of Things – the very term comes from this area, so it was decided to keep it as an explicit concept in the IoT Domain Model, although for a certain industrial partners this might not be intuitive.

Within the session on the IoT Reference Architecture, several questions were brought up, for instance whether we always assume a distributed case. This is not the case due to the point that we have created the IoT Domain Model in such a way that distribution (of different aspects, e.g. Device, Resource, Service) is possible, but an instance implementation does not have to separate these aspects. It can be implemented in one monolithic block, instead. Another question was raised about when an architecture is IoT-A compliant. The IoT Reference Model aims at being generic, i.e. ideally encompassing any IoT architecture. The IoT Reference Architecture is more specific, but we have not defined what has to be included for an IoT architecture to be compliant (e.g. a set of functional components, requirements on views and perspective etc). The participants also questioned why security is kept out of the applications. The answer was simple: It is not the case that applications are really “above” the Functional Group., Applications interact with Services and may have to use the Functional Component “Authorization”.

The discussion of how applicable the IoT ARM is for the industrial company led to the question if it is possible to use Virtual Entities (VE) as different Roles for the Physical Entities (PE): We may have different VEs representing the same PE taking into account different aspects. It is not clear, whether dynamically changing roles are best modelled in this way. Currently, we do not have roles as a core concept and new branches will not be introduced to the IoT ARM during the remaining lifetime of the IoT-A project. It is also possible to use type hierarchies to model specific aspects. Questions regarding difficulties in understanding the modelling of associations in the Information Model came up: Associations relates Virtual Entities with Service Descriptions, where the Service provides information or enables actuation on the Physical Entities that are described by the Virtual Entities. The aspect to which the service is related is described as an attribute, therefore the additional relation between association and attribute.

What the discussion with the industrial company mostly showed is that the details of the IoT ARM are not trivial to understand and there is a certain amount of discussion necessary to fully understand and use the IoT ARM. This is especially true, if the backgrounds of the potential users are not from the IoT Domain, so that they e.g. have a different concept of aspects such as Services or Resources. It is difficult to assess whether the industrial company would really adopt the IoT ARM, as much of their existing architectures come from different backgrounds and different perspectives. This indeed seems to be a general problem, namely that most architectures are not built from scratch. As we have shown in D1.4 [Magerkurth 2012], many existing architectures can however be mapped to the IoT ARM.

4.3.2 Peer Validation: IERC AC1

While the exchange with industrial companies is certainly central for evaluating a real-world adoption, the grounding in the academic community is also highly important, so that the work done during the lifetime of the IoT-A project could be continued after the project ends. In that respect, an exchange with the other projects of the European Research Cluster on the Internet

of Things (IERC), especially with the projects involved in the “AC1 - Architecture approaches and models” activity chain is vital. The IoT-A project has therefore organized several meetings, such as the IERC AC1 meeting in Regensdorf during the Y2 review of the IoT-A project in November 2012 and a dedicated follow-up meeting with some of the projects in Heidelberg in April 2013. In addition, the IERC itself organized several corresponding meetings with the IoT-A technical coordinator as chair such as in Turin, Brussels, or Delft in which the IERC AC1 projects were asked to evaluate the utility of the IoT ARM for their respective projects. While some initial feedback was given during the Regensdorf meeting in 2012, we have also set up a redmine installation that allows the AC1 projects to give detailed and actionable comments to the IoT ARM to be taken into account by the IoT-A project.

Consequently, the IERC has conducted an analysis of the IoT ARM as part of the AC1 validation activities. So far, we were able to condense 33 distinguishable comments from the IERC, based on the face to face meetings in Regensdorf and Heidelberg and from follow-up discussions by phone and various email exchanges. The cooperation with IERC proofed to be very positive and helpful. The main contributors were the iCore project and the Butler project. Out of the 33 distinguishable comments only two suggestions had to be rejected for being out of scope for an IoT ARM. All other comments found one way or another into our latest deliverables and therefore improved the outcome of the IoT-A project.

The feedback received from IERC was both on high level architectural questions, as well as detailed implementation issues.

A first batch of issues centered around Virtual Entities and their relationships to other components of the IoT ARM. The analysis has shown that some descriptions in our original deliverables were too vague and did not provide sufficient information for someone not that much into the topic as we were. For example, it was pointed out that there isn’t a description of what a Virtual Entity specification is or how a Virtual Entity is used. This led to further discussions with Miguel-Angel Monjas (from Butler) and to an updated Appendix C in the forthcoming deliverable D.15 providing a more detailed description of Virtual Entity specification. Furthermore, some clarifications were suggested: For example, making it clear that a Virtual Entity *represents* a Physical Entity, instead of *relates* to a Physical Entity as it was written in previous versions of the IoT ARM. These and related clarifications where accordingly taken into account.

Another batch of issues discussed Services and their relationship to elements in the IoT Domain Model. In the validation, the lack of a “formal” definition of Service descriptions was mentioned. Although a comprehensive description of the components of a description is not possible, as it depends on the concrete architecture realization, it was suggested to at least introduce an exemplary listing. This led to fruitful discussions about the abstraction level on which Service descriptions should be discussed, in the context of an IoT ARM. We concluded to explain what is the minimum information needed in a Service description and that the remaining content depends on design decisions. We made it clear what aspects of the Service description are mandatory, e.g. the service URL, and indicate that other parts are optional. Section 4.2.2.5 and the Appendix C in the forthcoming D1.5 deliverable were updated to discuss assumptions about the Service descriptions, including the Service locator.

Some more issues regarding Services were about the assumption that the Service description ID is added to the Service description once it is registered and whether it is part of the Service description itself or not in context of a resolution engine. During the discussions it became obvious that this is a design decision (whether the Service ID becomes part of the Service description or not). Therefore, we added the Service ID as a separate parameter to the operations where needed. An implementation can then simplify the signature of the operation and omit the separate parameter if it is already contained.

While most issues asked for more detail, there were also some concerns that some parts were too technologically dependent and not general enough: The interactions introduced in the guidelines section are technology dependent and related to deployment. To the experts from the IERC they seemed to be too narrow. Nonetheless, we wanted to show some real-world

examples and realizations of concrete design choices. We added a description to the introduction of the IoT ARM, stating that the scenarios presented in the following sub-sections address some of the most representative system-wide general use cases, proposing an analysis of possible design choices grounded on real-world examples when applicable. The scenarios were regrouped in three sub-chapters for readability: Service-centered scenarios (Mapping of CEP Reference Architecture onto IoT RA, Mapping of IoT RA to IoT aware business process model, Interworking of IoT Service resolution and VE Resolution), Communication-centered scenarios (Establishing and maintaining safe communication) and Management-centered scenarios dealing with modification of the IoT system (Configuration of the system when adding a Device, Changing a Device configuration)

The Functional Model diagram caused some confusion, as it looked like a layered architecture (n-tier), while in fact, it isn't. This became only obvious by reading the text. We spend some time on discussing the best way of representing the Functional Model as a diagram to make it directly understandable without having to read the explaining text. Again, the result can be gathered from the forthcoming D1.5 deliverable.

Additionally, in the context of the Functional Model, the question what Functional Groups are mandatory and what Functional Groups are optional was raised. This led to lengthy discussions spanning multiple phone calls and email follow-ups. It became obvious soon that mandatory and optional parts cannot easily be determined, even if there was an agreement that most probably at least every IoT-system will have an Application Functional Group, Communication Functional Group and Device Functional Group. The final conclusion was to not state anything about mandatory or optional parts, but consider such questions as part of the Guidelines Section and the design choices. We furthermore added a short section about this issue in the Process Section, discussing the minimum set of Functionality Groups.

Some questions were raised about the general advantage of the IoT ARM and its relationship to existing work. We extended the introductory sections of deliverable 1.5 explaining in more detail the general advantages of using an IoT ARM, and the design flow to be followed. It was agreed that the new text makes the advantages of using and following an IoT ARM clear.

Another direct result of the discussions with IERC (as well as discussions with other stakeholders such as Prof. Muller that we discussed below) is the introduction of an end-to-end example within D1.5. It was mentioned that the lack of an end-to-end example is a problem when diving into the IoT ARM. Therefore, we introduced such an example illustrating our overall vision.

Overall, it is clear that the discussions in the context of the IERC were highly relevant for the development of the IoT ARM. There have been numerous meetings, email exchanges and the redmine feedback that really helped ground the IoT ARM in the IERC and helped incorporate the views of the other projects from the IoT domain. As an example of a detailed feedback that even goes beyond the involvement of the IERC in general, we present the results of feedback documents provided by the IoT@Work project regarding the communication functionality outlined in the IoT ARM.

4.3.3 Peer Validation: IoT@Work Communication Functionality Validation

As part of the AC1 validation activities of the IoT ARM, the IoT@Work project has conducted an in-depth analysis of the communication functionality in both projects and reported this in an internal document that is available only upon request [Houyou 2013]. The major results of this analysis are re-reported in this section. For the sake of readability, quotations are not marked as such.

As agreed upon with the IoT-A project, IoT@Work had focused their work on communication functionality instead of giving only high level feedback, lacking sufficient detail for certain parts of the IoT ARM. The feedback is largely centered around two core topics, namely requirements relevant for communication and the communication functionality of the IoT ARM.

4.3.3.1 Requirements

For the requirements discussion, IoT@Work compared sixteen IoT@Work requirements pertaining to communications with a comprehensive selection of IoT-A requirements (27 in total). For four IoT@Work requirements, a good match with IoT-A requirements was found, while extensions/revisions of IoT-A requirements along the line of the remaining twelve were identified. The main source for the comparison was IoT-A D1.4 [Magerkurth, 2012] which largely represents the final list of requirements as they were are then published later in [Magerkurth, 2013] and on the IoT-A website.

At the first glance, the overlap between IoT-A and IoT@Work requirements is not really impressive, as the majority of requirements do not map to IoT-A requirements. The majority of the differences found were due to IoT@Work stipulating a very high and interworked level of network virtualization. The differences can also be in parts attributed to a higher level of concreteness in some of the IoT@Work requirements that is not appropriate for reference architectures that IoT-A deals with. Also, some of the requirements are more specific for the idiosyncrasies of IoT systems in the work context and thus require for instance integrity protection and support of confidentiality, while this is seen only as a Design Choice within IoT-A. An example for the former case of concreteness would be the the IoT@Work requirement "RN.07 Rapid and deterministic network initialization" [Rotondi 2011]:

"The whole network could take up at most a few minutes to finish all configuration phases."

The requirement provides a concrete quantification for how long network configuration and setup could take. IoT@Work recommends that IoT-A considers reasonable time limits for how fast the configuration should take. Due to the generic nature of the IoT ARM and the aim of the IoT ARM to remain relevant even for future technological generations, such quantification's are not regarded within the project.

4.3.3.2 Communication functionalities

For the communication functionalities, IoT@Work provides detailed comparison of the Network Communication Functionality Group with the respective concepts in IoT@Work.

In IoT-A, the Network Communication FC takes care of enabling communication between networks through Locators (addressing) and ID Resolution. The FC includes routing, which enables linking different network-address spaces. Moreover different network technologies can be converged through network protocol translations.

In IoT@Work, the concept of Network is seen as a composition of networking nodes of different type that offer heterogeneous capabilities. The IoT@Work architecture allows discovering the network capabilities by associating a SEP to each physical node. The SEP represents an agent that manages the network interfaces of an abstract network node or end-node. The node's IDs can be mapped to the SEPs' IDs, which could be an IP address or any kind of ID space. The mapping of end-points managed by a given SEP to the SEP ID is the key information in locating the application endpoints. This can be compared to mapping of URL to an IP address. The difference in view is that the slice system defines one identifier for each element considered in the slice decision making. However, these identifiers could be allocated by other services, or by using any other convention. To start with each networking node, the SEP has an ID, which could any unique ID (each SEP might then have an ID for each local interface it manages). The SEPs managing end devices, might report the associated end device ID (which could be the IP address, or DNS name); and the associated application endpoints through their IDs (which could be their URLs or local virtual interfaces).

IOT@work concludes that the communication model in IoT-A could adopt a more resource-centric approach to allocate network resources to applications through a generic service interface. The benefit of such an approach would be to address more IoT domains and not only constrained networks of "accessing things". The ideas of treating the network as a resource accessed as a service could then allow a better functional decomposition between network-related functions (such as addressing, QoS management, or managing critical traffic and less important communications), from the application elements (such as data mediators, or proxies)

which are concerned with managing the data in application-level annotators or brokers, filters, or indirection points. Both facets are important to an IoT architecture, but mixing them makes it hard to apply the same concepts to all domains.

4.3.4 Methodology Validation: Expert Workshop

So far, we have presented the results of our own project internal technological validation, the feedback from an industrial company, as well as the feedback and exchange we had with our peers from the IERC.

In order to validate the architecture methodology of the IoT ARM as such, an expert workshop with Prof. Gerrit Muller from Buskerud University College, Norway and Embedded Systems Institute, Eindhoven, took place on 17.01.2013 at the premises of Fraunhofer IML in Dortmund.

Prof. Muller is a leading expert in the field of system and reference architectures with a background in physics who has founded the Gaudí Project which is about “making the art and emerging methodology of System architecture more accessible and to transfer this know-how and skills to a new generation of system architects.” [Gaudí 2013]. Before becoming a professor at Buskerud University College, Mr. Muller had worked at Phillips for 17 years.

The aim of the workshop was to elicit feedback towards the IoT ARM from an expert’s perspective and about the procedure and methodology of the work on the IoT ARM. A detailed agenda of the meeting can be found in the Annex A.1.

A confidential, 22 pages report of the workshop is available on the consortium internal web platform of the project. The major conclusions drawn from the workshop relate to the following issues:

4.3.4.1 Performance Indicators

The project should clearly define key performance indicators against which to measure the success of the IoT ARM and should utilize the different work packages for assessing how helpful the IoT ARM is.

The primary performance indicator defined already in the description of work of the project is to sustain the IoT ARM even after the project is finished, so that other projects can pick up the work and develop the IoT ARM further in a structured way. This has already been achieved during the lifetime of the IoT-A project with the establishment of the IoT Forum [IoT Forum 2013]. Additionally, on a different level of abstraction, the business value of the IoT ARM must clearly be demonstrated for the IoT ARM to be successful and to achieve momentum on in the enterprise world. The entirety of chapter 5 in this deliverable is dedicated to this topic.

4.3.4.2 The IoT ARM itself

The project should increase the usability of the IoT ARM by

- Breaking D1.5 into easily consumable parts.
- Using concrete examples early on and throughout the entirety of D1.5.
- Use one (or a few) examples for shedding light on all the aspects covered by D1.5.
- Restructuring the Guidelines Section so that it is more than just a collection of text units. The emphasis lies on GUIDANCE.
- Adding safety to T/S/P and by addressing what lies outside IoT systems (but which has an influence on the former).

The efforts spent on improving the IoT-A deliverable D1.4 (“Converged architectural reference model for the IoT v2.0) [Magerkurth, 2012] addressing the feedback of Prof. Muller have been significant, as the forthcoming final version of the IoT ARM (D1.5) will show. The different sections of the document have been modularized and made more consumable. Due to the

nature of the description of work in the project, the final version of the IoT ARM still needs to be published as one document, however it will contain “almost-standalone” parts in the spirit of Prof. Muller’s view on the optimal granularity of documentation (see Figure 8)[1].

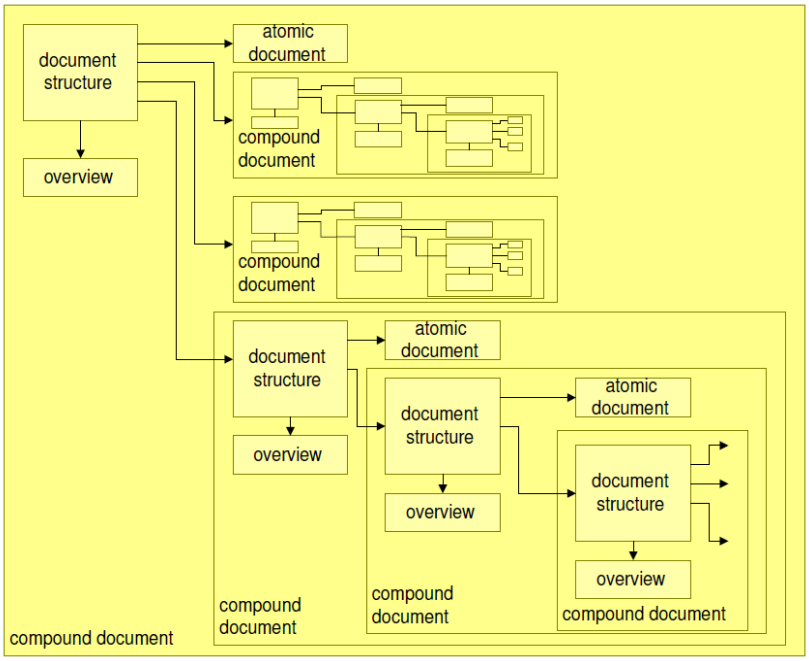

Figure 8: Granularity of documentation[1]

Especially the guidelines section now contains a fully fledged example for the process of applying the IoT ARM to a concrete use case and deriving a concrete system architecture. Special effort was also spent to develop a recurring example (a modified version of the use case developed in work package 7) that permeates the document like a “red thread” and is used to explain and introduce the different sections of the IoT ARM. This “red thread” method was already proven to be successful at the IoT ARM session at IoT Week 2013 in which the project consortium presented architectural issues of the IoT ARM utilizing the example introduced in D1.5.

In this context it should also be noted that one of the difficulties in providing an IoT ARM that is both user-friendly and easy to consume and provides sufficient detail is the fact that the IoT ARM needs to provide a high abstraction level on both the enterprise context and the individual parts or components of the IoT ARM. According to Prof. Muller, this results in an “IoT Architectural Hyper Model” (see Figure 9)[2]

[1] Figure taken from http://www.gaudisite.nl/info/DocumentationGranularity.info.html

[2] Figure taken from http://www.gaudisite.nl/info/DynamicRangeAbstractionLevels.info.html

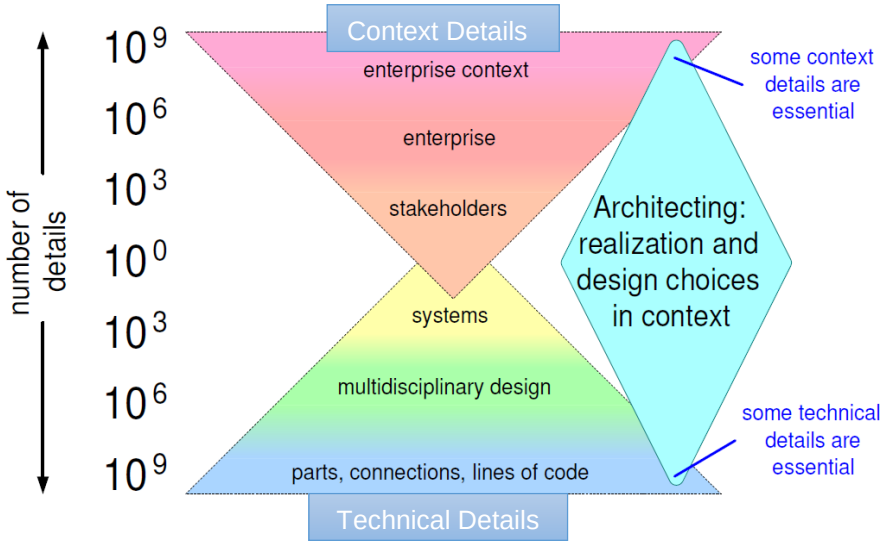

Figure 9: Architectural Hyper Model[2]

Obviously, the IoT ARM needs to bridge these very different domains with the high number of details as the diamond shape in Figure 9suggests. In order to cope with this difficulty, it is advised to provide real-world detailed examples which we now try to accomplish with the aforementioned “red thread” examples.

4.3.4.3 Dissemination

The project should provide its stakeholders with user-friendly diagrams, slimmer, focused text documents, and executive-summary deliverables including posters.

For the forthcoming final version of the IoT ARM (D1.5) the diagrams have already been revised in terms of usability, for instance significantly increasing the font size for the included UML diagrams and each deliverable now contains a lavish executive summaries section. The project, however, has not yet released “slimmer” documents due to the complex nature of the IoT ARM. In order to facilitate the accessibility of the IoT ARM, the project has released a set of very polished and professional looking visuals that are used e.g. in the project meetups or at conferences such as the IoT Week. Examples can be found in the annex.

Most importantly, the project is currently working on an additional book output (“Enabling Things to Talk - Designing IoT solutions with the IoT Architectural Reference Model”, to be published by Springer Verlag in 2013) that contributes excerpts of the IoT ARM along with several introductory chapters with the aim of also drawing non-technical experts towards the benefits of the IoT ARM.

4.3.4.4 Requirements

As requirements are a central part of architecture work, the project should make sure that:

- The term “requirement” is used rather broadly (aspiration, goal, wish) in the context of the project
- A dependency analysis is carried out, as requirements usually have dependencies among each other

Consequently, in the final requirements list (D6.3) [Magerkurth, 2013], a requirement dependencies analysis was performed. This analysis explicitly picks up the problem of internal consistency, dependencies and conflicts between requirements. Based on two different examples, the complex relationships between different requirements are visualized and interpreted, so that conflicts and dependencies are brought to attention.

Also with respect to the issue of potential performance indicators, it should be noted that this deliverable D6.3 also includes a coverage analysis with several projects outside of IoT-A, analysing their requirements and how the IoT-A Unified Requirements cover these. The result is that the huge majority of external requirements gathered within other projects can be covered by the final requirements of the IoT-A project.

In conclusion, the expert workshop with Prof. Muller has given the project a tremendous amount of valuable feedback towards its architecture methodology as such and also towards the presentation and inclusion of stakeholders. Especially the utilization of a “red thread” example, the modularization of the IoT ARM, and the importance of creating attractive visuals towards potential stakeholders have been directly addressed as central activities for improvement by the project.

4.4 Application of the IoT ARM to an Existing Architecture

A final method of technological validation is related to the mapping of the IoT ARM to an existing architecture. The forthcoming deliverable D1.5 includes a lavish section on reverse mapping. In most of the cases this mapping is performed between an existing standard and the IoT ARM. We have, however, also mapped the IoT ARM to a concrete architecture, namely the architecture of the MUNICH use case developed in WP7. While D1.5 will include the complete discussion of the MUNICH mapping, we already present an abridged version in this document.

The goal of reverse mapping an existing system towards the IoT Reference Model is to show that an existing system that has been designed without applying the IoT ARM can be redesigned according to the IoT ARM. By doing so, the IoT ARM shows its potential for being a reference model for any kind of IoT system. This exercise has been conducted successfully with the MUNICH use case.

Use Case Description

The use case is about counting stomach towels which are used inside the abdomen during surgery of a human. After the operation it needs to be assured that no towels are retained in the abdominal cavity of the patient’s body. Therefore, each towel is fitted with a 13.56 MHz RFID tag which enables tracing the towels before, during, and after the surgery. The RFID-tagged towels may be tracked by three antennas from different positions in the operating theatre:

- instrument table: towel is unused
- operation table: towel is in use
- used towel container: towel is used

Each towel will be used in a specific order. Every time an RFID reader recognises a tagged towel appearing or disappearing in its range an event is generated and stored in an event-log database hosted in the cloud.

Current System Architecture

So far the use case has been designed to run with a certain type of RFID-readers only that are connected via USB-cable to a laptop computer that is hosting the application. The MUNICH-platform provides a cloud storage system indicated as ‘Open Nebula Core’ that stores the events captured every time the ‘Object Inventory Service’ notice a change in the number of towels in their respective range by invoking the ‘Event Service’. The application that monitors the status of the towels during the operation invokes methods provided by the ‘Operation Theatre Service’. The API to store and retrieve information from and to the cloud storage system is technology-specific. If an architect decides at a later point in time to change from Open Nebula to another technology the system needs to be adapted to the changes in the API.

The following parts of the IoT ARM were utilized in order to map them to the existing architecture and finally come up with a concrete redesigned architecture (all discussed in more detail in D1.5):

Specification of IoT Process Model

In the IoT Process Model, the operation scenario is a sub-process of the overall Emergency operation process that may include the arrival of the patient via ambulance and the availability of data record for the patient in the hospital's data base. The towels being used during the surgery are associated to the patient identified in the database record. This way it is possible to verify which towels have been used for which patient. Each RFID reader sub-process sends events to the Event History database upon detection of tagged towels. The 'Monitor towel process' analyses the events that have arrived in the database, determines the current state for each towel, and calculates the number of towels that are currently inside the body of the patient.

Specification of IoT Domain Model

A Domain Model can be derived that identifies the Physical and Virtual Entities, the IoT Services, the Devices, Resources, and the users that are involved in the use case.

Specification of Functional View

The realisation of the use case according to the IoT ARM a Functional View is tailored to the use case needs to be specified. No IoT Service Resolution is required, because all needed services are already known to the system at design time. No Service Organisation functions are required in this use case since the binding of services is static and can therefore be hardwired. To accommodate IoT Business Process Management functionality that is required in the MUNICH platform the respective FG is included in the FV.

Specification of IoT Information Model

The IoT Information Model specified for this use case also addresses relationships between entities that are not depicted in the IoT Domain Model before. For instance it is depicted that an 'Operation' is held for a 'Patient' and thus the 'PatientIdentifier' (valid in the clinic) is assigned to an 'Operation'. Operations are processes with a defined status at any point in time. There is also an unknown status in case the status cannot be obtained. The towels are represented as VEs with domain attributes that are essential for the use case. The towel's identifier stored into a RFID tag is one of the attributes as well as the current state of a towel that can be one of 'unused', 'in use', and 'used'. Again there is an 'unknown' state specified in case the state cannot be obtained by the system. The aforementioned designated locations of the operating theatre are reflected in the Information Model as attributes of the VE 'Towel'.

Specification of IoT Services and Interactions

The use case is driven by events using asynchronous communication. Events are sent to the 'Event History' network resource every time an RFID reader recognises a change in the number of RFID-tags in its observation area by using IoT Service. The 'Event History' resource provides another IoT Service that allows the subscription to notifications about the change in the status of towels, e.g. from 'unused' to 'in use'.

MUNICH platform Conclusion

The previous Sections have shown that an existing system can be reverse engineered by applying the IoT ARM. Beginning from an existing system the modelling of the IoT Domain Model and Information Model has been demonstrated. With the help of these models the respective IoT Service Descriptions have been derived and the interactions between the Resources have been specified.

Making the use case demonstrator IoT-A conform means making the system more evolvable and future-proof. With the existing solution the software needs to be updated when a new type of RFID reader needs to replace a current one. Also extending the use case with another RFID reader or another type of sensor will be much easier once IoT-A is applied. The restriction in evolvability applies to the cloud storage component too since the current system is designed to be used with certain cloud storage software. In case the services are modelled according to technology agnostic IoT-A specifications the system will be more future proof. To conclude, not

only a mapping to the concrete MUNICH architecture is possible, but applying the ARM leads to beneficial aspects such as easy extensibility and modularization that were previously missing.

4.5 Other means of technological validation

While the sections above already outline the major validation technological activities performed by the project, it must be noted that are the activities are also being performed that can be regarded as technological validation, although they are rooted in other work packages and are not primarily planned as technological validation activities.

4.5.1 Reverse Mappings to standards

Related to the reverse mapping exercise that we reported in the previous section, we have also performed reverse mappings to existing standards in addition to the concrete MUNICH architecture. In deliverable D1.4 [Magerkurth, 2012] we consequently discuss the following standards:

- ETSI M2M
- EPCglobal
- uID / uCode

We conclude that the detailed discussion of the different standards shows, whether a mapping is possible or not largely depends on the level of detail that we apply to the mapping. From a high-level perspective, the IoT Domain Model usually maps rather well to the different standards. Also, the IoT Communication Model and security aspects are rather compatible between the standards and the IoT ARM. The latter is not surprising, as security aspects in the world of IoT are commonly derived from a well-established body of security research with fixed and clear terminology, quite unlike the Internet of Things domain. Also, it must be noted that the scope of IoT-A is broader than the scope of any of the individual standards which is actually the point of the validation: By the reverse mapping we validate that the IoT ARM is indeed broader by definition and fulfills the objective to provide a reference architecture for all different kinds of specific architectures and use cases. Different parts of the IoT ARM are therefore only partially or not covered at all by different standards. For instance, EPCglobal is highly RFID centric and therefore neglects certain aspects such as the IoT Communication Model, however the mapping to the IoT Domain Model and also to the Security and Information Model works reasonably well at the appropriate level of abstraction.

In any case, we believe that the mapping of a concrete architecture to the IoT ARM such as the MUNICH platform is potentially more valuable than the mapping of standards, as the level of abstraction cannot be arbitrarily changed and real architecture are after all what the IoT-A ARM aims to support.

4.5.2 Standardisation

In the upcoming deliverable D8.15 we will report on standardization activities that are fueled by the project results in the different work packages. While standardisation is naturally not the same as validation, it shows that the architectural concepts developed in the IoT-A project are technologically sound and obviously valuable, so that the consortial partners push for standardisation. For instance, for the work being conducted in WP2, SAP sees a high potential for standardisation on augmenting the standard for business process modelling notation (BPMN 2.0), with IoT specific extensions that allow for modelling and executing business processes taking the idiosyncrasies of the Internet of Things into account. These extensions include means of specifying the reliability or accuracy of real-world sensors, or the mobile nature of certain real-world entities as well as introducing the main concepts of the IoT ARM such as entities or devices. So far, the first functional prototypes of respective modelling and execution environments are being made available and are being introduced to company-internal stakeholders with the aim of bringing these IoT extensions developed in IoT-A to the respective business process management tools of SAP. Correspondingly, many of the protocol extensions developed in WP3 are already being standardized.

4.5.3 Requirements Mapping

As reported in D6.3 [Magerkurth, 2013], the requirements process of the project was central for the final shaping of the IoT ARM. During the requirements process, we have provided a mapping of the requirements to other requirements from different projects in order to investigate, whether our set of assumptions for the development of the IoT ARM have been found and in line with different other initiatives. The result as it is reported in D6.3 clearly shows that this is the case, as we were able to show that the vast majority of requirements from other projects mapped to the requirements gathered within the IoT-A project. This mapping of requirements can also be seen as a validation activity, although it is geared towards the foundation of the IoT ARM and not the IoT ARM itself.

Apart from the mapping to other requirements outside the project, a requirements mapping was also performed with respect to the IoT ARM components: Each requirement is traceable in the IoT ARM, i.e. we have an assignment of each requirement to the different components in the IoT ARM and by that have validated that the requirements are actually reflected in the IoT ARM. This means that there are no requirements that have not influenced architectural components in one way or another.

4.6 Conclusion

In this chapter, we have shown the very diverse activities performed by the IoT-A project related to technological validation. From the beginning of the project on, it had been crucial for us to include different measures of technical validation in order to do justice to the different perspectives of the different stakeholders related to the project. We have presented a very sophisticated and lavish internal validation in which the different technical work packages gave feedback to different parts of the IoT ARM early on in the project, before we approached external stakeholders. This activity helped bringing the IoT ARM to a state that matched the different perspectives of the consortial partners. After having gone through this internal validation process, we have approached our stakeholders, various experts, and our peers from the different IERC projects with whom we conducted several workshops, interviews, and email exchanges, and also set up a formal redmine installation in order to collect feedback in the structured way, so that we could make sure that it would be reflected in forthcoming versions of the IoT ARM. In addition to the manifold exchanges with experts outside the project, we have also performed an application of the IoT ARM to an existing architecture, as it is reported in the forthcoming deliverable D1.5. To complete the diverse picture, we also briefly touched upon in standardization and requirements related activities that are reported in different deliverables. Overall it is fair to say that a significant effort was put into technological validation activities during the course of the project, and we believe that this effort was well spent, as several of the activities conducted clearly and significantly contributed to a refinement and improvement of the IoT ARM.Business validation

In this chapter the IoT ARM will be evaluated from the business perspectives. Section 5 reveals the potential advantages of using the IoT ARM leading to certain business values. The following section 5.1 has an emphasis on the value chain concept explaining the relevance for industry companies and where they are potentially located in the value chain. However, it’s not enough to only show where companies are located in the value chain but also to highlight in how far processes are changed and how these changes impact financial results. This is shown in the business case. As business networks are increasingly important in an interconnected business world, section 5.3 deals with this subject.

5 Business value of the IoT ARM

The IoT ARM being evaluated was developed to provide support for IoT system architects and developers to build IoT systems on a common basis which ensures interoperability between IoT systems built on the IoT ARM. This support is also reflected in key benefits which positively impact in terms of business performance. Therefore the IoT ARM evaluated technologically in section 4 will be further assessed to identify potential economic implications based on its usage. By means of desk research different hypotheses regarding architecture benefits have been identified. These hypotheses have to be evaluated against economic relevance.

The goals of the IoT ARM are to provide a cognitive aid, a common grounding for the IoT field through the Reference Model, a basis for architecture generation through the usage of a Reference Architecture together with Guidelines and to achieve interoperability [Carrez, 2013]. This is associated with revealing the basic functional components and the interfaces between them. After using the IoT ARM to understand the “big picture” of an IoT system, a concrete architecture can be derived more easily which serves as architecture for a system implementation. The expectation is that this setup will reduce the risk and cost of implementing new IoT systems, by facilitating the use of standard components in a "plug-and-play" mode. Consequently, the stated vision is that IoT architects will develop IoT systems that are compliant with the IoT ARM, making the job of an IoT system integrator easier, quicker, and less risky. Figure 10 illustrates this vision in form of the development process including the influencing factors of each stage.

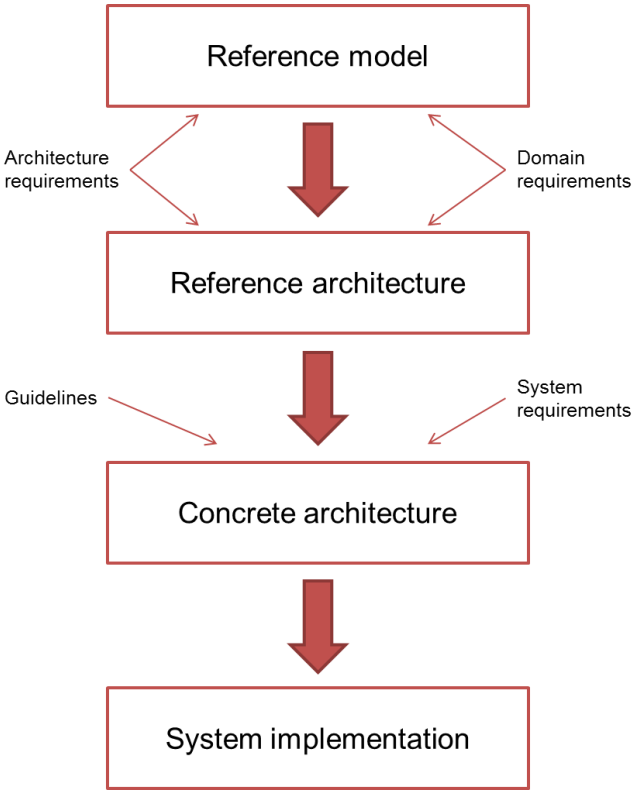

Figure 10: IoT system implementation process

For an IoT architect and developer it is thus important to understand, which concrete positive effects can be expected by using the IoT ARM. In addition, an IoT project manager responsible for the business benefits wants to have advanced knowledge about the related business impacts.

One of the goals which the IoT ARM aims at is to enable IoT system developers to build systems on-time, within costs, while meeting performance needs; the primary objective here is to drive down the cost of IoT system development and integration. Furthermore IoT system developers should be able to use the IoT ARM to integrate their IoT solutions into already existing IoT systems quickly and cost-efficient provided that all solutions are IoT ARM compliant. Under current practices, integration costs are very high. Point solutions are usually too expensive and often take too long.

Another important benefit aspect of architectural view is visibility into further component decomposition (e.g. the functionality groups in the RA) that provides a frame of reference to system developers, integrators and maintainers. In the latter case the maintenance of an IoT system will be easier, as the RA will provide a system maintainer the “map” of the system that will support locating a problem. Generally, this leads to a more cost-effective maintenance process.

The Reference Architecture specifies the interactions that occur between the various components that comprise an IoT system and thus assists in designing a new IoT solution. However, one of the key characteristics of architecting is that it is the vehicle by which system qualities are achieved. But what exactly are system qualities and how do they impact business? Qualities such as performance, security, and maintainability cannot be achieved in the absence of a unifying architectural vision, since these qualities are not confined to a single architectural element but rather permeate the entire architecture. To give an example, in order to address performance requirements, it may be necessary to take into account the time required for each component instantiated from the Reference Architecture to execute, and also the time spent in inter-component communication. Similarly, in order to address security requirements, it may be necessary to consider the communication model between components, and bring in specific security components where necessary. All of these concerns are architectural and, in these examples, bear on themselves with the individual components and the connections between them. Eventually all these architectural considerations impact an IoT system in terms of system quality which is closely connected with business value. A further business-related benefit of architecting is the possibility of assessing such qualities early on in the project lifecycle. Therefore architectural prototypes are often created in order to specifically ensure that such qualities are addressed as it is also the case for the WP7 use case implementations. This is of major importance since, no matter how accurate an architecture chart looks, an executable application system is the only true measure of whether the architecture has achieved such qualities or not.

The business benefits of quality are both broad and deep and it is not just the customer who benefits from a focus on high quality. Businesses that value quality become more effective at innovation, improve their competitive differentiation strategy, and eminently reduce their total cost of development.

Architecting supports the project planning process

Certainly, architecting supports the design and implementation activities of an IoT system, since the architecture is a direct input to these activities. However, the whole concept of the IoT ARM yields more benefits besides the process of architecting. Its major benefits are those related to project planning and management activities in general: work scheduling and allocation, cost analysis, risk management, and skills development. In terms of work allocation, the architecture can again help to identify areas that require particular skills and therefore particular resources (people) to which work can be allocated. The process of architecting can assist all of these concerns, hence the IoT architect and the project manager should have a close and regular communication.

As project costs almost always determine upon project realisation, the IoT ARM is also helpful in estimating the project costs. The costs associated with a project have different origins. Certainly, the individual task durations and the human resources allocated to each task will account for the cost of labour to be determined. Another focus of the architect is to identify and deal with technical risks related to the project. The appropriate management of technical risk

implies the prioritisation of each risk, and the elaboration of a fitting risk mitigation strategy. The priorities and risk mitigation strategies are provided as input to the project manager. With the help of the IoT ARM, discrete components of the solution can be identified that point up input in terms of the skills required on the project. If there is a lack of corresponding resources within the project or within the organisation, then the component-based approach of the Reference Architecture clearly helps to identify areas where skills acquisition is required. This may be achieved through developing existing staff, through recruiting, or through outsourcing.

The IoT ARM provides a basis for reuse

The process of architecting can support both the use and creation of reusable assets. As such, the IoT ARM offers a profound knowledge framework in order not to start an IoT project from scratch. The derivation of concrete architectures might result in reusable assets that are beneficial to an organization, since they can reduce the overall cost of an IoT system and also improve its quality.

The creation of concrete architectures is supported by the IoT ARM in that it provides the possibility of identifying reuse opportunities. For example, the identification of the architecturally significant components and their associated interfaces supports the search for and the selection of available off-the-shelf components, already proven systems, or other existing solutions that may potentially be used to implement these components. The concrete architecture itself might also prove the reusability of the Reference Architecture for subsequent IoT systems. Even new components emerged within the concrete architecture could be deemed worthy in other contexts.

Architecting supports impact analysis

An important benefit of building an IoT system on an architecture is that it enables to conclude the impact of making a change before it is undertaken. This especially holds true for system maintenance when changes to an IoT system are planned. The IoT ARM makes an IoT system transparent by structuring the major components and their interactions, the dependencies between components, and traceability from these components to the requirements on which they are based on. Consequently, a change to a requirement, for example, can be analysed in terms of the impact on the collaborating components that realise this requirement. Similarly, the impact of changing a component can be analysed in terms of related other components that depend upon it. Such analyses can assist to a large extent in determining and estimating the cost of a change, the impact that a change has on the system, and the potential risk associated with making the change, e.g. if security is undermined in some way.

Maintenance for system sustainability

The process of using the IoT ARM for architecting an IoT system can help reduce maintenance costs in a number of ways. Right at the front, the IoT architect should always be adamant that the prospective maintainer of the IoT system is a key stakeholder in the architecting process and that their concerns are addressed as a primary objective, not as an afterthought. The resulting architecture should not only be appropriately documented in order to facilitate the maintainability of the system, but also the IoT architect should ensure that reasonable mechanisms for system maintenance are incorporated, and will consider the adaptability and extensibility of the system when creating the concrete architecture. The IoT architect should also consider those parts of the IoT system most likely to require change and work in the future to pay special attention to them. This can be a straightforward task if the potential change impacts only a single component or a very small number of components. However, the consequences of some changes should be acknowledged, such as those relating to system qualities (performance or security) that cannot be unconditionally changed in this way. For this reason, architects must make sure that they consider likely future requirements impacting the IoT system, since introducing security mechanisms or scaling up a system to support thousands of users rather than tens of users, is virtually impossible without changing the architecture fundamentally.

The IoT ARM has an impact on the entire product lifecycle

When planning an IT project it is important to consider not only the project costs but also the subsequent benefits during the product's lifetime. While the project costs cause a high capital investment, the subsequent operating costs are lower over product lifetime. The benefits of an IT system are very high in the beginning when it is introduced and decrease over product lifetime. This is a usual process as, at the start, an IT system is well adapted to the current IT infrastructure. In most cases, the IT infrastructure changes over the course of time and the initially gained benefits decrease often because of a lack of flexibility of this IT system. Figure 11 gives an illustrative presentation how this process is usually passed through.

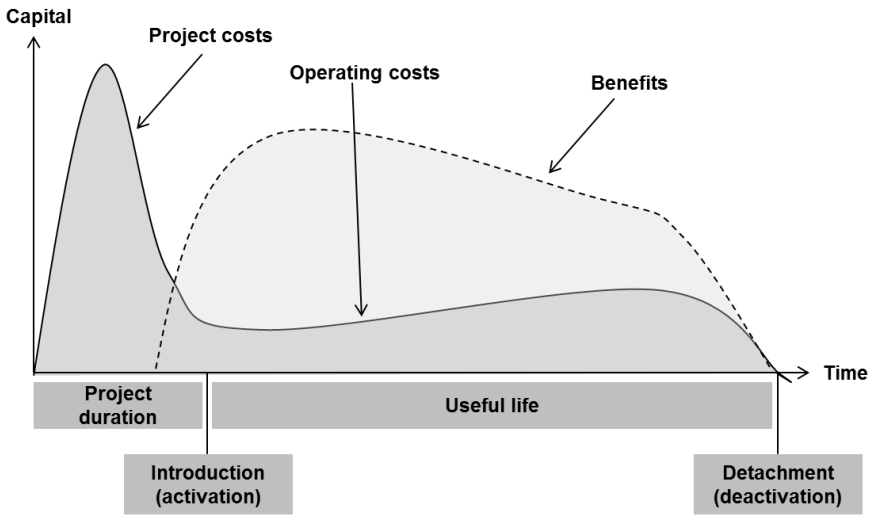

Figure 11: Benefits and costs over time [Bruegger, 2009]

Compared to the usual IT development cycle in Figure 11, the development of an IoT system is very similar. Thus, the potential benefits of using the IoT ARM as a foundation in an IoT project can involve manifold cost cuts. Certainly, high cost reductions can be expected in the development stage as in this timeframe the IoT ARM lays the foundations for project communication and collaboration. Once the IoT system is deployed, an overall higher system quality will account for decreasing operating costs. System maintainers will benefit from higher flexibility and extensibility, thus leading to decreasing maintenance costs which are part of the operating costs. These assumptions are summarised in Figure 12.

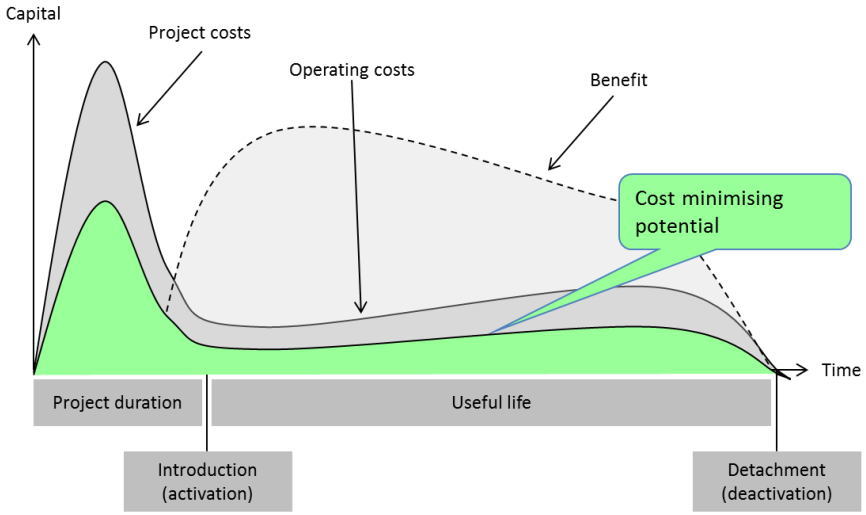

Figure 12: Potential reduction in costs by IoT ARM usage

5.1 IoT ARM in context of the value chain

5.1.1 Scope and Motivation

IoT-A envisions an information–shared world between heterogeneous firms. The potential for new business value based on the DIKW (data, information, knowledge, wisdom) generated by IoT is huge, opening the possibility of new technologies and services that take advantage of this new content. It is therefore of interest to identify the types of key players who could take advantage of these possibilities, and where they could fit in a future IoT ecosystem.

Value chain analysis can address this problem. The idea of the value chain can be described as a chain of activities undertaken by a firm in order to deliver a valuable product or service to the market [Porter, 1985]. Applied originally to singular firms in the domain of logistics and retail, the idea has thereafter been extended beyond the firm level. This extended value chain model also describes the role of other firms in a wider ecosystem of value generation. The original model has also been applied to other domains like health care [Porter, 2004].

This “family” of Porter models has the value of providing a parsimonious framework for how technology could add value to existing value chain processes in logistics and health. Since future IoT adoption must account for existing processes, an IoT value chain model based on the processes described in Porter would capture both the past and the future.

We take a two-step approach to showing the value of the IoT ARM in the context of the value chain.

First, in section 5.1.2 and 5.1.3 we adapt Porter’s model of the value chain and its extension in health care to two concrete use cases of IoT technologies, viz. the WP7 use cases in logistics and health [Fiedler, 2012]. This choice is in line with the project’s use of a reoccurring reference example and instantiates an otherwise infinite field of IoT applications, and this choice also complements the technical and social validation work already completed on these use cases. It establishes, at a general level, who, how and at which stage the key players could contribute to value creation. All these activities in their entirety form part of the overall economic structure and thus describe the correlation between the firm and the socio-economic level.

Secondly, in order to give a more concrete analysis of how processes and value chains are transformed by IoT-A, we conduct an in-depth business case analysis of two specific use cases.

5.1.2 Retail value chain

5.1.2.1 Eco-system description

This section describes the application of the basic value chain model published by Porter to the retail and logistics domain in the context of the use cases developed in the IoT-A project (see Figure 13).

In a value chain one distinguishes two kinds of activities: supporting and primary activities. The primary activities are those activities which have a direct value creating contribution to the manufacturing of a product or the execution of a service. In the basic model these activities are inbound logistics, production operations, outbound logistics, marketing and sales, and service. As the name implies, the supporting activities support the primary activities in their execution. However, supporting activities are not tied to one specific primary activity; rather supporting activities encompass and support all activities in a firm. In the basic model these activities are relevant for firm infrastructure, human-resource management, technology development, and procurement (see Figure 13). In the case of IoT-A and its very technological character it seems logical that the IoT-A use cases demonstrate the technical capabilities of the IoT based on the IoT ARM. The retail use case includes the primary activities with support of technology which is related to the technology development of the support activities in the value chain.

Furthermore a value chain could be regarded for one firm, and this value chain in turn is embedded in a sequence of many value chains. This is also depicted in Figure 13.

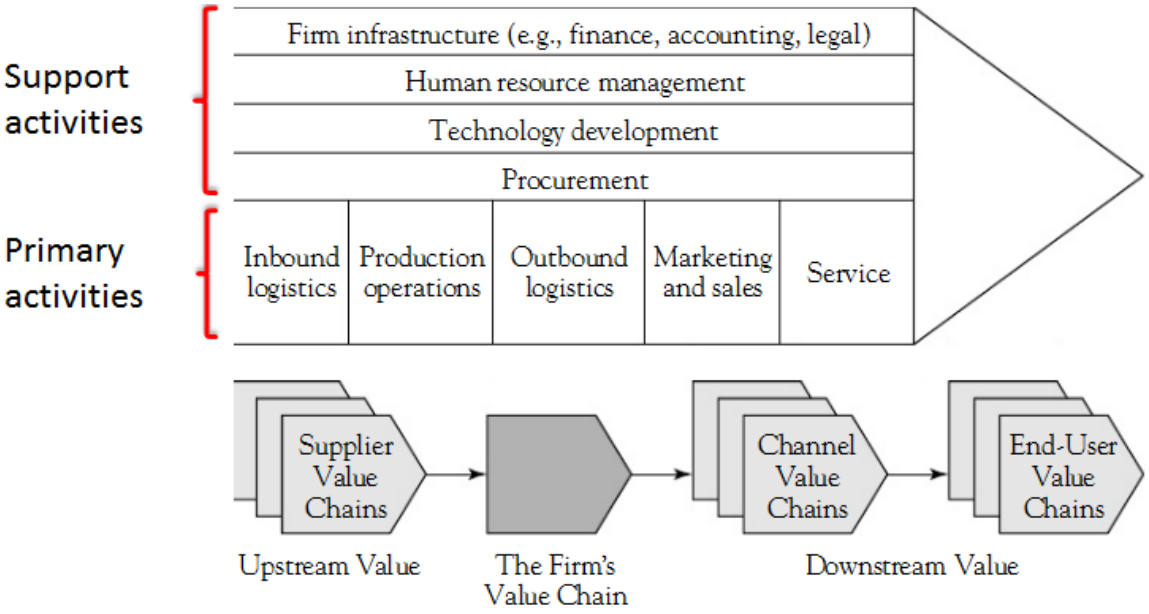

Figure 13: Basic model of a value chain (adapted from Porter (1985))

5.1.2.2 Explanation of Mapping & Possible Fit of WP7 Consortium Members

As mentioned in the previous section, the IoT-A use cases are primarily located in the technology development of the support activities, however, they are also related to primary activities. The following explanation of which consortium partners can potentially be mapped onto certain use cases within the value chain reveals their contribution in the use case development. Later on we also categorise the consortium members according to their very specific value chain profile. The mapping of the WP7 use cases onto the value chain is depicted in Figure 14.

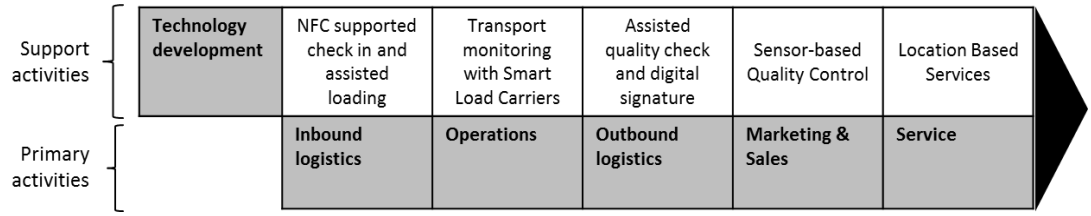

Figure 14: Mapping of the WP7 use case scenes to a basic value (retail/logistics)

As can be seen in Figure 14 the WP7 use cases cover all primary activities of the value chain. Each of the use cases are a result of the collaboration between the consortium members involved in the development, thus it can be said that all partner profiles, be it industry partners or research institutes, fit in almost each of value chain stages. Nevertheless we give a couple of examples of consortium members which provided their special knowledge in the respective use case. However, it is not possible to perfectly categorise each of the consortium members in the value chain as the concepts of IoT-A strike all consortium members to a greater or lesser extent. Hence we give only some examples in the list below which consortium member can possibly fit derived from his contribution in the development of the use case. This mapping cannot be regarded as generally accepted for the specific partner only since also other partners could fulfil this role.

- **SAP**: The use case on Sensor-based Quality Control shows how sensors monitor perishable goods in a store. The second use case in which SAP actively contributed, Location Based Services, shows the interaction of location tracking solutions – such as WiFi triangulation – with support of the IoT ARM to enable location aware applications which identify a customer's position in a store and provide location-based services. Furthermore, as a specialist in business-process management (BPM), SAP provides an innovative BPM modelling tool for IoT processes for modelling IoT business processes. These models can then be used for optimising the interplay between IoT technologies and business processes.

- **IBM:** With their Mote Runner, IBM provides a powerful infrastructure platform for wireless sensor networks that combines sensor and communication technologies. Mote Runner consists of two parts: a run time for mote-class hardware such as MEMSIC Iris motes, and a development environment for WSN applications. As such, Mote Runner is used in the use case "Sensor-based Quality Control" for tracking ambient conditions (e.g., temperature) and for transferring the gathered data to an information system. This system is then able to make decisions about the appropriate price of a perishable good.

- **FhG IML:** In the use case "NFC supported check-in and assisted loading" it is shown how one can use a device, such as an IoT Phone, for preventing mistakes in loading goods. This is achieved by automatically comparing loaded items with an order stored in an information system. The second use case deals with real-time sensor monitoring of smart-load carriers for preventing transported goods from being damaged because of environmental influences. The third use case demonstrates the capabilities of ownership transfer of goods and digital signature for supply orders. This is done in combination with an assisted quality check within the unloading process in the store. In all use cases FhG IML contributed by providing their special knowledge in logistics to appropriately manage the used technologies in each use case.

5.1.2.3 External Stakeholders in the IoT Value Chain – Retail

Even though a couple of external stakeholders come into question to be mentioned we focus on one specific company which interacted from the beginning of the project and thus demonstrated a clear interest in contributing in the project outcome. It relates to Groupe Casino and its representatives who attended to all the stakeholder workshops. The collaboration between IoT-A and Groupe Casinso was not limited to IoT-A events as Groupe Casino also invited consortium members from WP7 to a workshop. These consortium members who were

responsible for the use case development discussed certain use case scenes from the retail use case and the corresponding IoT-A concepts relevant to Groupe Casino. This collaboration showed that Groupe Casino can be considered as a perfect instantiation for an external stakeholder in the context of retail.

5.1.2.4 Conclusion

Overall it can be said that the IoT-A consortium members and external stakeholders are a small but representative group of technology providers in a future IoT world. By use of the Porter value chain model that even with this small group, their expertise in various IoT technologies map to a wide range of support activities can fit various links in the retail/logistics chains.

5.1.3 Health value chain

5.1.3.1 Ecosystem Description

The previous section described how the original Porter model was applied to the use-case domain logistics & retailing. As previously discussed, [Porter, 2004] introduced a framework for care units for instance all the stakeholders involved in the treatment of a specific disease (see Figure 15). This model emphasises the creation of value for the patient (in the top half of Figure 15). Similar to the retail case, there are discrete primary activities in each unit of care. These activities lead to direct value outcomes (highlighted in blue in Figure 15). The direct activities in turn are bolstered by support activities (highlighted in pink in Figure 15).

The unit-of-care relation to the wider health ecosystem was addressed by [Burns, 2002]. In the Burns model, the provider (or unit-of-care) is considered together with the payers of health care as well as intermediaries such as insurance companies (shown at the bottom in Figure 15). For completeness, we fused the Burns and Porter model in Figure 15.

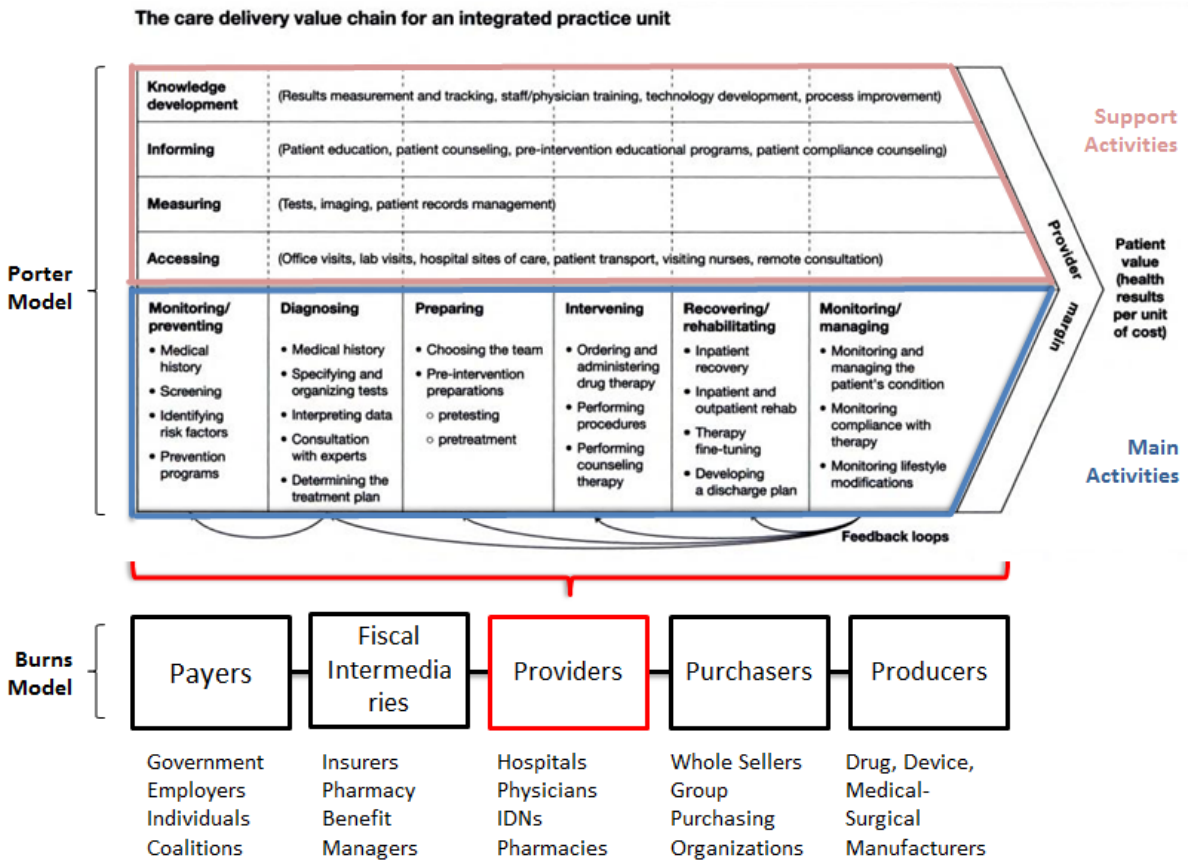

Figure 15: General framework for the health value chain ([Porter, 2004] & [Burns, 2002])

Our analysis focuses on the Provider unit described by the Porter model since the support of healthcare provision was the focus of the WP7 health use case.

5.1.3.2 Explanation of Mapping & Possible Fit of WP7 Consortium Members

As described earlier, within a unit-of-care model there are stakeholders and actions towards a health care outcome. In order to identify the type of key players and where they fit with actions and processes in a health IoT ecosystem, we mapped the use cases of WP7 to the Porter model. The mapping also tells us how other stakeholders similar to those in the consortium could contribute to IoT in the future.

It should be noted that the consortium partners are not primary health care providers but rather technology providers. As such, their potential lies in boosting existing health processes rather than affecting the direct intervention. MUNICH, the associate partner of IoT-A, is however involved in the intervention stage of healthcare.

The result of our mapping exercise is shown in Figure 16.

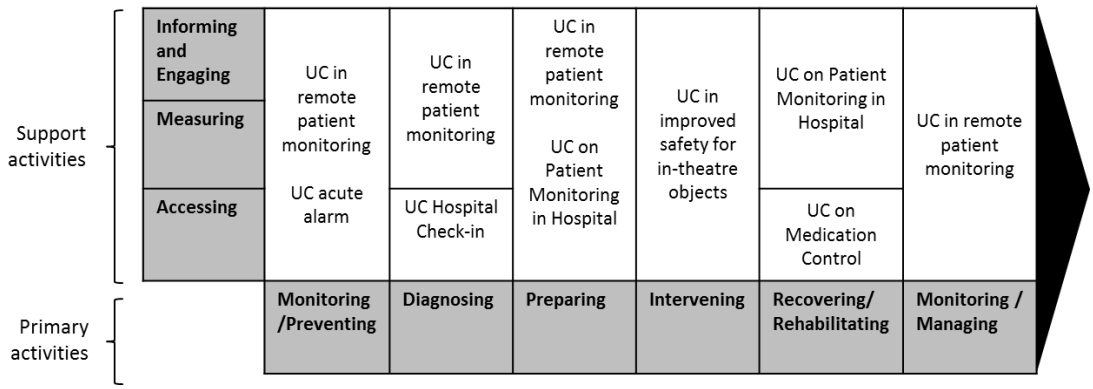

Figure 16: Mapping of the WP7 use case scenes to the value chain (health-care)

Figure 16 shows the healthcare use cases assigned to the respective primary and support activities of the value chain. A number of consortium members were responsible for the development of those scenes as it is was the case with the retail use case. To name but a few the following list shows which partner developed the use case and how it works.

Consortium members

- **Alcatel**: In their use case (Remote patient monitoring), ubiquitous sensors that are not part of a particular domain are seamlessly integrated and used by a remote health monitoring application. Patients are assisted and reminded remotely to take their medication and medical measurements, and their condition is also monitored. Thus, in a future IoT-A health care system, technology providers like Alcatel are involved in all three support activities (Informing & Engaging, Measuring and Accessing) for the health care steps of Monitoring/Prevention, Diagnosing and Monitoring/Managing. Their technology educates & informs patients and helps them to maintain care remotely. The information they generate is carried over to assist the intervention team in the Preparation stage as well.

- **CFR:** Their use case (Acute alarm) deals with monitoring acute syndromes of patients and triggering the necessary emergency services: as such they fit all support roles in the Monitoring/Preventing phase.

- **University of St. Gallen:** Their use case (Hospital check-in) employs sensors in every-day consumer goods in order to quickly identify patients and expedite unit-of-care check-in. All this is done by use of IoT-A's service-resolution framework. As such, this use case and technology facilitates access to the Diagnosis primary activity

- **University of Rome, Sapienza:** Their use cases (Patient monitoring in hospital and Medication control) deal with improving patient monitoring in the hospital by leveraging the IoT-A concepts of having mutually interpretable information from different sources. This concept is applied to dosage monitoring of medicine and monitoring of patients in the hospital. Such technology is helpful for Recovering/Rehabilitation in the hospital. Information carried over between Alcatel's remote monitoring and Sapienza's in-hospital monitoring would also assist the Preparation phase.

External stakeholder

- **MUNICH**: Their use case deals with tracking surgical towels and items in theatre / during operation, improving patient safety and quality of care. Accordingly, in a future IoT ecosystem, partners like MUNICH bring IoT-A support to the Intervening stage.

5.1.3.3 External Stakeholders in the IoT Value Chain – Health

Similar to the value chain for retail there were a number of external stakeholders in the value chain for health. The external stakeholders are those who participated in one of the six IoT-A stakeholder workshops or collaborated in another way with the IoT-A project.

This was the case for one stakeholder from Siemens healthcare, namely hearing instruments, who attended SW3. His contribution encompassed many aspects related to privacy and security of hearing aids and the integration of such instruments in the IoT. Furthermore he provided information about the development process how it is done today and the need for a common approach for which he thinks the IoT ARM concept could solve many issues. Regarding the value chain Siemens hearing instruments can be located in the last stage of the value chain as they provide post- treatment devices for patients.

Our associate partner MUNICH was also an important contributor to the IoT-A project. One of the stakeholders, Christoph Thuemmler, who attended all stakeholder workshops was the initiator of this cooperation. From the beginning of the project he was one leading person in discussions during the stakeholder workshops. Later on the cooperation between MUNICH and the IoT-A project provided the opportunity of performing validation with an already existing IoT application. As already explained above the MUNICH use case is located in the intervening stage of the value chain.

5.1.3.4 Conclusion

While the space of possible future external stakeholders in an IoT landscape is infinite, we note that these stakeholders cover a variety of IoT domains, and due to the fact that they were active in IoT-A as stakeholders, they are also likely to play a prominent role in a future IoT landscape.

The IoT-A consortium members and external stakeholders are a small but representative group of technology providers in a future IoT world. By use of the Porter value-chain model that even with this small group, their expertise in various IoT technologies map to a wide range of support activities can fit various links in the health-care value chains.

In this exercise, we have also identified a wide range of stakeholders beyond the scope of the project that can benefit in an even wider value chain. Therefore, future IoT projects should consider outreaching to these stakeholders (ex.care: insurers, drug manufacturers, payers) in order to foster widespread IoT adoption.

5.2 Business Case

In the previous section, we have identified at a general level what an overall value chain in retail/logistics and health could look like and what stakeholders could play a role in an IoT-A enabled world. In this section, we explicitly calculate and show what processes are changed and what value is generated by the IoT ARM.

To achieve this, we take two approaches in validating the business value of the IoT ARM.

In the first approach – the inductive forward development approach – taken for the retail business case, we look at use cases that were developed from the ground up and had used the IoT ARM explicitly as guidance. Accordingly, we select several use case scenes from WP7 – which we refer to collectively as the “virtual supply chain” - and evaluate their business value. In doing so, we show that the IoT ARM can assist development of IoT use cases which lead to value, and establish internal validity. The first use case consists of a supply chain for perishable goods and shows how novel technologies such as smart sensors – a combination of RFID and a sensor (e.g. temperature sensor) - can be integrated in a real world scenario to improve processes to be performed, as well as how they can facilitate decision making on a detailed, transparent, and real-time information basis. In the following the virtual supply chain use case will be referenced as use case 1 (UC1) and the corresponding business case as business case 1 (BC1).

In the second approach – the reverse mapping approach - taken for the health care business case, we focus on an already implemented IoT system, the MUNICH IoT platform. We first note that in D1.5, a reverse mapping exercise was conducted on the MUNICH IoT platform to show that the IoT ARM could describe and help realise such a system. We then show in this section the benefits of the MUNICH IoT platform. Combining the reverse mapping and the cost-benefit analysis conducted here, it then follows that the IoT ARM can help realise IoT systems of value, and not necessarily systems internal to the IoT consortium, thus establishing external validity. Cleary, not every instantiation of an ARM-based system would necessarily be a system of real world value, but this exercise would show that it sufficiently describes core concepts that can lead to real world value, thereby demonstrating the IoT ARM's relevance. In the health use case, patient safety is increased by means of surgery towels equipped with RFID. These towels can be tracked during a surgery and provide an electronic control in addition to a nurse keeping track of all used towels. In the following the virtual supply chain use case will be referenced as use case 2 (UC2) and the corresponding business case as business case 2 (BC2). Table 5 depicts all important steps of a business case that will almost completely be adopted for our business case.

Table 5: Business case structure [Schmidt, 2002]

Definition	Development & Methods	Validation	Results
- Subject - Purpose	- Cost model - Benefit model - Non-financial impact - Financial model - Financial metrics - Scope and main assumptions - Scenario model	- Sensitivity analysis - Risk analysis	- Conclusion - Recommendation

5.2.1 Business case framework

5.2.1.1 Structure

To be able to evaluate the performance of the two use cases, it is necessary to define a business case framework. This framework builds the structure, which guided the overall business case process. The goal of the framework is to deliver a decision support tool and highlight opportunities and potential risks [Bruegger, 2009]. Thus, this section focuses on the process and methodology, as well as key performance indicators of the framework for business case tools.

A business case is a "decision support and planning tool that designs the likely financial results and other business consequences and changes of an action or decision [Schmidt, 2003]. Hence, the reason why a business case is done is to support the decision making process before initiating a specific investment or project in order to make the best decision from an economic perspective. Therefore, a business case captures all required resources (e.g. personnel or money units), as well as demonstrates the potential benefits related to business activities [Ippisch, 2009]. After defining the income and outcome factors a comparison of the expected expenses vs. benefits aims to illustrate the result of the investment or project. To support the decision making process key performance indicators such as return on investment (ROI), cash flow (CF), discounted cash flow (DCF), cumulative cash flow (CCF), cumulative discounted cash flow (CDCF) and the net present value (NPV) are calculated to be able to compare the project or investment with alternatives [Schmidt, 2003].

Key elements of a business case are [Ippisch, 2009]:

- Background information on the project

- Assumptions and objectives of the project
- Applied methodology to acquire and generate data/information
- Project cost split into non-recurring and recurring cost elements of the investment
- Tangible and non-tangible benefits of the project
- Expected results and conclusions
- Potential risk and sensitivity analysis
- Limitations of the business case

Putting all these key elements into a process defining the workflow, the structure of the business case becomes apparent in Figure 36.

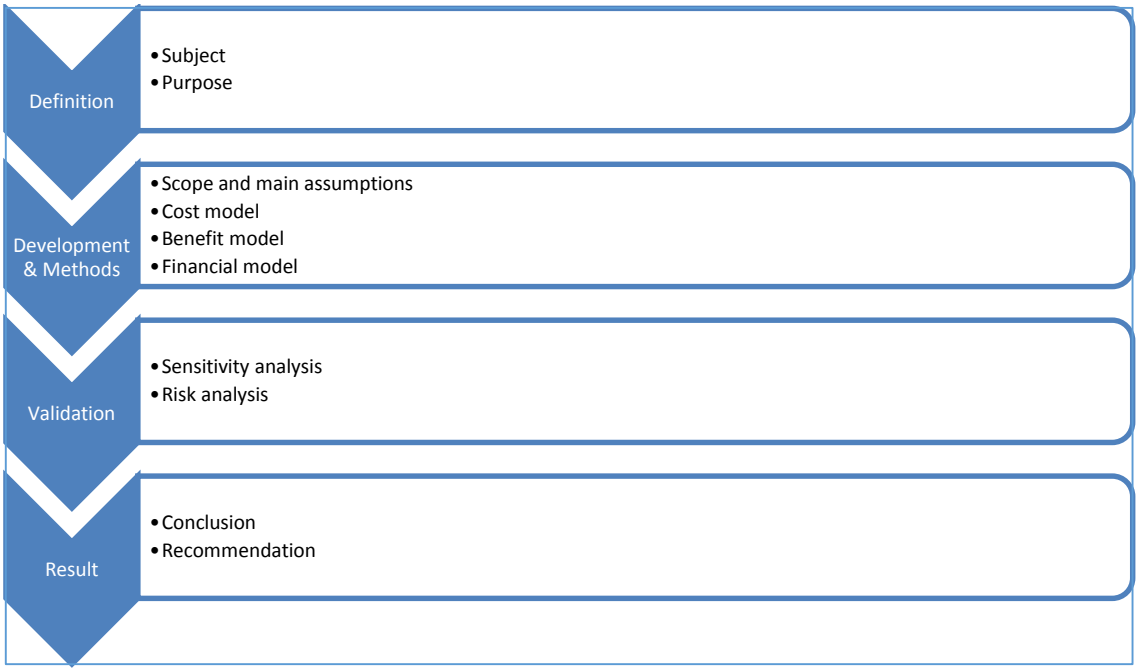

Figure 17: Business case process

5.2.1.2 Methodology

One of the essential challenges of a business case is (1) to identify and determine the required input variables and (2) to obtain the relevant data. Therefore, the corresponding costs for each use case have to be identified as well as the measurement and quantifying method of the benefits have to be determined [Ippisch, 2009].

To elucidate the methods, a short overview on how the data gathering is performed is given in this section. First of all, a literature review was done to search for comparable projects. This review includes the identification of common financial metrics, measurement methods, as well as general key cost drivers and key benefits from IT projects. As a next step, a number of market participants were interviewed to get basic data and background knowledge about the process and functionalities, as well as typical problem statements. Especially for UC1, the information acquisition was hindered by the fact of a highly competitive market environment in which the actors are not willing to disclose and share official information. Subsequently, workshops and expert interviews were conducted to identify potential risks, further developments, challenges, opportunities, and to validate the data. Furthermore UC1 was presented to different manufacturers, logistic providers and retailers on the international "fruit logistic exhibition" in Berlin 2013 to validate the data, get additional information and opinions, identify risks, process flow discussions and discuss further trends and operation topics. We need mention the naming issue of the experts particularly. Many of the assumptions were done

on the basis of statements from these experts but they are kept confidential as they did not want to be mentioned by name.

The business case for UC1 and UC2 use the same business case model, however the former is more related to the IoT ARM as it directly stems from the project while the latter is an external use case. The following sections explain the functionality and the information and workflow of the business case tool in general. Nevertheless, UC1 is much more detailed and has a bigger impact on different aspects due to higher number of scenarios. The following explanations for the business case tool should be regarded in the context of UC1 to understand the complete model. UC2 can be seen as a subset model of UC1, where calculation sheets not relevant to the UC were removed, which do not affect the total result and tool workflow. Considering this difference both business cases work equivalently.

5.2.1.3 Business case tool

Figure 18 shows the overall concept of the business case model and the general workflow of the tool. It can be seen as a graphical representation of the Excel sheet used to calculate the business case. The blue coloured arrows represent input factors that can be adjusted or/and have a significant impact on the following sheets. The input factors are used provide information as well as necessary parameters for the calculations. The red coloured arrows represent the results which are calculated in the respective part of the model. The results are used in later stages to calculate, generate or analyse further results of the business case. Figure 18 shows the slightly more complex tool BC1. The structure of BC2 does not include the sheets "Software development", "Project schedule" and "Demand and delivery" model (boxes are framed with dots).

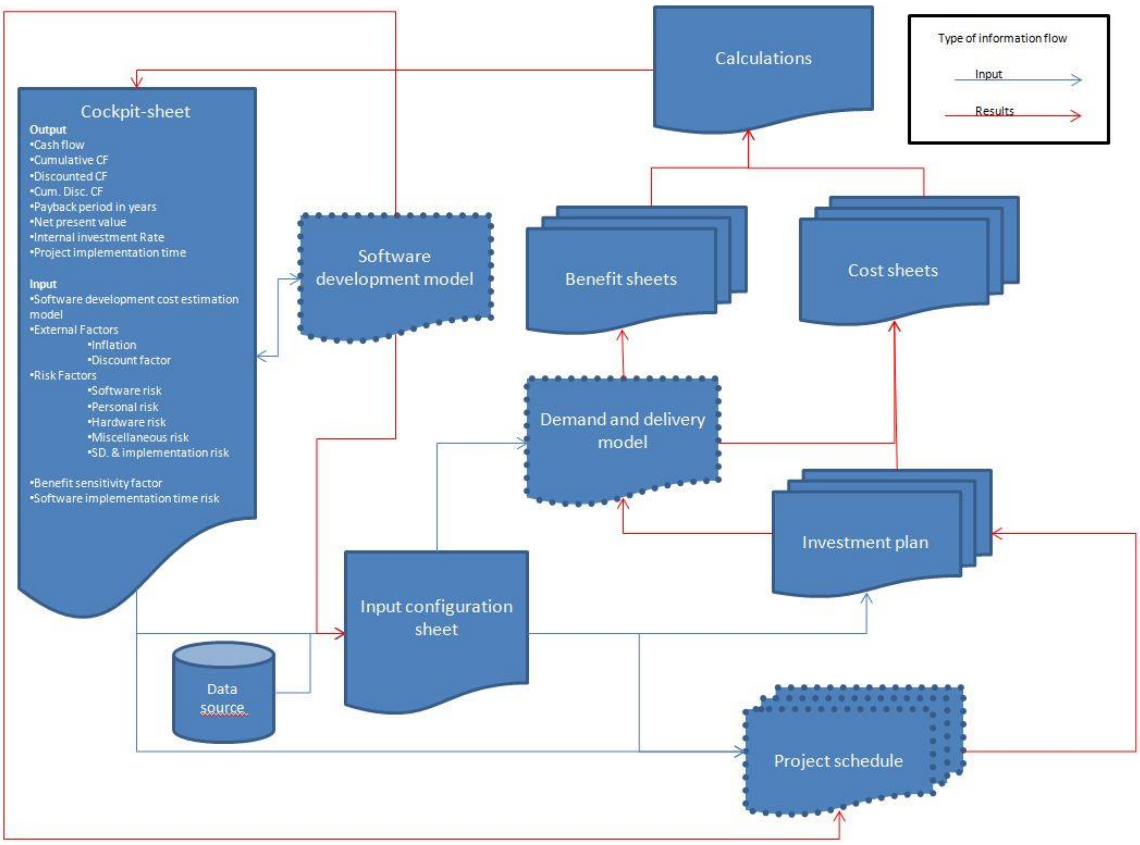

Figure 18: Business case tool functionality overview

In Table 6 it is explained how input data is used to generate the output and which tasks and goals are followed for each sheet. The variables and parameters which can be adjusted and configured are highlighted in the following chapters.

The “Cockpit sheet” is the central control unit in which the main input factors for sensitivity analysis, i.e. the risk factors, can be set. Moreover it presents the final result and key performance indicators.

The "Input Configuration" sheet is used to be able to do the fine adjustment of the business case. The sheet receives data from the "Data source" and "Software development model", as well as the overall parameters from the "Cockpit sheet". These are processed to create the basic input for the "project schedule" sheet(s), "Investment plan" sheet(s) and "Demand & delivery model" sheet. The data out of the database are basic parameters that are set at the beginning and does not change during the model simulation.

The “Project schedule” sheet(s) generates a project schedule based on the "Software development model" sheet and the basic input factors out of the "Cockpit sheet" and "Input configuration sheet”. The generated output is used to define the investment plan including the set parameters of the "Input configuration" sheet. The "Demand and delivery model" uses the data of the "Input configuration" to calculate the information for the benefits and cost sheets.

The cost sheets show all major cost drivers regardless of their type, and are associated with the cost owner. In this sheet the operation and recurring costs are integrated with the costs out of the investment sheet and also take into account the time value created in the project schedule sheet. The associated benefits receive the data from the "Input configuration" sheet and are processed and calculated in the "Demand and delivery" sheet. The calculated output from the different benefits and costs owner are consolidated in the calculations sheet. The information is merged and aggregated to present the final results in the cockpit.

Table 6: Information- and workflow of the business model

	Acronyms	Input data/ information	Task & goal	Output data/results for
Cockpit	CP	Result of CA	Set basic input parameter External factors Risk Factors Choose software estimation model Display aggregate results	SDM IC PS
Data source	DS		Define basic date that is not affected by input configuration or during simulation	Data for IC
Software development model	SDM	Expert interview	Cost and time estimation for software application development	Data for IC Information for IC Information for PS
Input configuration	IC	Data from DS Set factors from CP	Configuration and quantify input data for model Fine tuning of input data Enables case sensitivity analyse for benefit sheets	Data for DD Data for PS Data for IP
Project	PS	Set factors	Create and calculate project	Results for IP

schedule		from CP Set factors from IC Information from SDM	schedule plan Define time values	
Demand and delivery	DD	Set factors from IC	Created and calculate demand and deliver information	Data and results for B Data and results for C
Investment plan	IP	Set factors from IC Results from PS	Define investment plan for each cost owner Define time values for DD for each case	Results for C Results for B
Benefit	B	Data and results from DD	Calculate each Benefit based on the universal influence factor, calculate information and particular parameters	Results for CA
Cost	C	Data and results from DD Results from IP	Define the total cost per period per cost owner	Results for CA
Calculation	CA	Results from B Results from C	Calculate the results for the Cockpit Aggregate and summarized the information from Benefits and Cost	Results for CP

5.2.2 Business Case 1: Virtual supply chain

This subsection presents the business case for the virtual supply chain (UC1). First, the use case consisting of different scenarios is explained followed by the objectives pursued with the business case. Further the main part is presented, namely the calculation method and the calculation itself together with the results obtained. Since all calculations are based on assumptions we also perform a sensitivity analysis to show ranges in which the final results can be found.

5.2.2.1 Objectives

The goal for the sensor-enabled supply chain is to reduce potential risks and improve the process data flow. With the aid of generated information by IoT technologies, the decision making process can be supported e.g. sales, delivery scheduling, quality management and control. Besides short-, medium-term objectives and long-term objectives can be accomplished [Bruegger, 2009]. The focus of this business case is on the short- and medium-objectives, which are directly linked to the investment project. However, the usage of a standardised architecture generates long-term objectives as well.

The short- and medium-term objectives of the business case are aggregated into four main categories and depicted in Figure 19. In the following each will be explained in more detail.

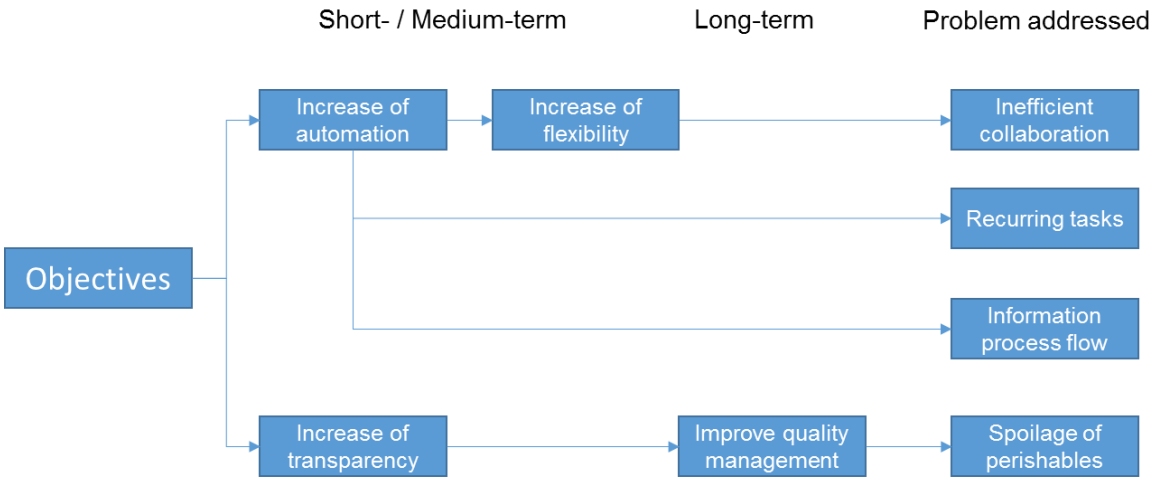

Figure 19: Short-, medium-, and long-term objectives

The short-term objective “Increase automation” addresses two problems in the cold chain. First, novel IoT technologies automate the information process flow in the cold chain and distribution. Second, the reduction of recurring tasks such as price labelling, quality control and load/unload control with support of IoT technologies increase the rate of automation.

Based on the increase of automation the objective “flexibility” emerges. The goal is on the one hand to increase the flexibility in the cold chain based on more and better information. That allows flexible order scheduling and planning as well as the integration of new partners in the supply and delivery chain. A further goal is the increase of transparency in the cold chain as a short-term objective. This mainly concerns the synchronisation between physical entities and their virtual representations, namely virtual entities, in the information systems. In this case not only real-time data of one parameter, e.g. temperature, increases the transparency of the cold chain rather than a combination of different parameters, e.g. temperature and humidity. Additional data obtained from a combination of sensors is accessible and can be processed along the different software applications.

The last objective is related to quality management. The requirements of the cold chain take into account environmental conditions during transports. The target is to improve the quality control along the chain with constant and real-time monitoring enabling the participants to react and solve problems instantly with the objective to reduce spoilage and loss of perishables.

Apart from short- and medium-term objectives companies involved in a cold chain follow long-term objectives. In a sensor-based cold chain the sensors and other IoT technologies produce a lot of data. The provided information is particularly useful if it is shared between all partners. Therefore trust and agreements are necessary aspects for collaboration. This is the reason why the stakeholders have to align their strategic relationships with each other to exploit the full value from novel IoT technologies [Bucherer, 2011]. Additional value can be created in case of data exchange within an involved company of a cold chain. As an example, quality information about products can be used by the daily quality control of perishables as well as for campaign management.

5.2.2.2 Problem statement

The main problem statements for the retail business case can be summarized into three major groups. The three main groups are:

- Software development
- Transport of perishable goods

- Customer satisfaction

A standardized software architecture improves the capability to develop flexible solutions for the cool chain that can be easily integrated and extended. Flexible means to be able to adapt new and different technology solutions and techniques. Transparency and standardized architectures should supply a solid fundament for the system architecture.

As a conclusion the former lack in transparency and real-time information about the transportation process is one problem statement in the state of the art process. The objective “automation and quality management” focuses on the reduction of the problems for this statement. Automation reduces manual errors and the transparency is increased by improved quality management with a real-time monitored cold chain [Atzori, 2010].

The last problem statement is the loss of customer satisfaction. The unavoidable necessity for the companies to react on potential bad reputation requires an accelerated search for solving this problem to maintain customer trust.

5.2.2.3 Risk

There are a number of risks associated with the successful implementation of the considered project. The major risks can be summarized in the following categories:

- Hardware risks, e.g. gateway for sensors are defect, service hardware break-down
- Software risks, e.g. software is not ready in time, insufficient system coverage
- Missing standard software and need for specific interfaces
- Willingness and readiness of the participants in the cold chain to share information and to invest
- Acceptance of the new system by employees
- Data security and privacy of the participants

5.2.2.4 Use case description

This use case addresses a logistics process in the cold chain for a retailer. The basic assumption of this use case is that perishable products are monitored with sensors and transported throughout the whole cold chain from a manufacturer via a logistic provider to a retailer. Information is generated and processed by the participants (manufacturer, logistic provider, and retailer). Different technologies used in the IoT, like Near-field communication (NFC), sensors, and electronic shelf labels (ESL) are integrated in the existing process to improve the workflow and provide real time data.

At the manufacturer we consider three different scenarios, namely flexible order scheduling, supported loading process and automated loading control. The logistic provider has the monitored transport scenario assigned while the retailer covers the automated receipt of goods, electronic price labelling and dynamic pricing scenarios. All scenarios are summarized in Figure 20 and explained in more detail in the following subsections.

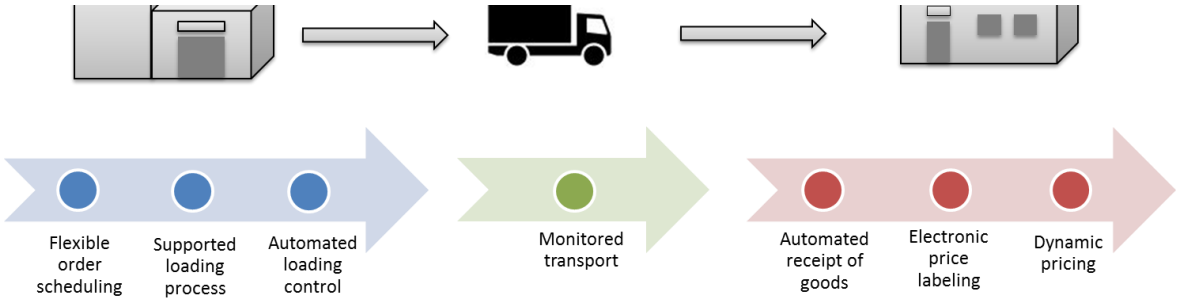

Figure 20: Use case scenarios considered in retail/logistics business case

Flexible order scheduling

A current problem in supply chains is that the participants have to react flexibly to last-minute order changes to adapt to new or changed demands. The new technology with Near Field Communication (NFC) enables the logistics provider, as well as the manufacturer to react flexibly to last-minute order changes. Nowadays the orders are planned and sent to the logistics provider at the day before or even earlier often without using electronic data transfer systems such as Electronic Data Interchange (EDI). If unexpected rapid order modification occurred the participants had difficulties to react. There are only a few options to handle the changes (e.g. fax message, phone call etc.). The benefit of the new IoT system will first of all keep the date synchronized with the information system and the order changes can be handled at a later stage so that only after the truck driver arrives at the manufacturer he becomes aware of the order changes when using his NFC device to receive the order list.

Supported loading process

Today data integration into the information system for the loading control is not fully automated and error-prone due to human mistakes. Typical errors are wrong loaded containers in terms of quantities of goods or false products. The usage of IoT technologies allows to reduce errors during the loading process at the manufacturer side. In other words sensor nodes are linked to the associated transport unit to enable a communication between the measurement systems (sensors) and the communication system (gateway).

Automated loading control

In the state of the art process the staff of the manufacturer has to check and control the loading process manually. This process step can be eliminated with the new system. Thus, the staff can be used for other activities and the loading control is done automatically.

Monitored transport

In the state of the art process during the transport no information about quality of the perishable goods is available. By means of a monitored transport via temperature or humidity sensors, alert messages can be issued in case of problems e.g. temperature or humidity fluctuations exceeding a pre-defined threshold.

Based on this information the truck driver can react immediately when a problem occurs and corrective actions can avoid damages of perishable goods.

Automated receipt of goods

The information provided by the sensor system also allows to avoid manual controls at the incoming goods control and the quality control activity in the storage as well as at the sales floor. The new system replaces manual activities by automation. Thus, the staff for this task can be used for other activities.

Electronic shelf labels

Electronic shelf labelling contributes significantly to the benefits as it enables selling prices to be displayed automatically. The manual labelling of prices can be avoided and the corresponding workload can be saved. To simplify the business case only the current price changes per day are considered.

Dynamic pricing

Electronic price labelling opens the opportunity to change product prices nearly every time in a retail store. The following two major benefits can be realized:

- Higher revenues via price discrimination
- Reduction of disposal quantities and respective cost

In the current process two price levels, namely full and half price, are assumed.

5.2.2.5 Business case model

The use case scenarios (2, 3, and 7) from WP7 are considered in the business case [Fiedler, 2012]. To exemplify the transformation process, Figure 21 shows the changes from a state of the art process to the target process for the loading process.

In the old process an employee has to check the loading container if everything was loaded correctly. In the target process this control step is done by the implemented system. Each container is equipped with a sensor to monitor the environmental parameters of the loaded products during the transport [Fiedler, 2012]. The logistic provider employee loads the container into the transporter and scans the container with his IoT phone to link the container with the transporter. Additionally, the information of the loaded container is checked against the order details to ensure a correct loading process. This automatic control process does not only improve the process flow, but is also essential for further process steps and the monitored transport. Due to this modification, the transparency of the process is increased with the support of IoT technologies, which also raises the rate of automations.

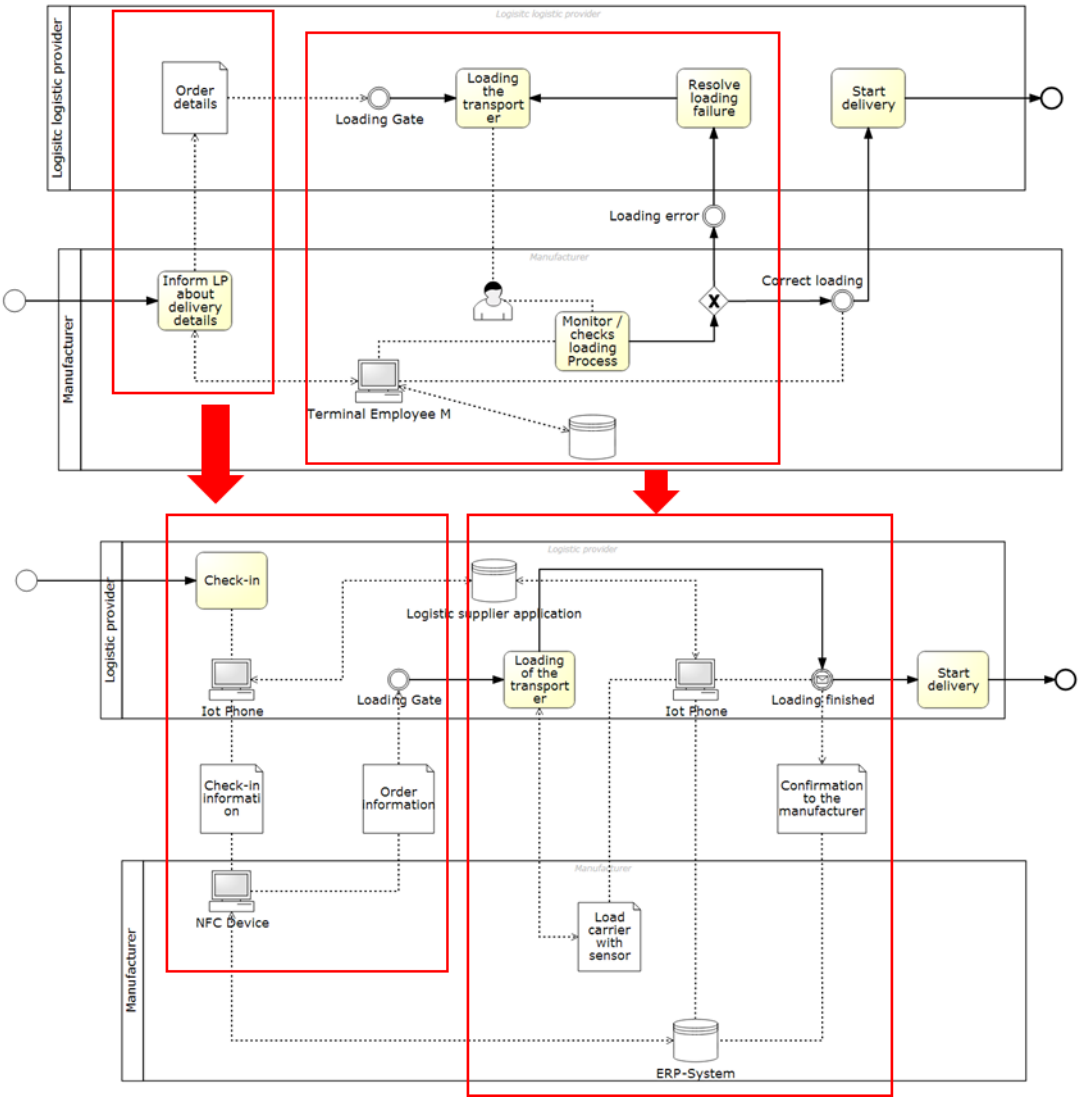

Figure 21: Transformation of loading process

5.2.2.6 Business case calculation

5.2.2.6.1 Assumptions and basis parameters

The figures used in the business scenario are mainly based on German conditions, especially income structure and working hours. The transporter units for the logistics provider have one delivery per day and are able to deliver goods for 5 retailer stores. The number of stores for the retailer is fixed to 20. For the calculation of the model it is also assumed that the ordered amount of goods in each category does not change and is constant for the analysis periods.

5.2.2.6.2 Costs

In the cost model the main cost drivers are identified. Table 7 shows the major cost drivers for the different participating organization units.

Table 7: Overview of cost drivers

	Cost driver	Cost objects
Virtual supply chain centre	Software development	Employees

	Project management & implementation	Consulting
	Software & hardware maintenance	Employees Eternal cost
Manufacturer	Hardware & rollout	IoT NFC device IoT IBM mote runner Employees
	Service and maintenance & ERP integration	Employees
Logistics provider	Hardware & rollout	IoT Phone IoT Gateway Employees
	Hardware maintenance	Maintenance Service cost
Retailer	Rollout project & ERP integration	Employees Consulting
	Hardware	Electronic Shelf Labels
	Hardware & software maintenance	Employees External costs

For the management unit "Virtual Supply Chain Centre" (VSSC), the main investment object is human capital. Fully trained employees are necessary for both the software development and the system and applications maintenance.

The cost drivers for the manufacturer and the logistics provider are hardware equipment. The running costs are mainly hardware maintenance and service. The manufacturer has additional ERP adoption and integration costs during the rollout phase. The main cost driver of non-recurring cost for the retailer are the rollout and hardware cost. Running costs are again mainly for maintenance of the hardware and software.

5.2.2.6.3 Non-recurring costs

The non-recurring cost (NRC) can be categorised in hardware, software development and project management and rollout costs. The software cost and time estimation as key influencing factors are particularly important for the project cost. Contingent on the results of the software development the project management and implementation schedule is generated. The software development as the main cost factor only concerns the VSSC. Besides small additional software development costs are necessary for the electronic price shelf labelling at the retailer.

To reveal the benefit of the IoT ARM we show the difference between the development of software applications with the support of the IoT ARM and the software development without IoT ARM. Thus, an appropriate cost estimation model is necessary that can be used in a very early development stage. In this case two cost estimation models taken into account, namely "Constructive Cost Model" (COCOMO II) in the second version and "Constructive Systems Engineering Cost Model" (COSYMO) [Akyazi, 2013], [Valerdi, 2005].

In order to obtain expert knowledge regarding the cost estimation for software development an expert workshop was set up. The first step of the workshop was, to introduce the software cost estimation models to the experts to build a common understanding for the application of both models. In a next step the COCOMO and COSYSMO model were completed for the case that the software development is done without the support of IoT ARM. Following the experts were presented the IoT ARM. The goal of this task was to identify benefits and disadvantages for using the IoT ARM in the software design and development process. After the differences were

identified another run through the cost estimation models was done to estimate the project schedule time and also determine the cost for the software engineering with IoT ARM.

The resulting data of the expert workshop were integrated into the COCOMO and COSYSMO software models [TOOL0, 2013]. Labour rate costs were set to 3.200 €/months [Gehaltsvergleich, 2013]. The final results of COCOMO and COSYSMO estimations are shown in Table 8 and Table 9.

Table 8: Estimations COCOMO

COCOMO	w/o IoT ARM	with IoT ARM
Schedule (Months)	13,1	9,1
Cost	181.423 €	59.541 €

Table 9: Estimations COSYSMO

COSYSMO	w/o IoT ARM	with IoT ARM
Schedule (Months)	13,1	4,9
Cost	275.877 €	138.975 €

Both cost estimation models demonstrate that the cost of software development is lower, if the IoT ARM is used. This is also underlined by the software development time.

In result of both models for the software development time without IoT ARM is around 13 months. But there is a difference in the development time with IoT ARM (4.9 / 9.1 months by COSYSMO / COCOMO). This time difference has a significant impact on the results of the business case and affects certain components of the model.

The business case model is constructed to use both estimation models and to switch between them in the Cockpit sheet. The underlying model in the business case is the COSYMO model as it is a more conservative assumption. The impact of longer development time is simulated in the risk analysis.

In case the IoT ARM supports the software development the non-recurring costs occur only in the first business plan period. Otherwise if IoT ARM is not used the non-recurring cost are extended to two business plan periods. The impact of the business model is that software development cost as well as hardware investment and rollout cost occur in the second period. The main effect of the later project implementation is that benefit realization is delayed.

As mentioned before, the retailer has also a small software integration for the electronic shelf label system. Cost occur with the amount of 60,000 € in case IoT ARM is used and raise around 62,000 € due to the time difference and inflation rate without IoT ARM.

5.2.2.6.4 Recurring costs

The recurring costs can be interpreted as the operating costs of the system. The biggest share of the operating costs are the maintenance and service cost for software applications and different hardware devices. Each recurring cost unit is added and is a risk factor to cover potential changes over the time and estimation errors.

The main cost driver of the operating costs are expenses for qualified personal. IT-administrators and software developers have to be hired to run the supply chain system, but also to maintain, upgrade and enhance the system. The employee cost are calculated with the average labour expenses for the appropriate personal and multiplied with the total amount of needed personal. Another smaller part of the operating cost belongs to the retailer. The different

retail stores need IT administrators to monitor the electronic shelf labels and to manage the dynamic pricing software solutions.

The training costs are assigned to the VSSC. The IT domain experiences very fast development cycles with many novel technologies. Therefore the employees need trainings and workshops to be able to adapt new technologies, increase the performance of the system and keep up to date with new developments.

Another important operating cost element is the network and infrastructure cost. The new sensor-based supply chain depends strongly on a working information infrastructure. The cost for training as well as network and infrastructure are derived from a similar IT-project.

Maintenance costs for the software and hardware are calculated with a typical factor of the original purchase price or production cost [Li, 2009], [Weier, 2013].

Software maintenance costs differ in the usage of IoT ARM or not. The cost for the case with IoT ARM are lower. The standardized system architecture allows to integrate additional software and hardware solutions easier. Further new employees can become familiar with the system more easily.

5.2.2.6.5 Benefits

The benefits can be split in two main categories, these are the tangible and non-tangible benefits. Subsequently, both are explained in more detail.

5.2.2.6.5.1 Tangible benefits

The tangible benefits are calculated in two different ways. The first method considers the benefit equal to the saved cost:

$$Benefit\ (B) = C_{saved\ cost}$$

The second method compares the cost in the state of the art process with the cost for the new process.

$$Benefit\ (B) = C_{goal\ process} - C_{state\ of\ the\ art\ process}$$

The start of the benefit realisation depends on the used software development estimation, either with or without the support of IoT ARM. The benefits are discussed without taking into consideration the time differences and discount rate to simplify the explanation.

In order to stick to our example of the loading process the following benefit calculation shows the results for this scenario, however, it is only one calculation out of 7. In the old process the loading control was done manually, as well as the integration of the data into the information system was not fully automated. In the state of the art process the data between information systems and the actual data might show considerable differences. A further problem is the error-proneness in the old process. Typical errors are wrong loaded container in terms of quantities of goods or wrong products. The new technology allows to reduce loading errors during the loading process at the manufacturer site. The employee of the logistics provider scans each loaded container with his IoT phone and the system checks the loaded products against the order list. If a wrong loaded container is loaded into the truck an error message is sent to the employee. He is the only person allowed to finish his tasks, if the loading process is fulfilled correctly.

The model takes into consideration that the manufacturer and logistics provider have to supply the retailer with a 100% correct order. Wrongly delivered goods cause additional extra transport cost in the state of the art process which can be significantly reduced with the new system. Table 10 gives an overview of the parameters and how they are used to calculate the benefits.

Table 10: Benefit calculation: supported loading process

Description	Variable / formula	Data	Source
Parameter that a failure occurs during loading process per week	z	2%	(Author 4. 2013)
Total volume of orders in transport units for one week	TU	260	Calculations: Demand & deliver model
Parameter that a failure during loading could be solved with the new system	y	0,9	Assumption
Cost for extra transport per container	S	150	(Author 4 2013)
Cost with old systems	CWOS= b*z*S	780	Calculation
Cost with new systems	CWNS = b*z*(1-y)*S	78	Calculation
Cost savings per week	CSW = CWOS-CWNS	702	Calculation
Cost savings per year	CSY	36.504 €	Calculation

5.2.2.6.5.2 Non-tangible benefits

Non-tangible benefits are mainly based on subjective and thus not measureable benefits which often includes hypothetical assumptions, e.g. higher flexibility (how can one use this flexibility?). As an example one can regard smart things which are spread across the process and generate new data and information. These have to be analysed to which extent they cause business value [Bucherer, 2011]. New warehouse management and distribution scheduling based on better quality information can also contribute to long-term goals such as acting as a sustainable company by reducing the volume of disposals [Dada, 2008]. There exist further effects in customer relation management if data is enhanced with meta-information a fully automatic reporting and analysis is possible. Trends and customer wishes can be discovered and individual offers can be provided to improve the customer satisfaction [Bucherer, 2011].

5.2.2.6.6 Benefit analysis

The sensor-enabled cold chain monitors the temperature conditions in each process step and generates new information value. An interesting aspect is to identify which of the benefit models has the highest impact on the business model result. For the purpose of comparability and to reveal the financial impact of each scenario Figure 22 shows a ranking for all scenarios based on a full operating year (2015). This year is suitable for an overall analysis, because this is the first time period where the case of development without IoT ARM achieves the same level of benefit as with IoT ARM and the further specifications and characteristics are equivalent for both cases.

The first step of the benefit analysis is the ranking of each benefit model (BM) according to its contributing value. The benefit models "dynamic pricing (BM7)","monitored transport (BM4)" and "electronic price change (BM6)" account for 91% of the total benefits. The highest value contributing to the business case is added by dynamic pricing with 67% of the total cash inflow (see Figure 22). This demonstrates that new generated information is not only used to create transparency and flexibility, as well as to improve automation levels but it also adds new business opportunities that increases the sales performances. Another conclusion of the analysis is that the three major benefits aim to improve the customer-focused solutions. The available data is processed to provide goods based on price differentiation to the customers.

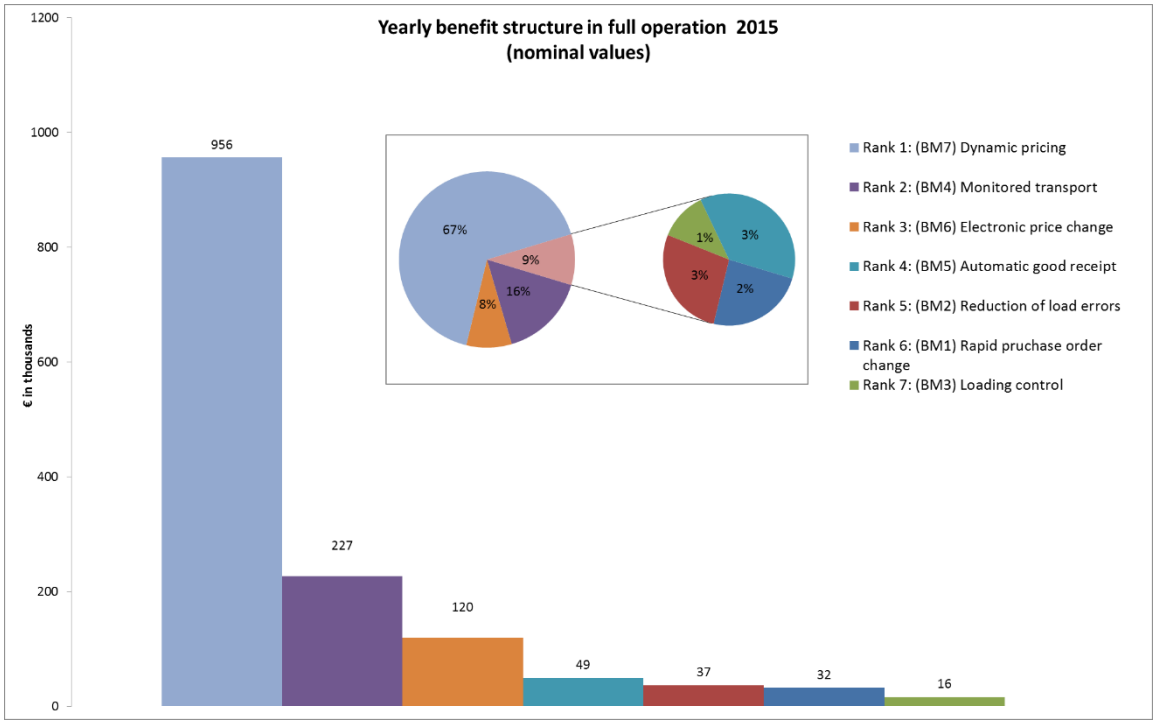

Figure 22: Benefit calculation: supported loading process

In the benefit development it has to be distinguished between the usage and non-usage of the IoT ARM during software development, especially in the first and second year (see Figure 23). In the case IoT ARM is used the benefits already arise in the first year and are still higher in the second year compared to the non-usage of IoT ARM. The differences between with and without IoT ARM is in the first year around 570,000 € and in the second year around 370,000 €. After the second period both models achieve the same amount of yearly benefits as the underlying assumption is that both solutions perform similarly. Overall the project using IoT ARM has higher cumulative benefits of nearly 938,000 € or 13% after all considered business case periods.

The reason for this gap can be identified by comparing the project time schedule. The assumed longer development time without IoT ARM leads to a total longer project implementation time. Therefore the benefits start not until the second period. The implementation with IoT ARM is completed in the first year and initial revenues can already be achieved. Full revenues can be achieved in the second year. Further constant but minor benefit increases in both cases are the effect of the inflation rate. This result confirms the expert opinions.

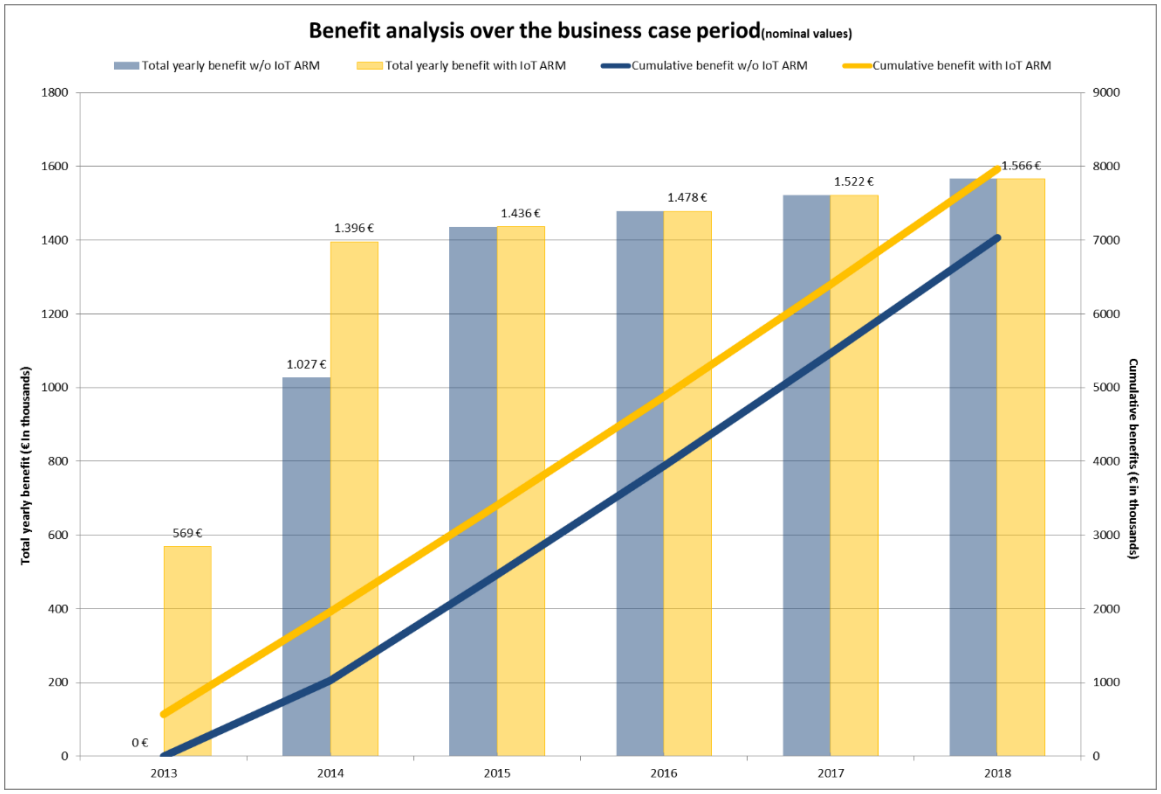

Figure 23: Benefit development over business case period

5.2.2.6.7 Cost analysis

In the cost analysis a general distinction between non-recurring cost (NRC) and recurring cost (RC) is necessary.

The NRC can be split in four cost elements:

- Software development
- Rollout
- Project-management
- Hardware

The main difference between the two project approaches resides in the software development for the two cases with and without IoT ARM. The remaining cost elements are for both cases almost equally big. The small differences emerge from a longer project implementation time and resulting price escalation.

Software development with IoT ARM is not only faster but also around 43% cheaper than the usual software development. This cost comparison illustrates another advantage of the IoT ARM development.

The RC consist of the following cost elements:

- Operating cost
- Hardware maintenance
- Training
- Network & infrastructure
- Software maintenance

The different amounts of the cost elements are shown in a full operation year (2015). The IoT ARM has also an advantage in the RC per year. The software maintenance cost (including

small modifications) are around 73,000 € cheaper by using IoT ARM. The gap can be explained with provided standardization of the architecture and the support by models and guidelines e.g. functional and information model.

The accruement of NRC and RC along the business case timeframe is presented in Figure 24. The NRC for the case without IoT ARM shows how the investment costs can be classified within the first two years. In the beginning the stakeholder has only to invest in the software development. The purchase of the hardware and the rollout start in the second year. Therefore the peak of expenses are in the second year. After the second year only the recurring costs occur, and due to inflation they rise slightly over the years.

If the system architecture and software applications are developed with IoT ARM, the development project finish earlier. This impacts the point in time when the purchase of hardware can be done as well as the rollout which both are done in the first year. Therefore the cost development has his peak in the first period. In the following years only the recurring cost remain. The RC are lower with IoT ARM due to the cheaper software maintenance cost.

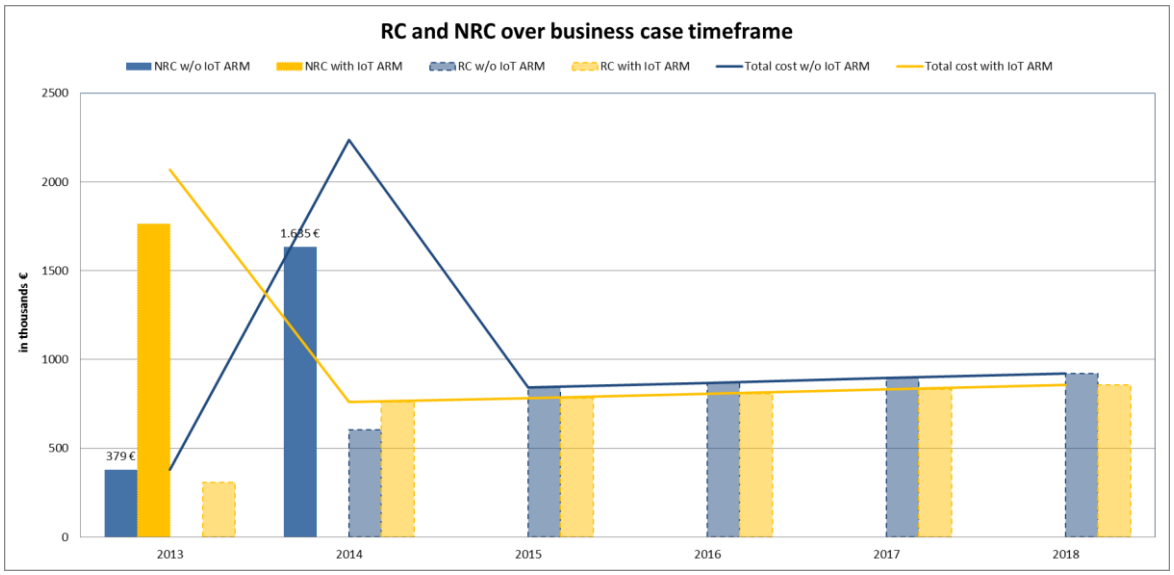

Figure 24: RC and NRC over business case timeframe

The results demonstrate that using IoT ARM yield advantages mainly in the shorter timeframe for development as well as considerable cost savings by the development and software maintenance cost. But looking at the total cumulative cost the difference of the two scenarios is small (40,000 €) due to the earlier operation time of the case with IoT ARM. These additional RC have to be taken into account and eat up the above mentioned cost savings by the software (see Figure 25). The major economic advantages using the IoT ARM lies in the speed of the development and the possibility to exploit earlier benefits.

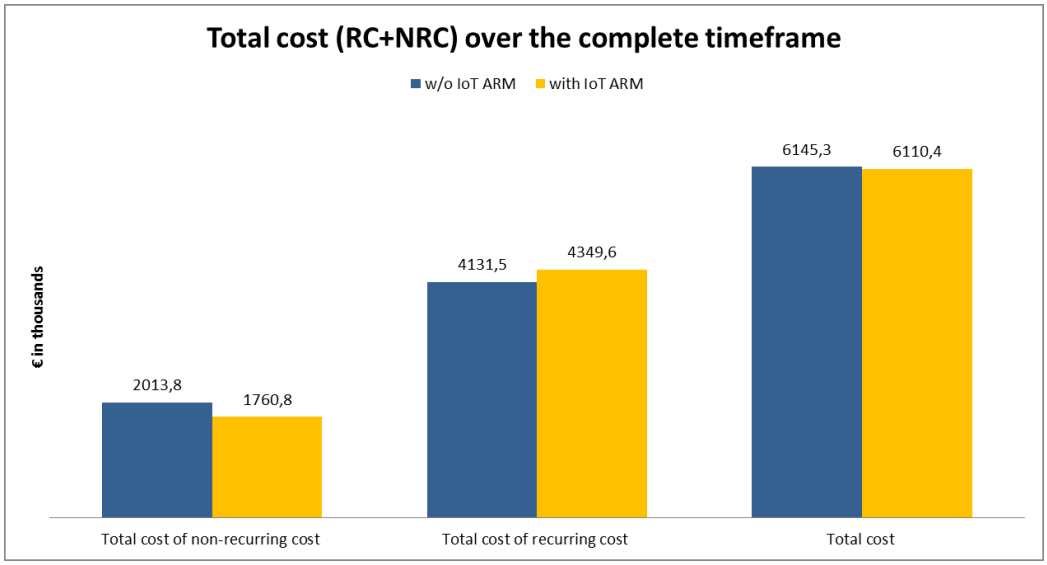

Figure 25: Total cost over the complete timeframe

5.2.2.6.8 Cost-benefit analysis

In Figure 26 the cash flow development over the business period of six years is shown. The implementation without IoT ARM has a lower negative cash flow in the first period, but after the second investment year the case with IoT ARM demonstrate a superior business performance for the remaining analysis periods. From the third period onwards the cash flow in both development scenarios are approximating with minor advantage for the scenario with IoT ARM.

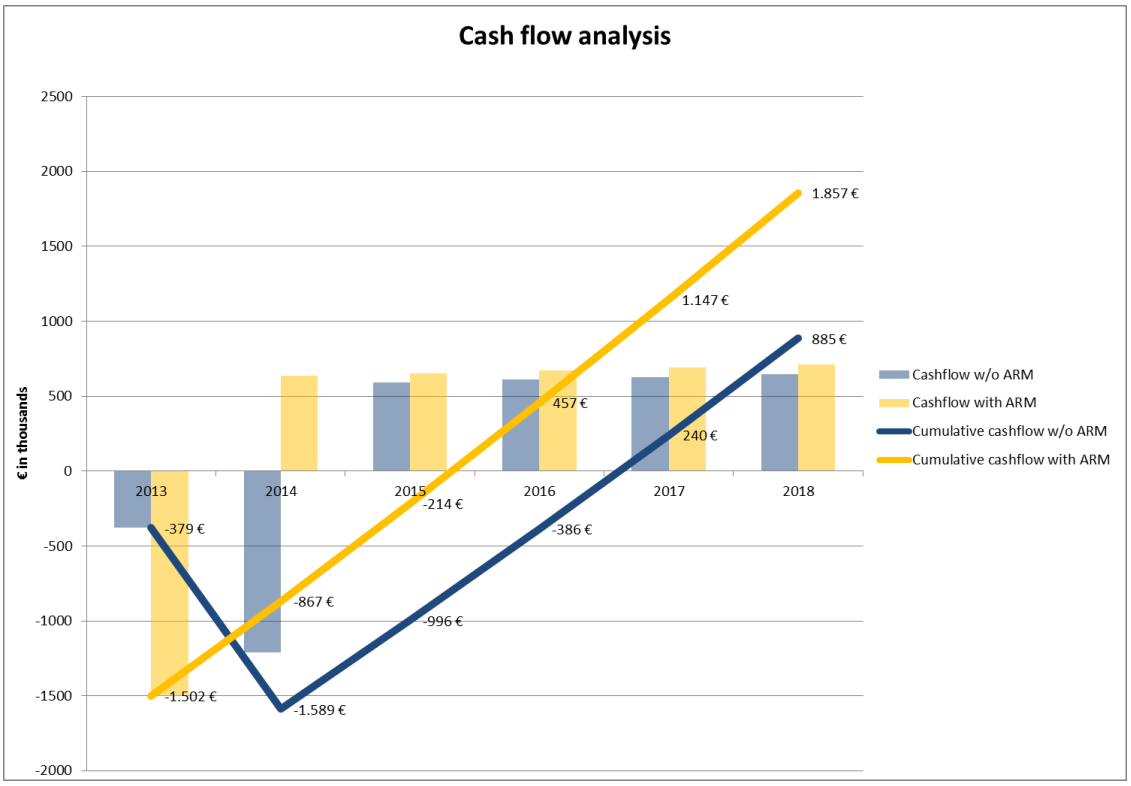

Figure 26: Cash flow analysis

The concrete advantage of IoT ARM conveys in the cumulative cash flow. The trendline indicating the cumulative cash flow of the implementation with IoT ARM raises from the beginning of the project. A positive result is already achieved during the third investment year and the end result is nearly 1.9 million €. In contrast to the previous trendline the trend of the cumulative cash flow without IoT falls in the beginning before it starts to raise. A positive result is not achieved before the fourth year. The cumulative cash flow in the sixth year is almost 1 million € lower than with IoT ARM.

The identified advantages of a shorter development time and lower cost are even more remarkable in an analysis with the discounted cash flow. The discount factor is used to calculate the present value of money that will be received in later periods.

The cumulative discounted cash flow (CDCF) shows a good comparability for all parameters of the business case model. Therefore several simulations of different influence factors can be done. This key performance indicator not only allows an analysis over time but also calculates the net present value of each scenario (see Figure 27).

The main difference between the two cash flow analysis models is that the cumulative curves are shifted rightwards and the payback time for the investor is achieved at a later period.

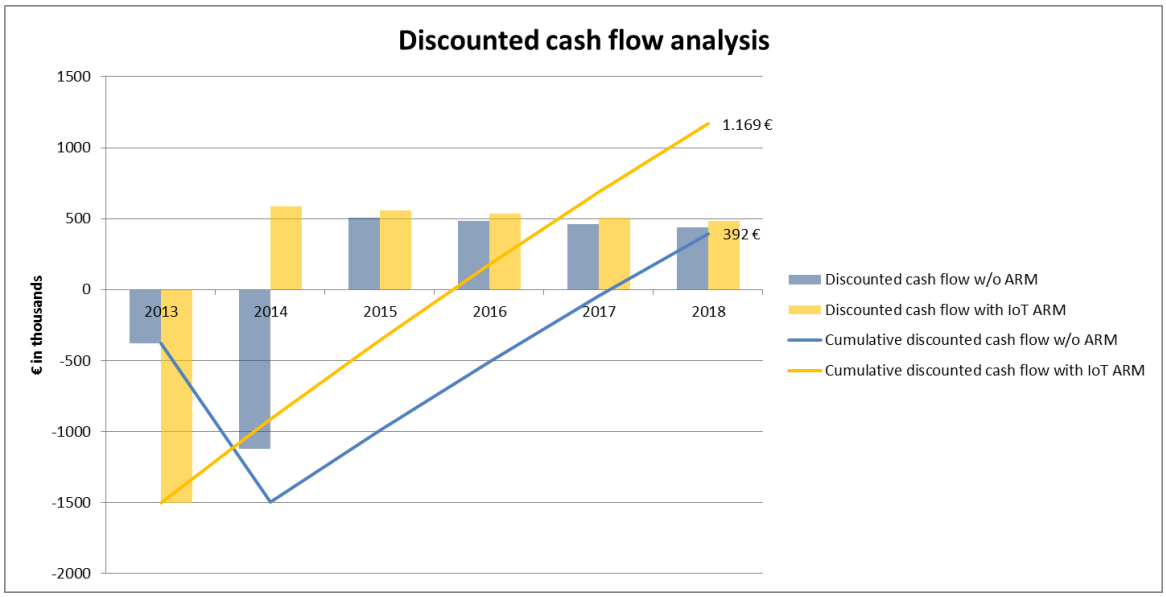

Figure 27: Discounted cash flow analysis

The final results of the major KPIs for the two cases of project implementation “with” and “without” IoT ARM are compared Table 11.

Table 11: KPI comparison

	w/o IoT ARM	with IoT ARM
Payback period in years	4,1	2,9
Net Present Value (T€)	419 €	1.200 €
Internal Investment Rate	18,58%	34,40%

Project implementation time in months	15,2	7

As explained before, the project implementation time determines the start of the running cost which impacts the payback period and the net present value. The business case results show that software architecture and software applications developed by the IoT ARM have a net present value of 1.2 million € or nearly three times the value of the case without IoT ARM. The internal rate of return (IRR) is 34.40% compared to 18.52% while the payoff period is 2.9 years compared to 4.1 years.

5.2.2.6.9 Risk factors

A business case is always developed under certain assumptions which potentially evoke risks. The configuration of these risk factors can be decisive for the result. The major parameters and their settings are summarized in Table 12.

Table 12: Basic sensitivity parameter overview

Risk factors	Abbreviation	Value
Inflation factor		3,00%
Discount factor	DF	8,00%
Critical Risk factors	CRF	
Software risk	SR	0,5
Personnel risk	PR	0,1
Hardware risk	HR	0,1
Miscellaneous risk	MR	0,20
Software implementation time risk	SITR	0,00
Benefit sensitivity factor	BSF	0

The retail case has a large focus on the software development and the two cases with and without IoT ARM. Therefore an additional parameter is created which covers the aspect of longer development times. In the basic analysis this factor is configured to 0% and changes will be discussed in the sensitivity analysis.

Another factor does not affect -as most of the preceding parameters- the cost side, this parameter focuses on the benefit side (BSF). The retailer case includes several benefits models and this parameter aims to demonstrate the sensitivity of the total benefit and the impact on the model on different scenarios. In the basic scenario this factor is also set to 0% and the specific impact on the model will be also analysed in the sensitivity analysis.

5.2.2.6.10 Sensitivity analysis

The positive result of the business case calculation shows a clear benefit for the usage of IoT ARM. In this chapter, the robustness of the business case model will be analysed in respect of possible changes of main influencing factors. The sensitivity analysis includes the following aspects:

- Higher and lower internal interest rate (6%, 10% 12%)
- Raise of the risk factors (+10%, +20%, -10%)
- Longer software development time (20%, 50%)
- Benefit robustness (-10%, +10%)

5.2.2.6.10.1 Sensitivity analysis of the timeframe of software development

For this reason the development time is increased by 20% and in the second simulation by 50%. For the case that IoT ARM is not used the development project time enlarge from 13.2 months to 17.8 and 21.7 months. This does not only lead to a later earning of the benefits, it also increases the NRC. For the case that the development time is 50% longer no positive net present value can be achieved in the given business case timeframe. The faster and shorter software development with IoT ARM is even robust to this negative effect. The simulated results clears show an increase in the NRC that also leads to reduction of the net present value, but overall still reasonable results can be achieved with the support of IoT ARM.

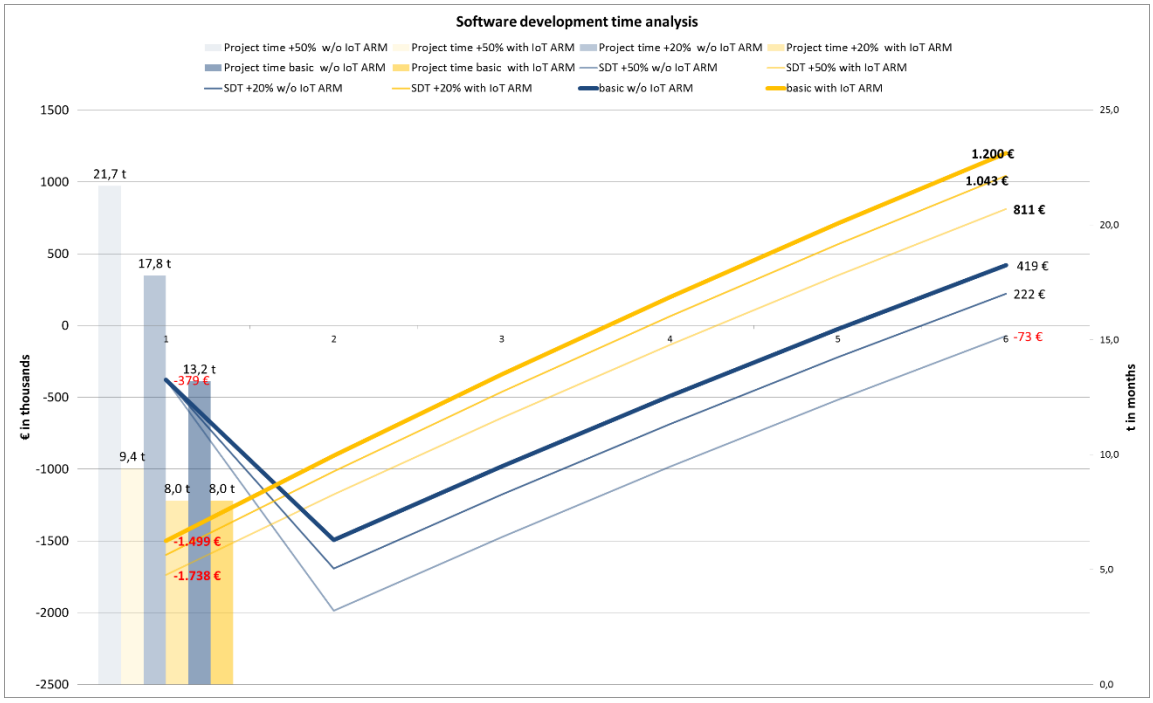

Figure 28: Software development time analysis

5.2.2.6.10.2 Sensitivity analysis of the robustness of the benefit model

The model behaviour is as expected. An increase of the benefit sensitivity factor shifts the cumulative discounted cash flow curve to the left side and raises the net present value as well as a reduction of the factor shifts the curve to the right sight and decreases the net present value. If benefits increase by 15% the net present value raises 1 mil € in case IoT ARM is used and vice versa 1 mil € NPV is eliminated if the benefits are reduced by 15%.

An adjustment of the benefit sensitivity factor by 1% increases or decreases the net present value by 64.5 T€ for the analysis in which IoT ARM is considered.

In the case without IoT ARM 1% increase or decrease of the benefits leads to a NPV change of 55 T€. If the benefits reduced by more than 7.5% no positive net present value can be generated. The Figure 33 shows a negative net present value if the benefits are reduced by 15%.

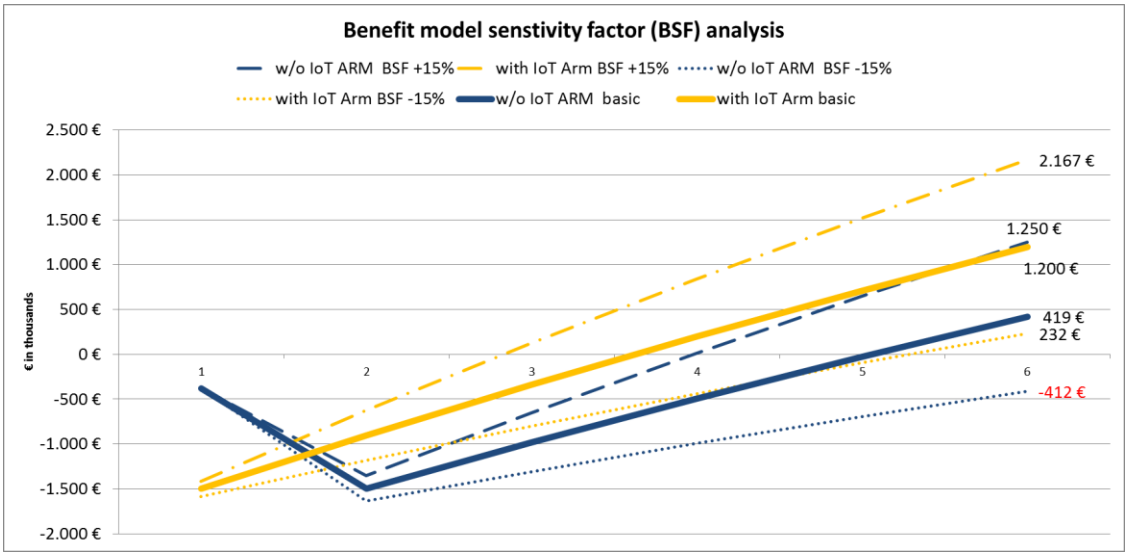

Figure 29: Benefit model sensitivity factor analysis

5.2.2.6.10.3 Sensitivity characteristics

The different types of sensitivity analysis and their impact on the business case model show the following results of their characteristics if one parameter is adjusted for 1%. The strongest impact with the highest amount of net present value change is the benefit sensitivity factor. This factor triggers all seven benefit models and leverages the total income of the benefit model. The next two major impacts on the simulation model are the critical risk factors and discount factor. The factor with the lowest impact measured by the net present value is the software development time factor (see Table 13).

Table 13: Sensitivity characteristic

Parameter	Impact on model	Effect	Net value for a change of 1%	Trend (DC decreasing also all factors over time)	Ranking
Critical Risk Factor **(MR;HR;SR;PR)**	Cost model	CRF↑ → Cost items↑ → NPV↑ CRF↓ → Cost items↓ → NPV↓	w/o IoT ARM: 54 ~ 55 T€ with IoT ARM: 57 ~ 56 T€	Constant	++
Discount Factor	Cockpit (Time series)	DF↑ → Future value of money↓ → NPV↓ DF↓ → Future value of money↑ → NPV↑	w/o IoT ARM: 49 T€ with IoT ARM: 71 T€	Decreasing by 2 T€ per percentage	++
Software development time factor	Project schedule → cost model & benefit model	SDTF↑ → Cost↑ & Benefit↓ → NPV ↓	w/o IoT ARM: 10 T€ with IoT ARM: 8 T€	Constant	+
Benefit sensitivity factor	Benefit model	BSF↓ → Benefit↓ → NPV↓ BSF↑ → Benefit↑ → NPV↑	w/o IoT ARM: 56 T€ with IoT ARM: 65 T€	Constant	+++
	↑ = increase | ↓ = decrease | T€ = thousand €				

A further analysis is also done by increasing the risk and external factors stepwise up to the point that a negative NPV is reached. Only the inflation rate is excluded as the only pure external factor. All parameters are increased incrementally by 1% steps. The first limit is reached for the case without IoT ARM at the second step. The case with IoT ARM reaches the limit by 6 steps (see Table 14).

Table 14: Parameter settings

Case	Parameter settings	Steps
Without IoT ARM	DC 11%; SR 53%; PR 13%; HR 13%; MR 23%; SDTF 3%; BSF 3%	2
With IoT ARM	DC 15%; SR 56%; PR 16%; HR 16%; MR 26%; SDTF 6%; BSF 6%	6

5.2.2.6.10.4 Best case & worst case scenario

As a first step two different condition changes are considered to generate different scenarios for the analysis.

In the best case scenario all critical risk factors are decreased by 10% and additionally we assume the project can be realized 10% cheaper. Likewise, the DF is reduced from 8% to 6%. The results show positive increase for the business performance. The best case scenario is driven by two assumptions. First, the cost for hardware will decrease over the time. Second, the cost savings can be achieved, due to standards for the architecture and technologies.

The worst case scenario simulates the situation that the stakeholders demand a higher safety margin, which increases the discount factor to 10%. Further the software development time increases by 25% and leads to a longer total project time. All benefits are reduced by 10%. The results are displayed in Figure 30. In this worst case scenario only the case with IoT ARM can save a positive net present value around 268,000 €. In the case without the IoT ARM the result shows a negative net present value of -409,000 €. The worst case scenario is based on the assumption that software development is still a risk intensive project. Additionally it is assumed that the benefit realizations do not behave as calculated, due to smaller margins.

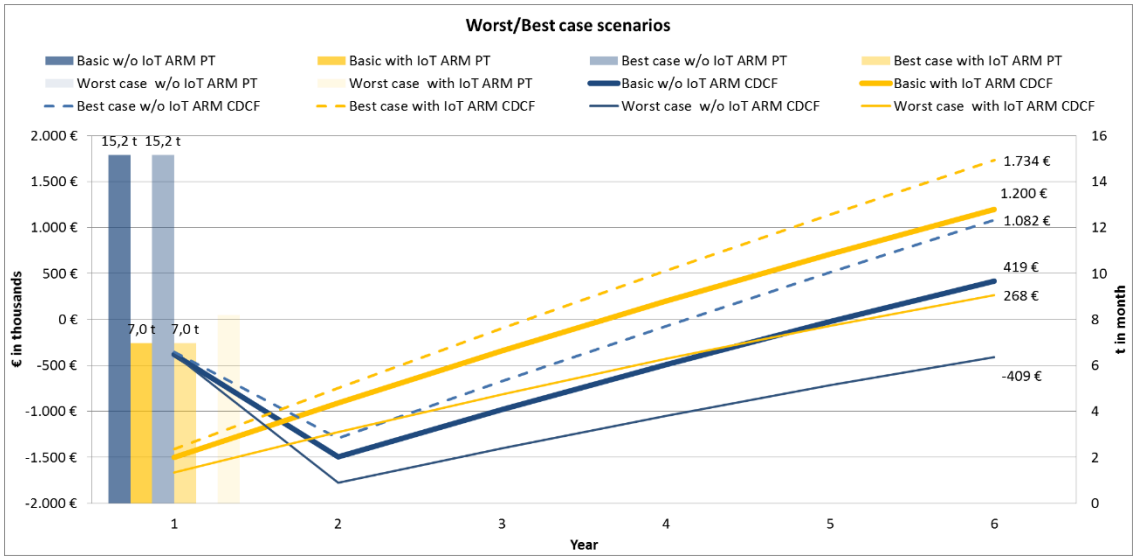

Figure 30: Worst/best case scenarios

5.2.3 Business Case 2: RFID-supported surgeries

In the health care case, medical surgery towels are equipped with RFID chips to help identify and keep track of them in the human body during surgery, with the goal of improving patient safety and automating manual and error-prone process steps. This process is supported with a cloud software platform that monitors the surgeries and supports the operation personnel in their tasks.

The goal of this business case is to evaluate the operating efficiency and profitability of such a system. In combination with the reverse mapping (see section 4.5.1), we show that not only can the IoT ARM describe and help realize existing IoT systems, but that these systems also bring value.

The results of the business case should support the decision process of the hospital management about the use of this solution in terms of economic feasibility. Accordingly, the focus of the business case is on the cost, benefits and risks. The software development itself is assessed by the supplying company and amortized in software service fee. The amount of the software development cost was not disclosed. In this respect, the business case does not reflect a cost comparison between the development process of the system application with and without IoT ARM [Zocher, 2013]. Instead, we see the IoT ARM as an enabler; Standards in system and architecture design like the IoT ARM fosters integration of new innovations, especially in a fragmented landscape like health care. For this reason, the business case assumes that the hospital management decided that new software solutions must be compatible with the IoT ARM framework to be able to provide a standardized basis for integrating future developments.

5.2.3.1 Background & objectives

Background

The use case was implemented and carried out by several companies and universities in the framework for the Initiative for Cloud Computing in Health Care (henceforth referred to as the "MUNICH platform"). This research initiative investigated the usage of RFID towels to support a surgical team.

Problem Statement

The MUNICH platform addresses two main problems, namely debris left in the human body after surgery and time consuming process steps without added value (“non-productive time”). A

third auxiliary problem is the ongoing integration of software and solutions from 3rd party providers, which the IoT ARM would address.

Regarding the debris problem, in spite of already implemented safety checks debris (tools, towels, consumables) left in the body still occurs in 1:10.000 cases [Kranzfelder, 2001] during surgical procedures. 70% of the debris come from surgical towels, and 30% come from remaining surgical equipment [Kranzfelder, 2001]. Risk factors which increase the retained surgical objects are emergency operations with unplanned changes in the procedure and patients with higher body mass indexes. The consequences for the patient are 40% morbidity rates and 5% is the mortality rates [Kranzfelder, 2001]. Accordingly, a solution that addresses the tracking of surgical towels would sharply mitigate this problem.

Regarding non-productive time, this refers to steps like documenting and registering towels in pre-operation, subsequent counting of towels during operation, and searching for towels when something is amiss; none of these steps add value, but instead address a problem created. Automating these steps, therefore, could eliminate much of these problems.

Objectives

Given the problems, the MUNICH platform's objectives and solutions can be mapped as shown in Figure 31:

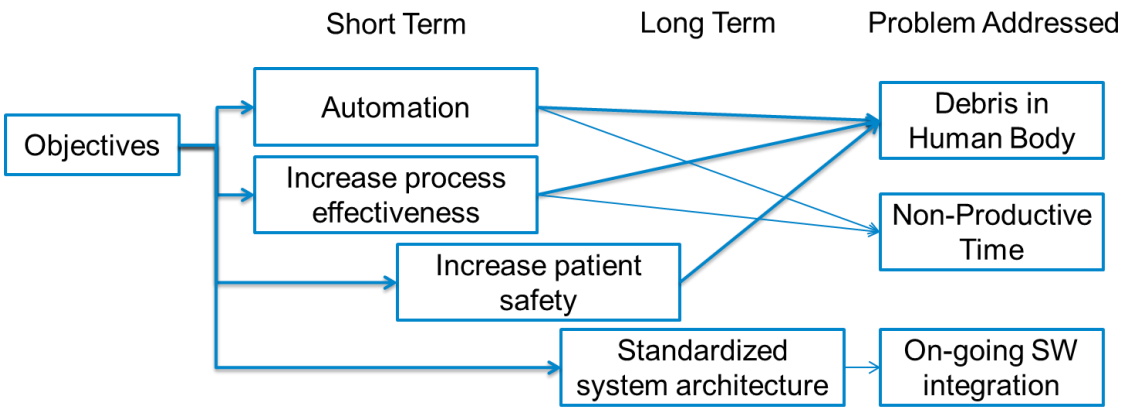

Figure 31: Objectives of the health care use case and the problems addressed

Real-time monitoring and location of all towels reduces the risk of debris in the human body, because of manual error prone counting and searching is avoided [MUWS, 2013]. Therefore, the automation reduces manual errors. The process improvement raises the transparency of the process and reduces the risk of documentation errors which also can lead to debris in the human body. The experts estimate that a 100% failure protection is possible with this solution [Kranzfelder, 2001]. Addressing the debris problem meets short term objectives of automation and improved process effectiveness, and in the mid-term, increases patient safety.

For the non-productive time problem, automation and the resultant process improvement removes the error-prone steps of documenting and registering towels in pre-operation, subsequent counting of towels during operation, and searching for towels when something is amiss.

For the long term problem of integrating new software developments from the hospital and their 3rd party solution providers, the IoT ARM provides a standardized reference architecture. This would simplify the complexity of the architecture and make integration of new components into the system easier. Other long term benefits include the fact that when the safety track record is improved, the image and reputation of the hospital will be enhanced [MUWS, 2013].

5.2.3.1.1 Risk

The following are some risk factors for the MUNICH platform. On the one hand, the solution is strongly depended on the communications infrastructure. If a breakdown of the network infrastructure occurs, safeguards has to be implemented. Also, the protection of the RFID tags from destruction is an important risk topic to ensure that the system is able to detect and locate the towels. The stakeholder also has to address the topic of data privacy.

5.2.3.1.2 Business case model

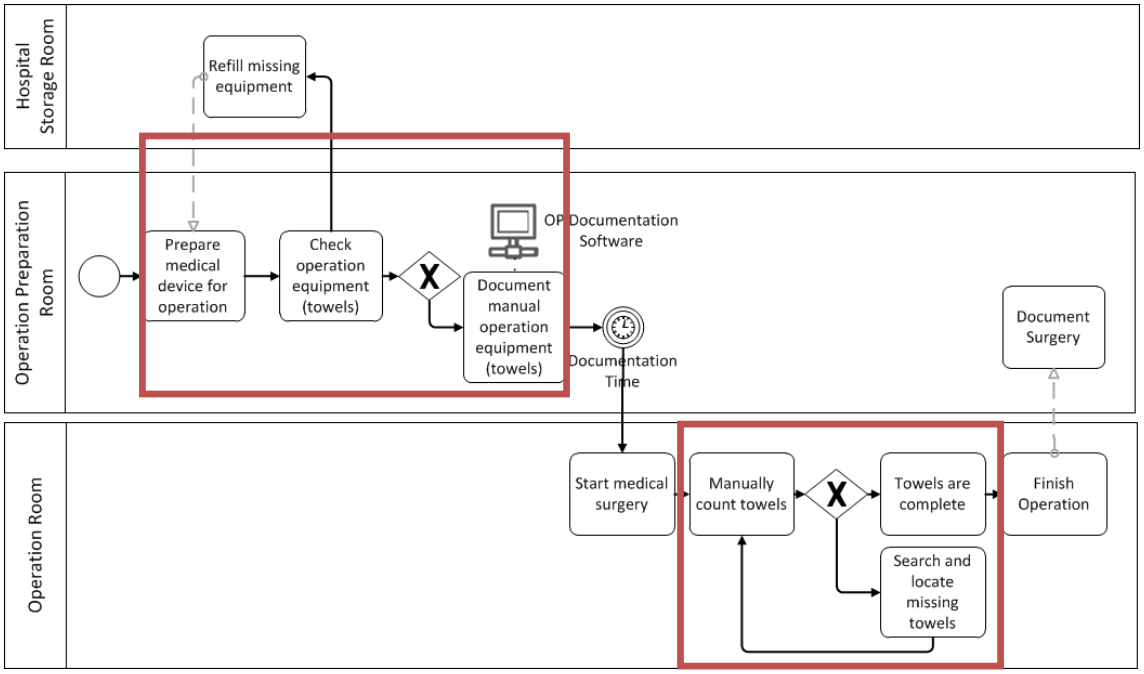

Figure 32: Current in-hospital process (Health care case) [MUWS, 2013]

Figure 32 shows the process steps which will be improved by the new system, namely towel registration in pre-operation documentation, counting of towels and searching of towels.

- The counting and documentation of the prepared towels is provided by the new system. In the target process, the towels with the implemented RFID tags are scanned and this information is processed to the report.
- The next two process improvements are related to the surgery phase. The RFID system is able to locate every single towel in the operation room whether a towel is in the human body, on the operation table, in the trash or at any other location in the operation room. Therefore, the retrieval of missing towels, as well as the counting control process, are avoided.

The improved target process flow of the "MUNICH platform" is outlined in a simplified form in Figure 33.

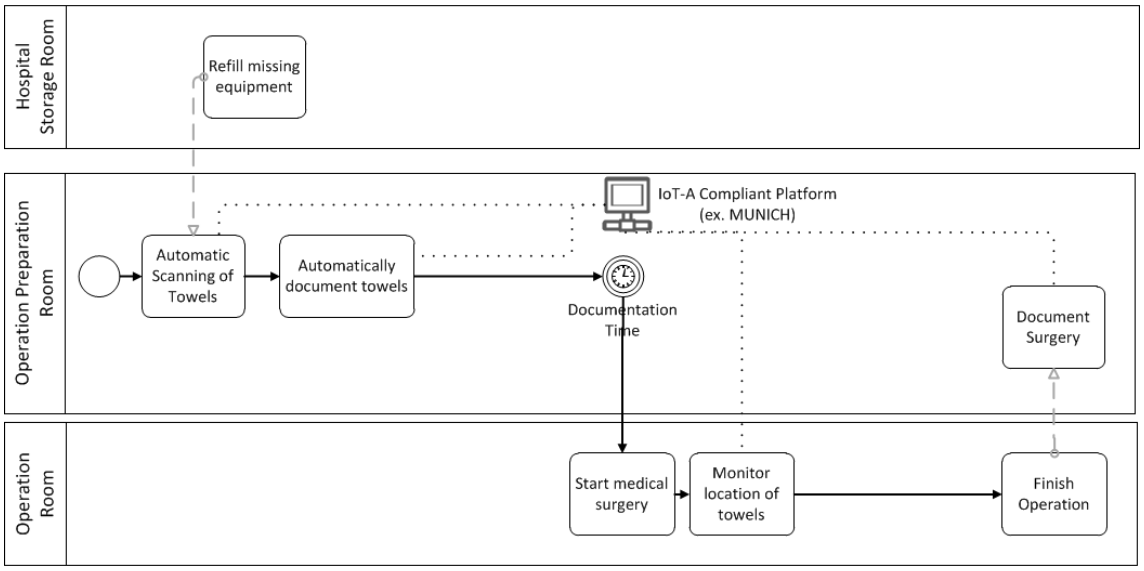

Figure 33: Target process (Health care case) [MUWS, 2013]

The implementation of the system and process changes is relatively easy for the hospital. It can be installed fast when the completed system are reliably available. The risk of the software development and the associated hardware, as well as the system integration of both are taken by a manufacturer. This company has to guarantee the necessary high performance. Due to the risk of human life, the reliability of the system has to be 100%. On the other side, this service provider charges relatively high operations costs per surgery [MUWS, 2013]. These are reflected in the business calculation.

There are limitations to the system. As outlined earlier, towels only represents roughly 70% of the debris forgotten in the human bodies during surgeries. Remaining objectives are other medical instruments (e.g. scalpel) or personal equipment (e.g. watch). These remaining 30% of sources for debris are outside the scope of the system and are still controlled by the error-prone manual process.

5.2.3.2 Business Case Calculation

This section defines the inputs and assumptions for the cost and benefit models.

5.2.3.2.1 Costs

Non-Recurring Cost (NRC)

The non-recurring cost can be categorized into three major cost elements:

1. **The hardware cost** consists mainly of the RFID antenna and RFID readers. The two devices are spread over the operation room. The amount of RFID devices per operation room and their unit costs are shown in Table 15.

Table 15 : RFID devices and IT-equipment

Location	Devices	Number of units	Unit Cost	Source
OP Table	RFID antenna	1	2000€	MUWS 2013
	RFID reader	1	200€	MUWS 2013
Cabinet	RFID antenna	4	500€	MUWS 2013
	RFID reader	1	200€	MUWS 2013
Trash	RFID antenna	1	500€	MUWS 2013
	RFID reader	1	200€	MUWS 2013

A detailed specification of the RFID devices can be found in paper by [Kranzfelder, 2001]. The IT equipment to operate in a surgery with this service is a normal personal computer, about 500 € per operation room. The number of operation rooms is set to 10 according the pilot scheme hospital "Rechts der Isar München" [MUWS, 2013].

2. **For network and infrastructure costs**, the software and system application is purchased as a cloud service. Therefore, the hospital has to ensure a solid network and communications infrastructure to guarantee a 100% performance which can only achieved with redundant systems. This leads to an additional cost of 10,000€.

3. **The rollout cost** to launch and implement of the RFID solution includes software integration, hardware and network installation, and finally testing and validation costs.

Recurring Cost (RC)

The recurring costs are split into four different elements:

1. **Towels equipped with RFID tags:** On a recurring basis, the new towels with equipped RFID chips have to be purchased for 1 € per towel. The advantage of these towels is not only the RFID implementation, additionally they can be reused between 2 and 5 times before durability is exhausted. Of course, they are more expensive of the existing one-way towels. The total cost is calculated based on the used amount of towels per year, which depend on the number of operations per year. In the model, the average of the last three years is the baseline. The reuse factor for the towels is configured with two times before disposal to be more on the conservative side [MUWS, 2013].

2. **Software and system service fees:** The major cost element of the recurring cost is the service fee for the system (“SFS”). It includes a user license, software maintenance and service, 24h support hotline for emergency cases, yearly legal and technical certification and software upgrades. The service fee is composed of a fixed monthly basic charge, and a variable fee for each surgery. The service fixed cost for the allocation is per month around 1,000€ for a hospital, regardless how many operation rooms are equipped. The cost per medical surgery is between 10€ and 20€. Due to a conservative cost model, the price per use is set to 20 € in the model [Anonymized Source 1. 2013].

3. **Staff Training:** The medical law and hospital regulation only allow employees to use the device and software application if they get training with a certification for the equipment. The total recurring training cost per year adds up to 10,000€, according to expert estimates [Anonymized Source 2. 2013].

4. **Maintenance Costs:** The yearly maintenance costs, including quality assurance of the system, are calculated with 10,000€ by the working group of the MUNICH platform. This fee is a certification from independent auditors and is included [Anonymized Source 2. 2013].

5.2.3.2.2 Benefits

This section details the benefit models in the business case. All models calculate the overall benefit of one year for all adequate surgeries; the system is not applicable for all surgeries, as not all operations utilize the towels. The experts estimate 60% of all surgery operations could be assisted by the MUNICH platform [Anonymized Source 2. 2013]. Based on three years of pasta data, the total amount of suitable surgeries (“SS”) is calculated (currently 20,008 surgeries).

The benefits are divided into tangible and intangible ones, and are discussed as follows.

Tangible Benefits

(1) RFID supported surgery preparation

The first benefit the MUNICH platform offers is support for automatic surgery preparation. A very important process step before the surgery can be started is to document the needed equipment. This step includes counting of the material, creating a surgery operation material protocol and inputting the data into the information system. With the new process the towels can be identified and documented automatically. And therefore, the preparation time of each surgery can be reduced by around 5 minutes [Anonymized Source 2. 2013]. An average surgery nurse cost between 31,000€ and 44,000€ per year [ÖDI, 2013]. This cost can rise if the nurse has management experiences. Additional cost factors are shifts in the night or during weekend/public holidays. In emergency case additional fees has to be added if extra personal is need in short notices. In order to consider all of these different aspects, the cost of one surgery nurse per minute is set to 1000€ [Anonymized Source 2. 2013].

The MUNICH expert team estimate a time saving of 5 minutes per surgery, which totals to 1667 hours or 100,000€ per year. The calculation details and results are shown in Table 16. Shorthand acronyms are presented in the "variable/formula" column.

Table 16: Benefits for RFID-supported preparation

Description	Variable / Formula	Data	Units	Source
Total amount of surgery per year	TAoS	33346	number	Anonymized Source 2. 2013
Surgery nurse cost per min	SNCPM	1	€/m	Anonymized Source 2. 2013
Parameter: percentage of adequate surgery	POAS	60	%	Anonymized Source 2. 2013
Suitable surgery	SS = TAoS*POAS	20008	number	Calculation
Saved preparation time	SPT	5	time in min	Anonymized Source 2. 2013
Total saved time in preparation process	TSTPP=SS*SPT	100039	time in min	Calculation
Benefit	**B=TST*SNCPM**	**100,039.00 €**	**€**	**Calculation**

(2) RFID supported surgery

Surgery is very cost intensive (Total cost of operations = "TCoOM" = 13 €/min) [Anonymized Source 2. 2013]. An important step during the surgery is to check that all used materials are not left behind in the patient body. Therefore, the new systems minimize the operations time by automating parts of the control process, via the ability to locate the locations of all towels in the operation room. This automation can check whether the towels were not used, are in the trash, or still in the body of the patient, or on another place in the operation room [MUWS, 2013].

The control time (SCT) that is needed to check the completeness of the towels is around 2 minutes if it is done manually. These two minutes can be saved for all suitable surgeries ("SS"). Additionally, the actual search for unaccounted equipment is a very time consuming process and the experts defined the average effort of this around 10 to 15 min ("SST"). This search task occurs in 1:7000 surgery cases [Kranzfelder, 2001]. Taking these facts into consideration, the benefit model of the surgery supported by RFID is calculated in Table 17. The total saved time is around 1004 hours with a corresponding amount of 783,000€ per year.

Table 17: Benefits for RFID supported surgery

Description	Variable / Formula	Data	Units	Source
Total amount of surgery per year	TAoS	33346	number	Anonymized Source 2.

				2013
Total cost of one minute operation	TCoOM	13 €	€/min	Anonymized Source 2. 2013
Parameter: percentage of adequate surgery	POAS	60	%	Anonymized Source 2. 2013
Suitable surgery	SS = TAoS*POAS	20008	number	Calculation
Saved control time	SCT	3	min	Anonymized Source 2. 2013
Saved search time	SST	15	min	Anonymized Source 2. 2013
Parameter: search time needed	PSTN	0.0007	%	Kranzfelder et. al., 1
Total saved time	TST = SS*SCT+SS*SST*PSTN	60233.5	min	Calculation
Benefit	**B=TST*TAoCOM**	**783,035.26 €**	**€**	**Calculation**

(3) Cost Savings from Prevention of Surgical Errors

The next benefit model focuses on the value of increased safety for patients and the cost savings from avoiding surgical errors. As explained earlier, the operations room team is now able to locate the position of the towels. Now, the surgery team can ensure 100% that no towel is forgotten in the body [Kranzfelder, 2001]. This critical problem is completely solved. To estimate the associated benefit, we can refer to liability models in case of malpractice or accidents incurred to a patient.

In the legal scene there is no single value defined for accessing the liability for loss of human life. According to experts in the MUNICH Workshops, American insurance companies assess the liability with loss of life to be on average with 10,000€ [MUWS, 2013]. Meanwhile, in Germany a hospital incurred cost of 2.8 million € due to a medical error [Spiegel, 2013]. Sources cite an amount of 1,650,000 € in Germany [Spengler, 2004], [FAZ, 2013]. Additionally, a hospital faces indirect damages from loss of reputation arising from frequent errors.

The mortality rate resulting from towels left in the patient is between 2% and 10% [Feussner, 2006], [Kranzfelder, 2001]. The following model assumes a mortality rate of 6% and a liability cost of 1,650,000€ to hospital per death, multiplied with the numbers of such incidences. This results in 139,000€ in liabilities per year that could be averted.

In case of non-fatal incidences, the hospital has to bear cost for post-surgical treatment, and depending on the case, legal fees. The model assesses this cost with a factor of 10% of the value of a human being. This estimation also factors in indirectly damages to the reputation of the hospital. In conjunction with the frequency of occurrence, the total liability that could be averted is 217,000€. Therefore, total benefit from averting fatal and non-fatal cases is around 356,000€ and shown in Table 18.

Table 18: Cost of surgical errors

Description	Variable / formula	Data	Source
Total amount of surgeries per year	TAoS	33346	Anonymized Source 2 2013
Percentage of adequate surgery	POAS	60%	Anonymized Source 2 2013
Average occurrences of	AOFSS	0.007%	Kranzfelder et

failure during surgeries that could be avoided			al., 1f
Suitable surgeries	SS = TAoS*POAS	20008	Calculation
Frequency of surgery failures occur	NSFO= SS*AOFSS	1.4 per year	Calculation
Value of human life	VOHL	1,650,000.00 €	Spengler 2013, 1
Mortality rate out of surgical failure	MOR	6%	Kranzfelder et al., 1f
Parameter of post-treatment and miscellaneous cost	PPTMC	10%	Assumption
Cost for post surgical treatment per year	CPPTMC = NSFO*VOHL* PPTMC*(1-MOR)	217,225 €	Calculation
Cost for mortality per year	CMOR = MOR*VOHL*NSFO	138,654 €	Calculation
Benefit	**B2 = CPPTMC + CMOR**	**355,879 €**	**Calculation**

Non Tangible Benefits

There are also non-tangible benefits, not directly linked to a monetary outcome. The improvement of the process leads to a time reduction for medical surgery. The hospital can improve the surgical scheduling per year and can increase the overall operations. Reputation is improved from the gain in safety. The platform also opens opportunities in integrating with other systems, as well as increasing the number of "Smart Objects" in theatre. Also the newly created information can used to reduce additional documentation effort [MUWS, 2013].

5.2.3.2.3 Benefit analysis

Before an analysis of the benefits and costs is conducted, we list our assumptions and basic settings in Table 19. The two new parameters introduced here are the service fee sensitivity (SFS) and the parameter which adjusts the total amount of surgeries (TAoS*factor).

Table 19: Basic parameters (health care case)

Parameter	Unit	Value
External Factors	unitless	variable
Inflation	%	2%
Discount factor	%	8%
Critical Risk Factors	unitless	variable
Hardware risk	%	10%
Personal risk	%	10%
Miscellaneous risk	%	20%
Software risk	%	50%
Sensitivity factor	unitless	variable
Reduction factor for risk	%	0%
Benefit sensitivity factor	%	0%
SFS +/- price unit	€	0
TAoS * (factor)	#	1

First the benefits are discussed assuming full operations have been reached (which we calculate would occur in 2015). Than the development of the benefits over the entire business case time period (2013-2018) are analysed.

Figure 34 shows the benefits according to their impact. The "RFID supported surgery" model provided the highest benefit. This benefit accounts for 63% of the total benefit, with an amount of 815,000€. 29% of the total benefits come from the avoided "Cost Savings from Prevention of Surgical Errors" (370,000€). The remaining part of the benefit comes from RFID supported preparation (104,000€).

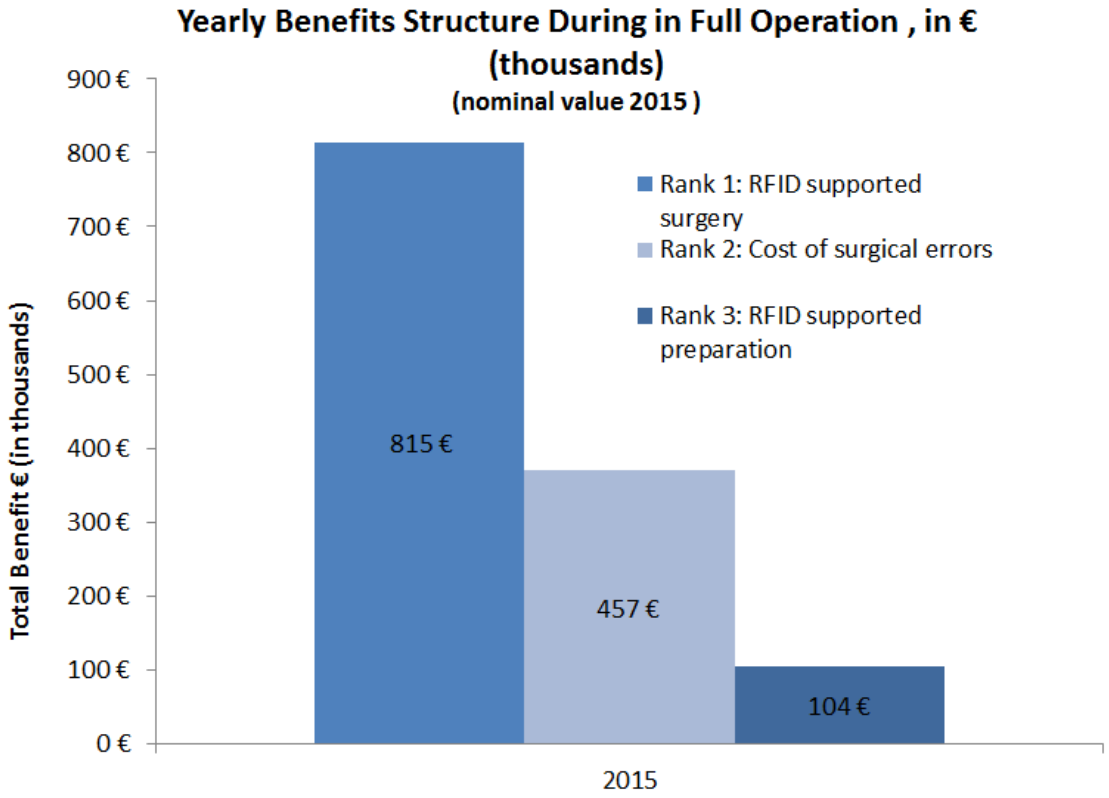

Figure 34: Yearly benefit structure in full operation (Health care case)

Figure 35 shows the development of the benefits over the business case timeframe. The total benefit accumulates to 7,923,000€ after 6 periods. The increase in benefit per year is explained by the effect of the inflation rate (2%).

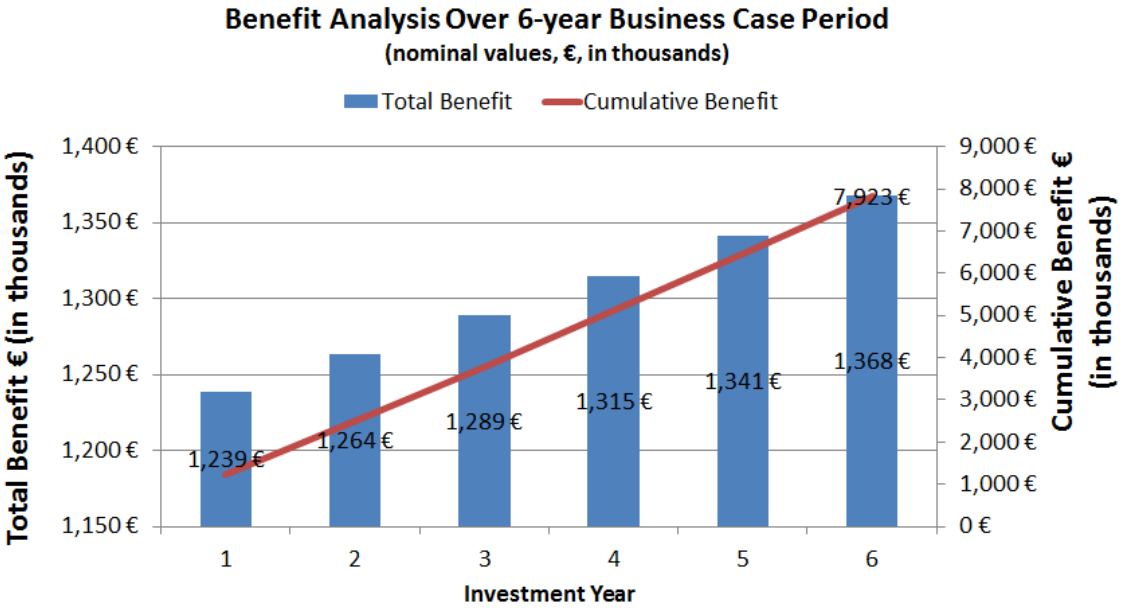

Figure 35: Benefit analysis over business case period (Health care case)

5.2.3.2.4 Cost analysis

For the cost analysis, it is sensible to distinguish between the Non-Recurring Costs (NRC) and the Recurring Costs (RC). In each category, the main cost drivers are identified and the associated costs are shown.

The first cost category is the non-recurring cost group and each cost element of the NRC is broken down in Figure 36 with its total value. The main cost driver is the hardware investment for the RFID antennas, which total 49,500€ - 58% of the total non-recurring cost (85,600€).

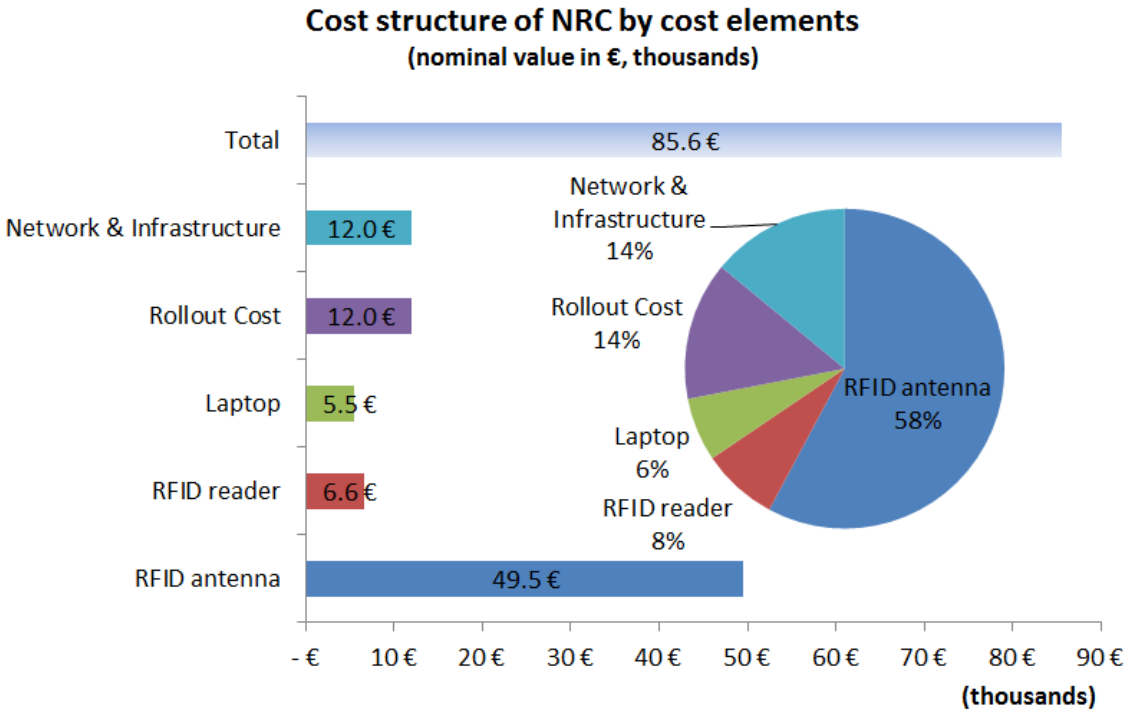

Figure 36: Cost structure of NRC by cost elements (Health care case)

The main cost driver of the recurring cost group is the operating fees of the system provider. This cost element has the most important impact of the cost model and counts for 98% of the yearly RC of 1,034,000€. A price change of the service fee has a dramatic impact on the total cost structure, over time. Therefore, this price change will be part of a specific sensitivity analysis.

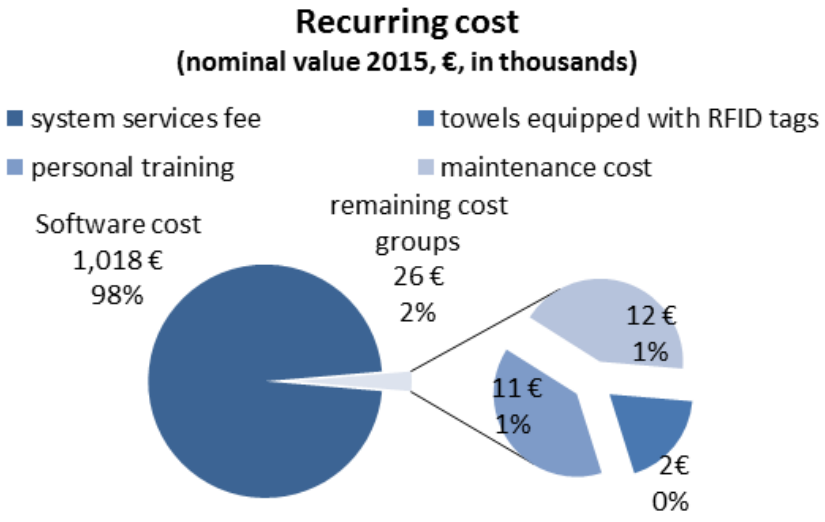

Figure 37: Recurring cost (Health care case)

The total cost (NRC+RC) development is shown in Figure 37. In the first year, the NRC is included and, therefore, the total cost is higher. In the outer years the inflation (2%) is factored in, and the cost increases.

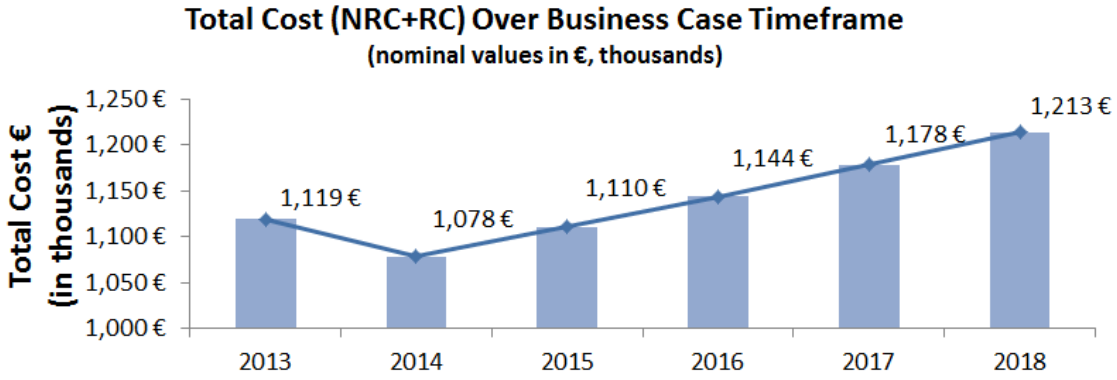

Figure 38: Total cost over business case timeframe (Health care case)

5.2.3.2.5 Cost- Benefit analysis

In Figure 39, the yearly and cumulative cash flows are presented. The cost-benefit analysis demonstrates a positive investment result. The discount factor is assumed with 8% and the net present value is 805,000€. The payback period is below one year. Within Germany, according to healthcare experts, this would meet the requirement of a one year payback period for new investments in a German hospital [MUWS, 2013].

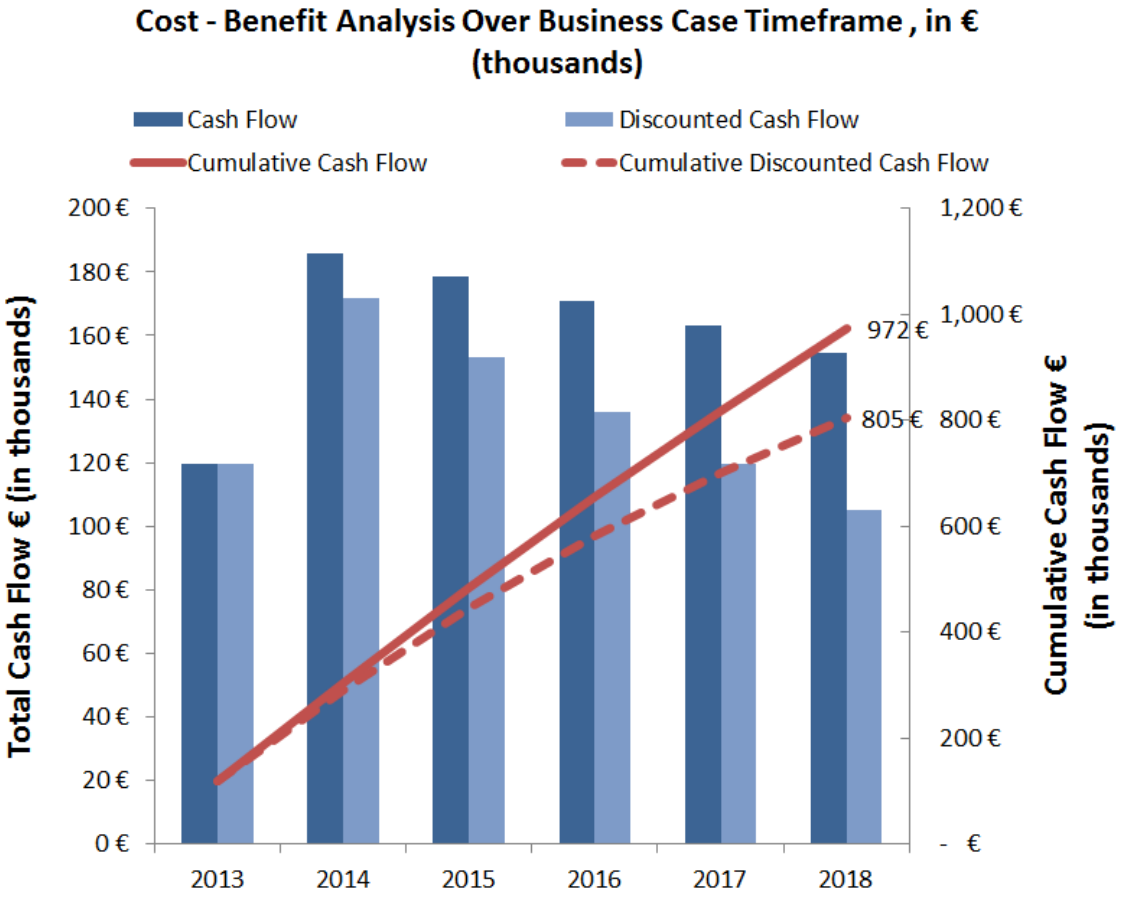

Figure 39: Cost-benefit analysis over business case timeframe (Health care case)

5.2.3.2.6 Sensitivity analysis

With the sensitivity analysis, we can investigate the impact of changing the major calculation variables. The following impacts shown in Table 20 will be discussed:

Table 20: Sensitivity analysis of health care case

Model element	Change of variables
Cost	→critical risk factors (software risk = SR, hardware risk = HR, personnel risk = PR, maintenance risk = MR) → system service fee (SFS)
Benefit	→benefit variation factor (BSF)
General calculation assumptions	→ benefit variation factor (BSF) → frequency of surgeries (TAoS)

The results of the sensitivities are always evaluated with respect to the final effect on the discounted cumulative cash flow. The sensitivity analysis will be summarized with a best-/worst case scenario.

Sensitivity Analysis of the Cost Model

The cost sensitivity model analysis investigates the impacts on the cost model if a parameter is changed. First the variation of critical risk factors (CRF) are considered: this risk refers to the increase in cost if the software (SR), hardware (HR), personnel (PR) or maintenance (MR) cost was to fluctuate. The reduction of the CRF by 10% leads to an increase of the total cash flow from 805,000€ to 1,187,000€ which is an increase of the net present value by 47%. On the other hand, the increase of the CRF +10% or +20% due to higher NRC and RC, lowers the net present value to 423,000€ or 41,000€ respectively.

The main cost driver for recurring costs (RC) is the systems service fee. An increase of 10% of the service fee per surgery from 20€ to 22 € reduces the net present value by 2/3 to 270,000€. The profitability limit is reached by an increase of the fee to 23 €/surgery. The cost model sensitivity analysis is depicted in Figure 40.

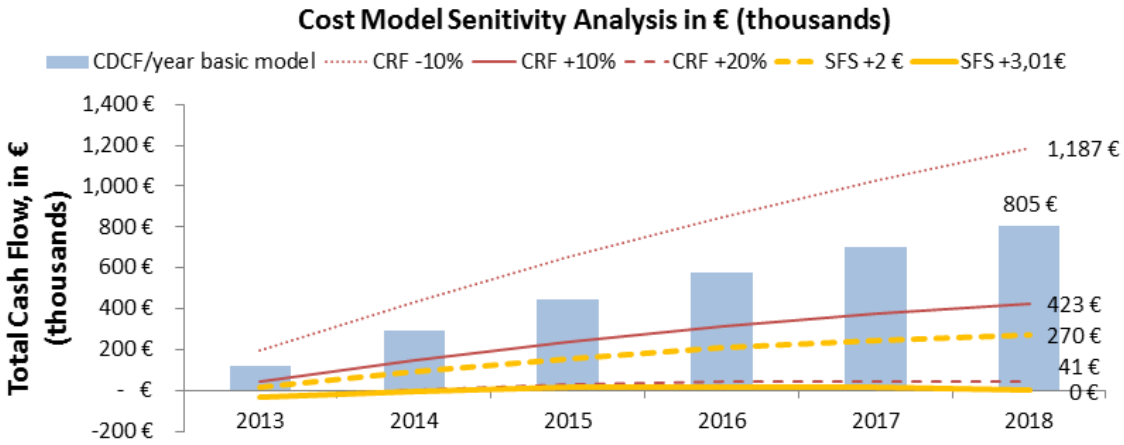

Figure 40: Cost model sensitivity analysis (Healthcare case)

Sensitivity Analysis Regarding Benefit Model Robustness

This analysis aims to investigate the robustness of the benefit model and the impact on the cost-benefit results. To demonstrate the development of the model three different scenarios are simulated: (1) Benefits increase by 10% (2) Benefits decrease by 10% and (3) Benefits decrease by 15%.

The results of these simulations are summarized in Figure 41. The increase of the benefits by 10% raises the net present value by 80% to 1,453,000€. In contrast, the 10% decrease of the benefits reduces the net present value by 80% to 158,000€. In the case where benefits are decreasing by 15%, the net present value is negative. The net present value is exactly 0 when the benefits are reduced by 12.4%.

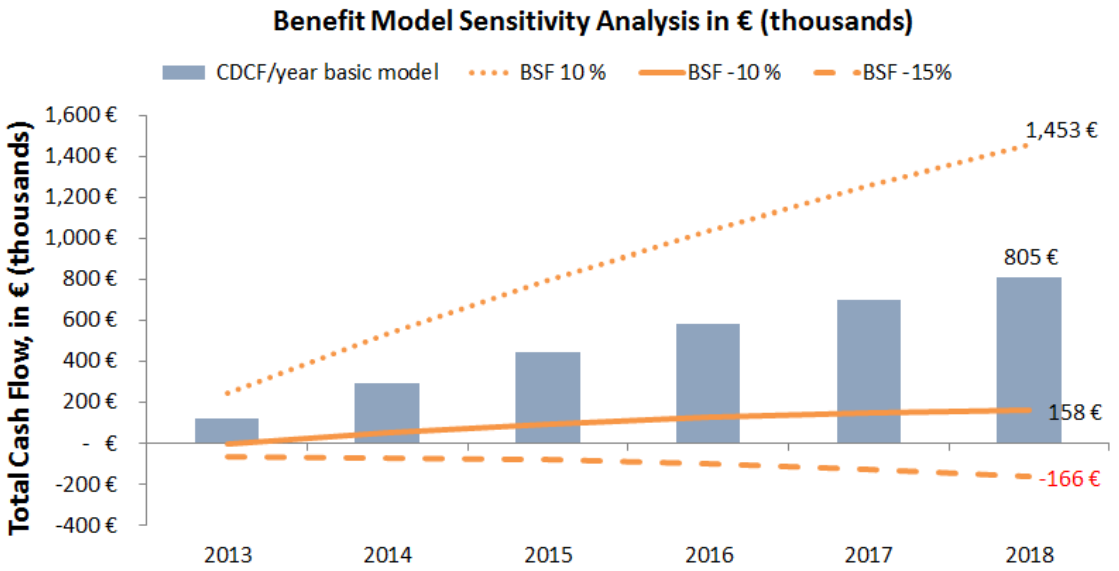

Figure 41: Benefit model sensitivity analysis (Health care case)

Sensitivity Analysis of the Assumptions in the General Calculation

After the sensitivity analysis of costs- and benefits variations, the analysis is extended to variations of the general calculation assumptions, which have effects on both models. Two parameters are used to simulate the results. The first is the change of the discount rate (DF) to reflect different risk perceptions and interest rate influences. The second parameter concerns the frequency of the surgeries per year (TAoS), which is a basic quantity variable (see Figure 42).

A variation of discount rate by +/- 2% leads to an increase/decrease of the net present value by +/- 4%. If 12% discount rate is assumed the net present value goes down to 741,000€ (-8%).

In case the hospital performs 25% less surgeries per year the net present value decreases to 524,000€ (- 35%). On the opposite end, if the amount of surgeries per year increased by 25%, the net present value goes up by 35% (1.087,000€). The net present value is zero in case the hospital performs -71,5% less surgeries per year.

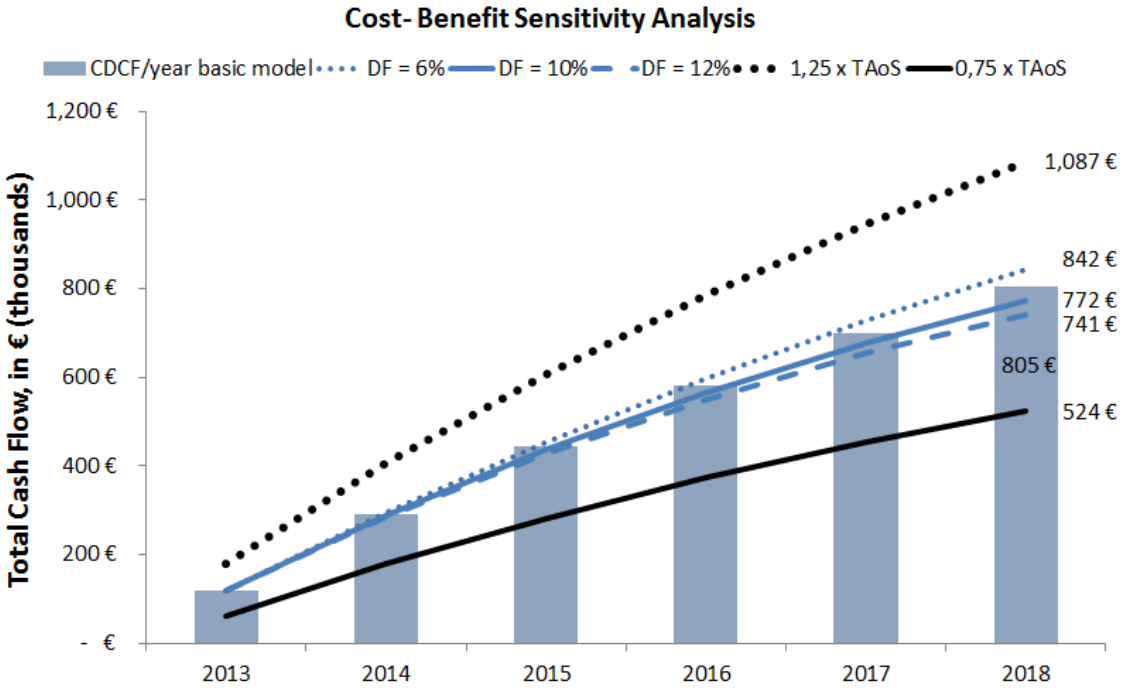

Figure 42: Cost- benefit sensitivity analysis (Health care case)

Best -/ Worst case scenario

By combining cost and benefit variation in the sensitivity analysis, best- and worst case scenarios can be elaborated. For example in case the system service cost is reduced by 1 €/surgery (= -5%) and the hospital performs 25% more surgeries annually than the net present value raises significantly to 1.421,00€ (+77%). The best case scenario is based on the assumption that the service provider can lower the cost of the service fee, due to cheaper maintenance cost, additional development support from using the IoT ARM, and from economies of scale effects. As a result of using the system and thereby reducing the errors, t is assumed that the hospital gains a better reputation and efficiency, and accordingly, the number of surgeries per year rise.

In a worst case scenario it is assumed that the benefits are lowered by 5%, the system service fee is 2 €/surgery more expensive (+10%) and the number of the surgeries is reduced by 25%. In this worst case scenario the net present value is completely destroyed and always negative (see Figure 43).

We observe that the economic feasibility of the case depends on a high degree of the system service fee of the service provider. The feasibility is also sensitive to fluctuations in the benefits. Further investigation about the reliability of the cost estimates are necessary. This information can be gained from the pilot deployments of the system with RFID equipped towels. A test case is currently running in Munich at the university hospital "Rechts der Isar". When the pilot case is finished a more reliable assessment of cost and benefits are possible. The service provider would then also have better information for the calculation of the cost for service fee.

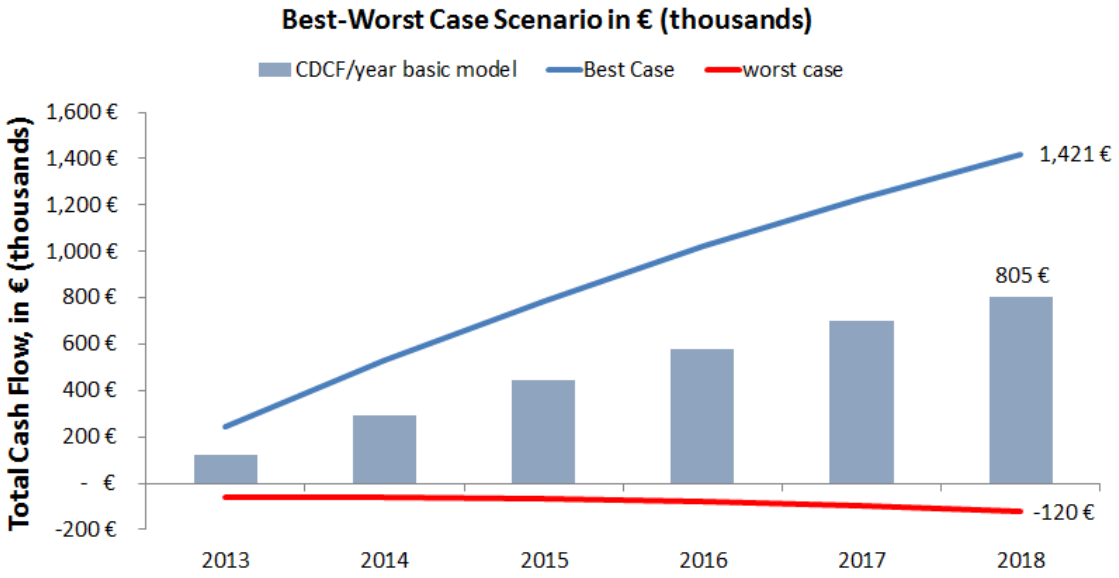

Figure 43: Best and worst case scenario (Health care case)

5.2.3.3 UC2 Conclusion

We showed in the health case that the overall benefit is positive for the hospital, within the bounds of probable parameters in a sensitivity analysis. Beyond the monetary benefit, the use of an IoT system like MUNICH also averts death and non-fatal complications arising from leaving a towel in a patient, is likely to improve the reputation of the hospital due to a better track record, and improve efficiency of processes.

5.3 IoT ARM in context of business networks

5.3.1 Definition of Business Networks

The key term Business Networks (BN) in this section is not commonly defined. Some important definitions are the following:

- In a dynamic network, numerous firms (or units of firms) are operating at each of the points on the value chain, ready to be pulled together for a given run (i.e., a particular customer order) and then disassembled to become part of another temporary alignment. [Miles, 1992]
- A BN involves a large number of actors contributing to providing service offerings triggered by actual demand based on their core capabilities. [Hoogeweegen, 1997]
- The network of connected and interdependent organizations mutually and cooperatively working together to control, manage, and improve the flow of materials and information from suppliers to end-users. [Christopher, 1998]

The excerpt above of existing definitions of BN shows not only the many interpretations of BN but also the commonalities, which describes that a BN consists of a set of network members collaborating for certain purposes.

Generally, companies and organizations, and related value chains and value networks need some kind of ICT support. A well and truly BN approach rethinks and rebuilds the operating support from scratch considering the current available ICT solutions and focusing on two key business features: (1) information contributions, to be generated by the activities in the processes involved, whether they are performed by human beings or automated systems or jointly by the two, in a coordinated way; and (2) automated information exchanges, to be

provided by the networked information systems. Furthermore information contributions and exchanges need to be supported by data storage and access control mechanisms (encryption, authentication, decryption), which both can be provided either as add-ons or as built-in features.

Figure 44 shows the main differences between traditional and new BN approaches in context of a supply chain. As one can see the new BN approach embodies and supports the concepts of the IoT of a flexible and quickly responding network.

Characteristics	Traditional Business Network Approach	New Business Network Approach
Products and services	Relative simple, unbundled, and slowly delivered products and services	Relative complex, bundled, and fast delivered products and services
Value creation	Supply chains with long term connected relationships	Demand networks with quick connect and disconnect relationships
Coordination and control	Hierarchical and central control and decision making	Network orchestration with distributed control and decision making
Information sharing	Information sharing with direct business partners	Information sharing over and with network partners
Infrastructure	Actor platforms with information silos and systems	Network platform with networked business operating system

Figure 44: Traditional vs. new Business Network approaches [van Eck et al., 2007]

5.3.2 From value chain to Business Networks

The value chain as both a concept and tool has been used for the last three decades to understand and analyse industries [Porter, 1985]. It has proved to be a very useful and valuable mechanism for illustrating the linkage of activities that exist and are carried out in the physical world within traditional industries, particularly manufacturing. Additionally, it has also developed our thinking about value and value creation. Traditional methods for examining competitive environments must be reassessed due to the highly competitive conditions of the “network economy”. The old linear models are not appropriate as they omit the nature of alliances, competitors, complementors and other members in BN. Traditionally, strategists use the value chain to closely examine the company and its major competitors to subsequently determine gaps between company performance and a competitor’s performance. When the gaps are revealed, the strategist can elaborate and implement a strategy to close them. In this sense strategy becomes primarily mastering the art of positioning a company in the right place on the value chain. Today the concept of the value chain must be extended to position a whole value chain in a business network approach. Organisations focus not any longer on the company or the industry, but on the integrated and value-creating system itself. These systems consist of many different economic actors – suppliers, partners and customers – collaborating to co-produce value within the BN. Figure 45 depicts such a BN system in which a couple of different actors in f.i. a supply chain fulfil the orders of customers. Each of the actors has a specific process performance, which determines the individual success or failure and impacts the BN. Looking at the BN in its entirety, one can also observe a jointly achieved BN performance.

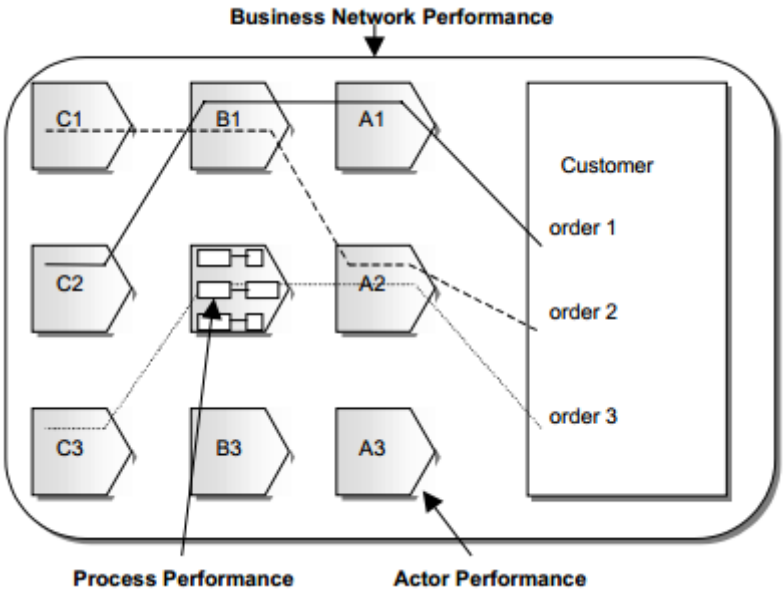

Figure 45: Business Network performance [Delporte-Vermeiren, 2003]

Similar to the value chain concept in which each individual firm aims to achieve a certain margin out of its activities, the same applies to BN. While in a value chain the margin is considered for an individual firm, the margin for a BN must be regarded as the sum of all activities of the BN actors. Broadly speaking, the BN revenues less the BN costs define the BN margin (see Figure 46). In examining a BN in contrast to a value chain, the same question as with value chain analysis is absolutely essential: “How is value created?” “Through the value chain” is the prompt and common answer to this question. In the networked economy, however, and the increasing movement of firms into the virtual market space, traditional analytical tools are not providing suitable means to unearth the true sources of value. Previously successful performed activities within a firm could be accounted for value creation. This has changed in the context of a BN as key competence lies in understanding how value is created in relationships. The deep understanding of value creation in relationships requires relationships in BN to be viewed as a whole – a network of intertwined relationships.

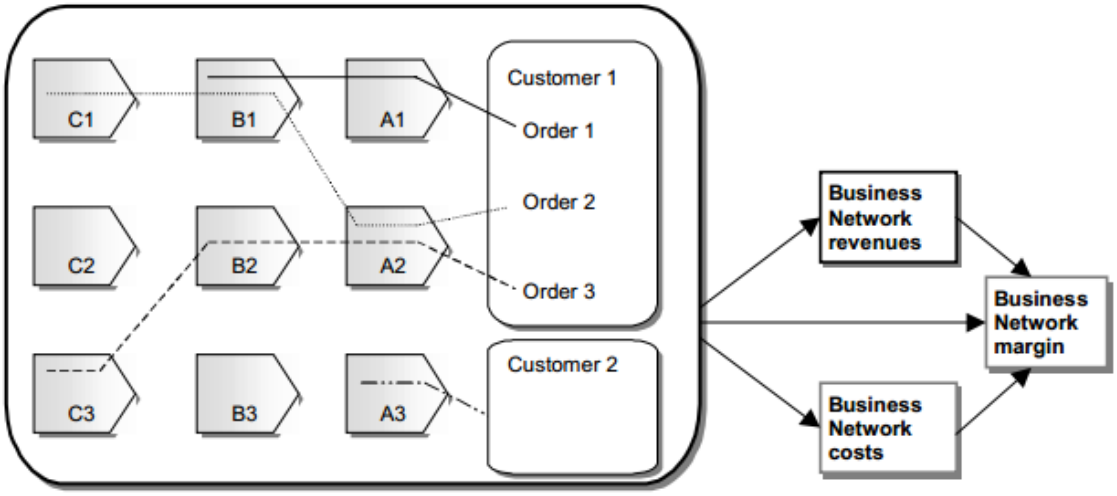

Figure 46: Concept of margin in the Business Network [Delporte-Vermeiren, 2003]

5.3.3 How are Business Networks supported by the IoT ARM?

To analyse value creation within a BN, one needs to proceed viewing how an organisation of multiple firms realises value creation instead of focusing on an organisation as an isolated unit. Consider a company developing a new smart device for the IoT. The success of this device depends on software developers writing applications that leverage the new device capabilities; other hardware manufacturers must build systems that can potentially accommodate or communicate with the new device, including any additional interface requirements. Companies using this device must be guaranteed that the device is compatible with the already available infrastructure, i.e. this ecosystem must be cultivated. This leads to the requirement of the aforementioned creation of value through relationships. To enable these relationships the IoT ARM can assist IoT system architects by selecting the protocols, functional components, architectural options, needed to build an appropriate concrete IoT system. This ensures interoperability between all the involved BN partners. Furthermore these relationships can be established more quickly with a higher flexibility. To explain the advantages we take as example a supply chain. A supply chain might use different sensors by different partners, e.g. RFID on goods or containers or NFC in smartphones. When a truck with goods is on its way from the supplier to a distribution center, the retailer is also aware of the current status. The main advantage is the availability of real-time information, i.e. if the truck has delay because of traffic or if the cooling system of the truck has a malfunction the retailer gets the information soon. In the case the container has perishable goods inside which are likely to perish before reaching the retailer, the retailer is able to reorganise other transportations from other distribution centers in order to possibly get the goods from them. Such integrated systems need a common basis on which they are developed and this is exactly what IoT ARM provides. Through a higher interoperability of these systems the integration of new devices used within the business network is easier and the business partners are then able to leverage the capabilities of these devices although they are not integrated in their own system infrastructure but can be reached through the cooperation of two or more business partners.

5.4 Conclusion

The chapter about the business validation showed that the IoT ARM will potentially have a positive impact on business. The qualitative evaluation of the business value reveals the utility of the IoT ARM when conducting an IoT system development project. Further we investigated the IoT ARM in context of the value chain. This exercise clearly demonstrates that the partner profiles representing technology providers in the IoT-A consortium can be generalised in order to locate these profiles in the value chain and to point which industry partner is likely to provide

certain services in these fields. The value chain analysis provided a high-level discussion on where and how other stakeholders can fit into logistics and health care value chains and identified a wide range of stakeholders beyond the scope of the project that can benefit in an even wider value chain. Therefore, future IoT projects should consider outreaching to these stakeholders (ex. for logistics: supplier, channel and end users; for health care: insurers, drug manufacturers, payers) in order to foster widespread IoT adoption. Our final section on the business case, performed on the retail/logistics use case and the MUNICH platform shows that both business cases have a better result considering the IoT ARM compared to implementations not using it. This is especially true for the retail/logistics business case in which we included the development costs considering the two cases “with IoT ARM” and “without IoT ARM”. To cope with the fact that our business cases are based on many assumptions we performed a sensitivity analysis. In this way we could reveal a range in which the benefits and costs are located by varying a number of assumptions, thus being able to demonstrate best and worst case scenarios under certain circumstances. Finally we showed how Business Networks are supported by the IoT ARM. This extended view of a value chain gives indication that the IoT ARM is not only important for specific value chains but can also support relationships between value chains to form a Business Network.

6 Socio-economic validation

The socio-economic validation contains two main activities: an IoT impact analysis on society and a privacy impact assessment. The former analysis aims to identify the impact of the IoT on the society as a whole by conducting a Delphi study. The study is not directly related to the IoT ARM rather than to the IoT in general, however, it reveals future potentials for deploying the IoT ARM. The latter is primarily intended to examine to which extent privacy is covered by the IoT ARM.

6.1 Delphi study

The objective of the Delphi study is to address major economic and societal issues encountered in the development of future scenarios for the IoT in general and the retail sector in particular. Therefore, a Delphi study has been started to estimate how certain projections in the context of the IoT will apply to future scenarios and in what way they will have an impact on macroeconomic development in general and additionally on the retail industry as a concrete example for a business sector. The study consists of three rounds (pre-study, first and second round).

6.1.1 Delphi method and process

As can be inferred from its name, the Delphi method can be traced back to the mythological Oracle of Delphi. As such it is mainly used as a forecasting method and was first used in technology forecasting studies initiated by the RAND (Research and Development) Corporation for the American military in 1944, to obtain expert opinions on the probability, frequency and intensity of possible enemy attacks. This process was repeated several times until a consensus emerged [Linstone, 1975].

The Delphi method starts from the assumption that group judgement is more valid than individual judgements. It is a multi-staged survey which tries finally to reach consensus on a specific issue or topic between a set of experts, the expert panel, having a broad knowledge in their field of expertise. As a widely used research instrument, it aims to close the gap of incomplete knowledge or to develop forecasts. A commonly accepted definition, on which most of the researchers draw, comes from [Linstone, 1975] who defines the Delphi method as “(…) a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem.”

The Delphi process usually consists of two or more rounds of consulting an expert panel either by mail or by online survey tools. After each round, a concise summary of the panel’s answers is made available to the experts in order to compare their answers with the mean value of the panel. Subsequently each individual expert is provided the opportunity to reconsider his opinion against the background of the overall opinion. Figure 47 depicts the overall process for the study which in the following will be explained in more detail.

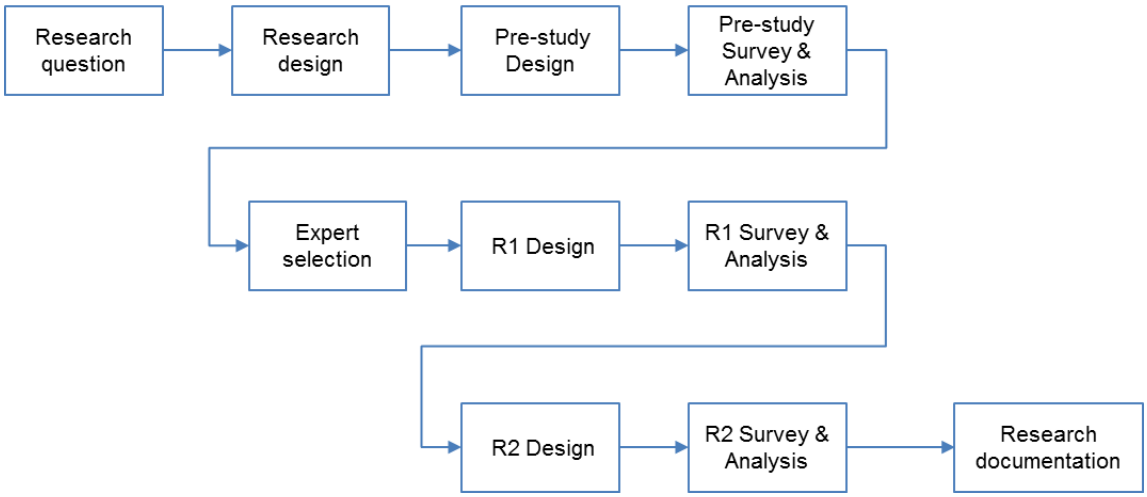

Figure 47: Delphi process

6.1.2 Research question

The Delphi process starts with defining the study's underlying research question. While the objective of the business validation is to scrutinise the micro-environmental level (i.e. to evaluate specific UCs within the healthcare and retail domain), the socio-economic validation aims at the macro-environment to estimate future developments for the IoT. The research question for the Delphi study therefore reads as follows:

> How will the macro-environment (political/legal, economic, socio-cultural, and technological structure) change in general and specifically of the retail domain in the context of the Internet of Things?

6.1.3 Research design

The methods used in the study are qualitative as well as quantitative. The structure how these methods are applied is as follows: For the pre-study, a qualitative approach was taken, in which a questionnaire with open questions was sent to the expert panel to give them the opportunity of answering the questions without any given answer format. This input was transformed into future projections, which then were assessed quantitatively in round 1 and 2 by the experts to reach consensus among them. For this we worked on the basis of the PEST analysis [Wilson et al., 2005] whose abbreviation stands for Political/ Economic/ Social/ Technological. Additionally, we introduced the retail industry to also identify how the IoT will not only impact the economy as a whole but also a specific industry sector. For each perspective, one open question was formulated to get input accordingly. The projections will be provided in the same structure so that for each perspective there will be a couple of projections to be assessed by the experts.

Pre-Study

The design of the pre-study questionnaire allowed the experts to provide their opinions on different IoT-related topics in an open-ended manner in the fashion of a brainstorming. The qualitative answers served as input for the subsequent quantitative rounds in which projections for the different PEST perspectives plus the retail industry were first formulated and then given to the experts to assess to which extent they apply. For the experts' answers we provided a standardised format in which first the impact, challenge or issue should be mentioned, but then also the cause(s) and effect(s) to get a clearer understanding of the context. The survey was

conducted with the help of the online survey tool “LimeSurvey[3]”. A set of IoT experts was asked to provide their opinions according to the PEST perspectives and the retail industry. This input was carefully scanned for potential projections. The target year for the projections was 2030 which means a time horizon nearly 20 years in the future. Additionally, a thorough desk research was conducted in order to combine the expert input with data from literature. All the draft versions of the projections were subjected to a number of internal revisions in order to obtain a high quality. As a result, 22 projections made it into the final list of projections (Table 21). From a structural point of view we maintained the structure of the PEST perspectives in conjunction with the retail industry.

Table 21: Final list of projections considered in round 1 and 2

No.	Projection for the year 2030
	Political
1	The Internet of Things (IoT) adoption process is slowed down due to the domination of influential standardisation organisations and missing real open standards.
2	Unregulated data generation and distribution has led to a consumer demand for more restrictions and laws to ensure better data protection and ownership.
3	The full potential of IoT cannot be exploited in consequence of too strict rules and regulations in data privacy.
4	The harmonisation of European data protection legislation has led to a coherent application of this legislation and a high level of enforcement.
	Economic
5	The growth of e-commerce and m-commerce, and rapid shifts in consumer behaviour, have increased the benefits for retailers. Multiple channels enable the retailers to almost constantly stay in touch with consumers.
6	The market leaders for Internet of Things solutions are located in the US and in China due to their leading roles in hardware and software development.
7	Big Data in the Internet of Things closes the information gap. This enables retailers to exploit real-time data and new data analysis methodologies to forecast consumer trends. This information is used to increase profits.
8	The issue of cost distribution of information and communication technology (ICT) in open loop systems is solved by payment models. Parties which benefit the most pay the most. Thus, supply chain information sharing works because each party acquires a financial interest.
9	Required information and communication technology (ICT) demands large capital investments, which can hardly be raised by small and medium-sized retailers alone.
	Social
10	People mistrust the Internet of Things because they are not aware of which data from them is becoming 'public domain'.
11	Changing patterns of employment affects the retail sector as well. It has become less important as a dominant employer due to an increasing degree of automation (e.g. self-checkout).
12	Retailers provide new concepts (e.g. remote order with home delivery) to cope with the continuous challenge of demographic change.
13	Consumers increasingly demand sustainable retailing, i.e. waste reduction of perishables, fair trade products.
14	Information security is perceived as a basic requirement in the provision of Internet of Things services, not only with a view to ensure information security for an organization itself, but also for the benefit of the citizens.
	Technological
15	Mobile payment acceptance, utilization, and confidence is well established. Cash will no longer be accepted which will have mutual benefit to the retailer and the shopper.
16	New technologies in retail obtain faster acceptance as compared to 2013.

[3] LimeSurvey is a survey service-platform to prepare, run and evaluate on-line surveys. (www.limesurvey.com)

17	Barcode systems are almost completely replaced by smart label systems (e.g. RFID).
18	RFID is the leading technology grounding the success of Internet of Things as it is the most mature Internet of Things technology. As a result of the declining unit prices, RFID remains the most prevalent enabling technology for the Internet of Things.
	Industrial structure
19	Retailers blend the online and offline shopping - the digital and the physical – into one seamless, omni-channel shopping experience.
20	Shoppers are willing to share personal information and shopper preference data. Retailers use this sensitive information appropriately to enhance the shopping experience.
21	Customers get advice at the point of sale through mobile shopping assistants or their own mobile device according to their preferences, presence of allergic components or the actual product quality.
22	Service and in-store experiences continue to break out of the one-size-fits-all offerings. These experiences have become more individualized and specialized for specific target groups.

Round 1

The final list of projections was the main outcome of the pre-study. The projections were evaluated to gather different metrics in order to measure the degree of consensus among the experts. The feedback metrics include the interquartile range (IQR), the arithmetical average, and the standard deviation (SD). For the second round a new set of experts was selected (see section 6.1.4). At the same time, pretesting to ensure reliability as well as content validity was performed at two stages in the Delphi process. First, after their initial formulation, the 22 projections were assessed project internally, and were checked for completeness and plausibility of the content. Second, after completion of the questionnaire design, another pretest was conducted by one project external expert to get feedback about the content and the needed time for completing the survey with “LimeSurvey”. The feedback was processed and suggestions for improvements were considered where necessary. To obtain the statistical measures all projections were evaluated for probability of occurrence, their impact on the European economy and desirability. The probability of occurrence was measured using a 9-point Likert-scale ranging from 10% to 90%. The reason why we left out values below 10% and above 90% is because none of the projections is absolutely unlikely and likely, respectively. The The impact was measured on a 5-point Likert-scale ranging from very high to very low. The last item to be evaluated was the desirability which was measured using a binary value, i.e. yes or no. After this validation step the distribution of the questionnaires was started. All contemplable experts received an invitation email with a one-pager about the Delphi study. Out of these invitations a set of 15 IoT experts could be framed who were willing to participate in the two-round Delphi study. The survey was online for two weeks and all experts completed the first round. After completion the results were processed in order to get the first descriptive statistical results (IQR, mean, standard deviation). Specifically, we focused on consensus and outliers. Regarding the consensus criterion we followed suggestions from literature indicating that an IQR of 2 or less suffices to claim consensus [De Vet et al., 2005]. These results were integrated in a feedback document for the experts. This document had to be generated for each participant individually as it included the estimated probability from each expert together with the group opinion. Furthermore we aggregated all formulated comments for each projection to give all experts an insight of opinions about the projections provided from each expert.

Round 2

Based on the results of round 1 the second questionnaire for round 2 was developed. After compiling the feedback document for each expert after the first round, the second round could be started. The purpose of the second round was to give the experts the opportunity to reconsider their assessments in accordance with the group’s opinion. Unlike the first round, for the second round the experts were only asked to reassess the probability of occurrence for the remaining projections, i.e. for those projections no consensus could be reached in the first round. The second round served for getting more concensus between the experts in the ratings for those projections which had no consensus in the first round. As in most past Delphi studies the number of rounds has not exceeded three rounds, the last round was round 2. The reason

is that usually in the first quantitative round appears the highest consensus while in the subsequent rounds the level of consensus does not vary significantly so that after a second round, at the latest third round, one can assume that the results won't increase the statistical accuracy, signficantly. Following this rationale, the second round was the last round in this Delphi study. Just as in round 1, the results of the second round were processed in order to obtain the same statistical measures as in round 1 for those projections which had no consensus in round 1. The results are summarised in section 6.1.5.

6.1.4 Expert selection

The appropriate selection of experts exposes a critical component of the Delphi process since the results depend on the right input factors. Therefore the study's participants stem only from the IoT community to ensure that the contributing experts have enough knowledge to give reasonable opinions. While in the first round the contributions for projections not only originated with IoT experts, in the second round we put a focus on IoT experts. Apart from parallel EU IoT projects, such as IoT-i and iCore, experts from the Internet of Things Council were invited to participate in this study. In this way only people who are related to the IoT were reached not to represent the general population, but rather to exploit their expert ability to answer the research question.

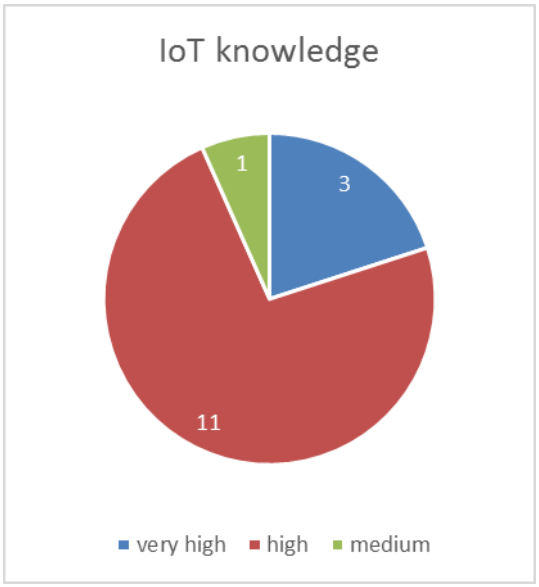

Figure 48: Expert knowledge in IoT

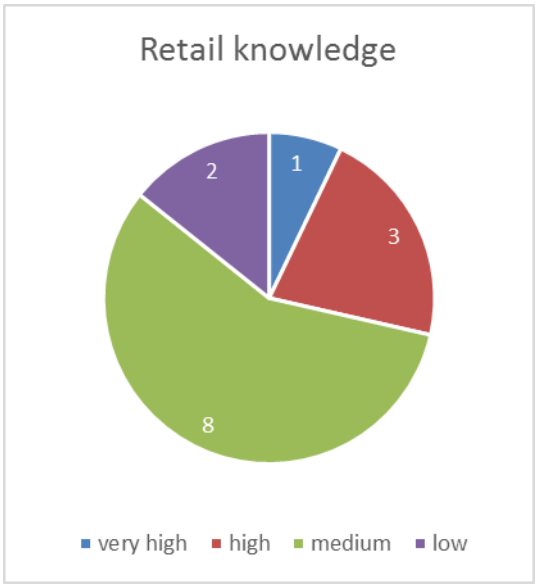

Figure 49: Expert knowledge in Retail

Figure 48 shows the self-assessments of the participating IoT experts. The figures reconfirm that our selection of experts regarding the topic IoT was reasonable. Almost all experts indicated to possess a high knowledge in IoT, two of them even have a very high knowledge. For the retail industry to be evaluated the self-assessments of the experts' knowledge are slightly lower but still entirely sufficient to evaluate the projections in order to achieve acceptable results (Figure 49). The countries the experts stem from are shown in Figure 50. As can be seen, most of the experts come from Europe.

Figure 50: Origin of participating experts

6.1.5 Results

In this section the statistical results from round 1 and 2 are summarised and discussed. Table 22 summarises the descriptive statistics from round 1 and 2. It is important to mention that in round 2 we could only get 13 completed questionnaires which means 13.3% from the participants in round 1 were not represented in round 2.

Table 22: Delphi statistics

	Round 1 (n = 15)			Round 2 (n = 13)				
Projection no. and short title	**IQR**	**Mean**	**SD**	**IQR**	**Mean**	**SD**	**Impact**	**Desirability**
Political-legal								
1. IoT adoption	3	3.4	1.6	2*	3.2	1.2	3.3	33.3
2. IoT potential	4	5.4	2.5	4	4.6	2.3	3.5	46.7
3. Privacy issues in consumer data	4	4.7	2.6	5	4.2	2.2	3.2	26.7
4. Legislation harmonisation	4	4.9	2.2	3	5.5	1.5	3.5	86.7
Economic								
5. Consumer interaction	3	7.3	2.0	2*	7.2	1.8	4.3	86.7
6. Global market share	3	5.4	2.4	3	5.5	1.5	4.1	20.0
7. Data analysis	6	6.7	2.8	3	7.2	1.8	3.9	80.0
8. ICT cost sharing	3	5.3	2.0	2*	5.5	1.4	3.6	73.3
9. ICT investments	3	3.3	1.5	3	4.1	2.2	3.4	13.3
Socio-cultural								
10. Societal distrust	6	3.9	2.7	4	3.7	1.9	3.3	20.0
11. Employment	4	4.7	2.2	3	5.5	1.4	3.4	33.3
12. Demographic changes	2*	7.3	1.8				4.0	93.3
13. Sustainable retailing	3	6.7	1.8	2*	6.3	1.4	4.1	100.0
14. Information security	2*	7.6	1.7				3.4	93.3

Technological								
15. Cash Elimination	2*	6.3	1.7				3.4	66.7
16. Technology Acceptance	4	6.3	2.5	3	6.6	2.1	3.5	73.3
17. Replacement of Barcode	3	7.1	2.1	2*	6.5	2.1	3.3	86.7
18. Technology maturity	3	5.5	2.2	4	6.0	1.9	3.7	60.0
Industrial structure								
19. Omnichannel retail strategy	4	7.1	1.9	3	7.1	2.0	3.7	73.3
20. Savvier Shopper	1*	6.4	1.5				3.6	80.0
21. Intelligent Shopping Applications	2*	6.9	1.8				3.5	80.0
22. Individualized services	1*	7.2	1.8				4.0	86.7

Note: An asterisk marks projections, where final consensus was reached, i.e. an IQR of 2 or less
IQR = Interquartile Range
SD = Standard deviation

In the first round consensus could be reached for 6 projections out of the 22, i.e. for 27.7% of all projections. In the second round the remaining 16 projections were given to the experts for reassessment. Another 5 projections reached consensus among the experts so that the total number of projections with consensus is 11, while the same number applies for projections with no consensus. Comparing the individual perspectives, the experts reached consensus in at least 50% of the projections for the socio-cultural, the technological and the retail industry perspective. Particularly for the latter perspective the experts showed a very high consensus already in the first round. Three of four projections reached consensus immediately while in two cases (projection 20 and 22), the consensus was even very strong, i.e. the IQR was 1. An analysis of the SD reveals a decrease for almost all estimated probabilities and in most cases significantly. Only in two cases (projection 9 and 19) the SD increased. This means the experts generally converged in their opinions in the second round. The values for (social) desirability within the socio-cultural perspective show common opinions about those projections. While projection 10 and 11 have a negative impact on society and are thus undesirable, the opposite is true for projections 12 to 14. In all their estimations the experts had a high consensus, either a very low or very high desirability.

The distribution of projections in Figure 51 provides interesting insights. It can be observed that all projections have an average impact above 3 and most of the projections have an average probability of 50% or more. Furthermore, Figure 51 shows that those projections for which consensus could be reached have a high concentration in the frame of a probability of occurrence of at least 63% and an impact of 3.3. Only two exceptions, projection 1 (IoT adoption) and 8 (ICT cost sharing), are outside of this frame. In general, this demonstrates the relevance of the projections developed in the first phase within the study. The results clearly demonstrate that projections, where consensus was not achieved, have an average probability significantly lower than where consensus could be reached and are highly distributed.

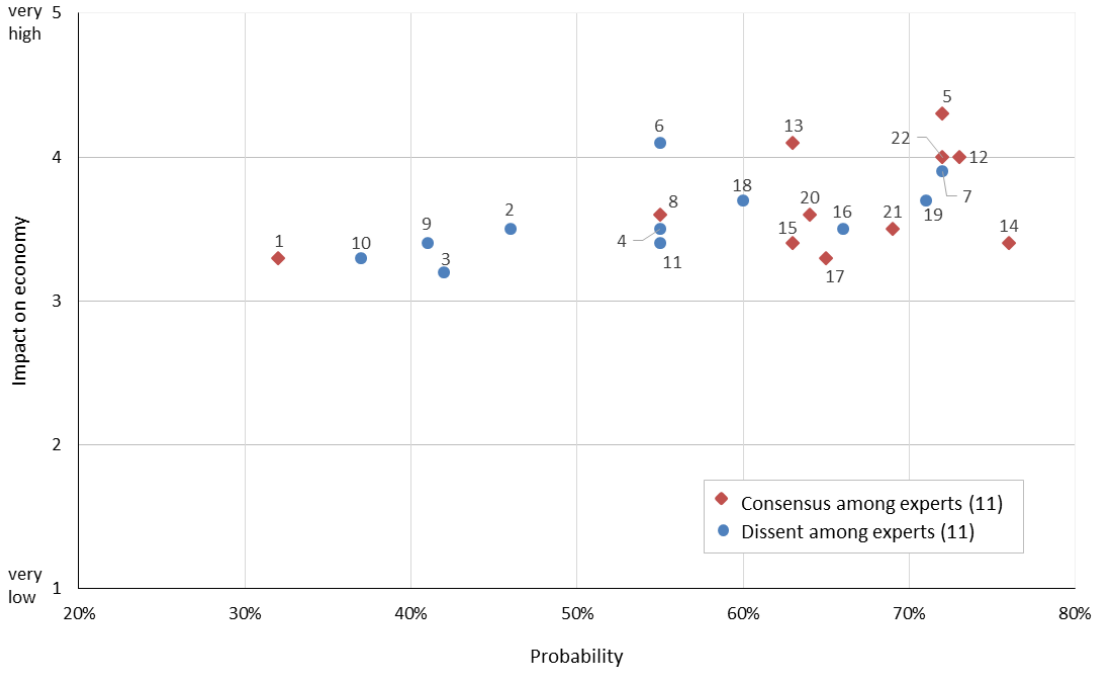

Figure 51: Overall evaluation of projections by probability and impact on economy

6.1.6 Conclusion

The study shows that IoT will play an important role in the future. Almost all projections in the context of IoT evaluated by IoT experts had a high probability of occurrence and a medium to high impact on the European economy. As a consequence one can assume that an increasing number of IoT systems will be developed in the next years for what a common grounding like the IoT ARM is even more important to ensure interoperability among the vast amount of potential IoT systems. Aside from the fact that the IoT will have significant impact on the economy as a whole, shown by the macroeconomic perspectives, the study shows that for some aspects in the retail industry the IoT experts showed a very high consensus. The results show that the experts had higher consensus for the projections of the technological and retail industry perspective which in both cases was 50% or higher. Looked at more closely, two projections of the technological perspective (15: Mobile payment and 17: Replacement of the barcode) reached consensus between the experts and can be seen as crucial for the future as they are already seen today. These two projections are prevalent topics related to the IoT which will be responsible for a transition from today's mostly used technologies to novel technologies such as NFC. An even higher consensus could be reached within the retail industry perspective in which the experts generally agreed. Three of the four projections had an agreement already in the first round and two of the three even had a very high consensus. This demonstrates that the IoT will have a strong impact on the retail industry and thus needs new and innovative IoT systems to cope with the customer demands of using intelligent and individualised services. Inferring from these expert opinions it can be foreseen that although the retail industry is already one domain in which the adoption of the IoT is faster than in other domains, it still has much potential for IoT implementations.

6.2 Security and privacy impact assessment

In this section, a privacy impact assessment (PIA) analysis of a specific IoT scenario is described. As a validation approach we try to find out if the IoT ARM supports or hinders a privacy compliant application development. A PIA out of a commonly accepted framework was followed in order to ensure valid results out of the privacy community. A selection of one scene out of the health use case demonstrators from WP7 was chosen to apply a PIA to. We took an

example of an implemented demonstrator with all implementation specific details out of [Fiedler 2013]. This simpler example served as an initial target to come to a specific analysis regarding privacy.

The following subsection explains the initial selection of an appropriate approach to fulfil such an analysis, while the sections thereafter explain the results in detail.

6.2.1 PIA method and process

In general there are many PIAs which may serve as a base for an IoT specific privacy analysis. We found the following ones to work with

- The paper of [Oetzel, 2012] introduces the general "Privacy-by-Design" approach and shows a generic, technology-neutral way to fulfil a PIA.
- The guidelines of [BSI 2011] are a complete PIA set consisting of guidelines similar to the [Oetzel, 2012] approach with focus to RFID applications. It also contains examples on how to use the PIA in different domains.
- The PIA tool of GS1 in [GS1 2012] focuses on EPCGlobal architectures only and also only covers RFID applications.

We choose to use the approach in [BSI 2011] for our analysis, as it directly covers the RFID technology field, which is regarding technology details in some parts similar to the IoT field. Besides that the given examples in the BSI guideline document were helpful to work out an own PIA of our specific chosen scene.

In a first step, the chosen guideline tries to give a decision for practitioners on what kind of PIA level an application needs to be examined as is shown in Figure 52.

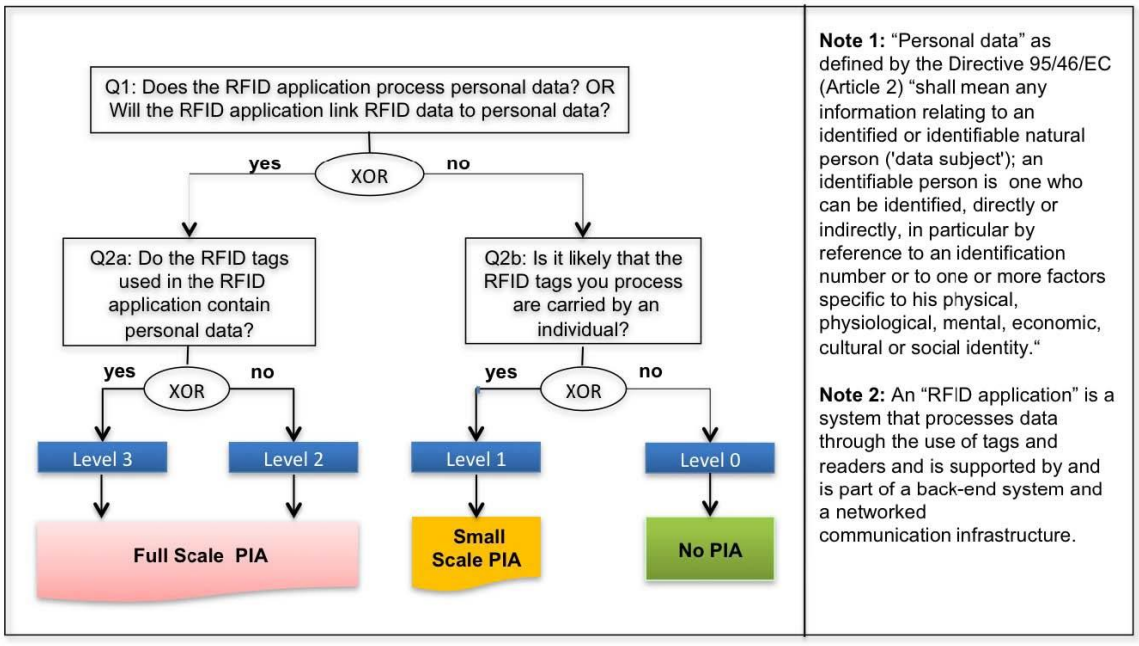

Figure 52: Decision tree for initial analysis ([BSI 2011])

The given decision tree is suited for RFID use, which is adaptable to the general IoT use. This is why the word "RFID" is exchangeable with IoT in the above figure.

Our chosen scenario does process personal data (Q1: yes), but the used IoT devices do not contain personal data (Q2a: no). With this answer we reach Level2 and have to perform a Full Scale PIA.

The following Figure 53 shows the general process of the privacy risk assessment methodology.

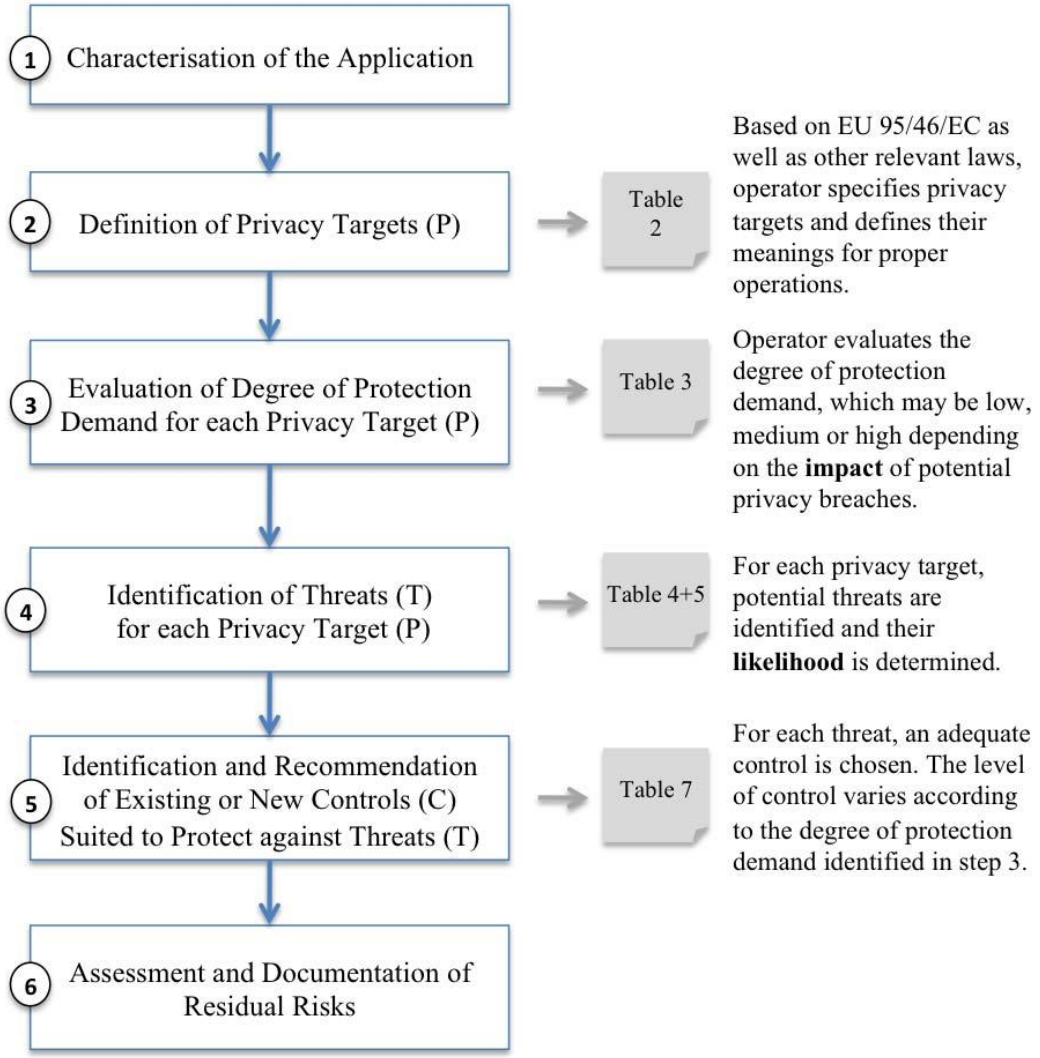

Figure 53: Privacy risk assessment methodology ([BSI 2011])

The steps 1-6 are in explained and executed in the subsections 6.2.3.1 to 6.2.3.6.

6.2.2 Preparation of the PIA analysis

To be able to do the PIA on a specific scenario it proved to be essential to involve the right personnel. To be able to answer all topics covered in the guideline the following experts should be involved

- Person with legal background
- Company's privacy officer
- Technician, implementation expert

- Business and/or application expert

As we took a scenario out of WP7, whose main purpose is more on the applicability of the IoT ARM in an implementation and less on real business scenarios we had to make assumptions on the latter. On the legal side several interviews were done with a law expert, so each legal term was explained and understood.

Finally the legal purpose of the application, meaning the service which is offered to the customer must be made clear to everyone to be able to understand the boundaries of it and limit errors due to misunderstanding.

6.2.3 Complete PIA analysis of example use case

We apply the chosen methodology in the following subsections step by step. .

6.2.3.1 Step 1: Application description

In a first step the application must be characterized in detail, so that the purpose of the legally defined application services and the planned implementation details (e.g. hardware, software, networks) is known. The chosen scene “Remote Patient Notification” is also explained in [Fiedler 2012] and [Fiedler 2013].

Technical service description

A patient living in his home is associated to an alarm and location service running on an IoT-Phone in the digital domain.

The remote patient care application looks up and resolves the alarm service associated to the patient. If found the alarm service is executed to draw the attention of the patient. After a timer expires in the remote patient care application the application searches in the resolution framework for the location service that is associated with the patient. The application executes the service to retrieve the location. With this information (location of patient) a location based search is done in the resolution framework to look for devices that can draw the attention of the patient. The response is that in the same location a remote switch is available and can be used for attention drawing.

The remote patient care application executes the remote switch service. The request is send to the fixed gateway with help of a IoT protocol. The gateway translates the request to the dedicated protocol and light is switch on/off.

When the patient still doesn’t react, the remote patient care application obtains from the electronic health record (EHR) the list of care givers that can be contacted.

With the information of the care givers a discovery of their locations is requested. The care giver most nearby the patient gets a notification on here IoT-Phone to trigger the patient to start taking his measurements.

Figure 54 shows the physical setup with used hardware and software components and the general network setup.

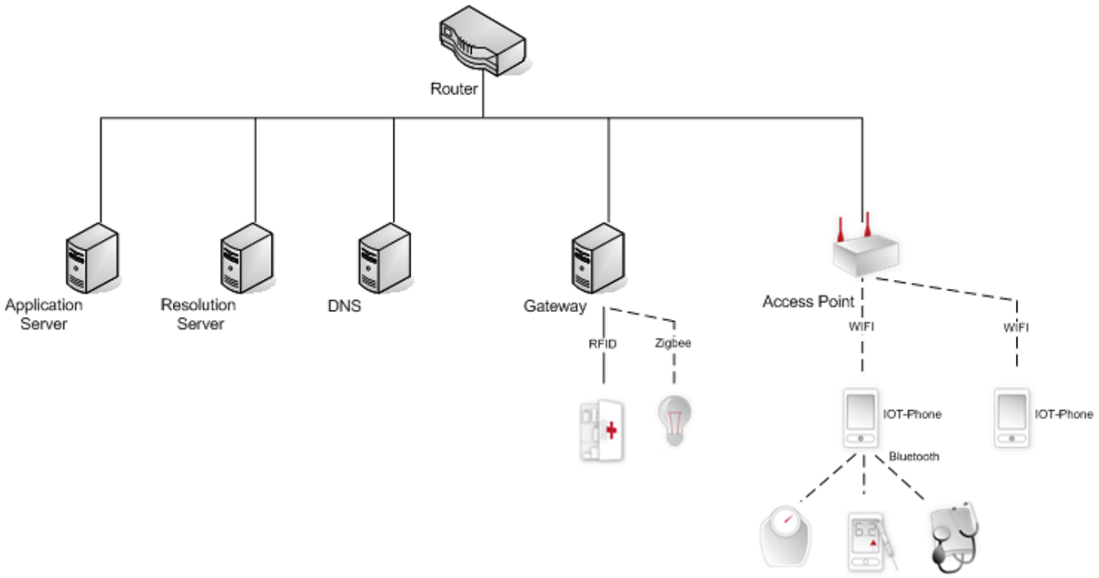

Figure 54: Physical setup of Remote Patient Notification demonstrator

Figure 55 shows the basic functionality regarding service and device usage of the scenario.

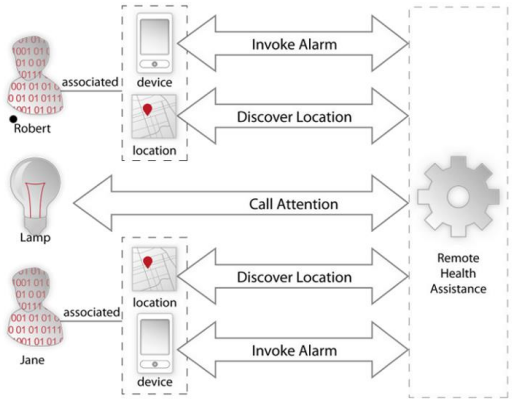

Figure 55: Used functionality of Remote Patient Notification

Overall purpose of service group

The examined scene is part of a larger scenario where follow-up scenes define a common purpose. In general the purpose of all coherent scenes is

- Remote and continuous monitoring of high risk patients (here: diabetes) organized by a health insurance company.
- In general the “Adherence and Conveyance” problem shall be solved. Patients tend to not take their medication as demanded by doctors, e.g. antibiotics are only taken the first days, but not the complete week. The system should remind the patient to do so in an automated way.

Purpose of Notification Service (considered in PIA)

The Notification Service out of the examined scene will be considered in the PIA. Other services out of the general service group will not be part of the analysis. The purpose of the Notification Service is

- The Remote Patient Care application notifies the patient that some actions are required be taken by the patient. These actions can be related to administering medicines or to taking measurements on a regular interval.
- The patient is notified by ringing an alarm on his IoT-Phone. This alarm is not acknowledged so the application will look for nearby resources such as light switches or buzzers in the vicinity of the last known location of the patient and use these devices to draw his attention. The patient shall finally acknowledge the alarm.
- The remote patient care application obtains from the EHR the list of care givers that are contacted when a patient does not react on the notification
- The care taker is informed about the purpose of the notification, e.g. Robert needs to take his measurements.

Involved parties

The following parties are involved in the scenario

- Health insure company, which runs the service
- Patient and Care Takers as End users

Gathered data

The following data is needed for the service to operate correctly

- Patient Virtual ID, list of care takers, measurements will be needed as long as any contract between patient and operator exists to fulfil the service. Temporary data like location should be deleted as soon as possible
- Current location of IoT-Phone (patient) [used by Notification Service]
- Lookup of nearby Devices [used by Notification Service]
- Lookup of caretakers out of EHR [used by Notification Service]

6.2.3.2 Step 2: Definition of Privacy Targets

In step 2 the general privacy targets relevant to the scenario are defined and examples on how to reach each privacy target are explained. The content is structured in Table 23.

Table 23: Step 2: Definition of Privacy Targets

Privacy target code and name		Contextual explanation	Examples for how to reach this target
P1.1	Ensuring fair and lawful processing through transparency	The operator must create internal and external transparency by explaining the IoT technology used and the data flows involved in operating the notification service and the notification of care takers. This information should be easily understandable and accessible for patient and associated care takers. Patient and Care taker should be able to understand the benefits and	Distribution of informational material, e.g. flyers, websites and a hotline

		consequences of participating in the notification service program.	
P1.2	Providing purpose specification and limitation	The operator must explicitly specify why patient location, lookup of a list of care takers and access to local, patient owned devices is needed to fulfil the service. It should be clear what data is used for which purposes, what data is linked and what data might be given to a third party. The service is limited to the Smart Home environment of the patient only.	Provide clear internal and external purpose specifications. Ensure that access rights are handled accordingly and patients and care takers are well informed about what their personal data is used for.
P1.3	Ensuring data avoidance and minimization	The operator must aim to design and implement the notification service so that only necessary consumer data is collected and processed. In this context, necessary means that the data is required for the fulfilment of the specified purpose.	Location information of patient and care taker should only be obtained and received when needed. Retrieving a name might not be needed at all. No historic data is needed to fulfil this service.
P1.4	Ensuring quality of data	The operator must ensure that patient data is correct and up-to-date. The operator must check that the current location of the patient is correct and that the associated information of the associated care takers is correct.	Sensors need to send accurate and correct information. Error in localizing the patient means the wrong notification devices are retrieved and contacted, e.g. a blinking light in a neighbours room. The patient needs to be enabled to correct his current location.
P1.5	Ensuring limited duration of data storage	The operator must only store the relevant data of the patient until the service is fulfilled. Patient virtual ID, care takers, measurements will be needed as long as any contract between patient and operator exists to fulfil the service. Temporary data like location should be deleted as soon as possible	Add strict delete rules (location, looked-up care-takers) when alarm is acknowledged and/or care takers are alarmed
P2.1	Legitimacy of processing personal data	When a patient participates in the remote patient notification program, check the validity of his or her consent to the use of his/her personal data.	The patient signs a consent form for personal data to be used by the service.
P3.1	Legitimacy of processing sensitive	Sensitive data is involved in the service. The measurements and	The patient signs a consent form for personal

	personal data	medication to be taken are communicated to the device of the patient and potentially to a care taker. Further the EHR is accessed to retrieve the list of care takers. It needs to be ensured, that the data is delivered only to authorized persons (or devices) and the patient needs to explicitly consent to the processing of this sensitive personal data.	data to be used by the service.
P4.1	Providing adequate information in cases of direct collection of data from the data subject	Data is directly collected from the patient/care takers through the notification switches/buttons. They are used to acknowledge the notification. Furthermore, the location of the patient is collected through its IoT device. Ensure that the patients and care takers are provided with information that describes the collected data.	Provide adequate information, see P1.1. Has to be acknowledged by the patient/care taker.
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	Several parties are involved in the notification procedure. The location of the nearby devices is retrieved from the system. If the patient does not react to an alarm, the identification and location of the care takers are obtained. Furthermore, the type of patient alarm is retrieved and shown to the care takers.	See P4.1
P5.1	Facilitating the provision of information about processed data and purpose	The patient can access all relevant information on whether and how his or her IoT data is used by the insurance company. Hence the patient has a contact point at the insurance company where it is possible to ask questions about subjects such as the existence of personal data, the purposes of the processing, the categories of data concerned, the recipients or categories of recipients (e.g. care takers, persons to be notified) to whom the data is disclosed, the data undergoing processing and any information as to the data's source, the logic involved in any automatic processing of data and automated decisions.	Provide a hotline or online access to the processed data
P5.2	Facilitating the rectification, erasure or blocking of data	Patients should be allowed to rectify, erase or block their data.	Enable patients to rectify, erase or block data about themselves via a web application. Provide patients with a contact address, form or

			the like that they can use to request rectification, erasure or blocking of their data.
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	The application contains data of 3rd persons, the care takers. The care takers need to be informed, if they are nominated or removed from the application.	Notification of 3rd party by e.g. email or phone.
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	Direct marketing and data sharing of patients' personal and sensitive data is not foreseen in this scenario.	Not applicable in this scenario. Objection to notification service provider is possible.
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	Patients should be able to object to being subject to automated decisions.	Objection to notification service provider is possible, e.g. deactivate service for some time.
P7.1	Safeguarding confidentiality and security of processing	BSI's TG 03126 needs to be considered. A specific security analysis must be performed. The data flows (resolution framework use, service use…) must be examined. Similar to this PIA any security relevant requirements and targets must be defined.	In-depth security analysis and implementation with according crypto. (IoT ARM Security FG)
P8.1	Compliance with notification requirements	Before going live with the notification service the supervisory data protection authority needs to be notified about the related processing of personal data. There is the need to provide the results of the PIA to the supervisory authority six weeks before the launch.	The operator should assign a person in their organisation to take care of these notifications. The assignee might need a project team to create the necessary documentation.

Privacy Target P7.1 requires an in depth security analysis. A specific security analysis must be performed. The data flows (resolution framework use, service use…) must be examined. Similar to this PIA any security relevant requirements and targets must be defined. The guideline [BSI 2011] suggests using BSI's TG 03126 for that purpose.

Besides that we suggest to use the approach in section 3.7 “Trust, Security, Privacy” and section 5.2.9 “Threat analysis” out of D1.5 [Carrez 2013].

6.2.3.3 Step 3: Evaluation of protection demand categories

In this step the general protection demand of each privacy target is defined.

Table 24 shows the defined protection demand categories we took in this step, taken out of [BSI2011].

Table 24: Protection demand categories and possible values ([BSI 2011])

Protec-tion demand	Criteria for the assessment of protection demand					
	General descrip-tion	Operator perspective		Data subject perspective		
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom
Low – 1	**The impact of any loss or damage is limited and calculable.**	Only **minimal** impairment or only internal impairment of the reputation / trustworthiness of the organisation is expected.	The financial loss is **acceptable** to the organisation.	The processing of personal data could **adversely** affect the social standing of the data subject. The data subject's reputation is threatened for a **short period** of time.	The processing of personal data could **adversely** affect the financial well-being of the data subject.	The processing of personal data **does not endanger the personal freedom** of those concerned.
Medium - 2	**The impact of any loss or damage is consider-able.**	**Considerable** impairment of the reputation / trustworthiness of the organisation can be expected.	The financial loss is **considerable**, but does not threaten the existence of the organisation.	The processing of personal data could have a **seriously adverse** effect on the social standing of the data subject. The data subject's reputation is threatened for a **longer period** of time.	The processing of personal data could have a **seriously** adverse effect on the financial well-being of the data subject.	The processing of personal data **could endanger the personal freedom** of those concerned.

High - 3	**The impact of any loss or damage is devasta-ting.**	An **international or nation-wide** loss of reputation / trustworthines s is conceivable, possibly even endangering the existence of the organisation.	The financial loss **threatens the existence** of the organisation.	The processing of personal data could have a **devastating** effect on the social standing of the data subject. The data subject confronts a **lasting** loss of reputation.	The processing of personal data could have a **devastating** effect on the financial well-being of the data subject.	The processing of personal data **could seriously endanger the personal freedom** or result in the injury or death of the data subject.

Table 25: Evaluation of protection demand for P1.1

Privacy target code and name		**Criteria for the classification of protection demand categories**					**Overall category**
		Operator Perspective		**Consumer perspective**			
		Impact on Reputation and Brand Value (a)	**Financial loss (b)**	**Social standing, reputation (c)**	**Financial well-being (d)**	**Personal freedom (e)**	
P1.1	Ensuring fair and lawful processing through trans-parency	2	1	2	1	2	2

(a) The service provider does not take sensitive data serious in health environment

(b) Financial loss is minor, due to a minor application

(c) Caretakers may obtain information on patient he is not aware of, e.g. which disease, when is he at home/does he take his medicaments.

(d) Financial well-being is a minor issue

(e) Care takers may obtain information on patient he is not aware of, e.g. when is he at home/does he take his medicaments.

Table 26: Evaluation of protection demand for P1.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P1.2	Providing purpose specification and limitation	3	2	3	2	2	3

(a) The misuse may have nation-wide impact on reputation with legal consequences.

(b) Significant repair actions may be needed.

(c) Sensitive medical data may be accessed by health insurance, employers.

(d) A breach might result in higher cost or even loss of insurance protection. A job loss is probable.

(e) The detailed use of the current location may be abused.

Table 27: Evaluation of protection demand for P1.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P1.3	Ensuring data avoidance and minimisation	1	1	3	2	2	3

(a) The operator's reputation can be minimally impaired because it is not very likely that customers will find out that the operator collects more data than necessary if the operator sticks to the specified purpose and services.

(b) The operator's financial loss can be acceptable if its reputation is only minimally impaired.

(c) Sensitive medical data may be accessed by health insurance, employers.

(d) A breach might result in higher cost or even loss of insurance protection. A job loss is probable.

(e) The detailed use of the current location may be abused.

Table 28: Evaluation of protection demand for P1.4

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P1.4	Ensuring quality of data	1	1	1	1	2	2

(a) Minor problem, the bad quality of data would be perceived as functional problem.

(b) Minor problem, the bad quality of data would be perceived as functional problem.

(c) Personal annoyance of patient and care takers only.

(d) Personal annoyance of patient and care takers only.

(e) Personal annoyance of patient and care takers only.

Table 29: Evaluation of protection demand for P1.5

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P1.5	Ensuring limited duration of data storage	1	2	3	2	2	3

(a) The data is not valuable

(b) Financial loss probable due to the management of higher data volumes (e.g. more servers and data space needed…)

(c) Sensitive medical data may be accessed by health insurance, employers.

(d) A breach might result in higher cost or even loss of insurance protection. A job loss is probable.

(e) Detailed use of the current location may be abused.

Table 30: Evaluation of protection demand for P2.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being d4)	Personal freedom (e)	
P2.1	Legitimacy of processing personal data	-	-	-	-	-	
See 3.1							

Table 31: Evaluation of protection demand for P3.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P3.1	Legitimacy of processing sensitive personal data	3	2	3	2	2	3

(a) A nation-wide impairment is possible, lawsuits may follow.

(b) Costly image campaigns might be needed, potential lawsuits may follow.

(c) Sensitive medical data may be accessed by health insurance, employers.

(d) A breach might result in higher cost or even loss of insurance protection. A job loss is probable.

(e) Detailed use of the current location may be abused.

Table 32: Evaluation of protection demand for P4.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P4.1	Providing adequate information in cases of direct collection of data from the data subject	1	1	1	1	1	1

(a) Minor problem, the use of the collected data is obvious to all parties.

(b) Minor problem, the use of the collected data is obvious to all parties.

(c) Minor problem, the use of the collected data is obvious to all parties.

(d) Minor problem, the use of the collected data is obvious to all parties.

(e) Minor problem, the use of the collected data is obvious to all parties.

Table 33: Evaluation of protection demand for P4.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	1	1	1	1	1	1

(a) Minor problem, the use of the collected data is obvious to all parties.

(b) Minor problem, the use of the collected data is obvious to all parties.

(c) Minor problem, the use of the collected data is obvious to all parties.

(d) Minor problem, the use of the collected data is obvious to all parties.

(e) Minor problem, the use of the collected data is obvious to all parties.

Table 34: Evaluation of protection demand for P5.1

Privacy target code and name		**Criteria for the classification of protection demand categories**					**Overall category**
		Operator Perspective		**Consumer perspective**			
		Impact on Reputation and Brand Value (a)	**Financial loss (b)**	**Social standing, reputation (c)**	**Financial well-being (d)**	**Personal freedom (e)**	
P5.1	Facilitating the provision of information about processed data and purpose	1	1	1	1	1	1

(a) Besides treatment data and care taker information, no other data is collected which could be sent to patient.

(b) Besides treatment data and care taker information, no other data is collected which could be sent to patient.

(c) Besides treatment data and care taker information, no other data is collected which could be sent to patient.

(d) Besides treatment data and care taker information, no other data is collected which could be sent to patient.

(e) Besides treatment data and care taker information, no other data is collected which could be sent to patient.

Table 35: Evaluation of protection demand for P5.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P5.2	Facilitating the rectification, erasure or blocking of data	2	1	1	1	1	2

(a) The service provider does not take sensitive data seriously in health environment

(b) Financial loss is considered minor.

(c) Personal annoyance of patient and care takers only.

(d) Personal annoyance of patient and care takers only.

(e) Personal annoyance of patient and care takers only.

Table 36: Evaluation of protection demand for P5.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	1	1	1	1	1	1

(a) Minor problem

(b) Minor problem

(c) Minor problem

(d) Minor problem

(e) Minor problem

Table 37: Evaluation of protection demand for P6.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	-	-	-	-	-	-
This privacy target is considered as not applicable.							

Table 38: Evaluation of protection demand for P6.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	-	-	-	-	-	-
Not applicable, due to completely determined flow and no relevant decisions.							

Table 39: Evaluation of protection demand for P7.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P7.1	Safeguarding confidentiality and security of processing	-	-	-	-	-	-
Not applicable here, see BSI TG 03126 and D1.5 [Carrez 2013].							

Table 40: Evaluation of protection demand for P8.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall cate-gory
		Operator Perspective		Consumer perspective			
		Impact on Reputation and Brand Value (a)	Financial loss (b)	Social standing, reputation (c)	Financial well-being (d)	Personal freedom (e)	
P8.1	Compliance with notification requirements	2	2	-	-	-	2

(a) The operator's reputation can be considerably impaired because he might get into conflict with the supervisory data protection authority. These conflicts might be exposed to the public.

(b) The operator's financial loss can be considerable if he is forced to pay fines, create the necessary documentation ad-hoc with the help of costly consultants and be subject to regular controls by the supervisory authority in the future

(c) Not applicable

(d) Not applicable

(e) Not applicable

6.2.3.4 Step 4: Identification of Threats for each Privacy Target

In step 4 the general threats are identified. Here we differentiated 4 options whether a threat is likely or not.

Table 41: Options of threat occurrence

Option	Description
y	The threat is likely to occur.
n	The threat is not likely to occur
y*	The threat may occur, depending on real implementation of application. Further details are needed on a real world instantiation, which were not covered in the prototype.
n*	The threat is not likely to occur, depending on real implementation of application. Further details are needed on a real world instantiation, which were not covered in the prototype.

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
T1	Lack of Transparency - Missing or insufficient service information	T1.1	Incomplete or insufficient information describing the service. The operation details (data flows, data locations, ways of transmission, etc.) and the impacts of the RFID application are not sufficiently explained to the data subject. An RFID emblem is not displayed on the website of the RFID	y*	Real implementation must explain usage/consequences of IoT application. Substitute or complement the RFID emblem with hints to the used technology, i.e. IoT logo (use case does not use RFID but IoT technology)
		T1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable.	y*	Real implementation must provide easy access to description of service.
		T1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	y*	y* == technical use case only covered, organizational topics are not covered. This has to be done in a real implementation
		T1.4	Existing information describing the service is not easily understandable and / or special knowledge is needed to understand it, e.g. jurisdictional terminology, company-internal abbreviations, a distinct	y*	

			language, etc.		
		T1.5	Existing information describing the service is not kept up-to-date.	y*	
		T1.6	Information provided in conjunction with an RFID emblem does not cover all areas and purposes for which RFID is used in a facility.	y*	adoption due to T1.1 (RFID emblem) needed
	Lack of Transparency - Missing or insufficient privacy statement	T1.7	No privacy statement is available.	y*	technical use case description only
		T1.8	Existing privacy statement does not explain sufficiently how data subject's data is processed.	n	Countermeasures of T1.7 must address the threat
		T1.9	The existing privacy statement does not provide contact information to reach the RFID Operator and does not provide contact details in case of questions or complaint.	n	Countermeasures of T1.7 must address the threat
		T1.10	The existing privacy statement is difficult to access; i.e. difficult to read, difficult to find, etc.	n	Countermeasures of T1.7 must address the threat
		T1.11	The existing privacy statement does not contain information about relevant third parties that also receive the data subject's data.	n	Countermeasures of T1.7 must address the threat
		T1.12	The existing privacy statement is not available in the various languages in which it will most probably be read.	n	Countermeasures of T1.7 must address the threat
	Missing RFID emblem	T1.13	At the entrance of a respective facility using RFID or in places where RFID readers are deployed, no RFID emblem notifies data subjects of the data collection process	y*	use of RFID emblem is not applicable/ sufficient in this application, IoT logo needed
		T1.14	No RFID emblem is displayed on the product and the product packaging.	y*	use of RFID emblem is not applicable/ sufficient in this application, IoT logo needed

	Unspecified and unlimited purpose	T1.15	The purpose of the data collection is not specified. It is not specified that the collected data is used only for a distinct purpose or service that is transparent to the data subject as well as to employees.	n	
		T1.16	The data collection purpose is not documented in an adequate way.	n	
		T1.17	Data that is stored and processed only for a specific purpose is not marked and / or managed accordingly; e.g. with corresponding access rights.	y	not specified in the use case
	Collection and/or combination of data exceeding purpode	T1.18	Collected data is processed for other purposes than the purpose it was originally obtained for. These different purposes are not compatible with the original purpose.	n	
		T1.19	Processing of data is not logged, thus misuse or processing for another purpose cannot be detected.	y	only in-memory processing
		T1.20	The data subject is required to provide personal data that is not relevant for the specified purpose of the service.	n	
		T1.21	There are no measures in place that ensure data-minimisation. Thus, there are no measures to ensure that only relevant data is processed and that it is not processed excessively in relation to the purpose.	n	foreseen implementation takes care of that
		T1.22	There are no measures in place that prevent the linking of data sets. Thus, data collected during the occurrence of the service can be combined with data acquired from a third party or with data from another service the operator / organisation is offering.	n	foreseen implementation takes care of that

		T1.23	There are no measures in place that prevent the reading and tracking of the tagged item through unauthorised parties. The RFID tag has no read protection	n	no RFID use in use case, potential inclusion of IoT technology required, for example use of discovery services
	Missing quality assurance of data	T1.24	Data collection tools / forms are not sufficiently checked for completeness and correctness.	n	no data collection tools / web forms
		T1.25	The identification of the data subject is not conducted thoroughly.	n	fingerprint reader etc.
		T1.26	Procedures that regularly check (either by contacting the data subject or automatically searching publicly available data) that data is accurate and up-to-date have not been implemented.	n*	EHR record needs to be up-to-date, e.g. information on relatives
		T1.27	Personally identifiable data-subject profiles are enriched by probabilistic algorithms that lead to false judgements about a data subject.	n	
	Unlimited data storage	T1.28	Data subjects' data as well as corresponding back-up data is not deleted or anonymised when it is no longer needed for the specified purpose. Erasure policies are missing.	n	no data storage, in-memory processing only
		T1.29	Data subjects' data, which is no longer needed for the specified purpose but cannot be deleted due to retention rules, cannot be excluded from regular data processing.	n	no data storage, in-memory processing only
T2		T2.1	Consent has not been obtained or has been obtained on the basis of incomplete or incorrect information.	y*	
		T2.2	Consent has been obtained based on an offer of advantage or threat of disadvantage.	y*	
		T2.3	The relevant legal basis (e.g.	y*	

			consent, contract, legal obligation, vital interests, public task, balancing interests) has been transgressed.		
T3		T3.1	Explicit consent has not been obtained or has been obtained on the basis of incomplete or incorrect information.	y*	
		T3.2	Explicit consent has been obtained based on an offer of advantage or threat of disadvantage.	y*	
		T3.3	The relevant legal basis (e.g. explicit consent, field of employment law, vital interests, not-for-profit-body, published sensitive data, defence of legal claims, special legal basis) has been transgressed.	y*	
T4	No or insufficient information concerning collection of data from the data subject	T4.1	At the time of data collection, the data subject is not or not sufficiently informed about all of the following: -the identity of the data controller and of his representative if any, -the purpose of the processing, -the recipients of the data (is the data given to any third party?), -which questions on the registration form are voluntary and which are optional and what are the consequences when not replying, -the existence of the right of access to and the right to rectify the data concerning him.	y*	Technical objective: notification. Organization notification means data collection
		T4.2	The relevant information is not provided in an adequate form (e.g. explicitly in the data collection questionnaire, small pop-up box that is	y	

			easily clicked away).		
		T4.3	The relevant information is not easily accessible but hidden (e.g. small print in a legal section).	y	
	No or insufficient information concerning data that has not been obtained from the data subject	T4.4	When data is obtained from a third party, the data subject is not sufficiently informed about all of the following: -the identity of the data controller and of his representative if any, -the purpose of the processing, -the categories of data concerned, -the recipients of the data (is the data given to any third party?), -the existence of the right of access to and the right to rectify the data concerning him.	y*	
		T4.5	The relevant information is not provided in an adequate form (e.g. easily readable and accessible).	y	
		T4.6	The relevant information is not easily understandable; therefore, it is possible that the data subject will not be able to understand that the operator obtained information about him or her from a third party.	y	
T5	Inability to provide individualised information about processed data and purpose	T5.1	At the time of processing, the operator does not provide any interface to the data subject that the subject can use to efficiently identify what data about him or her is processed and what the data is used for. Even if the data subject sends a request requiring information, there is no procedure to automatically obtain this individualised information from the operator's systems.	y*	Possible update of use case implementation: add simple form providing information on processed data

		T5.2	Access is possible but not to all relevant data, including: -confirmation as to whether or not data relating to the data subject is being processed, -the purpose of the processing, -the categories of data concerned, -the recipients or categories of recipients to whom the data is disclosed, -the data undergoing processing and any information as to the data's source, -the logic involved in any automatic processing of data and automated decisions.	y*	
		T5.3	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before allowing access.	n	fingerprint reader etc.
		T5.4	Successful access as well as subsequent data disclosure is not logged.	y*	
	Inability to rectify, erase or block individual data	T5.5	A procedure (technical means and / or processes) that allows the data subject to rectify, erase or block individual data has not been implemented.	y*	example: new device has been bought
		T5.6	Errors are not automatically rectified.	y*	
		T5.7	There is no procedure that allows the erasure of individual data in back-up data.	n	no backup-data defined
		T5.8	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before rectification, erasure or blocking of data.	y*	
		T5.9	Successful rectification,	y*	

			erasure and blocking is not logged.		
	Inability to notify third parties about rectification, erasure and blocking of individual data	T5.10	The operator has not implemented any procedure that would notify relevant third parties when individual data has been rectified, erased or blocked.	y	
T6	Inability to allow objection to the processing of personal data	T6.1	The data subject is not informed about the disclosure of his data to third parties or about the use of his data for direct marketing purposes and thus the data subject cannot object.	n	
		T6.2	A procedure (technical means and / or processes) that allows objection to the processing of personal data has not been implemented.	n	
		T6.3	The operator has not implemented any procedure that would allow the notification of relevant third parties in the case that a data subject has objected to the processing of his personal data.	y*	
	Inability to allow objection to being subject to decisions that are solely based on automated processing of data	T6.4	The data subject cannot object to automated decision procedures that are used in the realm of the offered service.	y	
T7	Refer to security-relevant threats that are defined in BSI's technical guidelines TG 03126.	T7.1	Refer to the description of security-relevant threats that are defined in BSI's technical guidelines TG 03126-4.	mentioned use cases in TG03126 are not applicable to health notification service scenario. Need to include technology specific security analysis guideline.	
T8	Non-compliance with notification requirements	T8.1	The operator does not notify the supervisory authority or the internal data protection officer as legally defined before carrying out personal	y*	

			data processing.		
		T8.2	The operator does not provide all the legally defined contents in his notification to the supervisory authority or the internal data protection officer.	y*	
		T8.3	The operator does not publish or does not ensure the availability of the legally defined notification contents to any person on request.	y*	
		T8.4	The operator does not ensure the availability of the PIA report six weeks before the launch or upgrade of the RFID application.	y*	

6.2.3.5 Step 5: Identification and recommendation of controls

In step 5 the identified threats are matched to specific controls, depending on the overall protection demand.

Sub-threat code	Control Code(s) and Name(s)		Assigned overall category (from step 3)	Description/Comment
T1.1	C1.1	SERVICE DESCRIPTION	2 (P1.1)	Real implementation must explain usage/consequences of IoT application. Substitute or complement the RFID emblem with hints to the used technology, i.e. IoT logo (use case does not use RFID but IoT technology)
	C1.4	INFORMATION TIMELINESS		
	C6.2	HANDLING OBJECTIONS TO AUTOMATED DECISIONS		
T1.2	C1.2	INFORMATION ACCESSIBILITY	2 (P1.1)	Real implementation must provide easy access to description of service.
T1.3	C1.1	SERVICE DESCRIPTION	3 (max(P1.1, P1.2))	y* == technical use case only covered, organizational topics are not covered. This has to be done in a real implementation
T1.4	C1.1	SERVICE DESCRIPTION	2 (P1.1)	

	C1.3	LANGUAGE/SEMANTICS OF INFORMATION		
T1.5	C1.4	INFORMATION TIMELINESS	2 (P1.1)	
T1.6	C1.1	SERVICE DESCRIPTION	3 (max(P1.1, P1.2))	adoption due to T1.1 (RFID emblem) needed
	C1.2	INFORMATION ACCESSIBILITY		
T1.7	C1.5	PRIVACY STATEMENT	2 (P1.1)	technical use case description only
T1.8	C1.5	PRIVACY STATEMENT		Countermeasures of T1.7 must address the threat
T1.9	C1.5	PRIVACY STATEMENT		Countermeasures of T1.7 must address the threat
T1.10	C1.5	PRIVACY STATEMENT		Countermeasures of T1.7 must address the threat
T1.11	C1.5	PRIVACY STATEMENT		Countermeasures of T1.7 must address the threat
T1.12	C1.5	PRIVACY STATEMENT		Countermeasures of T1.7 must address the threat
T1.13	C1.6	RFID EMBLEM	2 (P1.1)	use of RFID emblem is not applicable/sufficient in this application, define IoT logo
T1.14	C1.6	RFID EMBLEM	2 (P1.1)	Use of RFID emblem is not applicable/sufficient in this application, define IoT logo
T1.15	C1.7	PURPOSE SPECIFICATION		
T1.16	C1.7	PURPOSE SPECIFICATION		
T1.17	C1.8	ENSURING LIMITED DATA PROCESSING	3 (P1.2)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level. Details are not specified in the use case.
T1.18	C1.8	ENSURING LIMITED DATA		

		PROCESSING		
	C1.9	ENSURING PURPOSE RELATED PROCESSING		
T1.19	C1.9	ENSURING PURPOSE RELATED PROCESSING	3 (P1.3)	It is regularly checked that collected data is used only for the specified purpose. Corresponding access rights are regularly checked and updated. Access to data and processing of data is logged on a level that is sufficient to detect potential misuse or processing for another purpose than the specified one. Only in-memory processing is used.
T1.20	C1.10	ENSURING DATA MINIMISATION		
T1.21	C1.10	ENSURING DATA MINIMISATION		foreseen implementation takes care of that
T1.22	C1.8	ENSURING LIMITED DATA PROCESSING		foreseen implementation takes care of that
T1.23	C1.11	ENSURING TAG PROTECTION		No RFID use in use case, potential inclusion of IoT technology required, for example use of discovery services
T1.24	C1.12	ENSURING PERSONAL DATA QUALITY		No data collection tools / web forms
T1.25	C1.13	ENSURING DATA SUBJECT AUTHENTICATION		fingerprint reader etc.
T1.26	C1.14	ENSURING DATA ACCURACY	2 (P1.4)	EHR record needs to be up-to-date, e.g. information on relatives
T1.27	C1.14	ENSURING DATA ACCURACY		
T1.28	C1.15	ENABLING DATA		no data storage, in-memory

		DELETION		processing only
T1.29	C1.15	ENABLING DATA DELETION		no data storage, in-memory processing only
T2.1	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	
T2.2	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	
T2.3	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	
T3.1	C3.1	OBTAINING DATA SUBJECT'S EXPLICIT CONSENT	3 (P3.1)	
T3.2	C3.1	OBTAINING DATA SUBJECT'S EXPLICIT CONSENT	3 (P3.1)	
T3.3	C3.1	OBTAINING DATA SUBJECT'S EXPLICIT CONSENT	3 (P3.1)	
T4.1	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	1 (P4.1)	Technical objective: notification. Organization notification means data collection
T4.2	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	1 (P4.1)	At the time of data collection, the data subject has access to information that describes all relevant data: -the identity of the data controller and of his representative, if any, -the purpose of the processing, -the recipients of the data (is the data given to any third party?), -which questions on the registration form are voluntary and which are optional and what are

				the consequences of not replying, -the right to access and rectify the data about him. For example, this information might be accessible online via a link on the data collection form / tool and that leads to a separate web page that contains legal information.
T4.3	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	1 (P4.1)	At the time of data collection, the data subject has access to information that describes all relevant data: -the identity of the data controller and of his representative, if any, -the purpose of the processing, -the recipients of the data (is the data given to any third party?), -which questions on the registration form are voluntary and which are optional and what are the consequences of not replying, -the right to access and rectify the data about him. For example, this information might be accessible online via a link on the data collection form / tool and that leads to a separate web page that contains legal information.
T4.4	C4.2	PROVIDING INFORMATION ON THIRD PARTY INFORMATION PROCESSING	1 (P4.2)	

T4.5	C4.2	PROVIDING INFORMATION ON THIRD PARTY INFORMATION PROCESSING	1 (P4.2)	When data is obtained from a third party, the data subject has access to information that describes all relevant data: -the identity of the data controller and of his representative, if any, -the purpose of the processing, -the categories of data concerned, -the recipients of the data (is the data given to any third party?), -the existence of the right of access to and the right to rectify the data concerning him. E.g. this information can be accessed online via a link that leads to a separate web page that contains a lot of legal information.
T4.6	C4.2	PROVIDING INFORMATION ON THIRD PARTY INFORMATION PROCESSING	1 (P4.2)	When data is obtained from a third party, the data subject has access to information that describes all relevant data: -the identity of the data controller and of his representative, if any, -the purpose of the processing, -the categories of data concerned, -the recipients of the data (is the data given to any third party?), -the existence of the right of access to and the right to rectify the data concerning him. E.g. this information can be accessed online via a link that leads to a separate web page that contains a lot of legal information.
T5.1	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	Comment: Possible update of use case implementation: add simple form providing information on processed data
T5.2	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	

T5.3	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	1 (P5.1)	Comment: fingerprint reader etc.
T5.4	C5.2	LOGGING ACCESS TO PERSONAL DATA	1 (P5.1)	
T5.5	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	Comment: example: new device has been bought
T5.6	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	
T5.7	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS		Comment: no backup-data defined
T5.8	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	2 (P5.2)	
T5.9	C5.2	LOGGING ACCESS TO PERSONAL DATA	2 (P5.2)	
T5.10	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	1 (P5.3)	A contact address is available that can be used by data subjects to ask for rectification, erasure or blocking of the processing of their personal data. There are clearly defined processes that describe involved roles / employees, required actions and a time frame for answering a data subject's request. These requests are then individually processed and the respective data is individually rectified, erased or blocked. Contact addresses of involved third parties are available to the data subject and he is asked to request respective changes

				him- or herself.
T6.1	C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES		
T6.2	C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES		
T6.3	C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES	n/a (P6.1)	
T6.4	C6.2	HANDLING OBJECTIONS TO AUTOMATED DECISIONS	n/a (P6.2)	
T7.1	C7.1	SECURITY CONTROLS	mentioned use cases in TG03126 are not applicable to health notification service scenario	
T8.1	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	
T8.2	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	
T8.3	C8.2	PRIOR CHECKING	2 (P8.1)	
T8.4	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	

6.2.3.6 Step 6: Documentation of residual risks

In the previous analysis up to step 5 (section 6.2.3.5) privacy targets, threats, and controls are assessed. Since the demonstration scene does not represent a complete business application there is some information missing to get a full picture of open issues and to assess the risk if they cannot be covered by controls. For instance, a real implementation has to explain the usage and the consequences of the IoT application. If this is not done, then the user may have

insufficient information and there is a high risk that the application may be unfair or even unlawful.

In a real application it is sometimes impossible to control all threats and there are residual risks. According to the PIA recommendations “These residual risks should be documented in this step. It is recommended to provide a comprehensive description and an evaluation (low, medium, high) for each residual risk.”

Regarding the analysed use case scene it is impossible to list the residual risks without the knowledge of organisational setup and the concrete environment the application would be instantiated in.

6.2.4 Conclusion

The BSI privacy impact assessment (PIA) framework was used to validate the IoT ARM against the protection of user data. As such an assessment can only be performed by considering a concrete example and a concrete implementation, we used a single scene from the healthcare use case of WP7. Following the application description in step 1, the concerning privacy targets which relate to the chosen scenario were defined in step 2 and weighted in step 3 with protection demands for specific views. These steps are all related to the application itself and consequences of misuse of user data. Step 4 and 5 go more into the identification of threats and identification of possible controls in the (possibly planned) implementation.

It was found that IoT ARM components may help to address specific threats. In general in the design phase an application architect should follow the privacy principles of data avoidance and minimisation and define the purpose of each software component which stores or handles personal data. An architect may use the following IoT ARM Functional Components to design a protection of the personal data: Authentication, Authorization, Key Exchange & Management, Trust & Reputation, Identity Management.

In our analysed use case scene mainly the privacy of user data is addressed since the protection of privacy also includes the correct application of security features. It has been not possible to perform a full PIA because many organizational and some technical details are missing to achieve a real implementation. However, the application of the PIA to the IoT-A demonstration scene “Remote Patient Notification” ([Fiedler 2012] and [Fiedler 2013]) showed that the PIA is very useful to identify what measures have to be taken to achieve a real implementation respecting full privacy. Furthermore, it has been very obvious during the analysis that the use of the IoT ARM and of the PIA are independent of each other. Thus, IoT ARM does not interfere or hinder the implementation of a secure and private IoT scenario (orthogonal). Even more, they can be seen as two supporting elements to build a private and secure IoT application (parallel). The Sections 3.7, 4.2, 4.3, 5.2, 5.3 of the IoT ARM [Carrez, 2013] mention comparable security and privacy objectives, functionality, requirements, and methods for an architecture generation as the PIA. Therefore, the PIA framework is well suited to validate the privacy of an IoT application scenario and the IoT ARM is well suited to develop a secure and private IoT architecture.

7 Conclusion and outlook

Developing an IoT ARM is an inherently creative but complex activity. However, by employing an evolutionary process that explicitly captures architecturally significant requirements, exploits known architecture patterns and systematically validates the iterative versions, making the complexity manageable. The final validation of the IoT ARM is subject of this document, thus this deliverable described the validation activities and interactions regarding validation within the IoT-A project and between the IoT-A project and external stakeholders. The final validation report summarises the preparation, execution and reporting of the validation activities within the IoT-A project. The IoT ARM was validated according to which key success factors that were introduced in section 2.1. These factors correspond to each of the validation perspectives regarded in this document, viz. the technical, business and socio-economic perspective. Furthermore the most often applied validation techniques to achieve the goals of validation were presented.

The creation of the IoT ARM was not only based on the architecture team itself but also on the stakeholder interaction. Only after a project knows what their target people are expecting as outcome they can react accordingly. This is why in case of the IoT-A project a stakeholder group was set up in the beginning which played a decisive role in different activities. The first crucial stakeholder input could be obtained in the requirements engineering process as the first set of requirements stem from stakeholder workshop 1. On the basis of a refinement of the requirements the first iteration of the IoT ARM was built. Later on, the validation process considered not only the core stakeholder group but also many additional stakeholders from different sectors as outlined in section 3. This variety of people ensured a broad feedback to the development process of the IoT ARM and the appropriate people provided their input according to their specific background. Overall, the broad stakeholder community we could draw on was one of the crucial success factors that led to the final result.

The stakeholder input was specifically important in conjunction with the technical validation as explained in section 4. Although this part of validation was done internally to a large extent, the stakeholders brought in perspectives from the outside and could thus cover project needs as for instance non-technical input. For that reason, technical validation was integrated in the regular stakeholder workshops and irregular additional events where specific input was captured. With regard to technical feedback from stakeholder workshops, SW4 provided important results to understand in how far the Domain Model was understood by project-external people. The conclusion was that the Domain Model can be understood, but not easily applied within the context of the stakeholder's own domain of work. As this feedback has its origin in a very diverse group of stakeholders consisting of business as well as technical people, the IoT-A consortium had decided to conduct technical workshops with an audience (IERC, industry companies, Prof. Muller and selected experts) that comes from very technical and software architectural fields. The approach of setting up these expert meetings led to structured feedback which was processed and then subsequently implemented. Another important part of the technical validation was the reverse mapping of the IoT ARM onto an existing architecture, namely MUNICH. This exercise showed that an existing system that has been designed without applying the IoT ARM can be redesigned according to the IoT ARM. The combined approach of doing internal and external validation ensured meeting the high quality standards set in the beginning of the project to conclude with an IoT ARM that reached a mature state.

The business validation reveals in which way the IoT ARM can make a positive contribution to business. This part of the validation encompassed qualitative as well as quantitative results which clearly show that systems based on the IoT ARM may have significant advantages over those developed without considering the IoT ARM. This result is described in the context of the value chain. We highlighted the result by mapping the consortium partners which were responsible for the use cases onto the value chain and generalising their profiles we highlighted, at which points of the value chain specific industry companies are located and might generate additional value of the IoT ARM. This of course is not limited to only those mapped industry partners. Our section on the business case, performed on the retail/logistics use case and the MUNICH platform shows that both business cases have a better result considering the IoT ARM compared to implementations not using it. The better result is

especially true for the retail/logistics use case as in this business case the development costs are considered. But even so for the MUNICH platform we could identify value for using the IoT ARM, although we could not consider the development phase as it is an existing system. Overall the business case shows how processes and value chains are transformed by the IoT ARM. The final section about Business Networks extends the vision of the value chain by revealing the importance of collaboration between partners in a Business Network and the value of the relationships among them. The contribution of the IoT ARM can be seen in the common basis on which IoT systems are developed to ensure interoperability between all partners.

The last part of validation comprises the socio-economic impact. As a first activity we conducted a Delphi study which addresses the impact of IoT on the macro-environment as well as the retail industry as one example of an industry domain. The study results indicate that for many IoT projections the impact of the IoT on the economy as a whole will be tremendously which in turn requires a common ground like the IoT ARM to guarantee a high interoperability between future IoT systems. Furthermore the fact that privacy is a constantly recurring problem in the context of IoT we performed a privacy impact assessment based on a healthcare scene. The results show that the PIA is very useful to identify what measures have to be taken to achieve a real implementation respecting full privacy. Furthermore, it has been very obvious during the analysis that the use of the IoT ARM and of the PIA are independent of each other. Thus, the IoT ARM does not interfere or hinder the implementation of a secure and private IoT scenario (orthogonal). Even more, they can be seen as two supporting elements to build a private and secure IoT application (parallel).

The final validation report analysed the IoT ARM as the main outcome of the IoT-A project from different perspectives. As shown in section 2.3 validation was not only performed in WP6 but also in the technical work packages. The comprehensive approach undertaken and presented in this document gives proof that the IoT ARM is not only sound from a technical point of view but also relevant from a business and socio-economic perspective.

References

[Akyazi, 2013] Akyazi, M.: *Aufwands- und Kostenschätzung*. In: http://www4.in.tum.de/lehre/seminare/hs/WS0506/mvs/files/Ausarbeitung_Akyazi.pdf accessed on 25.02.2013.

[Atzori, 2010] Atzori, L.; Iera, A.; Morabito, G. (2010): *Internet of Things: A Survey*., In: Computer Networks, S. 1-19.

[Bruegger, 2009] Bruegger, R., „Der IT Business Case – Kosten erfassen, Nutzen erkennen, Wirtschaftlichkeit nachweisen und realisieren“, Springer Verlag, 2009.

[BSI 2011] Bundesamt für Sicherheit in der Informationstechnik (BSI), Privacy Impact Assessment Guideline for RFID Applications, in: https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/PIA/pia_node.html, 2011.

[Bucherer, 2011] Bucherer, E.; Uckelmann, D. (2011): *Business Models for the Internet of Things*. In: Uckelmann, D.; Harrison M.; Michahelles, F. (Hrsg): Architectin the Internet of Things. Springer, Berlin-Heidelberg.

[Burns, 2002] Burns, L. R. (2002). The Health Care Value Chain: Producers, Purchasers, and Providers (1st ed., p. 464). Jossey-Bass.

[Carrez, 2013] Francois Carrez (ed.), “Deliverable D1.5 – Final architectural reference model for the IoT v3.0”, 2013.

[Christopher, 1998] Christopher M.G. (1998), Logistics and supply chain management: strategies for reducing costs and improving services, London: Pitman Publishing.

[Dada, 2008] Dada, A.; Thiesse, F. (2008): *Sensor applications in supply chain: The example of quality-based issuing of perishables.* In: Floerkemeier, C.; Langheinrich. M.; Fleisch, E.; Mattern. F.; Serma, S., E. (Hrsg): *The Internet of Things*. Springer Berlin Heidelberg, S 140-154.

[De Vet, 2005] De Vet, E., Brug, J., De Nooijer, J., Dijkstra, A., De Vries, N.K., (2005). Determinants of forward stage transitions: a Delphi study. Health Education Research 20 (2), 195–205.

[Delporte-Vermeiren, 2003] Delporte-Vermeiren, D. (2003), Improving the flexibility and profitability of ICT-enabled business network: an assessment method and tool. Doctoral thesis.

[FAZ, 2013] FAZ Frankfurter Allgemeine Zeitung: Hat ein Menschenleben einen Geld Wert. In: http://www.faz.net/aktuell/wirtschaft/oekonomie-hat-ein-menschenleben-einen-geldwert-1230638. acessed on 05.04.2013.

[Feussner, 2006] Feussner, H.; Schneider, A. (2006) Der vergesssene Fremdkörper. In: März 2006 Fortbildungswoche.

[Fiedler, 2012] IoT-A Project Deliverable D7.2 - Exact definition use case 1 and use case 2.

[Gaudí, 2013] Website of the Gaudí project: http://www.gaudisite.nl/GaudiProject.html, accessed on 01.07.2013

[Gehaltsvergleich, 2013] Gehaltsvergleich: *Berufsbild Softwareentwickler/in*. In: http://berufe.gehaltsvergleich.com/s/Softwareentwickler-Softwareentwicklerin.html accessed on 01.02.2013.

[GS1, 2012] GS1 EPC/RFID Privacy Impact Assessment Tool, http://www.gs1.org/epcglobal/pia/, accessed on 01.07.2013

[Hoogeweegen, 1997] Hoogeweegen M. (1997), Modular Network Design: assessing the impact of EDI, Phd. Thesis, Erasmus University, Rotterdam, the Netherlands.

[IoT Forum, 2013] Website of the IoT Forum: http://www.iot-forum.eu/forum, accessed on 01.07.2013

[Ippisch, 2009] Ippisch, T; Bereuter, A.; Thiesse, F. (2009), Deliverable 2.5 - Business case framework with a special focus on small and medium sized enterprises. EU Project “Stop Tampering of Products”.

[Kranzfelder, et al. 2001] Kranzfelder, M.; Zywitza, D.; Jell, T.; Schneider, A.; Gillen, S.; Friess, H. Feussner, H. (2001): *Real-Time Monitoring for Detection of Retained Surgical Sponages and Team Motion in the Surgical Operation Room Using RFID Technology: A Preclincial Evaluation*. In: Journal of Surgucal Research, S. 1-8.

[Li, 2009] Li, L.; Ambani, S.; Ni, J. (2009): Plant-level maintenance decision support system for throughput improvement. International Journal of Production Research Vol. 47, No. 24, 7047-7061.

[Magerkurth, 2012] Carsten Magerkurth (ed.), “Deliverable D1.4 – Converged architectural reference model for the IoT v2.0”, http://www.iot-a.eu/public/publicdocuments/documents-1/1/1/D1.4/at_download/file, 2012

[Magerkurth, 2013] Carsten Magerkurth (ed.), “Deliverable D6.3 – Final Requirements List”, http://www.iot-a.eu/public/public-documents/d6.3/at_download/file, 2013

[Miles, 1992] Miles R.E, Snow, C.C. (1992), Causes of Failure in Network Organizations, *California Management Review*, summer, 1992, pp.53-72.

[MUWS, 2013] MUNICH Platform Workshop - Personal interviews with attendees. 28 Jan. 2013

[ÖDI, 2013] ÖDI: *Tarifvertrag für den Öffentlichen Dienst der Länder.* In: http://oeffentlicher-dienst.info/tv-l/west/ accessed on 01.06.2013

[Porter, 1985] M. Porter, Competitive Strategy: Techniques for Analyzing Industries and Competitors, Free Press, New York, 1980; and Competitive Advantage: Creating and Sustaining Superior Performance, Free Press, New York, 1985.

[Porter, 2004] Porter, M.E.; Teisberg, E.O. (2004), Redefining Health Care. Boston, MA: Harvard Business School Press.

[Rotondi, 2011] D. Rotondi et al., “D1.2 – Architecture requirements, assumptions and threats”, IoT@Work, 2011.

[Salinas Segura, 2011] IoT-A Project Deliverable IR6.1 - Initial validation on reference model, 2011.

[Salinas Segura, 2012] IoT-A Project Deliverable IR6.2 – Second validation report, 2012.

[Schmidt, 2003] Schmidt, M.J. (2003), What’s a Business Case? And Other Frequently Asked Questions. A Solution Matrix White Paper.

[Spengler, 2004] Spengler, H. (2004): Kompensatorische Lohndifferenziale und der Wert eines statistischen Lebens in Deutschland. *ZAF*, pp. 269-305.

[Spiegel, 2013] Spiegel: *Operationsfehler: Klink muss 2.8 mil € zahlen*. In: http://www.spiegel.de/panorama/justiz/operationsfehler-klinik-muss-2-8-millionen-euro-zahlen-a-815788.html accessed on 20.05.2013

[Oetzel, 2012] Oetzel, M. C., and S. Spiekermann, "Privacy-by-Design through systematic Privacy Impact Assessment – a design science approach", European Conference on Information Systems (ECIS) 2012, Barcelona, Spain, ECIS.

[TOOL0, 2013] TOOL0: *CSSE*. In: http://csse.usc.edu/tools/COCOMOII.php accessed on 01.05.2013.

[Valerdi, 2005] Valerdi, R. (2005): The constructive Systems engineering cost Model (COSYSMO). University of Southern California, California.

[van Eck et al., 2007] Van Eck, E.; Vervest, P. (2007), Smart Business Networks: How the Network Wins, Vol. 9, No. 6, Communications of the ACM.

[Walewski, 2011] Joachim W. Walewski (ed.), “Deliverable D1.2 – Initial architectural reference model for the IoT - v0.9”, http://www.iot-a.eu/public/public-documents/d1.2/at_download/file, 2011

[Weier, 2013] Weier, H. M. *Software Maintenance Fees*: *Time For This Model to Change*. In: http://www.informationweek.com/software/enterprise-applications/software-maintenance-fees-time-for-this/212902014?pgno=3 accessed on 29.04.2013

[Wilson et al., 2005] Wilson, R.M.S.; Gilligan, C., “Strategic Marketing Management: Planning, Implementation & Control“, 2005.

[Zocher, 2013] Zocher, W.: *RFID in OP*. In: https://www.youtube.com/watch?v=8PK-jpds2qk&feature=youtu.be accessed on 25.05.2013.

Annex

A.1 Meeting agenda of the expert workshop with G. Muller

Time	Topic	Caretaker	Comments
9:30	Earliest arrival. Ask for Andreas Nettsträter at the entrance.	Andreas Nettsträter	
10:00	Welcome by host (IML); logistics	Andreas Nettsträter	
10:05	Welcome by Validation Task Force; review of agenda	Joachim W. Walewski	
10:15	Introduction of participants	All	Everyone briefly introduces himself.
10:30	Architecture vision and goal of IoT-A	Martin Bauer	Presentation; brief introduction to IoT-A's architecture work and what is in D1.4/D1.5
11:00	Discussion	All	
11:10	Pre-ordering lunch	All	
11:20	Semantics and ontology: reference architecture v. meta architecture	Joachim W. Walewski	Presentation; short discussion of the very broad scope of IoT-A and why I think this is the source of many of our methodology and guidelines issues.
11:30	Discussion	All	
11:35	Hyper-methodology for hyper-models: our quest for reference-architecture and reference-model methodologies	Joachim W. Walewski	Opening presentation for question one (out of two): what are (recognised) methodologies for generating reference models and reference architectures (taxonomy, rating,…) or parts thereof?
11:50	Discussion	All	
~12:40	Lunch	All	
13:40	Requirements in IoT-A	Joachim W. Walewski	Presentation; brief overview of our requirements process and the requirements we've collected.
14:00	Discussion	All	One important quality goal within an architecture process is requirements traceability, viz. whether all requirements are covered by the architecture, and whether the bits and pieces of it (e.g., functional components and their behaviour) can be traced back to requirements. Is there anything similar to requirements traceability in a

			reference-architecture process? How to ensure traceability of requirements when translating our hyper models into concrete architectures. Does this even make sense? What are recognised methods for so doing?
14:30	How to use the IoT Architectural Reference Model?	Joachim W. Walewski	Outline of Section 5 of D1.5 (guidelines). Our thoughts behind each section.
15:00	Discussion	All	Is there any recognised methodology of how to devise usage guidelines for an architectural reference model? Any hints on how to best devise the subsections of our guidelines section (reference manuals, illustrations, interactions, process)?
16:00	Wrap up	All	
16:30	End of meeting		Itineraries permitting: brief tour of the IML test beds.

A.2 Technical Questionnaire

Dear SW4 Participant,

thank you for taking part in the Stakeholder Workshop 4, which is conducted in the context of the European research project Internet of Things-Architecture (IoT-A). For receiving feedback on the technical session of IoT-A WP6, we would kindly ask you to participate in this survey. The survey is expected to take 10 minutes.

Thank you very much,

your IoT-A team

What is your age?

○ younger than 20 ○ 20-29 ○ 30-39 ○ 40-49 ○ 50-59 ○ older than 60

What is your highest education level?

○ High School Degree
○ Professional Degree
○ University Degree

What is your main subject of work?

○ Business Management, Management, Economy
○ Computer Science
○ Information Management
○ Other

Are you familiar with UML class diagrams?

○ Yes
○ No

In which IoT-A Stakeholder Workshops did you participate so far?

☐ SW1
☐ SW2
☐ SW3

What do you think about the domain model?

	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
I think it is important having a domain model as one part of the IoT-A reference model.	○	○	○	○	○

1

I could easily understand the terminology used in the domain model.	○	○	○	○	○
I think the domain model contains all concepts needed to cover the IoT domain.	○	○	○	○	○
The terms and descriptions of the domain are clear to me.	○	○	○	○	○
The relations of the concepts in the UML model are located where I expect them to be.	○	○	○	○	○

Please indicate whether you miss any concept in the domain model.

Please indicate whether you disagree with any concept in the domain model.

Please indicate whether you disagree with any of the relations in the domain model.

What do you think about the application of the domain model?

Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree

I think, the IoT domain model is easy to use from a user perspective.	○	○	○	○	○
I am confident to apply the domain model myself to my dedicated domain.	○	○	○	○	○
I prefer to have an user manual to learn how to use the domain model.	○	○	○	○	○
My dedicated working domain does not benefit from the domain model.	○	○	○	○	○
It was easy for me to create a typical scene of my working domain.	○	○	○	○	○

Please indicate whether you had any difficulties of applying the domain model to your domain.

What do you think about the technical validation session at SW4?

	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
I liked the introduction to the domain model.	○	○	○	○	○
The graphical information was intuitively understandable for me.	○	○	○	○	○
The demonstrated mapping between the scene and the domain model was understandable for me.	○	○	○	○	○
I felt well prepared for the session.	○	○	○	○	○

Acknowledgements

We owe special thanks to Prof. Gerrit Muller who took the time to get involved with the project content and could provide us valuable input. Further we want to thank Christoph Thuemmler who was one of the key people within the stakeholder group from the beginning of the project. Last but not least we also want to thank Djordje Djokic who not only attended to stakeholder workshops but also actively supported us in various activities related to privacy.