[Scandinavian Journal of Information Systems](http://aisel.aisnet.org/sjis)

Volume 24 | Issue 1 Article 1

August 2012

Designing Controllable Accountabilities of Future Internet of Things Applications

Daniel Boos
ETH Zurich, Switzerland, dboos@alumni.ethz.ch

Gudela Grote
ETH Zurich, Switzerland, ggrote@ethz.ch

Designing Controllable Accountabilities of Future Internet of Things Applications

Cover Page Footnote

This research was funded by the ETH Research Grant TH -31/06-1. We would like to thank the EU funded project SToP (Stop tampering of products) for sharing of insights. We also thank Mikko Lehtonen, Katharina Kinder-Kurlanda, Johann Weichbrodt, Dominic Duckett and the editor Samuli Pekkola for their comments and support.

Designing Controllable Accountability of Future Internet of Things Applications

Daniel Boos & Gudela Grote
ETH Zurich, Switzerland
dboos@alumni.ethz.ch & ggrote@ethz.ch

Abstract. Within work environments, the emergence of Internet of Things applications creates radically new scenarios of use involving the enrichment of everyday objects with seamlessly integrated communication, sensing and computing capabilities and their integration into information systems. These changes can profoundly alter transparency of work processes, prescribe and prohibit actions, and change stakeholders' overall accountability and control capabilities. Actors' difficulties in meeting changed accountabilities due to an Internet of Things application may trigger severe disturbances in organizations. What actors are in control of and what they are held accountable for is partially prescribed by designers and involved stakeholders in the early stages of technology development. Therefore, this paper presents an approach for prospectively designing controllable accountabilities into envisaged Internet of Things applications. Three dimensions of accountability will be distinguished: visibility, responsibility and liability. Each dimension affects control requirements differently. The narrative network approach has been adopted to study envisioned organizational work processes along with the involved actors and their accountabilities and control capabilities. A description of how the approach can be used to prospectively align accountabilities and control capabilities is provided based on a case study of an Internet of Things application in product authentication. Advantages and limitations of the approach are discussed.

Key words: Designing for accountability, accountability, responsibility, liability, narrative network, organisational issues, Internet of Things technologies, information system

1 Introduction

Research on the use of information systems (IS) has shown the importance of managing the link between accountability and new information and communication technologies (ICT) (Button

Accepting editor: Samuli Pekkola

and Dourish 1996; Eriksén 2002; Lilley 1996; Kallinikos 2004; Munro and Mouritsen 1996; Suchman 2006; Yakel 2001; Winthereik et al. 2007). In the work environment, the use of Internet of Things (IoT) applications can create radically new scenarios of accountability leading to improvement in an actor's accountability, but also to disturbances in organizations or society (Boos et al. 2008; Hildebrandt 2008; Kinder 2008). Generally accountability is understood as a binary relationship between actors where one is accountable towards the other (Neyland and Woolgar 2002). In this paper accountability is defined as a relationship between actors comprising the dimensions visibility, responsibility and liability.

Several ways in which accountabilities are changed through ICT, especially IS, have already been identified in the literature (Hildebrandt 2008; Grote 2009; Kallinikos 2004; Munro and Mouritsen 1996; Newman and Westrup 2005; Neyland 2007; Suchman 2006; Yakel 2001). Firstly, studies have shown that changes in transparency and visibility caused by the use of ICT have significant consequences for an actor's accountabilities (Kallinikos 2004; Newman and Westrup 2005; Neyland 2007). Their actions can become accountable in new or changed ways because they can be attributed more clearly to individual actors, become visible to different actors (such as a distant supervisor), and can be looked at retrospectively through collected records (Newman and Westrup 2005). Secondly, ICT systems that rigidly prescribe work processes, reporting procedures and capabilities or those that are closely integrated into larger socio-technical systems, can create particular conflicts. They may compromise the ability to cope with local contingencies at particular workplaces, impair control accountabilities or respond poorly to accountabilities involving other local actors (Munro and Mouritsen 1996; Suchman 2006; Volkoff et al. 2007; Yakel 2001). Thirdly, depending on the model of supervisory control, increased automation leads to changes in accountabilities because an actor might lose the ability to appropriately control the system (Bainbridge 1983; Grote 2009) or because decisions are offloaded to the automated system (Anderson et al. 2003; Cummings 2006; Hildebrandt 2008).

Many studies on accountability and technology focus retrospectively at accountability changes in fully operational or partly deployed ICT systems providing a critique or recommendations on resolving operational problems deriving from misaligned or conflicting accountabilities (see Bowers et al. 1995; Winthereik et al. 2007; Yakel 2001). However, how a new system achieves accountability and to whom accountability is assigned is partially inscribed and prescribed by designers and involved stakeholders during the process of system development or configuration (Lilley 1996; Kortuem et al. 2007; Volkoff et al. 2007) and might become entrenched. While the enactment of a technology in practice might differ from a designer's intention, the user's freedom in enacting a technology is not indefinitely malleable and can be reduced by increasingly networked and distributed technologies (Orlikowski 2000). Therefore to avoid unintended consequences for organizations due to misaligned or conflicting accountabilities, prospective approaches to address accountabilities during the early stage of development supporting designers and project participants are a key issue.

In this paper, an approach for designing controllable accountabilities along an organizational work process in an early stage of technology development is presented. The approach allows a prospective analysis about future uses of a technology in a socio-technical system, satisfying the call for more prospective and prescriptive research into the use and acceptance of ubiquitous computing technologies (Lyytinen and Yoo 2002).

This paper focuses on emerging information and communication technologies projected to be widely used within the next five to ten years, currently only existing as prototypes or future visions. IoT applications are examples of such a novel technology. Research in the IoT is still mainly technology driven aiming at building potential prototypes and evaluating them in restricted field trials. IoT applications are highly distributed and networked computing technologies. They consist of everyday objects that are enriched with communication, sensing and computing capabilities (e.g., Radio Frequency Identification RFID chips) (Bullinger and ten Hompel 2007; Fleisch and Mattern 2005; Gershenfeld et al. 2004). Potential application domains include supply chain management, health and safety management, retailing and environmental monitoring (see Sundmaeker et al. 2010). IoT applications will make the flow of products along the value chain more accurate, transparent and visible in real time because information is updated automatically in IS (Fleisch and Tellkamp 2006; Bose et al. 2009). Also, media breaks, like transferring data from paper documents into IS, are eliminated and manual errors are reduced (Fleisch 2010). While emphasis is put on identifying business benefits, except for privacy, deterrents for the deployment of RFID and Internet of Things applications are less well researched (Kapoor et al. 2009). In particular, technology assessment studies point to the fact that IoT applications will change accountabilities, through increased transparency, the embeddedness into everyday objects and interconnectivity (Fleisch 2004; Hilty et al. 2004; Hildebrandt 2008; Koops et al. 2009; Meister et al. 2008).

This paper is structured as follow: It begins with a brief overview of existing approaches to designing for accountability. It proceeds to give an introduction of the concept of controllable accountabilities. This is followed by a description of the narrative network approach. After explaining the research setting, there is a description of a novel design approach illustrated with insights from an IoT application for product authentication. Finally, a discussion considers the contribution of this new approach to practice, existing design approaches and accountability changes due to IoT applications.

2 Approaches to designing for accountability

Ways for dealing with accountability in the design of IS can be separated into three approaches (see Table 1).

Interactive accountability approaches are present in the field of human computer interaction (HCI). The focus is on interactions and accountability. Under the term technomethodology (Button and Dourish 1996; Crabtree 2004), ethnomethodology is used to guide the design of interactions with or through IS. Interactions with computer systems should be designed in such a way so that the actions are observable and reportable in the situation of use (Dourish 2004). Belotti and Edwards (2001) address accountability and intelligibility in the design of ubiquitous computing systems, especially in the case of context-aware systems. McCarthy et al. (1997) have advanced the studies of interactive accountability approaches and technology with a framework for studying the relationship between accountability and work activities including the organizational context. Cummings (2006) addresses accountability during design to avoid a degradation of accountability due to automation.

Approach	*Description*	*Accountable actors*	*Core proposals*	*References*
Interactive accountability approach	Accountability as pervasive feature of everyday interactions.	Human User Computer	Importance of intelligible interactions and situation of use.	Belotti and Edwards (2001) Cummings (2006) Crabtree (2004) Dourish (2004) McCarthy et al. (1997)
Regulatory accountability approach	Accountability based on a system of assessments and to distribute competences (e.g. for compliance, finance, monitoring or auditing purposes)	Human User Organization	Design locally meaningful accountabilities.	Dechow et al. (2007) Hildebrandt (2008) Suchman (2006) Willmot and Bliss (1996) Winthereik et al. (2007) Yakel (2001)
Participatory accountability approach	Accountability of socio-technical system, which includes the development of new technologies and their implementation. Accountability for system provided.	- Stakeholder (e.g. human user, designer, system provider, organizations, society)	Increase participation of stakeholder and outline accountabilities of stakeholders.	Bodker et al. (2004) Grote (2009) Mumford (1996) Suchman (2002;2006)

Table 1: Approaches for designing accountability

Regulatory accountability approaches emphasize organizational and regulatory aspects of accountability and how ICT technologies can be used to support accountabilities. By introducing new IS, business processes are changed to enable new accounting or auditing practices (Davenport 1998; Lilley 1996; Willmot and Wray-Bliss 1996), ordering work systems (Suchman 2006), to increase management control (Dechow et al. 2007), to standardize procedures (Kallinikos 2004), to change responsibilities and roles (Volkoff et al. 2007), to integrate and automate coordination and control responsibilities in IS (Zammuto et al. 2007) or to enforce compliance of laws through technology (Hildebrandt 2008). Studies on regulatory accountability retrospectively analyse how IS influences organizational forms post deployment (Winthereik et al. 2007; Yakel 2001). These studies offer recommendations for the deployment of similar IS. For example IS ought to be meaningful locally, meaning that performance indicators should be known to local users; users should be able to influence interpretations of collected information; users should not be ”locked up“ in technology-enforced standard operation procedures; and users may benefit from the ability to generate data for their own interests rather than just producing reports for external bodies. In addition accountabilities must become part of organizational practices without conflicting with each other (see Winthereik et al. 2007; Yakel 2001).

Participatory accountability approaches look at accountability in a socio-technical system emphasizing the accountability of those involved in developing new technologies or those providing technologies for socio-technical systems. Different design strategies have been promoted to improve the accountability of the design process and the involved stakeholders (see Bodker et al. 2004; Mumford 1996). Participatory approaches involve users in the design process to improve the usefulness and acceptance of a new technology. Suchman (2002) explicitly addresses accountability of design practices. She calls for designers to make themselves more accountable towards the use of their technology at a particular site-of-use and to engage members of this specific site-of-use as collaborators in projects of technology production. Grote (2009) advocates increasing the accountability of the systems' designer or providers for their automated systems and relieving human operators from accountabilities over which they have no control. Rebalancing accountability towards the system designer or the organization operating the system would force them to address issues of accountability and improve the controllability of the system by a human operator.

3 A concept for controllable accountabilities

3.1 A multidimensional concept of accountabilities

Based on the aforementioned design approaches for accountabilities and research findings on accountability and technology, we have developed a multi-dimensional concept of accountability and its alignment with the actors' control capabilities (Boos 2011; Boos et al. 2012). Of particular importance for IoT applications are the dimensions visibility, responsibility and liability. For the reasons given above, these need to be anticipated during the early stage of a technology development project. The dimensions of accountability are about the role of the human actor as part of an organization. The dimensions allow us to analyse how and for what an actor is accountable and therefore improve the visibility of accountabilities along organizational work processes and in socio-technical systems.

The particular understanding of *visibility* is derived from studies and design approaches for interactive accountability (Belotti and Edwards 2001; Dourish 2004). A demand for visibility is made towards actors by asking them to provide an account of an activity allowing subsequent actors to perform their activities. Actions or reports on actions can satisfy visibility if they are transparent and intelligible for other actors in their respective situation-of-use. As with IS in general, IoT applications informate and make certain aspects of work processes visible and available for analysis by a larger audience (Zammuto et al. 2007). The capacity of IoT applications to automatically and wirelessly capture data through RFID chips and sensors changes the kind and amount of data used for visibility.

Responsibility addresses the distribution of competences and obligations of different actors to fulfil their duties. Responsibilities outline actors' accountabilities for specific elements of a joint task between interdependent parties (Okhuysen and Beckhy 2009). Responsibilities might stem from formal or informal rules, compliance with standards or procedures, professional norms or from the organizational work process. IoT applications influence responsibility in various important respects; they can create new responsibilities, which may be rigidly prescribed and they can assume some of the existing responsibilities or enable the monitoring and controlling of responsibilities.

Liability addresses an actor's legal responsibility towards laws, regulations or contracts. Actors risk facing severe consequences for failing to fulfill liability demands based on formal rules, such as governmental regulations, industry standards or health and safety laws. An IoT application might influence liability by providing proof, either in the form of information used for investigating a failure or as evidence of compliance to a law, procedures, regulations or contracts (Kinder 2009).

Beside the individual dimensions, multiple accountabilities, which mean that an actor might be accountable to more than one actor at the same time, are common organisations. Actors explicitly use technology to make their activities accountable to multiple actors simultaneously (Suchman 1993). Multiple accountabilities can conflict and are therefore regarded as important sources of disturbances in organizations (Bowers et al. 1995; McCarthy et al. 1997; Suchman 2006; Yakel 2001). Accountabilities might conflict because they are contradictory or mutually exclusive (Bowers et al. 1995; Orr 1996).

3.2 Actor control to satisfy accountabilities

The core design proposition is that actors should be able to satisfy accountability demands made upon them. Firstly, misalignments between accountabilities and control capabilities cause disturbances in organizations (Boos et al. 2012). Secondly, actors should not be held accountable for actions over which they have no control (Grote 2009; Merchant and Otley 2007). To assess whether an actor can satisfy accountability demands, we compare actors' accountabilities to their control capabilities. Control is understood as the actor's ability to influence conditions and processes in relation to the expected outcome for the actor (Grote 1997). Prerequisites for control are transparency, predictability and sufficient influence over processes or outcomes in a socio-technical system. Transparency and predictability address the actor's understanding of the functioning of a socio-technical system. For accountability, transparency means that actors needs to know their accountabilities. Predictability means that the actors know how their actions would contribute to satisfying their accountabilities. Influence addresses the issue of having the appropriate means, like tools, resources and time, and enough decision authority to achieve an intended outcome.

IoT applications might enable or constrain future actors accountabilities and control capabilities (Hildebrandt 2008; Kinder 2008; Spiekerman 2008). New accountabilities might be assigned to an actor. Existing accountabilities might be changed, like for example standardized. Accountabilities might be shifted between actors. Adding, changing and shifting the accountabilities and control capabilities might lead to misfits between them. Accountabilities and control capabilities therefore may have to be realigned, for a successful use of an IoT application. This, of course, also holds true for other ICT systems. However in case of the IoT, misalignments between accountabilities and control capabilities might be even more difficult to investigate prospectively due to the increased interconnectedness and wide distribution of computer systems, human actors and organizations (Hilty 2004; Hildebrandt 2008; Meister et al. 2008).

The approach provides a tool that explicitly addresses the fit between accountabilities and control capabilities already in the early stage of an IoT development project. The three dimensions of accountability allow us to analyse how and for what an actor is accountable. The approach increases the transparency of possible misfits and the predictability of how design decisions influence future actors' accountabilities and control capabilities. The increased transparency and predictability enables designers and involved stakeholders to make a more informed decision on the design and configuration of the IoT applications and envisioned organizational work processes.

4 Narrative networks to describe envisaged organizational work processes

IoT applications currently exist primarily in research laboratories and as future visions making their real-world observation or study problematic. However, many narratives exist about how IoT applications may be used (see Presser 2011; Sundmaeker et al. 2009). One approach to analyse narratives about future socio-technical systems is the narrative network approach (Pentland and Feldman 2007). The approach was developed to facilitate the study of new ICT systems that are modular, re-combinable, distributed, communicative and have memories. The narrative network approach builds on the theory of organizational routines, which differs from traditional business process redesign approaches by highlighting the difference between the formal description of an organizational work process (e.g., standard operation procedures or work flow descriptions) and its actual performance in practice (Feldman and Pentland 2003), which can be different, for example more complex. Consequently the narrative network approach provides a way to represent a broader range of possible variations of an organizational work process. It provides the means to describe and visualize actors, tools and tasks within an organizational work process.

A narrative network is a collection of narrative fragments combining both actors and functional events. Narrative fragments can include human actors or technological artefacts, which may be interchangeable. Narrative networks are representations of potential and actual narratives in a sequence of actions often containing alternative sequences of actions. These features of narrative networks make them a useful design tool for new organizational work processes or, in the terms of Pentland and Feldman (2008), to 'design routines.' This design capacity is achieved by investigating how technology developers and intended future system users envision the new organizational work process. The focus on organizational work processes is useful because the success of a new ICT system depends neither on the performance of a single interaction nor the construction of an artefact but on the establishment of a new organizational work process (Pentland and Feldman 2008).

The approach allows for the combination of different points of view by collecting narratives from different actors about the planned organizational work process. First, depending on the viewpoint, some actors or functional events are absent from the narratives because they are either not known or regarded as unimportant. Combining different perspectives from different participants therefore allows us to derive a more holistic view. Second, divergent views about the sequence of actions, performance of activities by actors, attribution of responsibilities or goals might be a source of disturbance and lead to a conflict of interests. Finally, most new organizational work processes are designed for an existing socio-technical system, where existing organizational work processes are performed. Therefore, the envisioned organizational work process needs to be aligned with other relevant organizational processes and adapted to common variations in their sequence of action. Designers and stakeholders might prefer only one pathway and no variations in an organizational work process. Variations in the sequence of actions however are a common phenomenon and regarded as an important source of change (Feldman and Pentland 2003). Allowing for variations is important, because actors need flexibilities to cope with uncertainties (Grote 2009). Narrative networks describe different pathways of an organizational work process purposefully taking significant variations into account.

5 Research setting: Case study

A case study approach has been selected as an appropriate vehicle to explore the implications of future IoT scenarios within the early stages of designing technologies. Case studies allow for exploration and development of theoretical approaches (Benbasat et al. 1987). This case study was conducted within an IoT research project concerned with secure authentication of products in supply chains.

From the outset questions of accountability were identified as important. This led to the development of a theoretical conceptualization of accountability (Boos 2011; Boos et al. 2012) which in turn developed into an approach for designing controllable accountabilities in the early stage of technology development. This approach was then applied to identify critical accountabilities and potential solutions. While using the approach we also checked for applicability, based on the evaluation criteria importance, accessibility and suitability (Carlsson et al. 2010). Concerning importance, the approach needed to identify accountabilities and possible misfits between accountabilities and control capabilities in an early stage of technology development. In terms of accessibility, the design approach had to be understandable. Suitability required that the design approach offered guidance for design in case of misalignments. The approach was adapted during the case study because it was found that the instructions on how to resolve misalignments were not specified in sufficient detail. An improvement was made to the design approach with a detailed concept of control and with options to resolve misalignments. There was no evaluation of the narrative network approach or the concept of control, because these approaches have already been extensively evaluated (Grote et al. 2000; Grote 2009; Pentland and Feldman 2007; Pentland and Feldman 2008; Pentland et al. 2007).

A study of real world application trials with developed prototypes was undertaken (see Lehtonen et al. 2009a for additional information on the IoT research project and results on human and organizational issues). The case study was conducted as part of trials in two pharmacies. Different points of view were collected about the envisioned organizational work process and accountabilities by interviewing two developers, two industry partners and ten potential future users, namely two pharmacy supervisors and eight pharmacy assistants. Additional documents provided by the IoT research project describing the application and by the pharmacies, were used to analyse organizational work processes, actor's accountabilities and control capabilities.

6 Designing controllable accountabilities

The design approach addresses the formulation of accountabilities from an organizational perspective. Its intended audiences are researchers, designers and stakeholders involved in the very early stage of technology development projects, when market opportunities, technological possibilities and new usage scenarios for the use of IoT technologies are embryonic.

As an overview, Table 2 outlines the main steps. The first step is the construction of a narrative network. The second step concerns identifying actors and list accountabilities. In step three designing the fit between actor's accountabilities and control capabilities is addressed. A detailed description is given in the subsequent subchapters, including additional explanations followed by an illustration from the case study. The steps are iterative and therefore variations and different pathways do occur depending on the results of each step. To visualize such variations and divergent pathways Table 2, represents this complexity in the form of a narrative network in. In brackets, references are added to the chapters containing its detailed description.

6.1 Envisioning organizational work processes with the narrative network approach

A prerequisite for the design of controllable accountabilities is a narrative network of the envisioned organizational work process. To construct a narrative network prior definition of relevant points of view needs to be established. Of interest are the conceptions of the designers or researchers on the future system, as well as the industry partners or experts with insider knowledge about intended use in the organization, and finally employees potentially using the system in the future. The necessary narrative fragments can be collected via different methods, such as interviews, observation or documents. Process descriptions can be used as a starting point. In subsequent interviews the interviewee is asked to describe step by step the envisaged organizational work process. With the collected narrative fragments a narrative network containing the main variations is constructed.

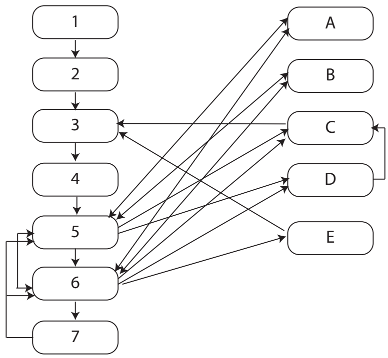
<table>
<tr><th>Design process for designing controllable accountabilities</th><th>Narrative Network</th><th>Variations to design fit between accountabilities and control capabilities</th></tr>
<tr><td>1. Compare current organizational work process with envisioned organizational work process and decide on new envisioned organizational work process (6.1)
2. Identify actors of envisioned organizational work process (6.2.1)
3. Identify stakeholder accountabilities in the envisioned organizational work process (6.2.2)
4. List relevant accountabilities of situation of use and organizational context (6.2.3)
5. Design fit between accountabilities and control capabilities along the envisioned organizational work process (6.3.1)
6. Design fit between accountabilities of newly envisioned organizational work process, situation of use and organizational context (6.3.2)
7. Stakeholder discussion on potential design decisions (6.3.3)</td><td>
</td><td>A. Change accountabilities
B. Increase actors control capabilities
C. Shift accountability to another actor
D. Automate fulfilment of accountabilities
E. Shift fulfilment of accountability to another position in the envisioned organizational work process</td></tr>
</table>

Table 2: Narrative network of designing controllable accountabilities

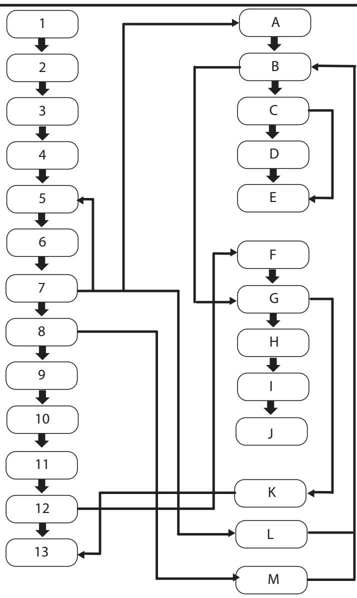
Narrative fragments of work process goods delivery	*Narrative Network*	*Variations*
1. Wholesaler delivers pharmaceutical product to pharmacy 2. Employee takes order receipt 3. Employee types in order number into the system 4. System displays order 5. Employee scans barcode of a delivered pharmaceutical product category 6. System tells employee about ordered amount 7. Employee compares amount available with amount needed 8. Employee manually adds due date for each product and how to store the product into own ERP system 9. Employee fills out order sheet 10. Employee puts order sheet in folder 11. Pharmacist checks the order and the bill 12. Pharmacist looks at the delivered products 13. Employee puts product on general stock or products pre-order by a client to special place for pre-ordered product		Missing product A. Employee sees that not enough products are delivered B. Employee informs pharmacist about issue C. Pharmacist looks at pending orders, to know how important a delivery is D. Pharmacist contacts wholesaler to learn about the delivery date E. Pharmacist issues an order to get the product Too many products F. Pharmacist detects that too many products were ordered G. Pharmacist checks in the system, to learn how many they usually need H. Pharmacist decides to send back some products I. Employee fills out a return shipment form J. Employee sends back the products 13. Additional pathways K. Pharmacist decides to keep product L. Employee sees that too many products are ordered M. Employee sees that the due date is too short

Table 3: Narrative network of the envisioned organizational work process

In a case study based on interviews with researchers, industry partners and future end-users a narrative network was constructed (see Table 3). It shows the actors involved and a number of variations including instances of missing products, too many products and some additional issues. During the real-world application trial, the IoT application developed was part of the organisational work process. The IoT application is based on a software component called Product Verification Infrastructure (PVI) and pharmaceutical goods with unique IDs, based on RFID and 2D barcodes. By scanning the unique ID either through the 2D barcode or the RFID chip a user was able to verify immediately whether a product is genuine.

6.2 Making accountabilities visible

In order to make accountabilities visible the planned organizational work process is first analysed to gather information about intended actors and their accountabilities. Second the envisioned organizational work process is used as a starting point to elicit additional accountabilities and control capabilities.

Identifying actors involved in envisioned organizational work processes

A comprehensive list of actors who will be part of the organizational work process and therefore will have accountabilities is a prerequisite for analysis. Due to the increased interconnectivity of IoT applications, which allows the connection of large numbers of local or distant actors, it can be problematic to know who would be involved in the envisioned organizational work process. However, the narrative networks can be used to get a list of all actors involved. From this the actors in the narrative fragments are identified.

In the case study, the analysis of the different narratives revealed many actors. Table 4 lists both individual actors and organisational entities in the scenario. The table demonstrates how a range of different actors need to be considered and that there are multiple actors involved both in design and future use. The first group consists of primary actors and organizational entities planned to directly use the system. The second group consists of indirectly involved actors, who will either set the standards and rules, design the technical system or otherwise define user access.

Accountabilities in the envisioned organizational work process

Demands of visibility towards an actor performing a functional event can be understood by clarifying which aspects of the previous functional events need to be intelligible for the actor to perform the functional event in question. For example, in the pharmacy's envisioned organizational work process the 'due date' would be automatically checked and added to a stock management system. This functionality requires the 'due date' not only recorded on the package, but also either incorporated in the planned identification technology (e.g. saved on an RFID chip) or made available on an accessible database. Therefore, a new visibility demand is created for the manufacturer who becomes responsible for providing 'due date' information in an accessible way for the new IoT application.

	Actors using the system	*Actors configuring or designing the system (setting of standards, rules and systems)*
Individual	Employee Pharmacist Customer / Patient	Developer
Organizations	Manufacturer Wholesaler Delivery company Up stream supply chain Customs Law enforcement Federal drug testing lab "Counterfeiter"	Standardization body Industrial groups System producer Governmental health agency Governmental regulator Pharmacists' association

Table 4: Actors involved in the envisioned organizational work process

By looking at the envisioned organizational work process, in particular at functional events and who they are assigned to, the analysis reveals the responsibilities of the different actors. For example, the responsibility for checking the pharmaceutical product was assigned to the pharmacy employee by using the PVI system. The PVI's responsibility is to check the genuineness and 'due date' of a product. The PVI system is subsequently responsible for displaying the result of the check to the pharmacy employee. Based on the result, the employee is responsible for the proper handling of the pharmaceutical product. In the new organizational work process, for the PVI system to be able to determine the genuineness of a product based on its delivery path, all previous actors handling the product need to make their activities visible by using the PVI that the product passed at each point in the process. Analysing the delivery path of a product, also understood as 'track and trace data', is one proposed strategy to determine the authenticity of products (Lehtonen et al. 2009b). If detailed 'track and trace data' becomes a prerequisite for the authentication of goods, all actors involved in the supply chain take on a new responsibility; checking the product with the PVI system.

Relevant accountabilities of situation of use and organizational context

Narrative networks alone do not contain information about the context or significance of events for the participating actors nor do they reveal actors' liabilities. To understand liabilities, additional information is needed about the organizational context including legal requirements or regulations influencing the organization of work. Investigating the organizational context also facilitates more information gathering about other relevant visibilities and responsibilities.

To achieve this, the narrative network is used to guide additional information gathering about accountabilities from project participants and intended users. Of notable interest are accountabilities originating from the envisioned organizational work process, organizational context, the work system, other relevant organizational work processes and the circumstances surrounding the situation-of-use.

Situation of use	*Accountabilities of pharmacy employee performing sequence of action*
Back office – incoming goods	• checking if order is correct • checking that product does not have an obvious problem (e.g. damaged package, suspicious package) • controlling and adding due date to in-house stock management system • sorting products according to pre-orders based on prescriptions • guarantee the appropriate storing of a product (temperature, dry) • *New: Verification of pharmaceutical goods with IoT application*
Dispensary – selling goods	• handing out the right products to the right client • providing instructions about the use of a product • providing a safe environment • documenting the sale of pharmaceutical products • *New: Verification of pharmaceutical products with IoT application*

Table 5: Relevant accountabilities during a particular situation of use

In the pharmacy case study the following accountabilities were identified as relevant. The organizational context is a highly regulated environment in which patient safety is paramount. For example there is a legal requirement for a pharmacist to be present in the pharmacy for work supervision and oversight of control activities. The situation-of-use is about where and when the technology should be used and those accountabilities that are of relevance in these particular circumstances. In the pharmacy, two situations-of-use were investigated, namely the back office, where goods are delivered and the dispensary, where products are sold to clients. Table 5 shows how accountabilities differ according to the situation-of-use.

6.3 Designing the fit between accountabilities and actors' control capabilities

Having identified the accountabilities of an actor, the next step is to analyse the fit between accountabilities and an actor's control capabilities. This will inform the process of design and configuration change to the IoT application to eliminate any misfits. The process of fitting accountabilities and control capabilities and changing the envisioned organizational work process can be iterative until a satisfactory solution for all involved stakeholders is found.

Table 6 provides guidance on how designers can influence the fit between accountability and control. For clarification it contains the results after the analysis of the envisioned organizational work process and the context. The table describes how accountabilities change, possible distur-

Accountability Dimension	*Changing accountabilities*	*Possible disturbances*	*Designer influence*
Visibility	Pharmacies might make every product they sell visible to additional actors, such as manufacturers, service providers, regulatory entities etc. The additional actors can use the information for their own activities, such as analysing the time until a product is sold.	Pharmacies lack transparency about who can use information provided by the new system. They are reluctant to make every product sold visible to the manufacturer because they wish to protect their own business data.	• Enabling or restricting intelligibility of account giving. • Automation of account giving and selection of captured data. • Representation of accounts in the system. • Providing or restricting actors' access to collected data. • Providing or restricting influence of an actor on what kind of data he or she uses for account giving.
Responsibility	A pharmacy employee is performing a new customer-facing check for counterfeits of newly delivered products. By doing this he or she responds to a newly introduced responsibility.	Visible checks for counterfeits in front of clients might interfere with other needs of the pharmacy, such as offering a trustworthy environment. Obligatory checks lead to a lack of control and influence because of conflicts between an existing accountability demand and a newly introduced one, which cannot be satisfied in combination.	• Defining functional allocation between IoT application and human actors • Prescribing work-flow. • Definition of monitoring rules. • Redesigning work processes.
Liability	A future regulation requires that every step of a product is tracked and checks are performed in front of the client. Pharmacies become liable for using a technology to check the genuineness of a product.	Emphasis is put on following those aspects that could be used to prove the fulfilment of legal requirements and less emphasis is put on those that are not measured by the system, but would have been relevant to achieving the original goal. For example, a pharmacist overlooks a tampered product deferring to the system detecting that the RFID chip on the package is genuine.	• Defining what can be used to provide proof and where the focus is. • Selection of rules that are integrated and monitored. • Rigidity of rule enforcement.

Table 6: Misfits in Internet of Things application and influence of designers

bances due to mismatches between control capabilities and accountabilities, and the potential influence of a designer to resolve any misfits.

Fit along the envisioned organizational work process

Each accountability originating from the envisioned organizational work process is analysed to determine whether it can be satisfied by an actors' control capability. Basically the prerequisites of control (transparency, predictability and influence) must allow fulfilment of all the actor's accountabilities in the envisioned organizational work process. For transparency, designers can ask if an actor knows to whom the actor is accountable and what for and why. The question is, 'how the IoT application contributes or restrains the actor's need for transparency and if this leads to difficulties in satisfying accountabilities?' For predictability, designers investigate if actors understand how their actions contribute to the fulfilment of their accountabilities. In addition, the actor can only contribute to the organizational work process as required if the actor has the appropriate capability to influence the organizational work process. To have enough influence the actor needs the appropriate resources, such as means, time and capability to act. When insufficient control capabilities lead to difficulties in satisfying an accountability demand, then designers need to address the misfit.

There are several possible ways to address the misfit (see Table 2, right column for an overview). Firstly, designers can reflect whether an actor's accountabilities could be changed so the actor gains the appropriate control capabilities. Secondly, designers can investigate whether the control capability could be changed to enable the actor to fulfil the accountability demand. Designers are advised to reflect on whether increasing transparency or providing additional means to influence the system would satisfy the accountability demand. They need to determine how to change an IoT application to adequately enable the actor's control capabilities. Thirdly, designers can also investigate if an accountability demand could be shifted to another actor. Shifting accountabilities might also lead to a change in the organizational work process. Before shifting accountability to another actor, however, designers need to analyse whether the newly accountable actor has the appropriate control capability to satisfy the reallocated accountability demand. Finally, designers should investigate whether an accountability demand could be taken over by an automated IoT application, but this raises a number of challenges. Automation might decrease actors' control over their accountabilities. The automated fulfilment of accountabilities might be hidden or its functioning unintelligible to relevant actors. Either eventuality might decrease the actor's experience of transparency and predictability. While the actor's control is decreased, automation might raise the control capabilities of those who are involved in system design or configuration. Subsequently new questions arise about the accountability for decisions on automation. In those cases those who can control the automated fulfilment of accountability, such as the system designer and the maintainer, should be held accountable for the proper functioning of automated accountabilities (Grote 2009).

In the pharmacy case, a new responsibility to check products with the PVI was assigned to the pharmacy employees. Difficulties arose through a lack of understanding about whether incidents were managed and reported manually or were handled by the system. Employee ideas ranged from sending a product triggering an incident back to wholesaler, manufacturer or even governmental organizations. To the employees it was neither transparent nor predictable what they had to do following an incident and what the IoT application did for them. The follow-up action after an incident is very important for a successful accomplishment of the organizational work process. As a solution, designers could, for example, increase the transparency of the organizational work process and inform pharmacy employees about the next steps to be taken after an incident. The pharmacy employee would then use the information to raise an alarm or send the product back. Designers could also impose another solution, by integrating automatic system interruption coupled with notification of a designated actor allowed to restart the system. This would amount to both automation, and to the transfer of responsibility either to the supervisor or an external authority. Shifting the responsibility to the supervisor, in this case to the pharmacist, could be an appropriate solution because it also matches the pharmacist's responsibility for the work system. Shifting the responsibility to a distant actor might be more problematic. Because of the distance, the actor might lack significant control capabilities, such as the capacity to intervene and guarantee the safe handling of a suspicious product.

Fit between envisioned organizational work process, situation of use and organizational context

By looking solely at the envisioned organizational work process and each accountability separately, an important source of disturbances in the form of multiple accountabilities is overlooked. To investigate a potential risk of conflicting multiple accountabilities, all accountabilities during an envisaged sequence of actions need to be checked for consistency. It can be helpful to challenge project participants or potential future users with the complete set of accountabilities, which are relevant to various discreet actions making up a larger process. Possible solutions might be found by changing an actor's accountabilities, changing an actor's control capabilities, shifting the accountability to another actor, automating the fulfilment of accountabilities or changing the sequence of action to minimise multiple accountabilities.

In the pharmacy case, one of the misfits between multiple accountabilities and control capabilities was during the operation of the dispensary system where the employee hands over the product to a client. Several employees pointed out this problem. From a security point of view everyone—designers, industry partners and pharmacists—agreed that it would theoretically make sense to check products as they were dispensed. However, any open and visible use of the system at the point of dispensing products was regarded as problematic by pharmacists and pharmacy employees because a check that was visible to the customer might interfere with the client relationship and invoke a trust issue for the pharmacy (see table 5 about responsibilities at the dispensary). Therefore the pharmacists preferred to use such a system for incoming goods or at least to hide its use from the customer. There was anxiety over the real possibility of an alert in front of the customer undermining their reputation as operators of a safe environment in which only genuine products are supplied to the customer. Furthermore, they did not want the responsibility for a problem the customer might have due to a mistake in a preceding work system, for example at the wholesaler. Checking authenticity of incoming goods in the back office was regarded as less problematic by the pharmacists, because they felt more in control should an issue arise. They could avoid the uncertainty of having non-genuine products on their shelves and would be able to avoid unpredictable situations involving customers. This solution to the problem however, demands a trade-off between two conflicting interests; how to guarantee the safe delivery of a pharmaceutical product and the varying interests of stakeholders where authentication needs to be performed. In addition, there seems to be a push by EU governmental regulators to establish authentication checks at the point of dispensing and not during incoming goods receipt (Taylor 2009).

Involving stakeholder in decisions on how to design the fit

Based on the principles of participatory design, all relevant stakeholders should be able to influence the design of the envisioned IoT application and be involved in decisions about which potential solution to use. Also the realization of a proposed solution might be beyond the control of the designer. For example they might lack the influence to decide, where and by whom a certain activity has to be performed. Therefore decisions on how to resolve misfits should also include the stakeholders with decision authority.

Findings were discussed with the participants of the IoT research project within the pharmacy case study was done. The discussion mainly focused on where the verification of goods should be done, namely at dispensing or during receipt of incoming goods. The potential conflict between multiple accountabilities was evident. In line with the research project's aims the findings were used to produce the required deliverables. Therefore the findings on accountabilities were used for the overall trial evaluation, to craft application guidelines and by distributing findings to interested groups.

7 Discussion

In this paper we provide a design approach to reflect prospectively on how to design controllable accountabilities in the early stage of technology development. We have shown its applicability through a case study, where an IoT application was developed.

7.1 Contribution

This paper's major contribution is conceptual in nature, both in terms of defining design objectives and defining a process to reach these objectives. The core design proposition, to align accountabilities with control capabilities, gives guidance for design decisions. The narrative network approach makes it possible to investigate accountabilities in the early stage of technology development. The approach supports stakeholders and designers in deliberating prospectively on the design of controllable accountabilities, which is the papers' more practice directed contribution. The approach gives guidance in the form of options on how to resolve misaligned accountabilities and control capabilities. The clarification and guidance can be tools for preventing misalignments, such as conflicts between multiple accountabilities or the lack of control capabilities to satisfy accountabilities. By making the accountabilities visible, discussions between involved stakeholders are fostered about whether accountability can or should be achieved, who should become accountable and to what end, and how an actor can satisfy the demands of accountability.

Overall the design approach contributes to research on the management of organisational issues during the early stage of technology development. First, the paper shows that decisions made by involved stakeholders and designers during the early stage of technology development influence future accountabilities, including the actors' capability to satisfy them. In this the paper supports existing research arguing that to avoid unintended consequences, accountabilities need to be addressed in the early stage of technology development. Second, it contributes to existing 'design for accountability' approaches. With the distinction of visibility, responsibility and liability, design approaches for accountability can benefit by expanding the current, narrow focus on singular aspects of accountability and by providing precise definitions of the relevant aspects. More specifically in the domain of regulatory accountability approaches, current retrospective study-based recommendations on accountability issues are extended by a novel approach that allows analysts to prospectively look at changing visibilities, responsibilities or liabilities. In addition with the narrative network approach, there is a contribution to the research on design approaches for accountability that integrates an organizational work process perspective. This is important, because, for many envisioned IoT applications, a process oriented approach is well suited. For example in the domain of supply chain management, the success of an IoT application depends as much on the successful establishment of a new organizational work process as on the artifact (Pentland and Feldman 2008). In the domain of participatory accountability approaches, the contribution is mainly about how different stakeholders points of view on accountabilities can be integrated into the design process. In particular, the narrative network approach supports the selection of the relevant stakeholders and an appreciation of their perspective. These features encourage increased participation of intended users of the technology in the early stage of a technology development.

Moreover, the paper progresses the understanding about how accountabilities change with the introduction of an IoT application. The case study indicates that IoT applications will lead to changing accountabilities of involved actors. As mentioned in the introduction, the manner in which accountabilities are changed through ICTs, namely increased transparency, prescribing actions and changes to actors' control capabilities become even more important and pronounced with IoT technologies. First, for transparency, the increased capacity to informate work processes make previously inaccessible work processes visible to a larger audience even outside the organization and therefore has consequences for an actor's accountability (Newman and Westrup 2005; Zammuto et al. 2007). The use of an IoT application makes activities inside a pharmacy visible to a larger audience, including the wholesaler, manufacturer and law enforcement. Second, the capacity to prescribe organizational work processes more rigidly limits the possibility to cope with local contingencies (see Suchman 2006; Yakel 2001). It allows, for example, the enforcement of a mandatory verification check to be performed in front of the customer. Third, with the capacity to automate parts of the responsibility for safety offloaded to the IoT application (see Cummings 2006), local actors lose some of their abilities to control the system (Grote 2009). Lastly, current research on IoT applications seldom looks closely at organisational issues and even less at the specific organisational issue of accountability (see Bose et al. 2009).

Therefore by investigating accountabilities and control capabilities, the paper contributes to the research on IoT applications and increases the knowledge on organisational issues.

7.2 Limitations and some practical challenges

Focusing on the alignment between accountabilities and control capabilities has some drawbacks and limitations. Several studies identified other reasons why organizations face critical accountability issues when introducing new ICTs (Dillard 2008; Willmott and Wray-Bliss 1996; Yakel 2001). For example, conflicts of interest or goals between actors (Wintherteik et al. 2007) cannot be resolved by just changing an actor's control capability. This paper extends the approach and addresses the issues during the final process step, when stakeholders discuss the ideas proposed by designers on how to resolve accountability issues (see Table 2, step 7). Further research to investigate how to provide systematic guidance to address those is needed.

This illustrative case study critically considered integrating a new organizational work process based on an IoT application into an existing organizational work process. This works well for many currently envisioned applications of IoT technologies focusing on additional services as a first step towards a wider distribution and use of IoT technologies. However, other application scenarios might aim at a complete replacement of an existing organizational work process with an IoT application. This paper's approach stopped short of such cases. In the case of redesigning or replacing an organizational work process, a user of the approach would additionally need to analyse how changing the sequence of actions of the functional events leads to accountabilities being shifted between actors.

With the focus on organizational work processes, organizational aspects are emphasized more then local contingencies of individual actors. The approach emphasizes a process-oriented view of work and only partially addresses the local situation of use of an actor. Further development of the approach could treat the organizational work process view and an individual actors' view more equally.

While using the approach, some practical challenges were also encountered. A main challenge was to identify and agree on the usage scenario and organizational work process. Usage scenarios might not be at all clear in the beginning of the development of an IoT application or might change over time. This approach recommends agreeing as early as possible with the project participants and relevant stakeholders on a potential usage scenario and a prototype. Only then it is possible to start with the identification of accountability issues. Another practical challenge encountered, is the definition of the boundaries of the investigation in accountabilities. This is especially difficult, because of the networked and distributed nature of IoT technologies. We recommend looking at the purpose of the IoT application for defining the boundaries. In the study, the purpose was to identify suspicious products before they were given to a customer.

A final limitation of the approach relates to the case study and the applicability check. The approach was evaluated in one early stage IoT research project. The first author participated in the project and discussed the topic with project members. The insights on the applicability have to be seen within this context. Notwithstanding the approach supported some design decisions and contributed to the deliverables in the early stage of an IoT research project. Therefore the approach meets the three evaluation criteria 'importance', as it addresses a real world problem in a timely manner, 'accessibility' because it was understandable for the users of the approach and 'suitability' measured by its success in providing concrete guidance and recommendations for at least one IoT research project (Lehtonen et al. 2009a). However to improve the applicability, further use of the design approach is needed. In addition more longitudinal studies could foster the understanding how early stage design decisions can prevent disturbances due to misalignments of accountabilities and control capabilities in the long run.

7.3 Conclusion

The increasing demand for accountability is part of a larger societal trend (Strathern 2000). IoT applications are expected to increase transparency and to support answering demands for accountability. Demands for accountability are also made towards designers and involved stakeholders about the future use of their products and services. A reason given for making them accountable for their products and services is their influence on the design of an IoT application. However, to satisfy their accountabilities, designers and stakeholders need design approaches allowing a prospective analysis of potential issues. With the design approach in this paper, designers and involved stakeholders can treat accountability issues systematically. This moves accountability issues more to the centre of attention helping to avoid later challenges once IoT technologies are deployed in organizations.

8 Acknowledgments

This research was funded by the ETH Research Grant TH -31/06-1. We would like to thank the EU funded project SToP (Stop tampering of products) for sharing of insights. We also thank Mikko Lehtonen, Katharina Kinder-Kurlanda, Johann Weichbrodt, Dominic Duckett and the editor Samuli Pekkola for their comments and support.

9 References

Anderson, S., Hartswood, M., Procter, R., Rouncefield, M., Slack, R., Soutter, J., and Voss, A., (2003). Making autonomic computing systems accountable: The problem of human-computer. *DEXA '03: Proceedings of the 14th International Workshop on Database and Expert Systems Applications*, IEEE Computer Society, Washington DC, USA.

Bainbridge, L., (1983). Ironies of automation. *Automatica*, (19:6): 775-779.

Bellotti, V., and Edwards, K., (2001). Intelligibility and accountability: Human considerations in context-aware systems. *Human-Computer Interaction*, (16:2): 193-212.

Benbasat I., Goldstein, D.K., and Mead, M., (1987). The case research strategy in studies of Information Systems. *MIS Quarterly*, (11:3): 369–386.

Bødker, K., Kensing, F., and Simonsen, J., (2004). *Participatory IT design: designing for business and workplace realities*, The MIT Press.

Boos, D., Günter, H., and Grote, G., (2008). Internet of Things—Designing accountability towards an unknown audience?, Paper presented at *24nd EGOS Colloquium*, July 10-12, Amsterdam, Netherlands.

Boos, D., (2011). Accountability and Internet of Things Applications. PhD Thesis, No. 19759, ETH Zurich.

Boos, D., Günter, H., Grote, G., Kinder, K., (2012). Controllable accountabilities: the Internet of Things and its challenges for organisations. *Behavior and Information Technology*. (Online First).

Bose, I., Ngai, E.W.T., Teo, T.S.H., and Spiekerman, S., (2009). Managing RFID projects in organizations. *European Journal of Information Systems*, (18:6): 534-540.

Bowers, J., Button, G., and Sharrock, W., (1995). Workflow From Within and Without: Technology and Cooperative Work on the Print Industry Shopfloor. *Proceedings of the Fourth European Conference on Computer-Supported Cooperative Work*, H. Marmolin, (ed.), Kluwer Academic Publishers, London.

Bullinger H.J., and Ten Hompel, M., (2007). *Internet der Dinge*. VDI Buch.

Button, G., and Dourish, P., (1996). Technomethodology: paradoxes and possibilities. In: *CHI '96: Proceedings of the SIGCHI conference on Human factors in computing systems*, ACM Press, New York, pp. 19-26.

Carlson, S.A., Henningsson, S., Stefan Hrastinski, S., Keller, C., (2010). Socio-Technical IS design science research: developing design theory for IS integration management. *Information Systems and e-Business Management*, (9:1): 109-131.

Crabtree, A., (2004). Taking technomethodology seriously: hybrid change in the ethnomethodology-design relationship. *European Journal of Information Systems*, (13:3): 195-209.

Cummings, M.L., (2006). Automation and Accountability in Decision Support System Interface Design. *Journal of Technology Studies*, (32:1): 23-31.

Davenport, T. H., (1998). Putting the enterprise into the enterprise system. *Harvard Business Review*, (76:4): 121-131.

Dechow, N., Granlund, M., and Mouritsen J., (2007). Management control of complex organisation; relationship between management accounting and information technology. *Handbook of Management Accounting Research*, C.S. Chapman, A.G. Hopwood and M.D. Shields (eds.), Elsevier, Oxford, pp. 625–640.

Dillard, J., (2008). Responding to expanding accountability regimes by re-presenting organizational context. *International Journal of Accounting Information Systems*, (9:1): 21-42.

Dourish, P., (2004). *Where the Action Is: The Foundations of Embodied Interaction*, The MIT Press, Cambridge.

Eriksén, S., (2002). Designing for accountability. *NordiCHI '02: Proceedings of the second Nordic conference on Human-computer interaction*, ACM, New York, pp. 177-186.

Feldman, M. S., and Pentland, B.T., (2003). Reconceptualizing organizational routines as a source of flexibility and change. *Administrative Science Quarterly*, (48:1): 94-118.

Fleisch, E., (2004). Business impact of pervasive technologies: Opportunities and risks. *Human and Ecological Risk Assessment*, (10:5): 817-829.

Fleisch, E., and Mattern, F., (eds.), (2005). Das Internet der Dinge: Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Berlin, Springer.

Fleisch, E., and Tellkamp, C., (2006). The business value of ubiquitous computing technologies. In: *Ubiquitous and Pervasive Computing New Frontiers for Electronic Business*, G. Roussos (ed.), Springer, London.

Fleisch, E., (2010). What is the Internet of Things? An economic perspective. Auto-ID Labs White Paper WP-BIZAPP-053, http://www.autoidlabs.org/uploads/media/AUTOID-LABS-WP-BIZAPP-53.pdf

Gershenfeld, N., Krikorian, R., and Cohen, D., (2004). The Internet of Things. *Scientific American*, (291:October): 76-81.

Grote, G., (1997). Autonomie und Kontrolle, Zürich, VDF Hochschulverlag.

Grote, G., Ryser, C., Wäfler, T., Windischer, A., and Weik, S., (2000). KOMPASS: a method for complementary function allocation in automated work systems. *International Journal of Human-Computer Studies*, (52:2), 267-287.

Grote, G., (2009). *Management of uncertainty: theory and application in the design of systems and organizations*, Springer, London.

Hildebrandt, M., (2008). Ambient intelligence, criminal liability and democracy. *Criminal Law and Philosophy*, (2:2): 163-180.

Hilty, L.M., Som, C. and Koehler, A., (2004). Assessing the Human, Social and Environmental. Risks of Pervasive Computing. *Journal of Human and Ecological Risk Assessment*, (10:5), 853-874.

Kallinikos, J., (2004). Deconstructing information packages: organizational and behavioural implications of erp systems. *Information technology and People*, (17:1): 8-30.

Kapoor G., Zhou W., and Piramuthu S., (2009). Challenges associated with rfid tag implementations in supply chains. *European Journal of Information Systems*, (18:6): 526-533.

Kinder, K., (2008). Ubiquitous computing for industrial workplaces: cultural logics in designing for the 'real world'. IET Conference Publications 2008(CP541): 1C3.

Kinder, K., (2009). Ubiquitous computing in industrial workplaces: cultural logics and theming in use contexts, PhD Thesis, Lancaster University.

Kortuem, G., Alford, D., Ball, L., Busby, J., Davies, N., Efstratiou, C., Finney, J., White, M. and Kinder, K., (2007). Sensor networks or smart artifacts? an exploration of organizational issues of an industrial health and safety monitoring system. *UbiComp 2007: Ubiquitous Computing*, J. Krumm, G. D. Abowd, A. Seneviratne, and T. Strang (eds.), Springer, Berlin, pp. 465-482.

Koops, B-J., Hildebrandt, M., and Jaquet-Chiffelle, D-J., (2009). Bridging the Accountability Gap: Rights for New Entities in the Information Society? ExpressO

Lehtonen, M., Boos, D., Graf von Reischach, F., Magerkurth C., Müller, J., Bogataj, K., Gout, E., Gourmanel, F., Ippisch T., Oertel, N., Dada, A., (2009a). Stop tampering of products, deliverable 1.5, final evaluation of project results according to the requirements identified. SToP, Karlsruhe, available from: http://www.stop- project.eu/Portals%5C1%5CSToP_D15.pdf. [Accessed 7 April 2011]

Lehtonen, M., Michahelles, F., and Fleisch, E., (2009b). How to Detect Cloned Tags in a Reliable Way from Incomplete RFID Traces. In: *2009 IEEE International Conference on RFID*, Orlando, April 27-28, 2009, pp. 57-264.

Lilley, S., (1996). Refining accountabilities: opening the black box of management systems success. In: *Accountability: power, ethos and technologies of managing*, R. Munro and J. Mouritsen, (eds.), Chapman and Hall, London, pp. 118-143.

Lyytinen, K., and Yoo, Y., (2002). Research commentary: The next wave of nomadic computing. *Information Systems Research*, (13:4): 377-388.

McCarthy, J.C., Healey, P.G.T., Wright, P.C., and Harrison, M.D., (1997). Accountability of work activity in high-consequence work systems: human error in context. *International Journal of Human-Computer Studies*, (47:6): 735-766.

Merchant, K.A., and Otley, D.T., (2007). A review of the literature on control and accountability. In: *Handbook of Management Accounting Research*, C. S. Chapman, A. Hopwood, M. D. Shields, (eds.), Elsevier, Oxford, pp. 785–803.

Meister, M., Pias, M., Töpfer, E., and Coulouris, G., (2008). Application Scenarios for Cooperating Objects and their Social, Legal and Ethical Challenges. In: *Adjunct Proceedings of First International Conference on The Internet of Things*, F. Michahelles, (ed.), pp. 92-97.

Mumford, E., (1996). Systems Design: Ethical Tools for Ethical Change. London, Palgrave Macmillan.

Munro, R. and Mouritsen, J. (eds.), (1996). Accountability: Power, Ethos and the Technologies of Managing, Chapman and Hall, London.

Neyland, D., and Woolgar, S., (2002). Accountability in action?: The case of a database purchasing decision. *The British Journal of Sociology*, (53:2): 259-274.

Neyland, D., (2007). Achieving transparency: The visible, invisible and divisible in academic accountability networks. *Organization*, (14:4): 499-516.

Newman, M., and Westrup, C., (2005). Making ERPs work: accountants and the introduction of ERP systems. *European Journal of Information Systems*, (14:3): 258-272.

Okhuysen, G.A., and Bechky, B.A., (2009). 10 coordination in organizations: An integrative perspective. *The Academy of Management Annals*, (3): 463-502.

Orlikowski, W.J., (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science*, (11:4): 404-428.

Orr, J.E., (1996). *Talking About Machines: An Ethnography of a Modern Job*. Cornell University Press.

Pentland, B.T., and Feldman, M.S., (2007). Narrative networks: Patterns of technology and organization. *Organization Science,* (18:5): 781-795.

Pentland, B.T., Haerem, T., Derek, W. and Hillison, D.W., (2007). Using Workflow Data to Explore the Structure of an Organizational Routine. In: *Organizational Routines - Advancing Empirical Research*, M. C. Becker and N. Lazaric, (eds.), Edward Elgar Publishing, London.

Pentland, B.T., and Feldman, M.S., (2008). Designing routines: On the folly of designing artifacts, while hoping for patterns of action. *Information and Organization*, (18:4): 235-250.

Presser, M., (2011). Inspiring the Internet of Things. The Alexandra Institute. http://www.alexandra.dk/uk/services/Publications/Documents/IoT_Comic_Book.pdf

Spiekermann, S., (2008). *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*, Shaker Verlag, Aachen.

Strathern, M., (2000). New accountabilities, Anthropological studies in audit, ethics and the academy. In: *Audit cultures. Anthropological studies in accountability, ethics and the academy,* M. Strathern, (ed.), Routledge, London, pp. 1-18.

Suchman, L., (1993). Technologies of accountability: On lizards and airplanes. In: *Technology in Working Order*, G. Button, (ed.), Routledge, London, pp. 113-126.
Suchman, L., (2002). Located accountabilities in technology production. *Scandinavian Journal of Information Systems*, (14:2): 91-105.
Suchman, L., (2006). *Human-Machine Reconfigurations: Plans and Situated Actions*. Cambridge, Cambridge University Press.
Sundmaeker H., Guillemin P., Friess P., and Woelffle, S., (2010). Vision and Challenges for Realising the Internet of Things. CERP-IoT – Cluster of European Research Projects on the Internet of Things. European Commission - Information Society and Media DG.
Taylor, P., (2009). EU 'could make brand owners liable for fakes', Securing Pharma Website, http://www.securingpharma.com/40/articles/199.php, retrieved 30.5.2010.
Volkoff, O., Strong, D.M., and Elmes, M.B., (2007). Technological embeddedness and organizational change. *Organization Science*, (18:5): 832-848.
Willmott, H., and Wray-Bliss, E., (1996). Process reengineering, information technology and the transformation of accountability: the remaindering of the human resource? In: *Information technology and changes in organisational work*, W. J. Orlikowski, G. Walsham, M. Jones, and J. L. Degross, (eds.), Chapman and Hall, London, pp. 62-88.
Winthereik, B.R., Van der Ploeg, I., and Berg, M., (2007). The electronic patient record as a meaningful audit tool: accountability and autonomy in general practitioner work. *Science Technology Human Values*, (32:1): 6-25.
Yakel, E., (2001). The social construction of accountability: Radiologists and their recordkeeping. *The Information Society*, (17:4): 233-245.
Zammuto, R.F., Griffith, T.L., Majchrzak, A., Dougherty, D.J., and Faraj, S., (2007). Information Technology and the Changing Fabric of Organization. *Organization Science*, (18:5): 749-762.