# The dual effects of the Internet of Things (IoT)
## A systematic review of the benefits and risks of IoT adoption by organizations

Brous, Paul; Janssen, Marijn; Herder, Paulien

**DOI**
10.1016/j.ijinfomgt.2019.05.008

**Publication date**
2019

**Document Version**
Final published version

**Published in**
International Journal of Information Management

**Citation (APA)**
Brous, P., Janssen, M., & Herder, P. (2019). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, *51*, Article 101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008

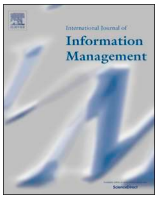
ARTICLE IN PRESS

International Journal of Information Management xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt



# The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations

Paul Brous*, Marijn Janssen, Paulien Herder

*Delft University of Technology, Techniek, Bestuur en Management, Jaffalaan 5, 2628 BX, Delft, the Netherlands*

ARTICLE INFO

*Keywords:*
Internet of things
IoT
Adoption
Big and open linked data
Case study
Asset management
Smart cities
Duality of technology
Structuration theory

ABSTRACT

The Internet of Things (IoT) might yield many benefits for organizations, but like other technology adoptions may also introduce unforeseen risks and requiring substantial organizational transformations. This paper analyzes IoT adoption by organizations, and identifies IoT benefits and risks. A Big, Open, Linked Data (BOLD) categorization of the expected benefits and risks of IoT is made by conducting a comprehensive literature study. In-depth case studies in the field of asset management were then executed to examine the actual experienced, real world benefits and risks. The duality of technology is used as our theoretical lens to understand the interactions between organization and technology. The results confirm the duality that gaining the benefits of IoT in asset management produces unexpected social changes that lead to structural transformation of the organization. IoT can provide organizations with many benefits, after having dealt with unexpected risks and making the necessary organizational changes. There is a need to introduce changes to the organization, processes and systems, to develop capabilities and ensure that IoT fits the organization's purposes.

## 1. Introduction

The "Internet of Things" (IoT), is a growing network of objects that communicate between themselves and other internet-enabled devices over the Internet (Hounsell, Shrestha, Piao, & McDonald, 2009; Ramos, Augusto, & Shapiro, 2008). IoT allows us to monitor and control the physical world remotely (Ramos et al., 2008). As such, adopting IoT may provide a wide variety of benefits for organizations and the resulting big data offers the potential for organizations to obtain valuable insights (Dwivedi et al., 2017; Hashem et al., 2015). However, risks and factors abound which may have significant, unintended effects on organizations and their intention in utilizing IoT (Scarfo, 2014). IoT may become part of the structures which constrain individual actions. For example, adopting IoT for access control to enter public transportation may improve efficiency, but removing the human element of conductors in trains and busses may introduce unexpected risks such as increased incidences of vandalism, requiring new organizational structures to mitigate these risks. Literature mentions different benefits and risks for organizations but there is no analysis synthesizing the duality of these benefits with related risks in a comprehensive overview. There is a need to address the potentially unanticipated impacts of IoT adoption (Ma, Wang, & Chu, 2013; Neisse, Baldini, Steri, & Mahieu, 2016) and to investigate the impact of IoT adoption on organizations in a systematic manner (Haller, Karnouskos, & Schroth, 2009). Little attention has been paid to how IoT adoption may impact organizations either with regards to achieving benefits or mitigating unexpected risks, leading to unintended consequences, which has led to calls for further research in this area (Hsu & Lin, 2018; Lin et al., 2017).

The *objective* of this paper is to analyze the impact of IoT on organizations. Without addressing the negative aspects as well as the positive we cannot fully describe the impact of IoT adoption by organizations. Technology and society are intertwined, and analytical efforts to analyze either as a distinct concept are increasingly being questioned (Boos, Guenter, Grote, & Kinder, 2013). This dual influence has not yet been recognized in studies that attempt to determine whether adoption of IoT has "positive" or "negative" (e.g. risks) effects on organizations. In this paper we address the need for understanding the impact of IoT adoption throughout the organization by taking a structural view and looking at how IoT adoption impacts organizations through a *duality of technology lens* (Orlikowski, 1992). The duality of technology integrates the assumption that IoT adoption introduces forces which result in certain (positive or negative) impacts and that IoT is adopted due to strategic choice and actions (Orlikowski, 1992). In other words, organizations choose to adopt IoT due to the benefits that IoT in general is expected to deliver, however, achieving these end-state benefits may lead to structural changes which are often unexpected. Organizations

---

* Corresponding author.

*E-mail addresses:* p.a.brous@tudelft.nl (P. Brous), M.F.W.H.A.Janssen@tudelft.nl (M. Janssen), P.M.Herder@tudelft.nl (P. Herder).

https://doi.org/10.1016/j.ijinfomgt.2019.05.008
Received 5 September 2018; Received in revised form 12 May 2019; Accepted 12 May 2019

Please cite this article as: Paul Brous, Marijn Janssen and Paulien Herder, International Journal of Information Management, https://doi.org/10.1016/j.ijinfomgt.2019.05.008

often underestimate the impact that IoT adoption has on the organization, and often do not fully understand the organizational conditions and consequences of successfully adopting IoT.

Orlikowski's (1992) concepts allow us to recognize that IoT adoption necessarily has both restricting and enabling implications for organizations. Which implication dominates may depend on a variety of factors, including the autonomy, capability, actions and motives of the actors implementing and using IoT, as well as the organizational context within which IoT is adopted (Orlikowski, 1992). The central research question is motivated by the lack of research on the analysis of IoT adoption in organizations, with specific regards to the limited understanding of the benefits and risks of IoT adoption in organizations, and asks how IoT adoption may impact organizations? We broke the main research question up into four sub-questions, namely:

1 What are the benefits of IoT for organizations?
2 What are the risks of IoT for organizations?
3 What are the organizational conditions of IoT adoption?
4 What are the organizational consequences of IoT adoption?

The methods used to answer the questions and achieve the objective include identifying potential benefits and risks of IoT adoption through a literature review and two case studies were analyzed using the multimethod approach. The cases selected were both located within a single organization, within the context of asset management with regards to large scale, physical infrastructure in the Netherlands. The organization under study is the Directorate General of Public Works and Water Management of the Netherlands, commonly known within The Netherlands as “Rijkswaterstaat” (RWS). RWS is part of the Dutch Ministry of Infrastructure and the Environment and is responsible for managing the major road and water networks within the Netherlands. The results show that in order to achieve the expected benefits, organizations often need to react to unexpected risks which arise during the adoption process by making organizational changes. The Duality of Technology (Orlikowski, 1992) is used as a theoretical lens to determine relationships and reactions during the adoption process. The main contribution of this paper are 1) the identification of potential benefits and risks of IoT, 2) empirically evaluate if the benefits and risks factors identified in the literature also materialize in practice, and 3) to analyze in detail how benefits are realized and risks are faced in different organizational and domain contexts.

The paper reads as follows: the literature review deriving a comprehensive list of benefits and risks is presented in Section 2; the methodology used in this research is described in Section 3. The results of the two case studies are presented in Section 4. The resulting benefits of IoT adoption in the cases are presented followed by the risks. The results of the cases are discussed in Section 5. Finally, conclusions and recommendations for future research are drawn in Section 6.

## 2. Literature review

The literature review method proposed by Webster and Watson (2002) was followed to methodologically analyze and synthesize quality literature. The goal of the literature review is to gain an understanding of the current knowledge base with regards to why and how organizations adopt IoT and what risks organizations may face once the adoption process has begun. This paper utilizes the Duality of Technology theory (Orlikowski, 1992) as a practice lens for studying IoT in organizations. We therefore discuss literature which helps us understand how IoT adoption structures organizations, taking into account research into the adoption and impact of technology on organizations as suggested by research on other disrupting technologies such as Electronic Data Interchange (EDI) and Enterprise Resource Planning (ERP) software. In order to understand the duality of IoT we look at the expected benefits and risks of IoT. Benefits help us understand why organizations choose to adopt IoT whereas understanding the risks involved helps us understand the impact of IoT adoption on the organization.

With regards to adoption of technology, in July 2018 the keywords: “adoption”, “technology” and “organizations” returned 23,391 hits in the databases Scopus, Web of Science, IEEE Explore and JSTOR. Filtering these results for the domains “Technology”, “Policy and Administration” and “Management and Organizational Behavior” returned 3585 hits. We selected 52 articles based on the criteria that the articles contained a theoretical discussion on adoption models of new technologies regarding the structuration of organizations through technology adoption.

With regards to the benefits and risks of IoT adoption, in July 2018 the keywords: (“Internet of Things” OR “IoT”), “benefits”, and “risks” returned 139 hits within the databases Scopus, Web of Science, IEEE explore, and JSTOR. We then filtered these results and performed a forward and backward search and selected fifty relevant articles based on the criteria that they specifically referred to potential benefits or risks with regards to the adoption of IoT in organizations. Following Webster and Watson (2002), we compiled a matrix of concepts into which the literature was grouped (see Table 3). The resulting risks and benefits found in the literature were often perceived benefits and risks and it was not clear if they actually could be found in practice and how the benefits and risks are interrelated. In the literature benefits and risks are often assumed to occur, but there was no systematic account of the evaluation in practice and if they were actually accomplished and for whom.

The following sections are organized as follows: first the adoption of technology in relation to duality of technology theory is discussed in Section 2.1, then the potential benefits of IoT adoption are discussed in Section 2.2 and finally the potential risks carried by adoption of IoT are discussed in Section 2.3.

### 2.1. Adoption of technology in organizations

Duality of technology (Orlikowski, 1992) describes technology as assuming structural properties whilst being the product of human action. As such, technology is created by actors in a social context, and socially constructed by actors by attaching different meanings to it, and thus, technology results from the ongoing interaction of human choices and institutional contexts (Orlikowski, 1992). Orlikowski (1992) explains that previous research studies in the fields of technology and organizations have focused on the views that technology is either an objective, external force that has a deterministic impact on organizational properties such as structure, or that human action is an aspect of technology whereby technology is an outcome of strategic choice and social action. For example, The technology acceptance model (TAM) (Davis, Bagozzi, & Warshaw, 1989) is often used for explaining and technology usage, the belief being that this behavior is influenced by attitude and intention. However, TAM is criticized as being incomplete for considering only part of the attributes of the innovation process (Wu & Wu, 2005) and Legris, Ingham, and Collerette (2003) suggest that it should be integrated into a broader model which includes social change processes. Similarly, (Rogers, 1983) Diffusion of Technology regards technology adoption as being a conscious decision to make “full use of an innovation as the best course of action available” (Rogers, 2010, p. 177), with diffusion being “the process in which an innovation is communicated thorough certain channels over time among the members of a social system” (Rogers, 2010, p. 5). Orlikowski (1992) suggests that both models are incomplete, and proposes a reconceptualization of technology that takes both perspectives into account, proposing a structuration model of technology by exploring the relationship between technology and organizations, based on Giddens., 1976 Giddens (1976),” Theory of Structuration”. Giddens., 1976 Giddens (1976)recognizes that “human actions are both enabled and constrained by structures, yet that these structures are the results of previous actions” (Orlikowski, 1992, p.404). In their structuration model of technology, Orlikowski (1992) identifies four main relationships, namely: 1) technology as a product of human agency, 2) technology as a medium of human agency, 3) organizational conditions of interaction with technology and, 4) organizational consequences of interaction with technology.

According to Orlikowski (1992), understanding technology as continually being socially and physically constructed requires discriminating between human activity which affects technology, and human activity which is affected by technology (López-Muñoz & Escribá-Esteve, 2017). Orlikowski (1992) identifies technology as being the product of human action, while it also assumes structural properties. Furthermore, technology is physically constructed by actors working in a given social context and socially constructed by actors through the different meaning they attach to it. Research in the sociology of technology suggests that the evolution of new applications is a process of social interaction between multiple agents (Allen, 2003; Kabanda & Brown, 2017). According to Orlikowski (1992), agency refers to capability not intentionality, and action taken by actors may have unintended consequences. For example, Mirvis, Sales, and Hackett (1991) suggest that technology can influence the layers of hierarchy in companies, with regards to delegation of responsibilities, or chosen strategy (Buonanno et al., 2005), the suggestion being that technology is an important factor driving organizational behavior (Mendel, Meredith, Schoenbaum, Sherbourne, & Wells, 2008; Subramanian & Nilakanta, 1996). As suggested by Boyne, Gould-Williams, Law, and Walker (2005), the successful usage of technology is dependent on constraints which include: 1) the context within which public organizations operate (Buonanno et al., 2005; Damanpour & Gopalakrishnan, 1998; Damanpour & Schneider, 2006; Quinn & Hall, 1983), 2) the characteristics of the organization (Law & Ngai, 2007; Wejnert, 2002), and 3) the nature of the technology itself (Peansupap & Walker, 2005). According to Orlikowski (1992), technology is interpretively flexible. However interaction of technology and organization is a function of the different actors and the socio-historical contexts implicated in its development and use. For example, (Law & Ngai, 2007) suggest that business processes being a close fit with the defined ERP processes are essential for ERP adoption success.

### 2.2. *Expected benefits of IoT adoption for organizations*

The impact of IoT adoption on organizations is primarily related to the data which IoT generates. IoT having three aspects “Big”, “Open”, and “Linked” (BOLD) (Dwivedi et al., 2017). Firstly, IoT generates large amounts of data which is often of better quality than data generated by traditional means, being: 1) of higher granularity and often greater accuracy; 2) being of greater heterogeneity, coming from a multitude of sources; 3) being more timely than traditional data, often being real or near real-time; and 4) having substantially larger volumes. As such, IoT data is often referred to as “Big” data, having volume, variety and velocity (Kaisler, Armour, Espinosa, & Money, 2013). However, IoT generated Big Data also carries associated risks, often related to the management of the data and to IT infrastructural limitations. Secondly, the open aspect of IoT means that data which is created for one particular use may be used in multiple applications to achieve multiple goals, and reveal previously unforeseen insights. However, this open aspect can also provide challenges related, for example, to security. Thirdly, the linked aspect of IoT allows organizations to combine data from a multitude of sources, combining data from “things” with more traditional data. However, this linked aspect can also provide challenges related, for example, to privacy. In the following sections, the expected benefits of IoT adoption are explored, followed by a discussion of the expected risks of IoT adoption. In this section we discuss the potential organizational benefits of IoT by addressing the three aspects of BOLD. We begin by discussing the improvements and benefits of Big Data generated by IoT, then we discuss potential improvements and benefits of IoT with regards to the open aspect of IoT, and finally we discuss the potential improvements and benefits of IoT with regards to the linked aspect of IoT.

#### 2.2.1. *Benefits related to big data generated by IoT*

An important enabling factor for IoT adoption is the blended integration of several technologies and communications solutions such as identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols, and distributed intelligence for smart objects (Atzori, Iera, & Morabito, 2010), Radio Frequency Identification technology, Electronic Product Code technology, and ZigBee technology (Chen & Jin, 2012). The heterogeneity of IoT means that, for example, many different types of sensors from multiple sources can be used for enabling public safety and compliance to regulations for example, potentially providing control mechanisms that are more effective than traditional methods (Atzori et al., 2010; Boulos & Al-Shorbaji, 2014; Chen & Jin, 2012; Chui, Löffler, & Roberts, 2010; Gubbi, Buyya, Marusic, & Palaniswami, 2013). As such, Big Data analytics can play an important role in enabling smart governance (Meijer & Bolívar, 2016), aiding collaboration between cooperating agencies (Hashem et al., 2016).

Chui et al. (2010) suggest that timely information from networked things improves decision-making, allow for improved analysis with regards to tracking or situational awareness. IoT applications not only enable more efficient data gathering but through automation they also allow capturing new data with higher granularity about processes and work activities. According to Rathore, Ahmad, Paul, and Thikshaja (2016), smart management of the traffic system with the provision of real-time information to the citizen based on the current traffic situation has a major impact on the citizen life and enhances the performance of the Metropolitan authorities. Rathore et al. (2016) also refer to the volumes of data that IoT produces, and reducing the standard error of mean in data analysis and can result in greater trust in the provided results (Barde & Barde, 2012). Kwon, Lee, and Shin (2014) suggest that big data adoption can have a major influence on data quality. As such, the improved timeliness and sheer volumes of data provided by IoT can enhance the performance of organizations, improving operational planning and the ability to react quickly to previously unforeseen events. Furthermore, especially in the asset management domain, IoT is increasingly being used to monitor the health and quality of organizational assets (Kwon, Hodkiewicz, Fan, Shibutani, & Pecht, 2016).

#### 2.2.2. *Benefits related to the openness of IoT*

According to Boos et al. (2013), IoT applications are mainly seen as allowing automation of data capture thereby making manual intervention for data capture unnecessary. IoT provides big data which may be made available for open general use (Hashem et al., 2016). Making data and information available to the public can improve organizational transparency (Castro, 2008), helping improve business processes (Brous, Janssen, & Herder, 2018), and reducing waste. Enabling consumer self-service though IoT can empower citizens and business through better access to information (Boulos & Al-Shorbaji, 2014; Gubbi et al., 2013).

Haller et al. (2009) and Fleisch, Sarma, and Subirana (2006) believe that business value can be derived from IoT by improving real-world visibility, and business process decomposition as IoT enables organizations to monitor what is happening in the real world at real-time, increasing service flexibility and service effectiveness, allowing better decision making, and often leading to new revenue streams (Bi, Da Xu, & Wang, 2014; Haller et al., 2009). Eventually, the capability of IoT to inform and automate can subsequently lead to a transformation of existing business processes (Boos et al., 2013).

#### 2.2.3. *Benefits related to the linked aspect of IoT*

According to Bi et al. (2014) and Fleisch (2010), the linked aspect of IoT can reduce labor costs and empower the public by enabling consumer self-service, such as self-service check-outs in supermarkets. The resulting collated data can then be aggregated leading to insights into product demand, helping supermarkets improve the quality of their selection and improve customer satisfaction. Fleisch (2010) believes that being able to link data from different sources means that IoT can enable fraud detection, reducing fraud related costs and increasing consumer trust. Furthermore, the insights gained by the linking of data from various sources allows organizations to communicate more effectively with their clients, providing new communication opportunities and supporting additional service revenues (Fleisch, 2010).

According to Hashem et al. (2016), effective analysis and utilization of big data are important success factors in many business and service domains. This involves the capacity of IoT technologies to cost effectively collect data about work processes without time consuming physical counts (Boos et al., 2013) so that insights from processed data and analysis can be used to improve efficiency, effectiveness and compliancy.

#### 2.2.4. *Synthesis of potential benefits*

As suggested above, the benefits of IoT technologies for organizations are primarily derived from the availability of more granular information which is automatically collected and readily shareable soon after it is generated (Harrison, 2011; Vesyropoulos & Georgiadis, 2013). By way of example, Harrison (2011) suggests that more granular information can provide better analysis of track and trace information, and can help balance supply and demand. According to Lytras, Mathkour, Abdalla, Yáñez-Márquez, and De Pablos (2014), trust in IoT as a reliable receiver and transmitter of critical information is important for the realization of more advanced business scenarios. Table 1 below summarizes the potential benefits of IoT for organizations.

In short, IoT can deliver a variety of benefits related both to the real-time measurement and analyses of sensor data efficiency of services, improved effectiveness of services, and improved flexibility of services as to trend analysis of historical data over time.

### 2.3. *Risks of IoT adoption for organization*

In this section we discuss possible changes to organizations caused by IoT adoption and the resulting risks that these changes bring about using the three aspects of BOLD.

#### 2.3.1. *Unexpected risks related to big data generated by IoT*

According to a number of researchers, data leaks could severely impact individual privacy by revealing sensitive personal information such as personal habits or personal financial information (Fan, Wang, Zhang, & Lin, 2014; Hossain & Dwivedi, 2014; Hummen, Henze, Catrein, & Wehrle, 2012; Skarmeta, Hernandez-Ramos, & Moreno, 2014). It is therefore important to prevent the unauthorized access and misuse of this information whilst allowing necessary and allowed access to generated data (Skarmeta et al., 2014). As such, whilst Big Data may provide us with the data we need to be able to uncover previously unforeseen insights, the duality of IoT can be found in the changes to organizations that are necessary to be able to convert Big Data into usable information whilst protecting the rights of the individual. Whilst big data is often believed to improve the quality of data, the veracity and velocity of big data may make interpretation more difficult (Wahyudi, Pekkola, & Janssen, 2018).

The duality of IoT also means that changes occurring in staff and organizational processes can in turn lead to further changes to the IT infrastructure as staff become more aware of the possibilities of Big Data and as new requirements become available. According to Dwivedi et al. (2017), there is not one proven or best infrastructure, and data quality is often unclear and needs to be investigated (Wahyudi et al., 2018). As such, unforeseen risks may also include technical issues such as limitations in information technology (IT) infrastructural capabilities (Fan et al., 2014; Hummen et al., 2012; Kranenburg et al., 2014; Prasad et al., 2011; Scarfo, 2014; Wiechert, Thiesse, Michahelles, Schmitt, & Fleisch, 2007; Yazici, 2014; Zeng, Guo, & Cheng, 2011), and data management (Blackstock & Lea, 2012; Gilman & Nordtvedt, 2014; Stephan et al., 2013).

Dealing with these risks often cause unforeseen costs, (Reyes, Li, & Visich, 2012) including reduced return on investment (Brous & Janssen,

**Table 1**
Synthesis of potential benefits of IoT for organizations.

| BOLD aspect | Improvements generated by IoT | Resulting Organizational Benefits |
|---|---|---|
| **Big** | Better data quality: higher granularity of data which is timely and accessible provides more insights for strategic managers | Real-time and accurate insights into strategic threats and opportunities due to improved forecasting and trend analysis |
| | Increased numbers and heterogeneity of data sources allow for predictive maintenance and ability to combine insight into potential service interruption with available staff, allowing organization to better planning with regards to capacity and priority | Improved planning with regards to management and maintenance |
| | Greater volumes of data provide insights into potential operational improvements such as reduction of unnecessary spending or greater potential for flexible capacity leading to reduced operational costs. | Reduction of costs due to insights into operational inefficiencies |
| | More timely data providing real-time information allows organizations to streamline services, reducing unnecessary overhead and improving the ability to react timely to events | Improved speed and efficiency of services due to the provision of real-time information |
| **Open** | Greater availability of data allows managers to better inform their clients | Improved reputation due to better transparency |
| | Increased numbers of data sources and the ability to combine different data provides insight into unexpected activity | More efficient enforcement of regulations |
| | In-time detection of events allows organizations to react more precisely and more accordingly to these events, improving the effectiveness of their services | Improved effectiveness of services due to in-time detection |
| **Linked** | Being able to link data from multiple sources allows improved interaction between client and organization, improving the ability of clients to make their specific needs known and improving the speed with which organizations can react to changing needs and provide bespoke services | Improved reputation due to higher levels of client empowerment |
| | Better oversight reduces the need for overly bureaucratic processes, allowing organizations to streamline policy and regulations. | More efficient regulations due to the ability to monitor activities from a distance |
| | Linking data from multiple sources provides potential for improved interaction with the client and may provide insight into previously unknown needs, leading to new product and service lines and new streams of revenue | New revenue streams due to insights into previously unforeseen product and service lines |
| | The ability to connect more data, of better quality from new sources such as IoT, providing greater insight into (potential) service disruptions, which allows organizations to have greater flexibility in their approach to resolution of service disruption or the generation of new, bespoke services | Improved flexibility of services: broader applications due to linking multiple sources |

**Table 2**
Synthesis of potential risks generated by IoT adoption in organizations.

| BOLD aspect | Unexpected Changes Caused by IoT Adoption | Resulting Organizational Risks |
|---|---|---|
| **Big** | Changes to laws and public opinion means that organizations need to be aware of potential disclosure of individual data which could reveal sensitive information such as personal habits or personal financial information. | Data privacy conflicts resulting in reputational damage and possible legal action. Changes in accuracy of data on which decisions are made. |
| | High development and implementation costs are important impediments to the implementation and application of IoT often results in unforeseen expenditure. | High implementation costs can result in unexpected, added pressure on tight budgets. |
| | Limitations in information technology (IT) infrastructural capabilities and data management with regards to increasing volumes and speeds of data delivery mean that structural changes to the IT infrastructure of organizations are often required. | Difficult interoperability and integration mean that architecture, energy efficiency, security, protocols and quality of service can be affected by IoT adoption. |
| **Open** | Technological and regulatory challenges regarding data sharing and data protection often need to be addressed during IoT adoption. | Data security breaches and data leaks leading to reputational damage, potential loss of intellectual property and lost production. |
| | Sophisticated mechanisms to publish and share things and ways to find and access those things often need to be developed. | The need for solutions for providing fine grained access control need to be developed restricts organizations in their ability to share data responsibly with the right people at the right time. |
| | A lack of standard IoT architectures and missing chains in IoT research and development means that organizations often need to develop their own architectures and technologies which, in turn can impact the market | Conflicting market forces of supply and demand mean that organizations often need to develop their own research and development regarding IoT, often in cases where IoT is not their core business. However, a lack of sufficient knowledge regarding IoT can inhibit this development. |
| **Linked** | Policies and regulations regarding IoT and the linking of data and things often need to be developed. | Lack of sufficient legal frameworks mean that organizations are often exposed to either over-linkage leading to security or privacy issues, or take unnecessary steps to prevent linkage, reducing the level of benefits. |
| | A lack of acceptance of IoT means that organizations often need to develop trust in the new systems. The greater the trust of users in the IoT, the greater their confidence in the system and the more willing they will be to participate. | Lack of trust in IoT means that implemented systems are often not fully exploited resulting in a reduction of benefits. |
| | The heterogeneity traits of the overall IoT system make the design of a unifying framework and the communication protocols a very challenging task, especially with devices with different levels of capabilities. | Linking heterogeneous data from heterogeneous data sources can create data quality issues resulting in misleading information. |

2015a; Brous, Janssen, Schraven, Spiegeler, & Duzgun, 2017). High costs should be considered an important risk to the adoption of IoT (Fan et al., 2014; Harris, Wang, & Wang, 2015; Nam & Pardo, 2014; Qiao & Wang, 2012; Yazici, 2014), as the costs of realizing a fully functional IoT system can be substantial.

### 2.3.2. *Unexpected risks related to the openness of IoT*

As discussed above, an important enabler of IoT is to permit others to access and use the things that have been published publicly on the Internet and many believe that should be possible for users to make use of things that others have shared and to make use of things in their own applications, perhaps in ways unanticipated by the owner of the thing (Blackstock & Lea, 2012). According to Zuiderwijk and Janssen (2014), much of the existing research regarding the “openness” of data has oriented towards data provision. However, the duality of the openness of IoT means that a mature set of mechanisms is required to publish and share things as well as ensure that they are findable and accessible (Blackstock & Lea, 2012). For example, Qian and Che (2012) describe search locality, scalability and real-time processing as strong barriers to IoT implementation. According to Qian and Che (2012), existing searching techniques are based on remote information sharing and often fail to effectively support local search of physical objects.

The duality of continuously monitoring a wide range of things within a variety of situations, means that there are several technological and regulatory challenges that need to be addressed. Often cited technical and regulatory challenges are related to data ownership (Hossain & Dwivedi, 2014), security, and sharing of information (Scarfo, 2014). However, new security issues are increasingly becoming evident (Ortiz, Lazaro, Uriarte, & Carnerero, 2013), and there are few convincing solutions for providing fine grained access control for IoT applications (Brous & Janssen, 2015a; Brous et al., 2017), especially when sensitive data is involved (Fan et al., 2014; Harris et al., 2015; Hummen et al., 2012).

### 2.3.3. *Unexpected risks related to the linked aspect of IoT*

According to Zeng et al. (2011) it is not uncommon for IoT systems to be both directly and indirectly integrated with existing applications, as, for example, RFIDs are often indirectly integrated through a RFID reader and directly integrated through an embedded server. IoT technology can be highly heterogeneous in terms of protocols and capabilities, etc. Whilst we have seen that some researchers argue the benefits of data heterogeneity, the duality is that the heterogeneity at the device level can also be a serious impediment to IoT adoption due to interoperability issues (Shadbolt et al., 2012; Zeng et al., 2011). Furthermore, consumers of data are often also heterogeneous (Brous & Janssen, 2015a; Brous et al., 2017), and different applications might employ different methods of data processing. According to Zeng et al. (2011) the heterogeneity of IoT makes the design of IoT architectures very challenging. This is underlined by Qian and Che (2012) as they determine that searching in IoT requires a methodology of architecture design of search engines as designing an appropriate search engine for IoT is non-trivial. This can mean that although linking IoT data can provide benefits (Brous & Janssen, 2015b), a lack of policies and implementation guidelines can also greatly impede the adoption of IoT (Shadbolt et al., 2012).

Adoption of IoT introduces the need for new skills, staff to provide these skills and new organizational forms and processes (Brous et al., 2018). For example, finding and employing qualified personnel can present enormous challenges due to shortages of skilled staff (Speed & Shingleton, 2012; Yazici, 2014), as well as limited training and educational options (Harris et al., 2015). Many researchers also suggest that a reluctance to change or to learn new technologies can be prevalent in many organizations (Pedro & Jaska, 2007; Reyes et al., 2012; Speed & Shingleton, 2012; Yazici, 2014).

### 2.3.4. *Synthesis of risks*

People must be willing to take part in the system as, according to Kranenburg et al. (2014), successful IoT implementations often depend on people participating and sharing information (Fan et al., 2014; Nam & Pardo, 2014; Zeng et al., 2011). Kranenburg et al. (2014) believe that trust and confidence in IoT and the perceived value that the IoT creates is of great importance. The more trust and confidence users have in the system, the more willing they will be to participate. Conversely, the less trust in the system, the less people will be willing to participate (Brous et al., 2017). As such, the duality of IoT suggests that organizations need to position themselves carefully within this arena (Harris et al., 2015; Stephan et al., 2013; Yazici, 2014) and should consider the role they play in enabling IoT development. For example, trust related conflicting market forces can play substantial roles in the success or failure of IoT (Fan et al., 2014; Misuraca, 2009; Qiao & Wang, 2012; Wiechert et al., 2007). Table 2 below synthesizes the potential risks generated by IoT adoption in organizations.

In short, IoT faces a variety of risks related to the proper use, such as privacy and security, for example, as well as proper management of the data collected by the vast number of interconnected things.

### 2.4. *Organizational conditions of IoT adoption*

Damanpour and Gopalakrishnan (1998) believe that due to the stability of the environments in which they occur, many organizations with low adoption rates have, in the past, tended to have a hierarchical or mechanistic organizational form, meaning that these organizations will adopt innovations infrequently. According to Damanpour and Gopalakrishnan (1998), because of the stable environments surrounding many public organizations, organizational change usually entails modifications to business processes and IT systems, forcing innovations to be incremental and to be designed to reuse existing systems in different configurations rather than to create new ones. Herder, de Joode, Ligtvoet, Schenk, and Taneja (2011) believe that organizations within the public sector need to be predictable and transparent. This may create a hesitation to apply new methods as witnessed by the resistance of asset managers to trust data driven insights. According to Damanpour and Gopalakrishnan (1998), organizational forms that are most effective in adopting innovations include the organic and adhocracy organizational forms (Quinn & Hall, 1983). This demonstrates a more organic structure in which the organization is designed to be a more creative environment with an emphasis on trust. Trust is identified as being critical to acceptance of IoT in organizations (Brous et al., 2017). Psychological resistance to IoT can have a strong negative influence on the acceptance of IoT by asset managers. Asset managers therefore need to be able to trust the system in order to have the confidence to make correct decisions at the right time based on secure and correct data. However, the case studies also show that asset managers often have an inherent distrust of systems over which they have little understanding and control (Backer, Liberman, & Kuehnel, 1986).

Furthermore, research in data governance (Brous, Janssen, & Vilminko-Heikkinen, 2016) has shown that a formalized data governance structure which is a fit with the specific organization, does need to be implemented in order to enable IoT adoption in asset management organizations. This is because automating decision-making often incurs business process related changes which can be found in aligning complex data structures. For example, decision making can be performed at a more strategic, regional level as opposed to at the local, operational level. It is important to ensure that data provenance is well organized so that it is clear where responsibilities and accountabilities lie throughout the data lifecycle (Brous et al., 2017). This may create tension in the organization due to a principle agent problem as suggested by Herder et al. (2011) in which the one who pays is not always the one who decides and is often not the one who benefits from the investment. It is therefore important that data provenance is organized in such a way that inter-departmental teams are aware of the goals behind IoT adoption so that they understand why certain activities need to be performed that may not necessarily have a direct influence on their part of the process. For example, when business processes become automated, people assume new or different roles and people-made decisions are often elevated to more strategical levels. This also often means changes in the organization as people are asked to perform other tasks in changing social and cultural environments and often in changing organizational structures (Damanpour & Schneider, 2006; Mitropoulos & Tatum, 1999; Skogstad & Einarsen, 1999). As such, with regards to organizational related changes brought about by IoT adoption and in agreement with Weber et al. (2009) there is no "one-size-fits-all" approach to data governance.

Environmental characteristics may refer to the sector within which the organization operates, or may represent cultural, societal, political or geographical conditions (Wejnert, 2002). According to Herder et al. (2011), settings resemble non-competitive, monopolistic environments should result in less incentive for organizations to quickly absorb best practices than would be expected in a competitive setting. However, as suggested by Aarons, Hurlburt, and Horwitz (2011), external policy and regulation may be positively associated with adoption of new technologies, including specific enactment of policies, legislation, or regulations on innovation adoption.

### 2.5. *Organizational consequences of IoT adoption in organizations*

According to Orlikowski (1992), understanding technology as continually being socially and physically constructed requires discriminating between human activity which affects technology, and human activity which is affected by technology (López-Muñoz & Escribá-Esteve, 2017). Orlikowski (1992) identifies technology as being the product of human action, while it also assumes structural properties. Furthermore, technology is physically constructed by actors working in a given social context and socially constructed by actors through the different meaning they attach to it. Research in the sociology of technology suggests that the evolution of new applications is a process of social interaction between multiple agents (Allen, 2003; Kabanda & Brown, 2017). According to Orlikowski (1992), agency refers to capability not intentionality, and action taken by actors may have unintended consequences. For example, Mirvis et al. (1991) suggest that technology can influence the layers of hierarchy in companies, with regards to delegation of responsibilities, or chosen strategy (Buonanno et al., 2005), the suggestion being that technology is an important factor driving organizational behavior (Mendel et al., 2008; Subramanian & Nilakanta, 1996). As suggested by Boyne et al. (2005), the successful usage of technology is dependent on constraints which include: 1) the context within which public organizations operate (Buonanno et al., 2005; Damanpour & Gopalakrishnan, 1998; Damanpour & Schneider, 2006; Quinn & Hall, 1983), 2) the characteristics of the organization (Law & Ngai, 2007; Wejnert, 2002), and 3) the nature of the technology itself (Peansupap & Walker, 2005). According to Orlikowski (1992), technology is interpretively flexible. However interaction of technology and organization is a function of the different actors and the socio-historical contexts implicated in its development and use. For example, (Law & Ngai, 2007) suggest that business processes being a close fit with the defined ERP processes are essential for ERP adoption success.

According to Brous et al. (2018), organizational consequences of IoT adoption include significant changes to business processes within the organization although automating business processes remains challenging (Mihailovic, 2016). As suggested by Herder et al. (2011), most organizations include a variety of actors and stakeholders and this multi-agent setting complicates the implementation of innovation as decision-making may often involve a long process which could involve political trade-offs and stakeholder consultations. As such, *people* related changes wrought about by IoT adoption in organizations may be seen in the way people themselves have to adapt to new technologies as suggested by Solomons and Spross (2011). In line with Solomons and Spross (2011), when there is no attention to the cultural dimension of asset management through IoT, improvement results are not acknowledged by the organization, success is not rewarded and improvement behaviors do not become embedded in practice. This suggests that the ability of tactical staff to observe meaningful results and achieve expected benefits is important to implementing and sustaining IoT adoption as suggested by Feldstein & Glasgow (2008).

## 3. Methodology

The paper uses case study research investigated using a multi-method approach to examine IoT adoption in organizations. According to Choudrie and Dwivedi (2005), case study is a widely chosen method for examining technology adoption issues. The research design follows the case study methodology proposed by Yin (2003). The design of case study research includes the research questions, the propositions for research, the unit of analysis, the logic which links the data to the propositions and the criteria for interpreting the findings (Yin, 2003). A background of relevant literature was developed in which the research was placed in context, and the expected benefits and risks that IoT adoption may bring were identified from previous research. The case study method was employed to examine how IoT adoption in real life settings have impacted organizations. Case study research was chosen as the main research method in order to exam the effects of IoT adoption in a real-world context (Eisenhardt, 1989; Yin, 2003). According to Eisenhardt (1989), a broad definition of the research question is important in building theory from case studies. As discussed above, this research asks how IoT adoption may impact organizations. IoT has much potential, however, the full impact of IoT adoption on organizations has not yet been investigated systematically and remains largely anecdotal.

This article relies on the concepts of duality of technology (Orlikowski, 1992) to derive preliminary propositions, assuming that organizations initiate IoT adoption in order to achieve expected benefits, but that these benefits often introduce unexpected risks which require mitigation as seen below in Fig. 1.

Duality of technology suggests that IoT adoption comprises decisions on a technical level, but these decisions cannot be isolated from organizational aspects. The unit of analysis, the organization, sets the boundaries for the case with regard to generalizability of its results. Duality of technology is also used as the logic which links the data to the propositions in the case analysis and serves as guidance for the interpretation of findings. The duality of technology lens was used in the following way: 1) viewing IoT as a *product of human action*, the IoT system and its development was described and expected benefits of the cases were listed; 2) viewing IoT as a *medium of human action*, the uses and constraints of the system were analyzed and described; 3) looking at the *institutional conditions of interaction* with IoT, the human and organizational changes which were deemed necessary to be able to use and manage the system were listed and analyzed; 4) looking at the *institutional consequences of interaction* with IoT, the actions which were taken to mitigate the experienced risks and achieve expected benefits were listed and analyzed. Derived from Orlikowski (1992), Table 3 below shows the propositions related to the types of influence of technology as suggested by Duality of Technology.

Following Ketokivi and Choi (2014), induction type reasoning was used in order to look for both similarities and differences across the cases and proceed toward theoretical generalizations. As with other multiple case study research (Otto, 2011; Pagell & Wu, 2009), the data analysis in this research contained both within and across case analysis (Miles & Huberman, 1994). Within case analysis helps us to examine the impact of IoT on organizations in a single context, while the across case analysis triangulates the constructs of interest between the cases. The paper describes how one organization approaches the issue of IoT adoption in different domains, namely water management and road management. Along with a clear understanding of the unit of analysis, case selection is crucial for building theory from case studies because it is case selection that determines the external validity of the case study and the limits for generalizing the findings (Yin, 2003). The cases selected were both located within RWS, within the context of asset management with regards to large scale, physical infrastructure in the Netherlands. The cases under study were selected from two different domains within RWS in order to ensure diversity and external validity through replication logic (Eisenhardt, 1989; Yin, 2003), in which each case serves as a distinct experiment that stands on its own as an analytic unit. The two cases of IoT adoption that were chosen were the automatic measurement of the weight of vehicles over the Dutch National Highways, “Weigh-In-Motion” (WIM), and the automatic measurement of hydrological data in Dutch Waters, “Landelijk Meetnet Water”, (LMW). These are both mission critical systems for RWS. Table 4 below presents an overview of the cases chosen.

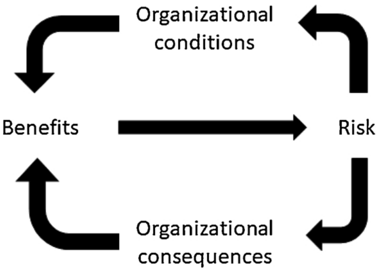


**Fig. 1.** The conceptualization of the relationship between expected benefits of IoT for the organization, encountered risks in practice and organizational (institutional) conditions and consequences.

The case study was conducted using a multi-method approach. In order to prepare the organization for the case study research project, RWS was provided with information material outlining the objectives of the project. Following the suggestions of Yin (2003), the research design is a multimethod design and multiple data sources were used. Primary data sources included the use of individual interviews and group discussions. Secondary data sources included relevant market research and policy documents as well as websites.

The cases were investigated over a period of eighteen months. At the start of the research, in June 2015, group discussions were held with personnel directly involved in the implementation project or who were tasked with managing and maintain the systems. Special focus was given to discovering expected and experienced benefits as well as foreseen risks. The group discussions helped to give a broad view of the case study from a formal, organizational perspective. This perspective was complemented by the findings from the secondary data. After eighteen months, individuals were then approached to gain insights into how the adoption process had proceeded and to gain personalized views as to the experienced impact of the adoption cases. Although our unit of analysis is the organization, by interviewing persons within the cases it helped to better understand and capture the underexposed and unexpected benefits and risks which may not have been revealed in a group setting due to the desire to maintain group or individual reputations. To address the construct validity of the case studies as suggested by Yin (2003), the researchers requested and were given unrestricted access to subject matter experts and internal documentation. Interviewees were selected on the basis that they were intimately involved in the project as early adopters. Interviewees were selected from three levels in the organization, namely the strategic, tactical and operational. The questions in the interviews were structured into two groups. First the need for IoT adoption and the expected benefits, and second, the risks and how these were mitigated.

The cases were investigated over a period of eighteen months. In January 2017, individual interviews were held with RWS personnel to identify unexpected risks which had been experienced during the implementation process. A challenge faced by the research, and also an identified risk to the adoption process, was the staff changes during the adoption process. In this research we mitigated the risk faced by interviewing different people by interviewing staff in the second round with similar roles to those interviewed in the first round. However, it is possible that different answers may have been given if the same people had been interviewed in both rounds. Internal documentation was selected which dealt specifically with the intended benefits or risks and issues faced by the adopting projects. Table 5 below summarizes the

**Table 3**
Propositions of the influence of IoT.

| No. | Type of Influence (Orlikowski, 1992) | Proposition (this research) |
|---|---|---|
| 1. | Technology as a product of human action | IoT is developed and implemented in order to achieve expected benefits |
| 2. | Technology as a medium of human action | IoT can facilitate human action, but also poses significant risks to organizations such that expected benefits are often not achieved |
| 3. | Institutional conditions of interaction with technology | Achieving benefits of IoT adoption requires new skills, roles and processes |
| 4. | Institutional consequences of interaction with technology | Mitigating the risks of IoT adoption often requires structural changes to the organization |

**Table 4**
Case studies overview.

| Attribute | Case 1 | Case 2 |
|---|---|---|
| Organization | RWS | RWS |
| Name | Weigh-In-Motion | Landelijk Meetnet Water |
| Domain | Road Management | Water Management |
| Number of Measuring Stations | 18 | 640 |

data sources used. All interviews were documented in writing. The documents were then analyzed and transferred into an integrated case document (one for each case). The first versions of this document were then sent to the interview participants for feedback and clarification of open points. Once all the additional information feedback had been incorporated, the final version was reviewed and discussed with the main contacts at RWS.

Triangulation of benefits and risks within the cases was made by listing benefits and risks found in internal documentation and comparing these to the benefits and risks exposed in the interviews. There were several iterations throughout the research as each case introduced new benefits and risks.

## 4. Findings

Using the Duality of Technology as lens we analyzed whether or not assumed benefits were confirmed in practice and whether other unexpected benefits or risks were experienced. The case studies were considered necessary in order to consider and include possible future consequences that go beyond the intended as suggested by the duality of technology. The case study research involved the use of multiple methods for collecting data.

### 4.1. Case study 1: weigh-in-motion

At present, RWS estimates that at least 15 percent of freight traffic on the Dutch national road network is overloaded. Overloading of heavy vehicles causes road pavement structural distress and a reduced service lifetime (Bagui, Das, & Bapanapalli, 2013; Mulyun, Parikesit, Antameng, & Rahim, 2010). Effectively reducing overloading reduces the damage to the road infrastructure, lengthening the road's lifetime and reduces the frequency of maintenance. The damage to pavements and installations by overloaded trucks in 2008 was estimated to be at least 34 million euros per year (Brous et al., 2017). The ambition of RWS is to increase the operational efficiency and effectiveness of the approach to overloading and thus reduce maintenance costs. Traditional enforcement of laws and regulations regarding overloading involved the use of physical measuring stations. This included manual checks by the police in which many vehicles were selected where overloading was suspected but uncertain. This often led to unnecessary inconvenience to citizens as vehicles were often stopped unnecessarily. Until 2010, The Netherlands had 5 measuring stations nationwide. It was suspected that many carriers were able to avoid these stations by choosing alternative routes whilst retaining their economic gain.

RWS has created a national network of monitoring points, the “Weigh in Motion” (WIM) network with the goal of improving the operational efficiency and effectiveness of monitoring services and improve the tactical efficiency and effectiveness of enforcement of regulations. The WIM system is one of the most advanced measurement systems in the world. In the period 2010–2013, RWS built a nationwide network of WIM stations, a total of 22 measuring stations. In addition to sensitive sensors, cameras are also are part of the WIM systems. The WIM network, consisting of measuring stations in the road on which the axle loads of heavy traffic is weighed, is used to support the enforcement of overloading by helping the enforcement agency to select overloaded trucks for weighing in a static location. Data on overloaded vehicles on the road are automatically sent from WIM to the Real Time

**Table 5**
Data sources.

| Name | Case 1: Weigh-In-Motion | Case 2: Landelijk Meetnet Water |
|---|---|---|
| Interviews | June 2015: Group discussion<br>Division Head<br>Project manager<br>Data manager<br>Functional manager<br>January 2017: Individual interviews<br>Program Director<br>Business Analyst<br>Project Manager<br>Service Delivery Manager<br>Project Manager | June 2015: Group discussion<br>Department Head<br>Domain Architect<br>Service Delivery Manager<br>Data Manager<br>January 2017: Individual interviews<br>Strategic Advisor<br>Solution Architect<br>Process Manager<br>Project Manager<br>Service Delivery Manager |
| Documents | A3 Weigh in Motion 03-10-2013 version 3<br>Guide to Road Management RWS (Wegwijzer Wegbeheer) 2005-2010<br>“Fixed maintenance manual” (Handboek vast onderhoud)<br>“Brochure assetmanagement in Rijkswaterstaat”<br>“Aspects of management”<br>https://www.rijkswaterstaat.nl/over-ons/nieuws/nieuwsarchief/p2014/10/Informatiesysteem-spoort-overbeladen-trucks-op.aspx | https://www.helpdeskwater.nl/onderwerpen/monitoring/landelijk-meetnet/<br>“Evaluation base measuring network water quality Dutch Northern Quarter”<br>Market consultation document LMW2-V 1.1 DEF<br>Notes from Information Market Consultation LMW2 V 1.0<br>Report Market Consultaton LMW2-V1.0 DEF |

Monitor (RTM) web application which processes, stores and publishes the data of all weigh points. The Inspectorate for the Living Environment and Transport (ILT) is then able to perform supervision and enforcement actions on overloaded vehicles in near-real time, improving the overall flexibility of the services as ILT and RWS are able to decide where and when offenders are controlled. The network provides access to information about the actual load of the main road, and about peak times when it comes to overloading. This provides RWS and ILT with the ability to collect information concerning the compliance behavior of individual carriers as, in addition to sensors, cameras are also are part of the WIM systems. Via camera footage, the ILT can identify the license plates of vehicles that are overloaded and therefore the detect owner and / or licensee and address. The strategy being to tackle overloading by integrating roadside enforcement along with targeting carriers according to behavior based on the information from the system.

### 4.2. *Case study 2: hydrological data collection*

RWS operates and maintains the National Water Measurement Network, at RWS known as “Landelijk Meetnet Water” (LMW). This is a facility that is responsible for the acquisition, storage and distribution of data for water resources. LMW has approximately 640 data collection points using a nationwide system of sensors. The data is then processed and stored in the data center and is made available to a variety of systems and users. The LMW was created from the merging of three previous existing monitoring networks: the Water Monitoring Network, which monitors inland waterways such as canals and rivers; the Monitoring Network North, which monitors North Sea oil platforms and channels; and the Zeeland Tidal Waters Monitoring Network which monitors the Zeeland delta waterways. LMW also includes data from third parties, including water data from foreign countries and other public organizations within The Netherlands. LMW enables timely data with regards to the situation in rivers, canals and sea via sensors at approximately 640 monitoring sites. Monitoring sites are managed and administrated partly by RWS (approximately 300 physical measurement locations) but also partly by external parties (approximately 340 monitoring stations). The locations measured include hydrological and meteorological data. Conditions at the different measuring stations can be location specific. RWS has standardized the method of converting raw sensor signals to metrics, including validations and conversion calculations. This is an internal RWS standard. Meteorological data are collected in close collaboration with the Royal Netherlands Meteorological Institute (KNMI). Hydrological data concerning the measurement of water levels, flow rate (average amount of water in m3/s), wave height and direction, velocity and direction and temperature. Also, in some locations water quality is measured in order to assess whether the water meets the norms of the European Union Water Framework Directive. Meteorological data concerning the measurement of wind speed and direction, air temperature and humidity, visibility, air pressure and cloud base is also collected. The LMW processes sensor information and upgrades this data to qualified readings.

### 4.3. *Cross-case comparison*

This section presents the results of the cross-case comparison, presenting the results of the case studies using a Duality of Technology (Orlikowski, 1992) lens to present the data. Tables 6 to 8 below present the results of the case studies for big, open and linked aspects of IoT respectively. In each table the first column states the case to which the description relates. The second column describes the expected benefit to be gained from the case. The third column describes the risks which were encountered whilst attempting to gain the described benefit. The fourth column describes the institutional conditions of gaining the expected benefit. The fifth column describes the institutional consequences which resulted from mitigating the encountered risks. In the

**Table 6**
Cross-case comparison: duality of *big* data aspects of IoT.

| Case | Expected Benefit(s) | Encountered Risk(s) | Institutional condition(s) | Institutional consequence(s) |
|---|---|---|---|---|
| WIM | WIM generates large amounts of data which is processed near to real time so that inspectors are able to quickly identify trucks for roadside inspection without unnecessarily disrupting traffic. | Uncertain data quality prevented trust in the results | Ensuring data quality required implementation of a Data Quality Framework to manage data: new skills, roles and processes required to manage data quality | Ensuring data quality resulted in structural changes to data management departments: new staff, new departments |
| | | Configuration complexities of the system:<br>-IoT technologies were adjusted to accommodate unexpected real world situations<br>-new specialized equipment need to be developed | The configuration needed to be closely monitored: new specialized skills required | New responsibilities to monitor configurations regularly meant new dedicated teams |
| | | IT infrastructure limitations:<br>-expansion of servers<br>- expansion of network | Mitigating limitations required expansion of existing IT infrastructure: -new specialized skills required | Expanding IT meant new, dedicated operational teams and extra staff to manage systems |
| | As WIM needed to be developed from concept, the market was encouraged to develop new products and create new business opportunities. | Framework agreements were insufficient as RWS also needed to work with small start-ups | Because RWS worked with framework agreements with established partners, RWS needed to rethink their approach to framework agreements to accommodate start-ups and smaller parties. New knowledge regarding procurement policies were developed | Structural changes to procurement policies and processes were required to accommodate partnerships with start-ups and smaller parties. |
| LMW | Due to the timeliness and volume of data, LMW makes it possible to automate processes based on accepted norms and using well tested models, greatly reducing the time required to act in emergency situations. | Uncertain data quality prevented trust in the results | Ensuring data quality meant that sensors needed to be regularly checked and cleaned by hand. | Checking and cleaning sensors meant new roles and responsibilities for maintaining sensors and new teams required to manage sensors (outsourced on managed internally) |
| | | Configuration complexities of the system:<br>-expansion of servers<br>-expansion of network | The configuration needed to be closely monitored: – new specialized skills required | New responsibilities to monitor configurations regularly |

following sections we present findings related to the big data aspects of IoT (Section 4.3.1), findings related to the open aspects of IoT (Section 4.3.2) and finally findings related to the linked aspects of IoT (Section 4.3.3).

### 4.3.1. *Big data aspects of IoT*

The main big data benefits of both case studies are related to amount of data as well as the speed with which it can be collected and analyzed. Both cases rely on (near) real-time data to be able to make operational decisions. LMW relies on a large variety of data in order to be able to predict water levels in time for storm-surge barriers to be able to close whilst WIM is required to identify freight trucks, measure their weights and transmit this to inspectors at near real-time. Achieving these benefits required a good deal of innovation and in both case studies, interviewees questioned whether or not the reliability of the data was sufficiently well equipped whilst some interviewees raised questions about the accuracy and reliability of the data. For example, in the WIM case one official suggested that at the start of the project, “the quality of the data needed to be quantified, and solving data quality issues was incident driven”. The reason for this is that the WIM system is able to differentiate between the vehicle and the load, but not all vehicles weigh the same. Not all number plates are placed in the same place on the vehicle, and not all drivers have the same driving style. Real world complexities meant that the system had to “learn” about the different real world possibilities. This was similar to the LMW case in which RWS officials initially could not completely trust the system due to fluctuations in data quality. This is because measurements of sensors can be polluted (due to algae growth, etc.) so that the signal weakens and reduces the quality of the measurement. Pollution of the measurement is (amongst other things) dependent on the temperature, light (the season), and the type of water (salt or fresh). The belief exists that the risks involved in completely trusting the LMW system to automate operations are often too great to allow complete automation due to the economic impact of closing storm surge barriers. If LMW distributes incorrect data due to either mechanical or human defects, the system may erroneously indicate that the storm surge barriers should close when this is not necessary, or worse, that the surge barriers should not close when it is necessary. Closing a storm surge barrier unnecessarily can have enormous economic impact as shipping is unable to offload goods according to schedule.

In both case studies, interviewees also cited several technological challenges which needed to be overcome, and which no single market partner could supply at the time. For example, in both cases, data could not initially be transported and stored with acceptable performance. The development of the system also meant that only few private organizations were capable of implementing WIM. This meant that if RWS would provide innovation opportunities to a single party, this would have provided that party with an unfair market advantage. Interviewees explained that it became important to develop a procurement strategy with regards to IoT adoption. In Table 6 below the results of the case studies as related to specifically Big Data aspects of IoT are presented.

### 4.3.2. *Openness aspects of IoT*

In the WIM case, opening the data for public use presented unique challenges with regards to privacy as any and all data related to individuals needed to be strictly anonymized before any of the data could be shared publicly. In the LMW case, privacy was not considered to be an issue as the data collected was strictly water and weather related data and not related to any persons. However, both cases did reveal that data integrity and therefore security was an issue with regards to open data, as although the data could be shared, opening the data meant that steps needed to be taken to ensure that it was not possible in any way for data to be tampered with or manipulated. With regards to WIM, for example, it must not be possible in any way to tamper with the “evidence” provided by the data. The interviewees believe that as an instrument to help roadside enforcement WIM works well, but there are difficulties in using WIM to legally prove offence. The Dutch legal system does not yet fully trust WIM to provide legally conclusive evidence with regards to overloading. It is not yet possible to entirely automate the enforcement process, as physical testing is still required to legally prove overloading. With regards to LMW, the economic impact of incorrectly interpreted data is such that data integrity needs to be ensured throughout the system.

Another issue surrounding the openness of the data is determining responsibilities and who bears the costs. Initially, RWS has born the majority of the costs for both LWM and WIM, despite providing the data free of charge to all other parties as “open data”. According to an RWS official, “because of the number of measuring stations and the geographic spread of the sensors, implementation and maintenance of the sensor network is a costly affair”. However, economic benefits have risen from opening the data, although not directly for RWS as businesses are able to provide new services using data created by the LMW network such as developing new models which are used in planning and maintenance or to provide services for the maintenance and management of the LMW sensors. Table 7 below presents the results of the case studies as related to the *openness* aspects of IoT.

### 4.3.3. *Linked aspects of IoT*

One of the initial challenges of both of the cases was the definition of the service and the identification of possible solutions. In both cases, initial proof of concepts used a combination of intermediate products to approximate the final solution. Innovation was required in order to be able to ensure the necessary precision of the data. For example, the ability to detect overloaded trucks is based on data and it is possible to ensure owners of the carriers and load are also identified and thus enforce regulations at source. According to a RWS Director, “in order to effectively manage the technology, it is important to have sufficient mandate to manage the entire chain”. Managing only the technology or parts of the system produces inefficiencies and can disrupt other processes, such as traffic management, if the overview of the system is not taken into account when planning maintenance. Outsourcing to external contractors meant that extra processes needed to be developed to be able to coordinate with other primary processes. The LMW provides a complete technical infrastructure for the gathering and distribution of water data and delivers the data to various stakeholders within and outside RWS such as the Storm Surge Barriers, hydro-meteorological centers, municipal port companies (among others Port of Rotterdam), flood early warning services and other private parties. As such, LWM has greatly improved the efficiency, effectiveness and flexibility of a wide variety of public services, as the gathering of this data is centralized and each service and party no longer has to gather the data themselves. However, there are various aspects that determine the limit of the life span of a measuring station such as availability of components, a dependable producer of components, the number of suppliers with similar components, life expectancy of the components, and maintainability of the software. Table 8 below presents the results of the case studies as related to specifically *linked* data aspects of IoT.

## 5. Discussion

The duality of technology describes technology as assuming structural properties whilst being the product of human action (Orlikowski, 1992). Technology is physically constructed by actors in a social context, and socially constructed by actors through the different meanings they attach to it, and thus, technology results from the ongoing interaction of human choices and institutional contexts (Orlikowski, 1992). Duality of technology was used as lens in this research to elaborate on the details of how benefits are realized and risks are faced in different organizational and domain contexts and to understand the importance of benefits and risk factors identified in the literature. The lens provided us with an efficient way of identifying relationships between the

**Table 7**
Cross-case comparison: duality of openness aspects of IoT.

| Case | Expected Benefit(s) | Encountered Risk(s) | Institutional condition(s) | Institutional consequence(s) |
|---|---|---|---|---|
| WIM | Analysis of the stored measurement data shows patterns, improving forecasting and trend analysis. There is obviously something wrong with vehicles that are frequently flagged in the system. That may be reason to perform roadside inspections in a subsequent inspection or to visit the parent company for an inspection. | Data privacy: making the data publicly available required ensuring privacy as images of car number plates are made by the system. | Additional data management processes were required to blur images and ensure that identifying attributes were removed | A new dedicated team was required to manage data and ensure that contractors delivered data as required. |
| | | Data integrity: it was vitally important that the data represented the actual situation and could not be manipulated by the system or unauthorized persons | Additional data management processes were required to ensure data integrity | Procedures and extra security measures were required due to the need to prove offence. |
| | | Data Governance: as the data was used by multiple organizations, it was important to define ownership and responsibilities with regards to cost and accountability | Governance processes and acceptance of accountability needed to be defined and accepted | Internal and external negotiations between stakeholders needed to be held in order to define accepted responsibilities |
| LMW | The centralized gathering of data has greatly reduced the overall cost of data collection as a whole, as the data is collected only once by one source and shared between partners, | Data integrity: due to the multiple technologies, interoperability and data integrity needed to be guaranteed. Action need to be taken to ensure that the data could not be manipulated by the system or unauthorized persons | Additional data integrity checks through the flow of data needed to be defined and implemented | Imbalance between cost and benefit for RWS. |
| | | Data Governance: RWS bears the brunt of the cost despite that the data is used by multiple organizations | RWS needed to accept responsibility for the total cost of ownership | Imbalance between cost and benefit for RWS. |

benefits of IoT and the risks which accompany the adoption of IoT in organizations and proved to be appropriate for this research. According to Leonardi (2013), the duality of technology model is important as a waypoint to Orlikowski (2000) practice lens. Leonardi (2013) believes that, having already conceptualized technology use as a constitutive feature of structure in its own right, Orlikowski (2000) introduced the development of the practice lens, the "technology-in-practice," which Orlikowski (2000), p. 405) defined as "a particular structure of technology use". As such, Leonardi (2013) argues that the practice lens tends to hide patterns of technology use into particular "technologies-in-practice" as people tend to interpret how technology could help them achieve their goals. Leonardi (2013) also criticizes the practice lens for offering an overly socialized view of technology. Leonardi (2013) critique is based on the idea that people choose to use technology in a certain way. As such, the technologies themselves "are only peripheral players that are subject to the whims of their users" (Leonardi (2013), p. 64). By way of example, (Leonardi (2013), p. 64) cites Orlikowski (2000) as arguing that "even though technologies have certain physical or digital properties that transcend specific contexts of use, users have the option to choose other options with the technology at hand, opening up the potential for innovation, learning, and change". Leonardi (2013) argues that technology-in-practice is therefore only a set of norms governing when, why, and how to use a technology in a specific setting. As such, using other theories such as socio-materiality may provide further insights, and more research in this area is recommended.

Case study methodology was used in this research to identify relationships between benefits and risks of IoT adoption in organizations in real-world situations. Both cases are involved in asset management in the public sector, and the number of measuring stations is similar. Significant differences are in the asset types and number of sensors utilised in the system. Both LMW and WIM are shared systems, which means that the data is shared with several parties and can be used in legal processes. In this research two interview rounds were used. In the second round, some interviewees were different to the first round due to staff changes. This limits the results of the research as it is possible that the original interviewees may have given different answers. However, it does highlight a risk faced by many IoT adoption projects, namely that staff does change during the project, and the need for substantial changes as other capabilities are needed for IoT adoption, but also meaning possible loss or gain of knowledge and possible changes to solution architectures.

The asset management domain was chosen because IoT has much potential for improving control and maintenance of assets. This might limit the generalizability to other domains, however, the essence of IoT generating data, driven by expected benefits is likely the same. The others might be context dependent and further research is recommended to investigate this. Expected benefits of IoT in asset management may introduce unexpected risks (Brous & Janssen, 2015a) for the improvement of asset management in public utility infrastructure networks. Public utility infrastructure networks such as electricity networks and transportation networks provide many of the services that are vital to the functioning, and security of society, and managing these assets effectively and efficiently is critical (Tien et al., 2016). IoT can be used to manage the physical world in various ways (Mihailovic, 2016; Neisse et al., 2016), and many of these infrastructure networks have an extensive range of physical and social sensors to detect damage and monitor capabilities (Aono, Lajnef, Faridazar, & Chakrabartty, 2016; Tien et al., 2016). However, as suggested by Damanpour and Gopalakrishnan (1998), many public utility organizations traditionally have a hierarchical organizational form with stable environments and low innovation adoption rates. The increasing rate of change driven by IoT may therefore create unique challenges for these organizations for IoT adoption. In asset management, benefits are often viewed as resulting from the use of IoT, in other words, IoT as medium of human action. Benefits resulting from other types of duality influences, such as

**Table 8**
Cross-case comparison: duality of linked aspects of IoT.

| Case | Expected Benefit(s) | Encountered Risk(s) | Institutional condition(s) | Institutional consequence(s) |
|---|---|---|---|---|
| WIM | WIM is capable of differentiating between the load and the vehicle. It is possible to identify not only the transporter, but also the owner of the load. Enforcement of regulations is therefore greatly improved. | Interoperability and integration: variety of technologies and lack of standards introduced difficulties integrating data | The definition of the service and the identification of possible solutions with regards to standards and integration. | Innovation and standard definition was required in order to be able to ensure interoperability. |
| | | Clashes in planning with other processes such as traffic management. | Communication and coordination of activities between primary processes needed to be defined and improved to avoid clashes. | Coordination mechanisms between primary processes needed to be developed. |
| LMW | Improved efficiency, effectiveness and flexibility of a wide variety of public services, as the gathering of this data is centralized and each service and party no longer has to gather the data themselves. | Interoperability and integration: lack of technical knowledge due to the wide variety of different types of equipment with different coupling technologies used by the measuring stations. | New skills needed to be acquired to be able to develop interoperable processes | IT infrastructure needed to be adjusted to introduce interoperating systems.<br>New, dedicated teams required to manage IT infra |

knowledge development, personal development of staff, or improvements to the organizational culture are often “hidden” or secondary benefits and may not be the main drivers of IoT adoption in the asset management domain. This may be different in other domains such as research and further research is required in these areas. In the following sections the results of the case studies are discussed in relation to the propositions outlined in Section 3. In Section 5.5 we take a step back from the propositions, summarizing how the duality of IoT may impact organizations, and discuss necessary steps that need to be taken before benefits of IoT can be achieved.

### *5.1. Proposition 1: IoT is developed and implemented in order to achieve expected benefits*

Orlikowski (1992) identifies technology as being the product of human action, while it also assumes structural properties. Furthermore, technology is physically constructed by actors working in a given social context and socially constructed by actors through the different meaning they attach to it. This requires discriminating between human activity which affects technology, and human activity which is affected by technology (López-Muñoz & Escribá-Esteve, 2017). As such, according to Kabanda and Brown (2017), duality of technology theory provides opportunities for understanding changes in the social order and helps us understand the innovation process in its specific socio-cultural context. According to Brous et al. (2018), IoT may bring an improved understanding of complex processes which is expected to help improve the efficiency of transport management and infrastructure services, and help with effective reporting. In Table 6 we notice that the adoption of the LMW system has allowed RWS to develop new predictive maintenance models for the maintenance and management of the LMW sensors. As such, IoT infrastructure could potentially be used to reduce costs in terms of time and money as traditional methods of inspecting infrastructure are often reactive in nature and require significant amounts of time and use of costly equipment. For example, Hollands (2008) describes a differentiation between smart cities that focus on IoT purely for economic prosperity and those that seek to become sustainable and inclusive.

### *5.2. Proposition 2: IoT can facilitate human action, but also poses significant risks to organizations such that expected benefits are often not achieved*

The duality of technology argues that actors use information technologies to constitute structures, but at the same time, information technologies become part of the structures constraining individual actions (see Orlikowski, 1992). The dual nature of technology suggests that adoption of IoT might result in new structures, but IoT can also be adopted within existing structures. In these situations IoT might have positive impacts, resulting in desired improvements, but when the necessary changes are not made could also exert negative effects. with forced mitigation of unexpected risks. For example, IoT can benefit organizations by providing enough quality data to generate the information required to help asset managers make the right decisions at the right time (Brous & Janssen, 2015b), but automating processes often necessarily leads to changes to organizational structures and cultures as tasks previously performed by people become automated, whilst other tasks and responsibilities which previously did not exist become apparent. As seen in Table 6, an unexpected risk which has previously not been recognized in literature is the realization that data quality is also a significant risk as well as being a potential benefit. Organizations and previous research often suggest that a large part of the business case of IoT lies with the improved quality (timeliness, precision etc.) of data. However, automating mission-critical primary processes means that data quality needs to be guaranteed, and real-world challenges often mean that system configurations need to be highly complex. Results of case studies described by Wahyudi et al.

(2018) suggest that suggest that decisions based on big data are often ad-hoc as decision-makers are often unable to make sense of the information delivered by big data. The WIM case shows that trust in the system and in the quality of data needs to be systematic and embedded in legal frameworks. As such, achieving benefits of IoT adoption often requires accounting for a variety of systematic risks. For example, sensors might not work or might emit the wrong signals, resulting in poor quality information, annoyance for the public, a reduction of trust in the system and damage to the reputation of the organization.

### 5.3. Proposition 3: achieving benefits of IoT adoption requires new skills, roles and processes

Research in the sociology of technology suggests that the evolution of new applications is a process of social interaction between multiple agents (Allen, 2003). According to Orlikowski (1992), agency refers to capability not intentionality, and action taken by actors may have unintended consequences. This is confirmed in our analyses shown in Table 3. For example, the intention of RWS to open WIM data to the general public has led to the development of extra data management and data manipulation processes to ensure privacy of citizens as number plates and people need to be made unidentifiable. This has meant extra costs, changes to IT due to new requirements and the development of required skills.

Initial research on IoT adoption has tended to focus on the potential of technology as a catalyst for IoT adoption, but more recent debates have increasingly stressed the voice of the citizen and the relationship of the citizen with public sector organizations (Castelnovo, Misuraca, & Savoldelli, 2015; van Waart, Mulder, & de Bont, 2015), stressing the duality of IoT. van Waart et al. (2015) go so far as to suggest that IoT technologies increase efficiency of public services such as public transportation, traffic management, or energy management but does not necessarily lead to an increased well-being of citizens. Using IoT to manage infrastructure from a purely economic perspective may be cheaper and more efficient, but ignoring the social impact of IoT may also introduce unexpected risks to the organization. Traditional inspections of infrastructure are often performed subjectively. In other words, inspectors visually inspect the asset at regular intervals and make expert judgments based on what they see and their past experience. However, the regularity of these inspections, and their subjective nature means that the inspection can often vary in quality and granularity (Phares, Washer, Rolander, Graybeal, & Moore, 2004).

### 5.4. Proposition 4: mitigating the risks of IoT adoption often requires structural changes to the organization

A duality of achieving cost reduction is the need for IoT maintenance requiring not only investments now, but also in the future. According to an RWS official, “because of the number of measuring stations and the geographic spread of the sensors, implementation and maintenance of the sensor network is a costly affair”. The duality is that new technology results in the need for a new maintenance departments, which in turn influences the technology to ensure low-cost maintenance of IoT devices. Although IoT adoption can improve management and maintenance planning and assist organizations with the development and enforcement of more efficient regulations, the heterogeneity of IoT and of the people using IoT means that interoperability of IoT data and IoT systems and the integration of IoT within new and existing processes can pose significant risks to achieving successful adoption of IoT and the achievement of the expected benefits. As suggested by Brous et al. (2018), new organizational processes are needed to ensure that IoT works properly. For example, the adoption of LMW has meant that the control of bridges (e.g. opening and closing and evaluating needs for maintenance) can be performed centrally, leading to a central department, but also that the skills required for maintaining the bridges are less focused on pure asset management and more on data and IT management. Nevertheless, there still is a need for physical inspection, as IoT cannot replace this, but it will be less and more focused by taking a data-driven approach. According to one interviewees “some LMW processes were adjusted too quickly”. Another interviewee suggested that “smaller contracts and a number of facility tasks should may have been better positioned with the line managers”. As such, the duality of introducing IoT for the purposes of improving planning and efficiency is that organizations often need to change and adapt predefined business processes (Brous et al., 2018). Resistance of staff to these changes and a lack of trust in the IoT systems can mean that achievement of benefits is limited. Furthermore, although IoT promises significant economic benefits to the organization due to automation of processes and previously unforeseen insights, IoT adoption also demands significant investment which can pose significant financial risk for organizations. An often overseen risk of economic savings in our cases was that staff need to be reassigned, re-educated or even be made redundant.

### 5.5. Summary: duality of IoT in organizations

The results of the case studies show that adoption of IoT is initiated by the desire to achieve certain benefits. Often the initial business case is based on the operational benefits that IoT may provide such as the provision of real-time data allowing for improved reaction times. For example, WIM inspectors can monitor freight traffic without having to pull each truck off the road to weigh them, and respond immediately when overloading is detected. Due to the specific requirements for each case, technology often has to be developed or configured to fit the specific environments and meet requirements. Development and implementation of IoT therefore also presents risks to the organization as well as the adoption process itself as there are often institutional conditions of IoT adoption, such as ensuring the necessary knowledge and capacity to use, manage and maintain the systems effectively. Mitigating these risks, which are often unexpected, can result in institutional consequences, new requirements, but also in new benefits. As such, Fig. 2 below shows that benefits of IoT are often only achieved once the institutional conditions of IoT adoption have been met, and the institutional consequences of IoT adoption have been accepted.

To illustrate the figure, (a) IoT is developed by people to provide improved data quality, and volumes of real-time data. (1) IoT can benefit organizations by improving forecasting and trend analysis which allows organizations to better predict the infrastructure needs of the future for developing communities. However, using IoT data ($b_i$) might also harm society through violation of privacy. For example, (2) organizations often encounter usability issues during privacy impact assessments. Table 7 shows that the analysis of the stored measurement data from WIM has revealed patterns, which allows ILT to perform roadside inspections in a subsequent inspection or to visit the parent company for an inspection. The duality is that organizations also need to be aware of potential conflicts related to data privacy issues (c) and to take necessary measures to ensure data protection. For example, new activities (3) are introduced to ensure that all WIM data is thoroughly checked and all number plates and other identifiable data are removed before any data is made “open” or publicly available. The new roles require structural changes (d) to the organization. For example, (4) the development of new skills and knowledge, and a lack of standardized architectures and solutions often force organizations to develop new departments, hire new staff and invest heavily in knowledge development. However, the organizational, process and staff changes have also led to changes in the technology as user requirements become clearer (5). This attention to privacy and security has also led to greater transparency in organizations (6), affecting the reputations of organizations and empowering the general public to be more self-sufficient and to make their needs better known. For example, making WIM data open has meant that all WIM processes are clearly defined and documented and opened for the general public. However, greater transparency also means that organizations are more vulnerable to public scrutiny and need to take greater care to ensure that policy, regulations, and legal frameworks are in place and strictly followed. Furthermore, the open aspect of IoT allows better data sharing so that multiple goals may be achieved with the same data ($b_{ii}$). For example, (6) the adoption of LMW has meant the introduction a single data collection process, but the openness of the data means that the data can be used to serve multiple goals such as monitoring water levels for the purposes of the storm surge barriers, but also messages to skippers and also for swimming water quality. We observed that more timely data providing real-time information allows organizations to streamline services, reducing unnecessary overhead and improving the ability to react timely to events. Table 6 shows that inspectors are able to monitor the weights of lorries in real time and are able to allow traffic to flow more easily instead of having to stop and check every lorry and physically weigh them.

Previous technology adoption models tend to describe adoption process as being linear. The model described in Fig. 2 develops the structuration model of Orlikowski (1992) and is further essentially different from previous adoption models and information system models as it demonstrates that not only is successful adoption of IoT dependent on both organizational and human conditions, as well as requiring the technology to be of sufficient maturity, but that adoption is a continuous cycle, as new knowledge and organizational forms provide new requirements and uses for the technology which drives further development of the technology. These new technological advances then, in turn have a social impact on the organization and people etc. Benefits of IoT are often only achieved once the institutional conditions of IoT adoption have been met, and the institutional consequences of IoT adoption have been accepted. These conditions and consequences often then lead to new insights, uses, and requirements.

## 6. Conclusions

Although IoT provides many benefits the use of the technology is a product of human actions and these actions determine the actual benefits to be gained. This research provides a systematic overview of potential benefits and risks of IoT and insight into the duality of IoT in two cases. The objective of this paper was to analyze the impact of IoT adoption by organizations. Four propositions were and defined and four research questions were asked.

The first research question asked what the benefits of adopting IoT in organizations are. The categories of benefits of IoT adoption in organizations can be summarized as:

- The capability to provide (more) timely information for decision-making and greater response times
- Automation of decision-making
- Improved planning due to insights created by higher volumes of data
- Reduction of operational costs due to improved data quality
- Insights into possible new revenue streams due to linking capability of data
- Better communication with clients due to open nature of the data

These conclusions suggest to researchers and practitioners that expected benefits are often related to the use of data generated by IoT, such as operational reactions to data generated by IoT sensors, and that IoT whilst obviously useful for action-reaction use cases, can provide organizations with much greater benefits than purely operational benefits. For example, the closing of storm surge barriers when sensors detect a rise in sea levels. The increased volumes and velocity of data being generated, as well as the possibility of being able to link the data to other data sources allows organizations to generate new insights into their primary processes allowing them to take pre-emptive actions instead of having to react to unexpected events.

However, adopting IoT can often introduce a variety of expected and unexpected risks to organizations, and the second research question asks what the risks of IoT adoption for organizations are. The categories of risks of IoT adoption can be summarized as:

- Non-compliance with privacy regulations
- High implementation costs
- Interoperability and integration issues
- Security risks
- Lack of knowledge and risk awareness
- Lack of trust

Researchers and practitioners should note that the openness aspect of IoT which allows better data sharing so that multiple goals may be achieved with the same data also places organizations at risk due to data privacy and data security issues, introducing the need for specific policies and legal frameworks and defined data governance structures and processes. Also, the linked aspect of IoT means the presence of security risks for organizations as well as risks related to interoperability and integration. This can in turn lead to the development of industry standards which, as witnessed in the WIM case has a dual impact on the technology itself through innovation.

As such there are often organizational conditions required for benefits of IoT to be achieved, and the third sub-question asks what the organizational conditions for IoT adoption are. The organizational conditions of IoT adoption can be summarized as follows:

- Implementation of a data quality framework
- Implementation of data governance
- Development of technical skills
- Ensuring IoT capabilities in IT infrastructure
- Ensuring flexible procurement policies
- Strong data architectures including standards and protocols

Researchers and practitioners should note that many of the issues which occur are interrelated, and there are often consequences that can go beyond the accomplishment of the intended benefits.

The fourth sub-question therefore asks what the organizational consequences of IoT adoption are. Organizational consequences of IoT adoption can be summarized as follows:

- Structural changes to data management departments – new roles, and often new departments such as the Chief Data Office
- New responsibilities to monitor configurations, often leading to new teams and structural changes to the organization
- Structural changes to procurement policies and processes
- Structural changes to business processes
- Structural changes to strategy and policy making
- Structural changes to communication

Improved planning and forecasting by means of IoT data required structural and significant changes to the IT infrastructure in our cases. Also new knowledge and specialist skills were required, leading to changes in staffing and organizational structures. For example, the development of WIM required a close alliance with knowledge institutions to develop the technology, and specific skills were needed to be developed in order to properly calibrate the system.

As seen in Fig. 2, this research shows that successful adoption of IoT depends on both organizational and human conditions, as well as requiring the technology to be of sufficient maturity. Furthermore, we may conclude that adoption of IoT is a continuous cycle, as new knowledge and organizational forms provide new requirements and uses for IoT which drives further development of the technology. It is clear that IoT can provide organizations with many potential benefits, however, organizations should realize that achieving these benefits carries potentially unexpected risks and, as suggested by the duality of technology, introduces changes to the organization and the systems.

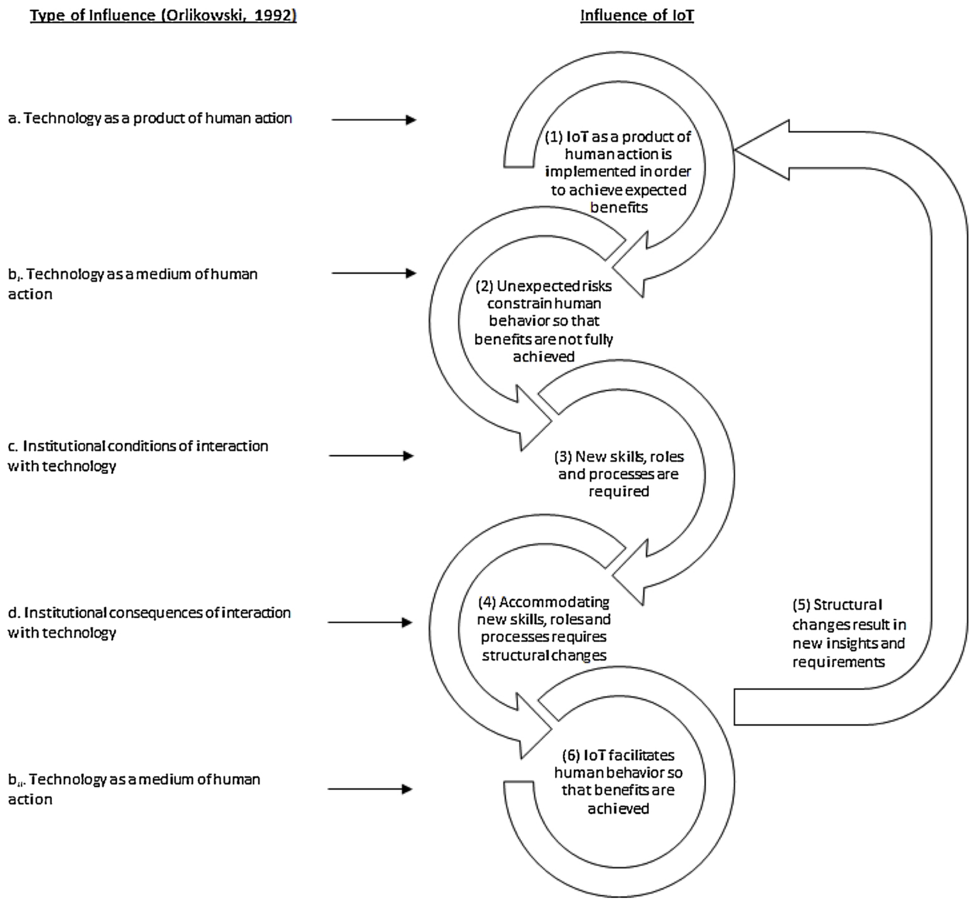


**Fig. 2.** The impact of IoT adoption on organizations.

More research is required into the potential long-term consequences of IoT adoption and practitioners need to make the necessary organizational changes to fully profit from IoT.

## Funding

This work was supported by Rijkswaterstaat, Netherlands.

## References

Aarons, G. A., Hurlburt, M., & Horwitz, S. M. (2011). Advancing a conceptual model of evidence-based practice implementation in public service sectors. *Administration and Policy in Mental Health and Mental Health Services Research, 38*(1), 4–23. https://doi.org/10.1007/s10488-010-0327-7\.

Allen, J. P. (2003). The evolution of new mobile applications: A sociotechnical perspective. *International Journal of Electronic Commerce, 8*(1), 23–36.

Aono, K., Lajnef, N., Faridazar, F., & Chakrabartty, S. (2016). *Infrastructural health monitoring using self-powered internet-of-things. 2016 IEEE international symposium on circuits and systems (ISCAS)*2058–2061.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

Backer, T. E., Liberman, R. P., & Kuehnel, T. G. (1986). Dissemination and adoption of innovative psychosocial interventions. *Journal of Consulting and Clinical Psychology, 54*(1), 111–118.

Bagui, S., Das, A., & Bapanapalli, C. (2013). Controlling vehicle overloading in BOT projects. *Procedia – Social and Behavioral Sciences, 104*, 962–971. https://doi.org/10.1016/j.sbspro.2013.11.191.

Barde, M. P., & Barde, P. J. (2012). What to use to express the variability of data: Standard deviation or standard error of mean? *Perspectives in Clinical Research, 3*(3), 113–116. https://doi.org/10.4103/2229-3485.100662.

Bi, Z., Da Xu, L., & Wang, C. (2014). Internet of Things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics, 10*(2), 1537–1546.

Blackstock, M., & Lea, R. (2012). IoT mashups with the WoTKit. *2012 3rd international conference on the internet of things (IOT),* 159–166. https://doi.org/10.1109/IOT.2012.6402318.

Boos, D., Guenter, H., Grote, G., & Kinder, K. (2013). Controllable accountabilities: The internet of things and its challenges for organisations. *Behaviour & Information Technology, 32*(5), 449–467.

Boulos, M. N. K., & Al-Shorbaji, N. M. (2014). On the internet of things, smart cities and the WHO healthy cities. *International Journal of Health Geographics, 13*(1), 10.

Boyne, G. A., Gould-Williams, J. S., Law, J., & Walker, R. M. (2005). Explaining the adoption of innovation: An empirical analysis of public management reform. *Environment and Planning C: Government and Policy, 23*(3), 419–435. https://doi.org/10.1068/c40m.

Brous, P., & Janssen, M. (2015a). A systematic review of impediments blocking internet of things adoption by governments. In M. Janssen, M. Mäntymäki, J. Hidders, B. Klievink, W. Lamersdorf, B. van Loenen, & A. Zuiderwijk (Eds.). *Open and big data management and innovation* (pp. 81–94). . https://doi.org/10.1007/978-3-319-25013-7_7.

Brous, P., & Janssen, M. (2015b). Advancing e-government using the internet of things: A systematic review of benefits. In E. Tambouris, M. Janssen, H. J. Scholl, M. A. Wimmer, K. Tarabanis, M. Gascó, & P. Parycek (Eds.). *Electronic government* (pp. 156–169). . Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-22479-4_12.

Brous, P., Janssen, M., & Herder, P. (2018). Internet of Things adoption for reconfiguring decision-making processes in asset management. *Business Process Management Journal*. https://doi.org/10.1108/BPMJ-11-2017-0328.

Brous, P., Janssen, M., Schraven, D., Spiegeler, J., & Duzgun, B. C. (2017). *Factors influencing adoption of IoT for data-driven decision making in asset management organizations.* 70–79. https://doi.org/10.5220/0006296300700079 September 8, Retrieved from.

Brous, P., Janssen, M., & Vilminko-Heikkinen, R. (2016). Coordinating decision-making in data management activities: A systematic review of data governance principles. *International conference on electronic government and the information systems perspective,* 115–125.

Buonanno, G., Faverio, P., Pigni, F., Ravarini, A., Sciuto, D., & Tagliavini, M. (2005). Factors affecting ERP system adoption: A comparative analysis between SMEs and large companies. *Journal of Enterprise Information Management, 18*(4), 384–426.

Castelnovo, W., Misuraca, G., & Savoldelli, A. (2015). Smart cities governance. *Social Science Computer Review, 34*(6), 724–739. https://doi.org/10.1177/0894439315611103.

Castro, D. (2008). *Digital quality of life: Government (SSRN scholarly paper No. ID 1285002).* Retrieved from website:Social Science Research Networkhttp://papers.ssrn.com/abstract=1285002.

Chen, X.-Y., & Jin, Z.-G. (2012). Research on key technology and applications for Internet of Things. *Physics Procedia, 33*, 561–566. https://doi.org/10.1016/j.phpro.2012.05.104.

Choudrie, J., & Dwivedi, Y. K. (2005). Investigating the research approaches for examining technology adoption issues. *Journal of Research Practice, 1*(1), 1.

Chui, M., Löffler, M., & Roberts, R. (2010). The internet of things. *McKinsey Quarterly, 2*(2010), 1–9.

Damanpour, F., & Gopalakrishnan, S. (1998). Theories of organizational structure and innovation adoption: The role of environmental change. *Journal of Engineering and Technology Management, 15*(1), 1–24. https://doi.org/10.1016/S0923-4748(97)00029-5.

Damanpour, F., & Schneider, M. (2006). Phases of the adoption of innovation in organizations: Effects of environment, organization and top Managers1. *British Journal of Management, 17*(3), 215–236. https://doi.org/10.1111/j.1467-8551.2006.00498.x.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003 Retrieved from JSTOR.

Dwivedi, Y. K., Janssen, M., Slade, E. L., Rana, N. P., Weerakkody, V., Millard, J., ... Snijders, D. (2017). Driving innovation through big open linked data (BOLD): Exploring antecedents using interpretive structural modelling. *Information Systems Frontiers, 19*(2), 197–212. https://doi.org/10.1007/s10796-016-9675-5.

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review, 14*(4), 532–550. https://doi.org/10.2307/258557.

Fan, P. F., Wang, L. L., Zhang, S. Y., & Lin, T. T. (2014). *The research on the internet of things industry chain for barriers and solutions, 441*, 1030–1035 Retrieved from Scopus.

Fleisch, E. (2010). What is the internet of things? An economic perspective. *Economics Management and Financial Markets, 2*, 125–157.

Fleisch, E., Sarma, S., & Subirana, B. (2006). High-resolution management. *IESE Alumni Magazine,* 8–13.

Giddens, A. (1976). New rules of sociological method: A positive critique of interpretative sociology. London. *Hutchinson.*.

Gilman, H., & Nordtvedt, J.-E. (2014). Intelligent energy: The past, the present, and the future. *SPE Economics & Management, 6*(4), 185–190 Retrieved from Scopus.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010.

Haller, S., Karnouskos, S., & Schroth, C. (2009). The internet of things in an enterprise context. In J. Domingue, D. Fensel, & P. Traverso (Eds.). *Future internet – FIS 2008* (pp. 14–28). . Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-00985-3_2.

Harris, I., Wang, Y., & Wang, H. (2015). ICT in multimodal transport and technological trends: Unleashing potential for the future. *International Journal of Production Economics, 159*, 88–103. https://doi.org/10.1016/j.ijpe.2014.09.005.

Harrison, M. (2011). The'Internet of Things' and commerce. *XRDS: Crossroads, The ACM Magazine for Students, 17*(3), 19–22.

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., ... Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management, 36*(5), 748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems, 47*, 98–115.

Herder, P. M., de Joode, J., Ligtvoet, A., Schenk, S., & Taneja, P. (2011). Buying real options – Valuing uncertainty in infrastructure planning. *Futures, 43*(9), 961–969. https://doi.org/10.1016/j.futures.2011.06.005.

Hollands, R. G. (2008). Will the real smart city please stand up? *City, 12*(3), 303–320. https://doi.org/10.1080/13604810802479126.

Hossain, M. A., & Dwivedi, Y. K. (2014). What improves citizens' privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach. *International Journal of Information Management, 34*(6), 711–719. https://doi.org/10.1016/j.ijinfomgt.2014.07.002.

Hounsell, N. B., Shrestha, B. P., Piao, J., & McDonald, M. (2009). Review of urban traffic management and the impacts of new vehicle technologies. *IET Intelligent Transport Systems, 3*(4), 419–428. https://doi.org/10.1049/iet-its.2009.0046.

Hsu, C.-L., & Lin, J. C.-C. (2018). Exploring factors affecting the adoption of internet of things services. *Journal of Computer Information Systems, 58*(1), 49–57. https://doi.org/10.1080/08874417.2016.1186524.

Hummen, R., Henze, M., Catrein, D., & Wehrle, K. (2012). *A Cloud design for user-controlled storage and processing of sensor data.* 233–240. https://doi.org/10.1109/CloudCom.2012.6427523.

Kabanda, S., & Brown, I. (2017). A structuration analysis of Small and Medium Enterprise (SME) adoption of E-Commerce: The case of Tanzania. *Telematics and Informatics, 34*(4), 118–132. https://doi.org/10.1016/j.tele.2017.01.002.

Kaisler, S., Armour, F., Espinosa, J. A., & Money, W. (2013). Big data: Issues and challenges moving forward. *2013 46th Hawaii international conference on system sciences (HICSS),* 995–1004.

Ketokivi, M., & Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management, 32*(5), 232–240. https://doi.org/10.1016/j.jom.2014.03.004.

Kranenburg, R. V., Stembert, N., Victoria Moreno, M., Skarmeta, A. F., Lopez, C., Elicegui, I., & S´anchez, L. (2014). *Co-creation as the key to a public, thriving, inclusive and meaningful EU IoT.* Retrieved fromhttp://www.scopus.com/inward/record.url?eid=2-s2.0-84921646101&partnerID=40&md5=c287936b64841916510915466136c59b.

Kwon, D., Hodkiewicz, M. R., Fan, J., Shibutani, T., & Pecht, M. G. (2016). IoT-based prognostics and systems health management for industrial applications. *IEEE Access, 4*, 3659–3670. https://doi.org/10.1109/ACCESS.2016.2587754.

Kwon, O., Lee, N., & Shin, B. (2014). Data quality management, data usage experience and acquisition intention of big data analytics. *International Journal of Information Management, 34*(3), 387–394. https://doi.org/10.1016/j.ijinfomgt.2014.02.002.

Law, C. C. H., & Ngai, E. W. T. (2007). ERP systems adoption: An exploratory study of the organizational factors and impacts of ERP success. *Information & Management, 44*(4), 418–432. https://doi.org/10.1016/j.im.2007.03.004.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*(3), 191–204.

Leonardi, P. (2013). Theoretical Foundations for the Study of Sociomateriality (SSRN Scholarly Paper No. ID 2212225). Rochester, NY. *Social Science Research Network*.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200.

López-Muñoz, J. F., & Escribá-Esteve, A. (2017). An upper echelons perspective on information technology business value. *European Research on Management and Business Economics, 23*(3), 173–181. https://doi.org/10.1016/j.iedeen.2017.02.003.

Lytras, M. D., Mathkour, H., Abdalla, H. I., Yáñez-Márquez, C., & De Pablos, P. O. (2014). The social media in Academia and EducationResearch R-evolutions and a paradox: Advanced next generation social learning innovation. *Journal of Universal Computer Science, 20*(15), 1987–1994.

Ma, M., Wang, P., & Chu, C. H. (2013). Data management for internet of things: Challenges, approaches and opportunities. *2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE cyber, physical and social computing,* 1144–1151. https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.199.

Meijer, A., & Bolívar, M. P. R. (2016). Governing the smart city: a review of the literature on smart urban governance, Governing the smart city: A review of the literature on smart urban governance. *International Review of Administrative Sciences, 82*(2), 392–408. https://doi.org/10.1177/0020852314564308.

Mendel, P., Meredith, L. S., Schoenbaum, M., Sherbourne, C. D., & Wells, K. B. (2008). Interventions in organizational and community context: A framework for building evidence on dissemination and implementation in health services research. *Administration and Policy in Mental Health and Mental Health Services Research, 35*(1–2), 21–37. https://doi.org/10.1007/s10488-007-0144-9.

Mihailovic, A. (2016). Liberalising deployment of internet of things devices and services in large scale environments. *Wireless Personal Communications, 92*(1), 33–49.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook.* SAGE.

Mirvis, P. H., Sales, A. L., & Hackett, E. J. (1991). The implementation and adoption of new technology in organizations: The impact on work, people, and culture. *Human Resource Management, 30*(1), 113–139.

Misuraca, G. (2009). Futuring e-government: Governance and policy implications for designing an ICT-enabled knowledge society. *Proceedings of the 3rd international conference on theory and practice of electronic governance,* 83–90. https://doi.org/10.1145/1693042.1693060.

Mitropoulos, P., & Tatum, C. B. (1999). Technology adoption decisions in construction organizations. *Journal of Construction Engineering and Management, 125*(5), 330–338.

Mulyun, A., Parikesit, D., Antameng, M., & Rahim, R. (2010). Analysis of loss cost of road pavement distress due to overloading freight transportation. *Journal of the Eastern Asia Society for Transportation Studies, 8*, 1020–1035.

Nam, T., & Pardo, T. A. (2014). The changing face of a city government: A case study of Philly311. *Government Information Quarterly, 31*(Suppl. 1), S1–S9. https://doi.org/10.1016/j.giq.2014.01.002.

Neisse, R., Baldini, G., Steri, G., & Mahieu, V. (2016). *Informed consent in internet of things: The case study of cooperative intelligent transport systems. Presented at the 2016 23rd international conference on telecommunications (ICT).*

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

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science, 3*(3), 398–427. https://doi.org/10.1287/orsc.3.3.398.

Ortiz, P., Lazaro, O., Uriarte, M., & Carnerero, M. (2013). Enhanced multi-domain access control for secure mobile collaboration through linked data cloud in manufacturing. *2013 IEEE 14th international symposium and workshops on a world of wireless. mobile and multimedia networks (WoWMoM),* 1–9. https://doi.org/10.1109/WoWMoM.2013.6583372.

Otto, B. (2011). Organizing data governance: Findings from the telecommunications industry and consequences for large service providers. *Communications of the Association for Information Systems, 29*(1), 45–66.

Pagell, M., & Wu, Z. (2009). Building a more complete theory of sustainable supply chain management using case studies of 10 exemplars. *The Journal of Supply Chain Management, 45*(2), 37–56. https://doi.org/10.1111/j.1745-493X.2009.03162.x.

Peansupap, V., & Walker, D. (2005). Exploratory factors influencing information and communication technology diffusion and adoption within Australian construction organizations: A micro analysis. *Construction Innovation Information Process Management, 5*(3), 135–157.

Pedro, M. R., & Jaska, P. (2007). Is RFID right for your organization or application? *Management Research News, 30*(8), 570–580. https://doi.org/10.1108/01409170710773706.

Phares, B. M., Washer, G. A., Rolander, D. D., Graybeal, B. A., & Moore, M. (2004). Routine highway bridge inspection condition documentation accuracy and reliability. *Journal of Bridge Engineering, 9*(4), 403–413. https://doi.org/10.1061/(ASCE)1084-0702(2004)9:4(403).

Prasad, K. H., Faruquie, T. A., Joshi, S., Chaturvedi, S., Subramaniam, L. V., & Mohania, M. (2011). *Data cleansing techniques for large enterprise datasets.* April 29135–144. https://doi.org/10.1109/SRII.2011.26.

Qian, X., & Che, X. (2012). Security-enhanced search engine design in internet of things.

*Journal of Universal Computer Science, 18*(9), 1218–1235.

Qiao, H., & Wang, G. (2012). An analysis of the evolution in internet of things industry based on industry life cycle theory. In R. Chen, D. Sun, & W. P. Sung (Eds.). *Frontiers of advanced materials and engineering technology, Pts 1-3* (pp. 785–789). . Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84862928741&partnerID=40&md5=7efea368946ebc1149f867087d911307.

Quinn, R. E., & Hall, R. H. (1983). Environments, organizations, and policymakers: Toward an integrative framework. *Organizational Theory and Public Policy,* 281–298.

Ramos, C., Augusto, J. C., & Shapiro, D. (2008). Ambient intelligence-the next step for artificial intelligence. *IEEE Intelligent Systems, 23*(2), 15–18. https://doi.org/10.1109/MIS.2008.19.

Rathore, M. M., Ahmad, A., Paul, A., & Thikshaja, U. K. (2016). *Exploiting real-time big data to empower smart transportation using big graphs.* 135–139. https://doi.org/10.1109/TENCONSpring.2016.7519392.

Reyes, P. M., Li, S., & Visich, J. K. (2012). Accessing antecedents and outcomes of RFID implementation in health care. *International Journal of Production Economics, 136*(1), 137–150. https://doi.org/10.1016/j.ijpe.2011.09.024.

Rogers, M. E. (1983). *Diffusion of innovations.* The Free Press.

Rogers, E. M. (2010). *Diffusion of innovations.* Simon and Schuster.

Scarfo, A. (2014). Internet of things, the smart X enabler. *2014 International Conference on Intelligent Networking and Collaborative Systems (INCoS),* 569–574. https://doi.org/10.1109/INCoS.2014.98.

Shadbolt, N., O'Hara, K., Berners-Lee, T., Gibbins, N., Glaser, H., Hall, W., & Schraefel, M. C. (2012). Linked open government data: Lessons from Data.gov.uk. *IEEE Intelligent Systems, 27*(3), 16–24. https://doi.org/10.1109/MIS.2012.23.

Skarmeta, A. F., Hernandez-Ramos, J. L., & Moreno, M. V. (2014). A decentralized approach for security and privacy challenges in the internet of things. *2014 IEEE world forum on internet of things (WF-IoT),* 67–72. https://doi.org/10.1109/WF-IoT.2014.6803122.

Skogstad, A., & Einarsen, S. (1999). The importance of a change-centred leadership style in four organizational cultures. *Scandinavian Journal of Management, 15*(3), 289–306. https://doi.org/10.1016/S0956-5221(98)00028-1.

Solomons, N. M., & Spross, J. A. (2011). Evidence-based practice barriers and facilitators from a continuous quality improvement perspective: An integrative review. *Journal of Nursing Management, 19*(1), 109–120. https://doi.org/10.1111/j.1365-2834.2010.01144.x.

Speed, C., & Shingleton, D. (2012). *An Internet of cars: Connecting the flow of things to people, artefacts, environments and businesses.* 11–12. https://doi.org/10.1145/2307874.2307883.

Stephan, E. G., Elsethagen, T. O., Wynne, A. S., Sivaraman, C., Macduff, M. C., Berg, L. K., & Shaw, W. J. (2013). *A linked fusion of things, services, and data to support a collaborative data management facility. 2013 9th international conference conference on collaborative computing: networking, applications and worksharing (Collaboratecom)* 579–584.

Subramanian, A., & Nilakanta, S. (1996). Organizational innovativeness: Exploring the relationship between organizational determinants of innovation, types of innovations, and measures of organizational performance. *Omega, 24*(6), 631–647. https://doi.org/10.1016/S0305-0483(96)00031-X.

Tien, I., Musaev, A., Benas, D., Ghadi, A., Goodman, S., & Pu, C. (2016). *Detection of damage and failure events of critical public infrastructure using social sensor big data.* 435–440.

van Waart, P., Mulder, I., & de Bont, C. (2015). A participatory approach for envisioning a smart city. *Social Science Computer Review, 34*(6), 708–723. https://doi.org/10.1177/0894439315611099.

Vesyropoulos, N., & Georgiadis, C. K. (2013). Web of things: Understanding the growing opportunities for business transactions. *Proceedings of the 6th Balkan Conference in Informatics,* 267–274. https://doi.org/10.1145/2490257.2490287.

Wahyudi, A., Pekkola, S., & Janssen, M. (2018). Representational quality challenges of big data: Insights from comparative case studies. In S. A. Al-Sharhan, A. C. Simintiras, Y. K. Dwivedi, M. Janssen, M. Mäntymäki, L. Tahat, & N. P. Rana (Eds.). *Challenges and opportunities in the digital era* (pp. 520–538). Springer International Publishing.

K. Weber, B.Otto, H. Österle. One Size Does Not Fit All—A Contingency Approach to Data Governance. Journal of Data and Information Quality.(2009). 1, 4:1–4:27.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), 13–23.

Wejnert, B. (2002). Integrating models of diffusion of innovations: A conceptual framework. *Annual Review of Sociology, 28*(1), 297–326. https://doi.org/10.1146/annurev.soc.28.110601.141051.

Wiechert, T. J. P., Thiesse, F., Michahelles, F., Schmitt, P., & Fleisch, E. (2007). *Connecting mobile phones to the internet of things: A discussion of compatibility issues between EPC and NFC, 7*, 4436–4446. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84870202182&partnerID=40&md5=1ac35c9ee485cda5772bf7deed2ae293.

Wu, I.-L., & Wu, K.-W. (2005). A hybrid technology acceptance approach for exploring e-CRM adoption in organizations. *Behaviour & Information Technology, 24*(4), 303–316.

Yazici, H. J. (2014). An exploratory analysis of hospital perspectives on real time information requirements and perceived benefits of RFID technology for future adoption. *International Journal of Information Management, 34*(5), 603–621. https://doi.org/10.1016/j.ijinfomgt.2014.04.010.

Yin, R. K. (2003). *Case study research: Design and methods.* SAGE Publications.

Zeng, D., Guo, S., & Cheng, Z. (2011). The web of things: A survey. *Journal of Communications, 6*(6), 424–438. https://doi.org/10.4304/jcm.6.6.424-438.

Zuiderwijk, A., & Janssen, M. (2014). The negative effects of open government data – Investigating the dark side of open data. *Proceedings of the 15th Annual International Conference on Digital Government Research,* 147–152. https://doi.org/10.1145/2612733.2612761.