A Systematic Review of Impediments Blocking Internet of Things Adoption by Governments

Paul Brous, Marijn Janssen

A Systematic Review of Impediments Blocking Internet of Things Adoption by Governments

Paul Brous[1,2,*] and Marijn Janssen[1]

[1]Delft Technical University, Delft, The Netherlands
{P.A.Brous, M.F.W.H.A.Janssen@tudelft.nl}
[2]Rijkswaterstaat, Delft, The Netherlands

Abstract. The Internet of Things (IoT) has high promises and might provide many benefits, yet has been given scant attention in e-government literature. Within the IoT, physical objects, "things", are networked and connected to the Internet. These "things" are able to identify themselves to and communicate with other devices or "things". There are many impediments blocking the adoption of IoT, and there is limited insight in these barriers. In this paper, impediments for the adoption of IoT are investigated by conducting a literature review and carrying out two case studies. The impediments found in literature were confirmed and extended using the case studies. Results show that impediments are interrelated and occur on the strategic, tactical and operational level. For adoption the impediments needs to be addressed in concert. Research on e-governance can benefit from understanding these interrelated impediments.

Keywords: Internet of Things · IoT · adoption ·open data ·e-governance ·e-government · smart cities · impediments · barriers· challenges

1 Introduction

The term, the Internet of Things (IoT) refers to the increasing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems [1–3]. The IoT makes it possible to access remote sensor data and to monitor and control the physical world from a distance, allowing many physical objects to act in unison, though means of ambient intelligence [1]. These devices and the communication between these devices can benefit e-government by providing enough quality data to generate the information required to make the right decisions at the right time [3], but in order to achieve this, a variety of impediments need to be overcome. For example, Inductive loops embedded in the road surface are a key technology for traffic detection. An inductive loop is a simple and reliable way to detect the movement of vehicles over a road surface and is extensively used in traffic responsive traffic signal systems to collect traffic data to optimise signal timings accordingly [2]. Such loops provide data on traffic density, flows and speeds for trend analysis as well as providing a key input to real-time traffic models which predict queues or delays. However, installing these loops is costly and the flow of traffic can be obstructed during instal-

adfa, p. 1, 2011.

lation. Another example is that of the application of sensors for the inspection and testing of levees (smart levees) in levee management [4], [5]. The sensors embedded in the levees supply a wide range of data. This data is centrally stored and used for the real time visualization of the measurements in a dashboard displaying the sensor results. The data is then directly interpreted for detection and warning systems. These sensors are increasingly being used for the management and monitoring of water barriers, but the technology and the models required to fully analyse the data are still in their infancy and managers are unable to fully trust the system.

The benefits of IoT for governments are known [3] and often emphasized in work. However, less attention has been given to the impediments, or barriers, of IoT, especially with regards to the management and maintenance of large physical infrastructure, have till now not been investigated systematically. Several researchers mention the need for further research in this area [6], [3, 7]. This research explores systematically the potential impediments of the IoT by investigating real world case studies and reviewing state of the art literature.

The methodology used in this research is described in section two. A first overview of IoT impediments will be presented in section three on the basis of state of the art literature. Explorative case studies at the Directorate General of Public Works and Water Management of the Netherlands will be presented in section 4. The Directorate General of Public Works and Water Management of the Netherlands is commonly known within The Netherlands as “Rijkswaterstaat”, often abbreviated to “RWS”, and is referred to as such within this research. RWS is part of the Dutch Ministry of Infrastructure and the Environment and is responsible for the design, construction, management and maintenance of the main infrastructure facilities in the Netherlands. The results of the literature review and the case studies, and the potential impediments of IoT adoption in e-governance will be discussed in section five. The results show that IoT has a variety of potential impediments at the strategic, tactical and operational levels. Finally conclusions will be drawn in section six.

2 Research Method

We followed two main research steps to determine the potential impediments of IoT for e-governance. First the common impediments of IoT were identified from a rigorous review of literature. The keywords: “Internet of Things” (or “IoT”), “impediments” (or “barriers”), and “e-governance”, returned zero hits within the databases Scopus, Web of Science, IEEE explore, and JSTOR. When we replaced the keyword “e-governance” with “governance”, we retrieved the same result. The query [all abstract: ("impediments" OR "barriers") AND “internet of things" AND "e-governance"] searching between 2000 and 2015 returned fifty-five hits in Google Scholar. Removing the word “governance’ totally from the search string returned more results (67, 0, 13, 6, and 3170 hits respectively).

We found that a great deal of these articles mentioned IoT as being a potential facilitator for achieving the goal of a Smart City based on IoT technology, and some touched on the impediments, barriers or challenges of the implementation of IoT, but most articles relied on anecdotal evidence. Very few articles found were of a general

nature. We then filtered these results and performed a forward and backward search and selected relevant articles based on the criteria that they specifically referred to potential impediments, barriers or challenges with regards to the use or implementation of IoT within potential e-governance applications. The results of the literature lead to a framework within which we developed the case studies.

We used explorative case studies to extend and refine the list from literature the potential impediments of IoT within e-governance applications as the second main research method. Two cases were studied within the context of RWS, which gave the researchers access to subject matter experts and internal documentation for all the cases. This helped ensure the construct validity of the case studies [8]. The cases were selected based on their use of IoT for e-governance purposes – the unit of analysis being programmes within RWS which use and develop IoT for e-governance purposes. The Netherlands is an e-participation leader according to the United Nations e-government survey [9] (2014). This contributes to the validity of the cases as being good representations of e-governance. The cases under study were selected from different domains within RWS in order to ensure diversity and external validity through replication logic [8], [10], in which each case serves as a distinct experiment that stands on its own as an analytic unit. The domains selected were road management and water management respectively.

We studied two separate cases to refine and extend the list of benefits from literature. In the Netherlands there are many similarities, but also, subtle differences in how processes are managed between the "wet" or, water management domain and the "dry", or road management domain. For example, when dealing with objects in the water domain, it is not always possible to be highly accurate with regards to location, as objects placed in water are less static and are often more difficult to physically get to than objects on the ground. We felt it necessary to select cases from both these domains in order to gain a more rounded perspective of the implementation of IoT within e-government in the Netherlands. The cases selected were: 1. Sensor information gathered for the purpose of road management; 2. Sensor information gathered for the purpose of water management. The first case deals with sensor information gathered by RWS with regards to traffic and road management. The second case study deals with sensor information gathered by RWS with regards to water management. The case studies were explorative in method and descriptive in nature. Unstructured interviews were held with managers, subject matter experts, and consultants within RWS. Internal documentation was also studied. Finally, the results of the cases were shared with and verified by subject matter experts within RWS. The pattern-matching technique [11] was used to analyse the case study evidence. Such logic compares an empirically based pattern (findings from the case studies) with a predicted pattern suggested by the literature review, strengthening the internal validity of the research [8]. The technique was applied in the following way. First the common impediments of IoT found in literature were listed. These common impediments were then compared with the evidence of the impediments of IoT from the case study analysis. There were several iterations throughout the research as each case introduced new potential impediments. The potential impediments of the IoT are expressed in italics within this paper.

3 Literature Background

Public and private organizations are increasingly turning to the IoT as new sources of data. However, there are several technological and regulatory challenges that need to be addressed. Scarfo (2014) believes that the most important of them are related to data ownership, security, privacy and sharing of information [12]. It is clear that the implementation of IoT for e-governance faces a variety of impediments. We list the possible impediments of IoT according to strategic/political, tactical and operational divisions. This is a popular division [13, 14], which is suitable for e-governance research.

3.1 Strategic/political

Skarmeta et al. (2014) consider security and privacy to be the main obstacles for a full acceptance of IoT [15]. IoT devices generate a huge amount of data. The sensitivity levels of the information, is a crucial aspect to be considered by the access control mechanism. Disclosure of user data could reveal sensitive information such as personal habits or personal financial information. The unauthorized access to this information can severely impact user privacy [12, 15–20].

Data produced by IoT devices can be combined, processed and analysed, creating additional insights, so it is important to allow access to data generated by other IoT devices, whilst preventing the unauthorized access and misuse of this information [15]. However, as the IoT becomes more widespread, new security issues become evident [21]. Ortiz et al. (2013) believe that whilst these technologies have been widely investigated for traditional technologies such as relational databases, so far there are no convincing solutions for providing fine grained access control. This hinders the uptake of IoT in e-governance applications dealing with sensitive data [12, 15–22]. In this way, IoT requires novel approaches to ensure the safe and ethical use of the generated data [23], requiring a strong data governance [12, 18, 19, 24, 25]. A weak form of data governance can impede the safe and ethical use of data generated by IoT devices.

A lack of, or poorly coordinated, policies and regulations regarding IoT can also greatly impede the implementation and application of IoT. According to Misuraca (2009), IoT brings with it a wealth of new business opportunities. There is enormous scope for developing applications and selling new services [26]. Governments need to develop policy and regulations and position themselves carefully within this arena [19, 22, 25]. In this regard, public organisations should consider carefully the role they play in the enabling IoT development in the private sector. Market forces of supply and demand can play substantial roles in the success or failure of IoT [17, 26–28]. For example, according to Qiao et al. (2012) the IoT industry, in the short term, will demonstrate an inevitable outbreak growth at the growth stage of the Industry Lifecyle Theory [29]. The internal mechanism of explosive growth is that the whole networking industry chain achieves linkage development between supply and demand [27], but there is a danger that IoT may miss this linkage development due the chain of IoT industry being blocked by a tactical barriers such as a lack of technology breakthroughs, standards bottlenecks and cost barriers [27].

3.2 Tactical

Although reduction in overall costs is an often cited benefit of IoT for e-governance ([3]), many researchers also cite high development and implementation costs as an important impediment to the implementation and application of IoT for e-governance [17, 19, 22, 27, 30]. According to Yazici (2014), high maintenance costs are often rated as the largest impediments to IoT implementation. A fully functional IoT system based on RFID technology can be substantial. By way of example, Yazici (2014) quotes Wal-Mart's vendors as having spent US$1 to US$3 million on a RFID implementation.

The Internet of things is more than one device, application or network. In order to ensure sustainable connectivity, all interfaces and communication protocols require unified industry standards [17]. However, Fan et al. (2014) believes that the large number of standards-setting organizations has led to a situation in which the top standard has not yet been set. Vendors are free to choose which standard they find best fits their production line, leading to a wide variety of available types which impedes interoperability and integration of data [12, 17, 22, 25, 28, 31]. According to Zeng et al. (2011), there are two methods to integrate things to the Internet: direct integration and indirect integration.

Home appliances are usually directly integrated whilst RFIDs are indirectly integrated through a RFID reader with an embedded server. It is not uncommon for a system to utilise both methods. But IoT requires that a large number of devices be integrated with the existing Internet. These devices can be diverse in terms of data communication methods and capabilities, computational and storage power, energy availability, adaptability, mobility, etc. The heterogeneity at the device level is, in this way, a serious impediment to IoT adoption [16]. This is especially complex as consumers of data are also heterogeneous [16]. Their needs vary in terms of capabilities and data quality. Furthermore, different applications might implement disparate data processing or filtering [16]. Zeng et al (2011) believe that it is these heterogeneity traits of the overall system that make the design of a unifying framework and the communication protocols a very challenging task, especially with devices with different levels of capabilities. This issue is exacerbated in a large distributed environment.

According to Zeng et al (2011), Universal Plug and Play (UPnP) is currently the most popular solution for personal network implementation [16]. However, there is no authentication protocol proposed for UPnP. All devices are allowed to configure the other devices on the personal network, without any user control. This can result in a critical security issue when the smart things become available on the Internet. The attention given to security by a number of authors ([12, 15–18, 22]) suggests that a lack of security standards is becoming a serious impediment to IoT implementation. Whilst there are many standard technologies and protocols to address many security threats, the severe constraints on the IoT devices and networks prevent a straightforward implementation of these solutions [15]. Furthermore, IoT devices generally have to work in harsh, uncontrolled environments, where they may be prone to attacks, misuse or malicious intentions [15]. If a mission critical system is hacked or becomes unavailable, this can lead to a breakdown of trust in the system [15, 17].

According to Kranenburg et al. (2014), the success of user-centric services based on IoT technology depends primarily on people participating and sharing the infor-

mation flows [20]. Willingness on the part of people to participate in these systems is therefore required [16, 17, 19, 21, 24, 28, 30, 32]. Kranenburg et al. (2014) believe that this willingness is predominantly dependent on the perception of people: the perceived trust and confidence in IoT and the perceived value that the IoT generates for them. 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 [20]. A lack of trust in the system can be a strong impediment to the effectiveness of IoT.

3.3 Operational

Operational barriers include human capital issues such as difficulty in employing qualified personnel, lack of specialists, and personnel skill shortage to operate new applications [19, 32], [22], as well as insufficient IoT oriented training and educational activities [22]. Harris et al. (2015) also identify personnel reluctance to change or to learn new technology as a barrier. A lack of understanding about how IoT works, the possible benefits, and how to make the business case for IoT implementation were also found to be barriers by a number of researchers [19, 32–34]. Reyes et al. (2012) also includes calculating the return on investment and the payback period in this category [34].

Operational barriers also include technical issues such as limitations in information technology (IT) infrastructural capabilities [12, 16–20, 28, 35]. According to Scarfo (2014), the main technological challenges include architecture, energy efficiency, security, protocols and quality of service [12]. An important enabler for the IoT is to permit others to access and use the things that have been published publicly on the internet. It 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 [31]. This requirement means we need a sophisticated set of mechanisms to publish and share things and ways to find and access those things [31]. A lack of these mechanisms as well as the level of knowledge required to implement, manage and maintain the available toolsets can form an important barrier to implementing IoT for e-governance purposes.

Data management issues are also of concern. Public organisations are often faced with a complex legacy of data and applications when implementing IoT solutions [24]. Many public organisations may have several generations of systems running in parallel, and much of the data fed into the system has been done manually, with associated risks in terms of data quality [24, 25, 31].

In short, IoT faces a variety of barriers related to the proper use (privacy and security for example) and proper management of the data collected by the vast number of interconnected things. *Strategic/political barriers are: data privacy issues, data security issues, weak or uncoordinated data policies, weak or uncoordinated data governance, and conflicting market forces. Tactical barriers include: costs, interoperability and integration issues, acceptance of IoT, and trust related issues. Operational issues are: a lack of sufficient knowledge regarding IoT, IT infrastructural limitations, and data management issues.*

4 Case Studies

The goal of the case study research was to refine and extend the list of impediments from literature and to understand the real life impediments of IoT in the most complete way possible. The case study research therefore involved the use of multiple data collection methods. The cases were selected from the primary processes of RWS. Generally IoT is implemented in RWS with the specific intention of ensuring the good working of the primary processes to achieve the primary objectives. In RWS there is a subtle divide in how processes are managed between the water management domain and the road management domain. In order to gain a rounded perspective of the benefits of IoT within RWS, it was believed necessary to select cases from both these domains.

4.1 Case Study 1: Road Management Data Collection at RWS

RWS builds, manages and maintains the Dutch national highways. Correct data is required to do this effectively. Over the years, RWS has developed several methods for obtaining the necessary data from the highways it manages, collecting, processing and making the data available to traffic and road management teams. Measurements are generally made by placing sensors in the road in many different locations. These sensors produce large amounts of data which is mainly used in mid-term planning, long term projections, air quality predictions and noise calculations which have an impact on health and safety measures as well as the environmental impact, and improving service efficiency with regards to road works management.

RWS has created a national network of monitoring points, the "Weigh in Motion" (WIM) network. 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 [36], [37]. Effectively reducing overloading reduces the damage to the road infrastructure, lengthening the road's lifetime and reduces the frequency of maintenance. 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. The WIM system is one of the most advanced measuring systems in the world. Between 2010 and 2013, RWS built a nationwide WIM network with a total of 18 measuring points. The network consists of 6 newly remodelled measuring stations and 12 new measuring stations. The network provides access to the actual load of the main road, about peak times when it comes to overcharging and it provides RWS with the ability to collect information concerning the compliance behaviour of individual carriers. This forms the basis for business inspections and legal follow-up programs.

RWS faces and has faced a variety of impediments and challenges during the implementation and maintenance of the WIM network. There are different perceptions of the level of ambition pursued by the WIM maintenance process. For example, According to RWS officials, RWS has not yet implemented a structured learning cycle with regards to data quality - "the quality of the data has not been quantified, and solving data quality issues is incident driven". In this regard, learning takes place in

practice and is not formally addressed. Although there have been no direct accusations made between departments, there is also little inter-departmental trust exhibited. According to RWS officials, "Implementation of new technology takes too long, and the implementation process is difficult to follow". There appears to be insufficient knowledge and expertise within the CID to independently manage the WIM systems [38]. The CID reports only on the technical availability of the systems and no information can be provided regarding the performance of the WIM network. RWS is unable to guarantee the reliability of the data due to a lack of a framework of standards. Requirements that exist for managing WIM are not included in the project tender. In 2011, the management of the database with the WIM data was transferred to the Inspectorate General for the Environment and Transport (IET). However the related expertise was not successfully shared. At the present moment, RWS has no access to the data held in the IET databases. The technical requirements were incomplete and some still need to be developed. IET systems are not yet ready to automatically manage the data. There are several legacy issues as technical management is only focused on the availability of the current IT systems. At the time of writing there were technical problems with the license plate recognition system. Governance and mandate appears unclear – it is unclear how the process is coordinated, and the IT supply organisation, the Central Information Department (CID), is unaware that they are also responsible for the sharing of data within the WIM systems. There is no single substantive authority that brings the parties from the entire supply chain together (there is no single authority that assumes responsibility for the entire chain). There is no well-designed change process; changes in the maintenance process are difficult to implement. The representative of the CID in the steering committee has no mandate.

The impediments for the adoption of IoT by e-governance identified in this case are: *1. Strategic/political barriers: data privacy issues, weak or uncoordinated data policies, weak or uncoordinated data governance, and conflicting market forces. Tactical barriers include: interoperability and integration issues, acceptance of IoT, and trust related issues. Operational issues are: a lack of sufficient knowledge regarding IoT, IT infrastructural limitations, and data management issues.*

4.2 Case Study 2: Water Management Data Collection at RWS

Information regarding water quantity and water quality is essential for the primary processes of Rijkswaterstaat: ensuring that flooding does not occur, sufficient clean water and smooth and safe traffic on the water. RWS also collects data on biology and chemistry, measuring nutrients and (micro) pollutants in surface water, suspended matter, sediment and aquatic animals.

The National Water Measurement Network, at RWS known as "Landelijk Meetnet Water" (LMW), is a facility that is responsible for the acquisition, storage and distribution of data for water resources. LMW has more than 400 data collection points using a nationwide system of sensors. The data is then processed and stored in the data centre and is made available to a variety of systems and users. The LMW was created from the merger of three previous existing monitoring networks: the Water Monitoring Network, which monitored inland waterways such as canals and rivers; the Monitoring Network North, which monitored North Sea oil platforms and chan-

nels; and the Zeeland Tidal Waters Monitoring Network which monitored the Zeeland delta waterways. Four main types of measurement activities can be identified: water quantity, water quality, meteorological data and control information on infrastructure. The LMW measures a wide variety of hydrological data such as water levels, flow rates, wave heights and directions, flow velocity and direction, and water temperature. The LMW also measures meteorological data such as wind speed and direction, air temperature and humidity and air pressure amongst others. This meteorological data is collected in close collaboration with the Dutch Royal Meteorological Institute. The LMW provides a complete technical infrastructure for gathering and distribution of data and delivers the data to various stakeholders within and outside RWS.

According to RWS officials, there is often not clear who is ultimately responsible for the entire information chain. It has been discovered that the different departments work with different targets [39]. For example, the goals of the project organisation are to get production legitimacy of payment and to execute system contract management whilst the goals of the asset manager are to prevent flooding, to show demonstrable compliance with the statutory requirements and to reduce probability of failure. This results in different levels of the organization addressing different points of discussion. RWS officials report that a major impediment is "the lack of agreement and decision-making regarding vital strategic choices such as the form of contract management, the tender strategy, and outsourcing of personnel". The experience is that there is a failure to align the implementation with business targets as management teams tend to focus purely on the supply chain with a lack of awareness for possible risks or opportunities that occur outside of the supply chain. Whilst agreements occur between management teams, collaboration does not always occur in operations. There appear to be significant impediments regarding the coordination of activities and projects. RWS officials also quoted a lack of trust in the private sector to be able to manage and maintain the systems adequately. The perspective of RWS is that the private sector is not adequately developed regarding the necessary technical knowledge required by such an intricate system. RWS officials have stated that one of the reasons for this perspective is the intricacy of the RWS technical architecture itself. The experience is that the current architecture and legacy data make future integration of data very difficult.

The impediments for the adoption of IoT by e-governance identified in this case are: *1. Strategic/political barriers: data security issues, weak or uncoordinated data policies, weak or uncoordinated data governance, and conflicting market forces. Tactical barriers: interoperability and integration issues, acceptance of IoT, and trust related issues. Operational issues: a lack of sufficient knowledge regarding IoT.*

5 Discussion

The objective of this research was to identify potential impediments of the IoT for e-governance purposes. The IoT is important because a physical (or sensor) object that is able to communicate digitally is able to relate not only to a single entity, but also becomes connected to surrounding objects and data infrastructures. This allows for a situation in which many physical objects are able to act in unison, by means of ambient intelligence [1]. These devices and the communication between these devices

can benefit e-government by providing enough quality data to generate the information required by government and citizens to make the right decisions at the right time.

We used two main research methods: (1) a literature review, (2) analysis of two IoT case studies. The literature review provided us with an overview of the existing body of knowledge, allowing us to analyse where gaps in knowledge or focus occur. It also provided definitions for the key concepts and helped develop a broader knowledge base in the research area. Case study research is a widely used qualitative research method in information systems research, and is well suited to understanding the interactions between information technology-related innovations and organizational contexts [40]. Following the advice of Yin (2003), the protocol used in the case study included a variety of data collection instruments. In order to counter the possible influences of bias, multiple research instruments were employed to ensure construct validity through triangulation [8].

The results of the literature review and the case studies demonstrate that the IoT is faced with a variety of impediments with regards to adoption b which correlates with impediments identified in the literature review. Table 1 below lists the main impediments of IoT, differentiating between strategic, tactical and operational benefits.

Table 1. Impediments of IoT for e-governance in relation to the case studies.

		Impediments	**Literature**	**Case 1**	**Case 2**
Strategic	Social Responsibility	Data privacy issues	✓	✓	
		Data security issues	✓		✓
		Lack of legal framework	✓	✓	✓
	Productivity	Weak or uncoordinated data policies	✓	✓	✓
		Weak or uncoordinated data governance	✓	✓	✓
	Market standing	Conflicting market forces	✓	✓	✓
Tactical	Profitability	Costs	✓		
	Physical resources	Interoperability and integration issues	✓	✓	✓
		Lack of a framework of standards	✓	✓	✓
	Worker attitude	Acceptance of IoT	✓	✓	✓
		Trust related issues	✓	✓	✓
Operational	People	Lack of sufficient capabilities/ knowledge	✓	✓	✓
	Technology	IT infrastructural limitations (issues with	✓	✓	

	Impediments	Literature	Case 1	Case 2
	legacy systems)			
Processes	Data management issues (data quality issues)	✓	✓	

Formulating strategy requires defining goals and initiatives based on available resources and an assessment of the internal and external environments in which the organization competes [41]. Strategic impediments can therefore exert an important influence on an organization's likelihood of success. IoT is capable of providing a continuous stream of "trusted" data which managers can use to make informed, decisions, but the adoption of IoT for this purpose needs to be carefully coordinated by strong data policies and strong governance of the data with a purposeful awareness of opposing market forces and the capability of the private sector to provide critical services. Public sector organisations also need to address data privacy and data security issues for IoT adoption to be successful. These issues are interrelated as legal frameworks and strong policies provide guidelines within which organisations can face the pitfalls placed by security and privacy issues.

The main impediments appear to manifest during implementation, once organisations decide to operationalize the business plan. At that stage it becomes clear that although the technology is ready for widespread implementation, IoT remains an innovation which needs to not only integrate with current legacy systems but for which standards, policy, and legal frameworks still need to be developed with regards to social, technical and ethical issues.

Achieving a strategic plan or objective requires the administrative process of selecting among appropriate ways and means. Tactical planning is short range planning that emphasizes the current operations of various parts of the organization [42]. The case studies show that a good deal of attention should be paid to coordinating "soft", organisational issues such as trust and acceptance of IoT solutions as well as to the coordination of harder, technical, issues which require standardization in order to ensure interoperability and integration of data and systems. Significantly, costs were only mentioned in the case studies as an impediment with regards to a negative business case. Since the primary processes of RWS are directly connected with health, safety and security of Dutch citizens, cost was disregarded as secondary to achieving the primary objective. It is possible that cost may be a more significant impediment in countries with less accessibility to the necessary funding than RWS.

A primary use of IT in government is to improve the efficiency of government operations [43]. As with many other organisations RWS uses IoT as a tool in industrial automation, in which simple manual tasks such as opening and closing bridges are automated. This reduces very low-level coordination work that was previously executed by humans, but complete automation or outsourcing of work can lead to a lack of sufficient knowledge within the organisation regarding the technique and the management of the data. This situation can develop into a significant impediment to the maintenance of IoT in e-governance applications. Technology continues to advance,

but whilst many RWS officials were confident that technology was generally not a serious impediment, it is important to ensure that chose technique is compatible with the IoT architecture.

6 Conclusion

This paper represents one of the first papers on IoT for e-government. There has been limited research in the field of e-government regarding IoT, and there is much potential as expressed by the potential benefits, but the adoption of IoT within e-governance applications requires careful preparation and coordination. The IoT makes it possible to access remote sensor data and to monitor and control the physical world from a distance, and combining and analysing captured data allows governments to develop and improve services which cannot be provided by isolated systems, but this can only be achieved by addressing the potential impediments of to IoT adoption at all levels.

This research provides a systematic insight into the potential impediments of the IoT for e-government purposes by means of case study analysis and a review of literature. The research shows that impediments range from the political to the operational level. Specifically impediments for e-government can be attributed to data privacy issues, data security issues, weak or uncoordinated data policies, weak or uncoordinated data governance, and conflicting market forces, costs, interoperability and integration issues, acceptance of IoT, and trust related issues, a lack of sufficient knowledge regarding IoT, IT infrastructural limitations, and data management issues.

Many of the issues are interrelated; interoperability and integration issues have a direct impact on costs and on trust in the systems, and many issues can be resolved with sufficient knowledge and capabilities within the organisation. But the issues do need to be resolved in concert. It is important that governments address dominant impediments, such as privacy and security issues, within public policy and legal frameworks to assist public organisations with implementation of IoT. Similarly, technical and knowledge issues are very much interrelated with a lack of standards and impediments regarding interoperability and integration of data.

Acknowledgements

We acknowledge and thank the people of the Rijkswaterstaat who gave of their time and expertise during the case study research. This research is funded by Rijkswaterstaat.

References

1. Ramos, C., Augusto, J.C., Shapiro, D.: Ambient Intelligence-the Next Step for Artificial Intelligence. IEEE Intell. Syst. 23, 15–18 (2008).

2. Hounsell, N.B., Shrestha, B.P., Piao, J., McDonald, M.: Review of urban traffic management and the impacts of new vehicle technologies. IET Intell. Transp. Syst. 3, 419–428 (2009).
3. Brous, P., Janssen, M.: Advancing E-Government Using the Internet of Things: A Systematic Review of Benefits. Presented at the IFIP Egov (2015).
4. Stichting Ijkdijk: livedijk-utrecht, http://www.ijkdijk.nl/nl/livedijken/livedijk-utrecht.
5. RTV Utrecht: Proef met dijksensoren in Woerden en Nieuwegein, http://www.rtvutrecht.nl/nieuws/859256/proef-met-dijksensoren-in-woerden-en-nieuwegein.html.
6. Marche, S., McNiven, J.D.: E-Government and E-Governance: The Future Isn't What It Used To Be. Can. J. Adm. Sci. Rev. Can. Sci. Adm. 20, 74–86 (2003).
7. Haller, S., Karnouskos, S., Schroth, C.: The internet of things in an enterprise context. Springer (2009).
8. Yin, R.K.: Case Study Research: Design and Methods. SAGE Publications (2003).
9. United Nations, Department of Economic and Social Affairs: United Nations e-government survey 2014: e -government for the future we want. United Nations, New York (2014).
10. Eisenhardt, K.M.: Building Theories from Case Study Research. Acad. Manage. Rev. 14, 532–550 (1989).
11. Trochim, W.M.: Outcome pattern matching and program theory. Eval. Program Plann. 12, 355–366 (1989).
12. Scarfo, A.: Internet of Things, the Smart X enabler. In: 2014 International Conference on Intelligent Networking and Collaborative Systems (INCoS). pp. 569–574 (2014).
13. Ivanov, D.: An adaptive framework for aligning (re)planning decisions on supply chain strategy, design, tactics, and operations. Int. J. Prod. Res. 48, 3999–4017 (2010).
14. Ackoff, R.L.: Towards a System of Systems Concepts. Manag. Sci. 17, 661–671 (1971).
15. Skarmeta, A.F., Hernandez-Ramos, J.L., Moreno, M.V.: A decentralized approach for security and privacy challenges in the Internet of Things. Presented at the 2014 IEEE World Forum on Internet of Things, WF-IoT 2014 (2014).
16. Zeng, D., Guo, S., Cheng, Z.: The web of things: A survey. J. Commun. 6, 424–438 (2011).
17. Fan, P.F., Wang, L.L., Zhang, S.Y., Lin, T.T.: The research on the internet of things industry chain for barriers and solutions. (2014).
18. Hummen, R., Henze, M., Catrein, D., Wehrle, K.: A Cloud design for user-controlled storage and processing of sensor data. Presented at the CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science (2012).
19. Yazici, H.J.: An exploratory analysis of hospital perspectives on real time information requirements and perceived benefits of RFID technology for future adoption. Int. J. Inf. Manag. 34, 603–621 (2014).
20. Kranenburg, R.V., Stembert, N., Victoria Moreno, M., Skarmeta, A.F., L´opez, C., Elicegui, I., S´anchez, L.: Co-Creation as the Key to a Public, Thriving, Inclusive and Meaningful EU IoT. (2014).
21. Ortiz, P., Lazaro, O., Uriarte, M., Carnerero, M.: Enhanced multi-domain access control for secure mobile collaboration through Linked Data cloud in manufacturing. In: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a. pp. 1–9 (2013).
22. Harris, I., Wang, Y., Wang, H.: ICT in multimodal transport and technological trends: Unleashing potential for the future. Int. J. Prod. Econ. 159, 88–103 (2015).
23. Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Computer. 44, 51–58 (2011).

24. Gilman, H., Nordtvedt, J.-E.: Intelligent energy: The past, the present, and the future. SPE Econ. Manag. 6, 185–190 (2014).
25. Stephan, E.G., Elsethagen, T.O., Wynne, A.S., Sivaraman, C., Macduff, M.C., Berg, L.K., Shaw, W.J.: A linked fusion of things, services, and data to support a collaborative data management facility. In: 2013 9th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom). pp. 579–584 (2013).
26. Misuraca, G.: Futuring e-Government: Governance and Policy Implications for Designing an ICT-enabled Knowledge Society. In: Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance. pp. 83–90. ACM, New York, NY, USA (2009).
27. Qiao, H., Wang, G.: An analysis of the evolution in Internet of Things industry based on industry life cycle theory. (2012).
28. Wiechert, T.J.P., Thiesse, F., Michahelles, F., Schmitt, P., Fleisch, E.: Connecting mobile phones to the internet of things: A discussion of compatibility issues between EPC and NFC. Presented at the Association for Information Systems - 13th Americas Conference on Information Systems, AMCIS 2007: Reaching New Heights (2007).
29. Audretsch, D.B., Feldman, M.P.: Innovative clusters and the industry life cycle. Rev. Ind. Organ. 11, 253–273 (1996).
30. Nam, T., Pardo, T.A.: The changing face of a city government: A case study of Philly311. Gov. Inf. Q. 31, Supplement 1, S1–S9 (2014).
31. Blackstock, M., Lea, R.: IoT mashups with the WoTKit. In: Internet of Things (IOT), 2012 3rd International Conference on the. pp. 159–166 (2012).
32. Speed, C., Shingleton, D.: An Internet of cars: Connecting the flow of things to people, artefacts, environments and businesses. Presented at the Sense Transport'12 - Proceedings of the 6th ACM Workshop on Next Generation Mobile Computing for Dynamic Personalised Travel Planning (2012).
33. Pedro M. Reyes, Patrick Jaska: Is RFID right for your organization or application? Manag. Res. News. 30, 570–580 (2007).
34. Reyes, P.M., Li, S., Visich, J.K.: Accessing antecedents and outcomes of RFID implementation in health care. Int. J. Prod. Econ. 136, 137–150 (2012).
35. Prasad, K.H., Faruquie, T.A., Joshi, S., Chaturvedi, S., Subramaniam, L.V., Mohania, M.: Data Cleansing Techniques for Large Enterprise Datasets. Presented at the SRII Global Conference , San Jose, USA April 29 (2011).
36. Mulyun, A., Parikesit, D., Antameng, M., Rahim, R.: Analysis of Loss Cost of Road Pavement Distress due to Overloading Freight Transportation. J. East. Asia Soc. Transp. Stud. Vol. 8, 1020–1035 (2010).
37. Bagui, S., Das, A., Bapanapalli, C.: Controlling Vehicle Overloading in BOT Projects. Procedia - Soc. Behav. Sci. 104, 962–971 (2013).
38. Evert, H., Servaas van der Valk, W.: A3 Weigh in Motion, (2013).
39. Hopman, F., Meijer, E., Cyt, A., Piarelal, S., Hoogervorst, O.: RWS LMW HHS Adviesrapport.docx.
40. Janssen, M.: Designing electronic intermediaries: An agent-based approach for designing interorganizational coordination mechanisms, (2001).
41. Nag, R., Hambrick, D.C., Chen, M.-J.: What is strategic management, really? Inductive derivation of a consensus definition of the field. Strateg. Manag. J. 28, 935–955 (2007).
42. Tactical planning vs strategic planning, https://managementinnovations.wordpress.com/2008/12/10/tactical-planning-vs-strategic-planning/.
43. Castro, D.: Digital Quality of Life: Government. Available SSRN 1285002. (2008).