Distrust as a Hazard for Future Sustainable Mobility Planning. Rethinking Employees’ Vulnerability When Introducing New Information and Communication Technologies in Local Authorities


Author post-print (accepted) deposited by Coventry University’s Repository

Original citation & hyperlink:

DOI 10.1080/10447318.2020.1860547
ISSN 1044-7318
ESSN 1532-7590

Publisher: Taylor and Francis

This is an Accepted Manuscript of an article published by Taylor & Francis in International Journal of Human-Computer Interaction on 01/01/2021, available online: http://www.tandfonline.com/10.1080/10447318.2020.1860547

Copyright © and Moral Rights are retained by the author(s) and/ or other copyright owners. A copy can be downloaded for personal non-commercial research or study, without prior permission or charge. This item cannot be reproduced or quoted extensively from without first obtaining permission in writing from the copyright holder(s). The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the copyright holders.

This document is the author’s post-print version, incorporating any revisions agreed during the peer-review process. Some differences between the published version and this version may remain and you are advised to consult the published version if you wish to cite from it.
Distrust as a hazard for future sustainable mobility planning. 
Rethinking employees’ vulnerability when introducing new information and communication technologies in Local Authorities

Ann-Marie Nienaber\textsuperscript{a}, Sebastian Spundflasch\textsuperscript{b}, Andre Soares\textsuperscript{c}, and Andree Woodcock\textsuperscript{d}

\textsuperscript{a}Centre for Trust, Peace and Social Relations, Coventry University, Coventry, UK;
\textsuperscript{b}Faculty for Electro and Information Technology, Ilmenau University, Germany;
\textsuperscript{c}Institute for Advanced Manufacturing and Engineering (AME), Coventry University
\textsuperscript{d}Centre for Arts, Memory and Communities, Coventry University, Coventry, UK

*corresponding author Ann-Marie Nienaber, Professor in Human Resource Management and Organisational Behaviour, Centre Trust, Peace and Social Relations at Coventry University, UK; email. ann-marie.nienaber@coventry.ac.uk
Distrust as a hazard for future sustainable mobility planning.
Rethinking employees’ vulnerability when introducing new information and communication technologies in Local Authorities

The implementation of innovative technologies to support the planning and implementation of new transport schemes in cities requires staff to not only gain appropriate technical capabilities, but also to have the willingness to adopt innovative technologies. Taking a sociotechnical approach, focussing on the Technology-Acceptance Model (TAM), we highlight employees’ distrust and unwillingness to become vulnerable as additional challenge for Local Authorities (LAs) to cope with the introduction of new information and communication technologies (ICTs) for mobility solutions in their transport departments. Using data from semi-structured interviews and workshops held across Europe (conducted as part of H2020 CIVITAS SUITS), two key indicators have been identified relating to the unwillingness of potential users to adopt new technologies for mobility solutions, i.e., incongruence of values and attribution of negative motives. Furthermore, we show behavioural intentions’ that indicate that users’ are not willing to become vulnerable and thus, provide evidence of signs for an organisation to look for that may show that the likelihood of their technological implementation is relatively high. The practical guidelines provided at the end of the paper have been derived from our experiences of introducing new technologies for mobility solutions in partner cities of the SUITS project and highlight how users’ can be persuaded to ‘become vulnerable’ and actual using new technologies for future mobility solutions.

Keywords: Local Authorities, new technology adoption, transport, trust, vulnerability
Introduction

The rapid developments in the field of information and communication technologies (ICT) have changed the mobility sector over the last few years. New mobility services and service providers have entered the market exploiting the possibilities offered by innovative ICT to provide new mobility options for the users and simplify their use. Cities are transforming into smart cities, in which ICTs collect and process huge amounts of data. Within the transport sector, sensor technology captures traffic flows and data on air pollution in real time, intelligent information and support systems facilitate the search for parking spaces or simplify the use of public transport and complementary micro-mobility services. At the same time, these systems provide data on travel behaviour and utilization rates that may inform the planning of future transport systems and more bespoke services (not always within the transport sector) Local Authorities (LAs) are responsible for shaping the mobility systems of their cities, and need to be mindful of the opportunities and risks arising from new technologies and data.

The implementation, integration and use of such systems presents a major challenge for smaller LAs. Wide scale introduction of technologies, the huge amount of data generated by sensor technology and its potential use in informing a wide scale city transformation, has left public sector employees threatened in a number of substantive ways and made them feel vulnerable. When people have to cope with ICTs\(^1\), they are not familiar with, they have to be willing to feel vulnerable as they progress along the learning curve. They have to develop positive expectations that this new technology will not harm them (e.g. through redundancy or making their job harder), or their cities in

\(^1\) In the following we refer to the broader term technology.
the long-run (e.g. through misuse of data, unfavourable benchmarking) (e.g. Nienaber and Schewe, 2014) and that the technologies will lead to better outcomes for them and their city. On the one hand, employees have to understand how a new technology will contribute to the goals and strategies of their business, but at the same time they need to realize how that technology is congruent to their own values and expectations and what impact it will have on their daily work.

Without such conformations, there is a high risk that employees won’t support fully buy into the technology, because they may be afraid, for example, that new ways of working will take more time and effort, that their productivity may decline while they are learning to use the system, or that they will not be able to understand how to use it – leading to ridicule and negative staff appraisals. In other words, they fear to become vulnerable. Following Chambers (2006), vulnerability is defined as exposure to contingencies and stress, and difficulty in coping with them since vulnerability comprises an external side of risks, shocks and stress to which an individual is subject; and an internal side which is defencelessness, meaning a lack of means to cope without damaging loss” (p. 33).

Having positive expectations towards a new technology such as urban transport management systems, and the willingness to become vulnerable when adopting and actual using it, are the key elements of trust (Rousseau, Sitkin, Burt, and Cramerer, 1998; Nienaber, Hofeditz, and Romeike, 2015b). Trust is correspondingly the key factor for the actual use of new ICTs (Nienaber and Schewe, 2014). When employees are not willing to become vulnerable and may not share positive expectations towards a new technology, distrust may occur. Following Bijlsma-Frankema and colleagues (2015) distrust is a psychological state, comprising the unwillingness to accept vulnerability, based on negative perceptions and expectations.
Accordingly, distrust in our context is the unwillingness by potential users to become vulnerable and the expectation that the technology may harm them (e.g. failures may likely, expectation of poor benefit, etc.) or their city. Failures in transport systems may be catastrophic for citizens and significantly reduce the quality of life and the attraction of a city. In the literature distrust has been connected to a variety of negative consequences such as a lack of cooperation (Cho, 2006), the avoidance of interaction (Bies and Tripp, 1996), or the unwillingness to share knowledge or information (Bijsma-Frankema, Weibel, and Sitkin, 2015). Distrust can therefore be conceptualised as an unrecognised and neglected hazard that derives from feelings of not willing to become vulnerable, which consequently leads to non-use of a new technology. In operational terms, this means that where employees are reluctant to use, or slow to understand technology, implementation will be delayed, or impeded, or in the worst case expensive systems will simply not be used. Thus, tackling distrust is crucial for forecasting people’s attitudes and behaviours and therefore for accepting and adopting new ICTs (e.g. Van de Walle & Six, 2014).

This paper is based on the authors’ experiences of trying to introduce ICT to small-to-medium LAs wishing to implement sustainable transport measures. It is believed that big, open source data collection and analysis, will lead to new insights and better transport planning. It is also ‘believed’ that even more benefits can be accrued by linking up data sets across departments e.g. combining data from land use, transport, environmental sensing and public health and comparing data across cities. For traditional LAs, which may operate in quite rigid silos, interdepartmental working and sharing of data is a challenge in itself, even without the introduction of new ICT.

We highlight the importance of the employees’ perspective in technology implementation. Thus, we present a unique approach to understanding technology
acceptance, in the context of future mobility planning, using research from psychological and business-related scholars to re-imagines hazard and resilience as issues of distrust, understood via attention towards lived experiences of vulnerability. This approach is based on sociotechnical systems theory that recognises the importance of behavioural change when implementing technological innovation (e.g. Cherns, 1976, 1987; Clegg, 2000).

The paper draws on the results from thematic multi-stage analysis of semi-structured interviews and workshops with representatives of transport planning departments across Europe, who are in the process of implementing new technology. Best practise examples will be shown of how LAs can reduce employees’ vulnerability, enhance their employees’ resilience and foster the implementation of new technology. Although the research takes place in the context of mobility it may be applicable to other departments in LAs, e.g. public health, environment and energy all of which are facing similar problems.

The structure of the paper is as follows. Firstly, the theoretical foundation of vulnerability and trust in relation to technology adoption will be introduced, followed by a description of the negative consequences, which may result from an unwillingness to become vulnerable. From this, a theoretical framework will be developed based on recent findings regarding the Technology-Acceptance Models (TAM). The thematic multi-step analysis coding of comprehensive interview and workshop material, has enabled us to develop this framework by indicating behavioural intentions that may trigger unwillingness to become vulnerable and its negative consequences. Finally, we describe best practises in guidelines on a) how to reduce the chances of a user being unwilling to become vulnerable and b) how to overcome this.
Theoretical framework

Trust and users’ vulnerability when implementing new ICTs for mobility solutions

The implementation of new mobility solutions adopting ICTs brings new challenges to small, traditional organisations, in our case in relation to future sustainable mobility planning. Organisations have to become more effective and resilient to new ICTs and new ways of working in order to gain the benefits they bring. However, most change programmes focus solely on technological or/and technical change highlighting the importance of training and seminars to enhance employees’ abilities to cope with these innovations, but ignore the importance of social and behavioural aspects. As such they may end up failing (e.g. Nienaber and Schewe, 2014; Nienaber, Spundflasch, and Soares, 2019) or creating deep concern among employees.

In this paper, in line with Rousseau and colleagues (1998), we define trust as the individual willingness to be vulnerable based on positive expectations that another party will not take advantage of this vulnerability. In relation to the implementation of new technology we can define trust as the individual willingness to be vulnerable based on positive expectations towards a new technology and its possible benefit for the individual. Scholars highlighted that trust consist of two components: the affective side called the vulnerability and the cognitive side describing the positive expectations towards another party (Nienaber et al. 2015b). In the area of public management, we have to consider additionally, that LAs have a commitment and responsibility to their city and its citizens. They may therefore have an added burden in technology adoption. They do not want to put their citizens at risk (e.g. from data breaches), they do not want their citizens to be exploited (e.g. through the selling of data), and they want the best possible city.
The affective side of trust has been not well documented (see Nienaber et al., 2015b). We believe that one of the key reasons for failures in the implementation in organisations is the perceived individual vulnerability when it comes to the actual use of the new technology. Although users of a particular technology may perceive its’ usefulness and also may be understand how easy its’ use might be, they are still not willing to use it since they are afraid of its’ consequences for themselves and their city. In this paper, we want to elaborate whether this affective side of trust, thus the vulnerability, plays a vital role here.

In terms of sociological factors, Chambers (2006) explained vulnerability by means of two indicators: external threats and a lack of internal coping mechanisms. When implementing new technology in an organisation (e.g. new financial systems, conference systems), external threats may relate, for example to the lack of transparency of a potential supplier (e.g. where is the data stored, who potentially has access to it within and externally to the organisation) or the complexity of the technological solution. Internal coping mechanisms relate to the final end user, who may feel cognitively challenged or overwhelmed by the thought of the new system and the added demands this may place on them. Inculcated and familiar with old ways of working and tacit knowledge of how things work, they may not have positive expectations about the new technology. Also if they are viewed as or see themselves as expert user with former system, they may be unwilling to become vulnerable when learning to use the new system (e.g. through loss of prestige and respect).

Our argument, in line with sense-making theory, suggests that risky experiences such being in unfamiliar situations, are characterized by negative feelings in the form of disorientation or foreignness (Louis, 1980). Following Weick and colleagues (2005), the key question related to sense-making is ‘same or different?’ As long as something
seems to be similar to something well known already, individuals perceive it as less risky and thus, may have positive feelings towards it (e.g. a system upgrade as opposed to new software environment). This means that when a new technology is implemented and perceived as familiar and/or can be connected to something well known, the implementation and actual use of the new technology is very likely. Whereas, something that is not known and very different from previous experiences might be perceived as threatening and thus, employees do not want to become vulnerable and accordingly may not use it. This may result in implementation failure or suboptimal use.

_Distrust as negative consequence of users’ unwillingness to become vulnerable_

Distrust is defined in several ways, either in contrast to trust (e.g. Lewicki and Tomlinson 2003), or as a distinct concept, in which it is described in terms of confident negative expectations and perceptions about the intentions and beliefs of another party (Lewicki, McAllister, and Bies 1998; Lewicki, Tomlinson and Gillespie, 2006). In this paper, distrust is defined as a psychological state, comprising the unwillingness to accept vulnerability, based on pervasive negative perceptions and expectations towards someone or something unknown (in line with Bijlsma-Frankema et al., 2015).

Research has consistently shown the negative consequences of distrust that can harm organisations trying to implement new technologies. One key consequence is the avoidance of interaction with the new technology or its suppliers (Bies and Tripp, 1996; Bijlsma-Frankema, 2004; Bijlsma-Frankema et al., 2015; March and Olsen, 1975). The rationale for this is that potential users try to reduce or prevent future harm. This is accompanied at the organisational level by less knowledge, increased knowledge hiding and levels of conflict (Sitkin and Bijlsma-Frankema, 2018). All these become real obstacles when trying to introduce new technology. The unwillingness to interact with a technology and act cooperatively with higher management (who commissioned it) will
hinder implementation as employees will not adopt and use the technology as planned. Even worse, when some potential users perceive the technology as harmful, distrust may spread from one employee to another. This will lead to a distrustful climate across the organisation which will impede further changes or technologies (pervasiveness of distrust, see Bijlsma-Frankema et al., 2015).

**Technological Adoption Model extended by users’ vulnerability**

The adaptation and the use of new technologies presents a central challenge for organisations and is a key research topic in the field of “Information Systems”. While organisations invest a lot of money and effort on new technology, managers may not see the [expected] increases in productivity. This may be due to lower rates of new technology (Sichel, 1997), as employees fall back to old ways of working (especially when they encounter difficulties). Given the increasing ubiquity of technology, user acceptance of it, needs further research. The Technology Acceptance Model (Davis, 1989; Davis, Bagozzi, and Warshaw, 1989) (TAM) makes substantial theoretical and empirical support to address this challenge. This model compares favourably with alternative models such as the Theories of Reasoned Action (TRA) and of Planned Behavior (TPH) (Venkatesh, 1999). TAM theorizes that an individual’s behavioural intention to use a new technology is based on two different beliefs: the perceived usefulness and the perceived ease of use. While the perceived usefulness can be defined as the extent to which a person believes that using the new technology will improve his or her job performance, perceived ease of use describes the extent to which a person believes that using the new technology will not result in an increased effort.

Several meta-analyses have demonstrated that TAM is a valid and powerful model. Lederer and colleagues (2000) for example proved the predictability of the model for different technologies in their analysis of over fifteen studies over a period of
10 years (from 1989 to 1999). They looked at the relations between factors such as perceived ease of use, perceived usefulness, attitude to use, and actual use of ICTs and were able to state that the model showed a high level of predictability. King and He (2006) analysed eighty-eight different published studies that had used TAM and were able to confirm that the model can be used in a wide variety of contexts. Based on these findings, we are convinced of TAM’s robustness and have adopted this model in our study.

Understanding the relevance of social factors in technologically driven approaches, some scholars have already started to integrate trust into the TAM (e.g. Gefen, Karahanna, and Straub, 2003; Hsu and Lin, 2008; Alalwan, Baabdullah, Rana, Tamilmani, and Dwivedi, 2018). In this paper, we will build on this by (a) including distrust and (b) focusing on the two components of distrust when it comes to the “non” use of new technologies, i.e. the negative expectations (cognitive side of distrust) and the unwillingness to become vulnerable (affective side of distrust). While research shows that users are not willing to invest time and effort using a new technology when they do not understand the benefit of it (perceived usefulness) or when they are convinced that it is not easy to use (perceived ease of use), we also assume that potential users are interested in the intended values of a new technology (e.g. perceived ethical acceptability, fairness). Users may compare these perceived values with their own values and check whether the two value systems are congruent. When users feel there is an incongruity they may not be willing to take on the responsibility for using a new technology, will not change their attitude towards it and may avoid any interaction with it. Figure 1 shows the theoretical framework of our approach, focusing on distrust.
Figure 1. Theoretical framework on distrust and TAM

**Method**

**Sample**

Data was gathered during intensive cooperation with the LAs of six European cities and their wider stakeholders in the H2020 CIVITAS SUITS project. Supporting Urban Integrated Transport Systems (SUITs) is a four-year research and development project, aiming to increasing the capacity of small to medium cities to plan and implement sustainable mobility measures. The project addresses the ongoing major transformations in the transport sector which requires LAs to work in new ways, with new partners, regulations, new modes of transport and notably, with innovative technologies.

The new technologies we are referring to in this paper are defined under the umbrella of ICTs. Within the transport sector, sensor technology captures traffic flows and data on air pollution in real time, intelligent information and support systems facilitate the search for parking spaces or simplify the use of public transport and complementary micro-mobility services. Since these systems provide data on travel
behaviour and utilization rates that may inform the planning of future transport systems and more bespoke services LAs have to deal with such new technology. Even though the relevant technology is usually planned and implemented by the respective supplier, a precise understanding of the functionality, possibilities and limits of the technology is essential on the side of the local authority in order to formulate requirements within the planning process. It is the task of the organisation’s employees to operate the corresponding systems for data visualization and evaluation. This technology was part of the interview and workshop discussions for example.

The approach is to transfer learning from larger cities, to smaller ones, making them more effective and resilient to change in the judicious implementation of sustainable transport measures. In the course of the project, the six cities of Kalamaria (Greece), Valencia (Spain), Alba Iulia (Romania), Rome and Turin (Italy) and West Midlands (UK) have embarked on a change journey that involved, in part, the adoption of new technology. The adoption of the new technology was the subject of various workshops with city partners and in-depth semi-structured interviews, over 3 years, each lasting around one to two hours. Since research on distrust related to TAM is missing so far, we decided to follow a qualitative approach in our study to best answer our research question and to gain in-depth explanations and understanding. As we wanted to understand a very complex decision-making process in the local authorities’ transport planning departments and wider organisation, we decided to apply a qualitative analysis approach as this kind of approach is often interlinked with complex decisions as deviating nuances with respect to the diverse approaches (e.g. “Glaserian and Straussian versions of grounded theory”) are given which hamper comparative decisions (Holloway and Todres 2003: 354). Our data sample mainly consists of the interview transcripts from 12 different representatives of the transport planning
departments from six LA partners. The participants were selected by the local authorities. As we worked with different sized LAs, in some cases the two representatives of a local authority constituted the whole transport planning department/team or at least 10% of it. Further, we paid attention to a balanced sample in relation to gender, age, tenure and management level.

Data collection
Semi structured interview were conducted in line with the recommendations by Bryman, 1988; Buchanan, 1993). The interview questions were designed to allow the participants to interpret and describe their experiences and feeling when adopting new technology in their own way. The interview questions focussed on (1) trustworthiness and trust towards unknown technology; (2) previous experience with technology adoption; and (3) their attitude and intention to use the proposed systems in their workplace. Each participant was given the interview protocol one week prior to the interview and all were well prepared to explain their views. At the start of the interviews, the participants were asked to talk freely about the questions and to discuss them from their own experiences. All interviews were conducted in English either in the participants’ workplaces or during video conferences, and were audio recorded and transcribed in full.

Workshops have been previously used to integrate different types of information and bring multiple members – here of the transport planning departments from all local authorities together - to think through potential solutions for complex problems (Huntington et al., 2002; Knapp et al., 2011). Such workshops have been shown to facilitate knowledge sharing and social learning, build trust, and increase participant understanding of the subject matter (Patel et al. 2007; Dreelin and Rose 2008). We used participatory workshops to evaluate and integrate tools to enhance trustworthiness and
reduce the employees’ unwillingness to become vulnerable and to allow positive expectations to develop. Each workshop, lasted around one day and was designed to provide many opportunities for feedback and discussion in both small and large groups. Small-group interaction has been suggested as an effective way to facilitate knowledge sharing in workshops (Patel et al. 2007). These workshops represent the culmination of three years of work collecting data in form of documentation of long-term qualitative knowledge. Throughout the project, researchers worked with the LAs on a regular basis, through biannual community research meetings, interviews, fieldwork, and participant observation.

**Data analysis**

The data gathered in the interviews and workshops has been used in two ways. Firstly, to understand the concerns and expectations of the participants when dealing with new technologies. These insights were used to build models of trustful behaviour concerning technology adoption. Secondly, we used the transcript material to provide short cases and quotes to enliven and illustrate the results and decision processes identified.

The objective of the analysis was to examine the perspective of the different participants highlighting the similarities and differences and generating new insights, using a thematic analysis as suggested in the literature (Braun and Clarke, 2006; King, 2004). Three main question have been used as a starting point: “do LAs’ employees feel vulnerable when new technology is implemented and have negative expectations towards this technology?” and if so, “what are the main issues that make those employees feeling vulnerable or having negative expectations?” and “what are the consequences of the unwillingness to become vulnerable and the negative expectations in LAs?”.
An advantage of thematic analysis is that it can be widely used across a range of epistemologies and research questions (Nowell, Norris, White & Moules, 2017). It provides a systematic yet flexible approach to the analysis of qualitative data providing rich and detailed account of data (Nowell et al., 2017). More specifically, theoretical thematic analysis has been used. Theoretical thematic analysis or deductive thematic analysis are mainly driven by a specific theoretical framework and research question chosen by the researcher (Braun and Clarke, 2006). Accordingly, the transcribed interviews were coded using an a priori codebook, developed from a rigorous literature review on employees’ vulnerability when introducing new technology in organisations.

The data analysis followed three main steps. The first step checked the existence of actual unwillingness to become vulnerable. Therefore, the coding strategy has been driven by the first question, regarding whether employees feel or do not feel vulnerable when adopting new technology. In this step, the literature about distrust, and more specifically about vulnerability as a key element of distrust, was used to support the analysis of the interviews. The results provided support for a second step, which consisted in the identification of the main indicators and consequences of the existence of unwillingness to be vulnerable.

In this second stage, inductive thematic analysis was used to identify the reasons for employees’ feelings of vulnerability. To do this, codes were considered for distrust and trust as a belief and as a behaviour (Bijlsma-Frankema et al. 2015; Guo, Lumineau, and Lewicki, 2017), “trustworthiness” as well as ‘distrustworthiness’ (e.g. incompetent, self-interested, exploitative, volatile, opportunistic), and the “actual use of the new technology”. Data was coded at the explicit, rather than implicit, level, and results organised thematically, based on the patterns which emerged from the discourse (Deacon, Pickering, Golding and Murdock 2007). In this way, we progressed from
deductive ‘first-order codes’ to inductive ‘second-order themes’, guided as appropriate by coding (such as that listed above) and thematic terminology found in similar studies (e.g. Nienaber and Schewe, 2014; Rousseau et al., 1998; Searle and Patent, 2019). The findings section describes the most frequently found themes in relation to our research aim and theoretical framework.

The aim of the third step was the validation of the identified themes from the interviews and the refinement of these through discussions in six workshops. All LAs participated jointly in the first, third and fifth workshop. Workshop two and four were each held three times, with each workshop having the participation of three LAs. The workshops were conducted by two members of the research team, who produced a report for each workshop. The reports were analysed by a third member of the research team to establish a link between the workshop results and the results of the interviews. The objective of this approach was to increase the reliability of our results by using methodological and researcher triangulation (e.g. Bryman, 2013).

Using two coders to analyze our interview data necessitates establishing interrater reliability. We checked for intercoder reliability by applying Krippendorff’s alpha (Krippendorff 2004) which is commonly used in content analysis to quantify the extent of agreement between raters, it differs from most other measures of interrater reliability because it calculates disagreement (as opposed to agreement). We achieved a Krippendorff’s alpha of more than .900, which is very good (Krippendorff 2004).

**Results**

The first section of the results shows how we investigated whether employees’ vulnerability is actually present in the LAs (step 1 of the analysis). The second section will highlight the identified key aspects that foster unwillingness to become vulnerable and its negative consequences in the LAs when it comes to using new technologies.
(here the sensor technologies which captures traffic flows and data on air pollution in real time, intelligent information and support systems that facilitate the search for parking spaces or simplify the use of public transport and complementary micro-mobility services) in the field of sustainable mobility planning.

**Existence of employees’ unwillingness to become vulnerable**

Scholars have highlighted several ways in which the existence of distrust, based on the unwillingness to become vulnerable, may show itself. These include wariness (Chang and Fang 2013; Lewicki et al. 1998; Ou and Sia 2010), concern (McKnight, Kacmar and Choudhury 2004), deception (Deutsch 1958), suspicion (Lewicki et al. 1998; Kramer 1996; Ou and Sia 2010; Deutsch 1958), or message questioning (Sitkin and Stickel 1996).

The participants made it very clear that most employees feel uncomfortable using and adopting new technology they are not familiar with. Taking the idea of sense-making theory into account, we can assume that such situations are perceived as “risky” by employees and thus, may lead to negative feelings of not willing to become (or show themselves to be) vulnerable. This can be illustrated by a practical example from our work in the SUITS project. We noticed a lack of cooperation between a technology supplier, who as part of the agreed research plan, required mobility datasets to be provided by the cities to iteratively develop the system. Key to this was that the supplier could then understand what and how data was being collected, and develop different types of visualisations to help the LAs to gain a better understanding of mobility patterns in their city.

The city partners had not seen the software before, but did not ask questions or support to understand its’ benefit when it was demonstrated. They only expressed doubts as to whether they would derive any direct benefit from it in the end. One quote
for example was “I am not familiar with that tool and I do not see the benefit of it except that I have to invest time and effort” [LA 4, representative from transport planning department].

The service provider clearly demonstrated what he needed to make the new tool running and kept his request for data simple, asking for “open data” in any format, of any size to remove the onus of reformatting data from the LAs. Theoretically all city partners should have been able to deliver some data - without any obstacles in relation to confidentiality issues or technological skills. Instead this seemed to make them even more suspicious. They argued “We do not have the data; another department is responsible for this data; We do not know really what kind of data is required”.

After two years, some partners kept arguing that the requested data would not be available and that they did not know whether their data format would work for the new technology. Such statements are indicators for employee’s vulnerability as it seems employees try to find excuses to hide their own unwillingness to share data with someone outside the organisation (e.g. afraid of the negative consequences of it such as negative publicity in the city; increased workload). The reluctance on the part of public authorities to share data can also be explained through their concerns over data security and privacy in general, and GDPR in particular. This was introduced at the start of data sharing discussions and no one was entirely sure of the system, and certainly did not want to jeopardize their organizations by providing data in contravention to GDPR.

Additionally, the participants indicated concerns about the supplier’s motives. They could not understand a business model in which the supplier offered services without payment. Indeed, the service provider was just interested in providing a test for demonstration purposes, to get testimonials, increase its’ reputation and further research and innovation in the mobility sector.
Based on this example it seems, that not just the technology has to be perceived as trustworthy, but also the supplier behind the technology.

Several hints for distrust indicate the existence of the unwillingness of employees to become vulnerable when using a new technology, such as:

“I [LA 6 representative] am concerned what they will do with the data in the long run and thus, I do not want to provide data for this tool.”

“They do not really care about how we [employees’ of LA 4, transport planning department] feel or what such a technology means to us”

“I [LA 3 representative of the transport planning department] do not belief in what they tell us, I am questioning the benefit of the tool [data analysis tool]”

“We told them [supplier] several times that we do not know what kind of data they want, so we are not willing anymore to ask again [LA 1 representative]”

Table 1. Hints for the existence of the unwillingness to become vulnerable

Many of the comments occurred during the introduction of GDPR and also at a time of major security breaches and misuse of data, so although they occurred within the context of transport data, they are representative of the feelings of many employees and organisations in the late 1990s.

Afterwards we undertook thematic analysis (step 2). Based on the results we adopted our extended TAM by adding (1) indicators that may raise the likelihood of employees’ unwillingness to actually use new technology and that demonstrate that employees will not adopt the new technology in the long-run. These indicators will help senior management to recognize at a very early stage that an implementation may fail and help them to be proactive in reducing the likelihood of a failure.

In sum the indicators:
(1) will help to avoid the development of an employee’s unwillingness to become vulnerable and thus, prevent the development of obstacles that will hinder the actual use of a new technology.

(2) will give hints to the management that their employees’ will very likely not use the new technologies.

**Key indicators for employees’ feeling actual vulnerability in LAs**

From our results the following indicators could be identified that increase the likelihood of the existence of distrust when focusing in particular on the users’ unwillingness to become vulnerable.

**Perceived uselessness and uneasiness of use.** In line with previous research, working with the LAs has provided evidence that perceived uselessness or usefulness as well as the estimated amount of effort that it will take to get familiar with the new technology, are decisive factors in deciding to use a technology or not. Both indicators are aligned to the new technology itself and the positive expectations a potential user may have. Both factors relate to the cognitive dimension - is this new technology worthy to be trusted? While these merely support the TAM, we want to highlight two additional indicators: perceived value incongruence and negative attribution towards motives.

**Perceived value incongruence.** Perceived value incongruence has been defined as the belief that others adhere to values that are perceived as incompatible their own core values (Bijlsma-Frankema et al., 2015). Thus, when an individual identifies that their own values are not compatible with the values of someone or something else, the unwillingness to become vulnerable emerges. Perceived value incongruence has been proposed as a determinant of negative perceptions and expectations of the trustee’s motives and behaviours (Sorensen & Sorensen, 1974). Following Chambers (2006)
understanding of vulnerability as exposure to contingencies and stress, and difficulty in coping with them, we can see that a perceived value incongruence stresses an individual as the individual feels a lack of means to cope without damaging loss. This was observed in our sample: the majority of our city partners failed to explain their particular technological requirements due to their lack of technological expertise. The supplier may perceive such behaviour as an unwillingness to become vulnerable.

As a result, the supplier could not tailor the offering to the real needs of the LA. Instead he could only supply generic, off the shelf solutions or made assumptions of needs based on prior experience. This further reinforced the employee’s unwillingness to become vulnerable (e.g. increased scepticism of the suppliers’ intentions in general) and fostered negative expectations such as “the supplier does not really care about us [as LA]. They just want to sell their product.” [LA 3, representative of the transport planning department].

The next example also shows the negative circle of a perceived value incongruence. During the SUITS project, two technology suppliers tried to convince partners from the LAs to share data with them to test more efficient ways handling of big data – which would in fact be a large benefit to all small LAs who lack the computational capacity to process large amounts of data. However, the unwillingness of the LAs to share the data was driven by different underlying value systems among the involved parties. The LAs could not understand the reasons and benefits of the new technology for which they were asked to provide data, given that they had some systems in place already. The benefits of the new systems were not sufficiently explained, so they were not able to recognize the advantages of the new solution for their future needs. Additionally, new General Data Protection Regulation (GDPR) came into force during discussions about data transfer. This complicated the whole process for several
months. Everyone was vulnerable, as it was not clear which data could be shared by whom and for what purpose. Legacy mobility data has not been collected systemically within and across LAs. Data may be collected in an ad hoc, non-standardised way to provide evidence for new transport infrastructures, or it may be collected as part of projects. Once the project is over, the data remains. It is potentially a useful source of data to ‘experiment with’ e.g. to show how it can be visualised or merged with other data sets. However, uncovering this data, finding out who owns it, and how it could be used is a daunting challenge, especially if it places an organisation in violation of GDPR. So, even though LAs had a lot of data, and will need to handle more data in the future they did not feel secure enough to hand over current data without a Data Management Plan. This put them in a position of vulnerability with respect to the technology providers.

Project trials in Kalamaria in which real-time mobility data was collected showed the need for a lot of post processing to ensure anonymization of data collected automatically for vehicles. Lacking the skills to do this, and knowing it is now required, could be an added perceived vulnerability for the LAs especially with the introduction of fines for organisations found to be in breach of GDPR.

Additionally, the cities raised concerns regarding the confidentiality of their data and the long-term use of the data once it is passed to a private company. One statement was for example “We expect that we have little in common with the others and the others intentions may different to ours in the long run. Maybe that can harm us sometime.” [LA 2, representative of the transport planning department].

The LAs have a responsibility for the data they collect, and for the citizens who provide that data. Even in cases where anonymised data can be used to help develop better transport systems and services, LAs are still wary. Distrust arises as others come
to be characterized as unpredictable and threatening, thus fostering a sense of uncertainty and vulnerability (Sitkin & Roth, 1993). Although research shows that low levels of distrust are healthy and prevent individuals to make failures or trust “blindly”, the indicated level of wariness was relatively high (e.g. Lewicki et al., 1998) and thus, not healthy anymore.

**Attribution of negative motive.** The attribution of negative motives can also be an indicator for distrust. Attribution is the process through which people try to explain their own and others’ behaviours (Abramson, Seligman, & Teasdale, 1978; Heider, 1958; Kelley, 1967). The proposed relation between the unwillingness to become vulnerable and motivational attributions is built on the notion that individuals feel the urge to interpret behaviours of others that are salient to oneself, such as harmful behaviours. Our data indicated several aspects that may be summarized as attributions of negative motives. Negative experiences with new technologies in the past foster such attributions. A once failed new technology will thus increase the attributions of negative motives and foster distrust towards innovations. Several participants referred to such negative experiences.

In some cases, a technological solution has been poorly developed and not sufficiently adapted to the user needs or the technology had been poorly introduced to the employees by senior management. When employees do not understand the benefits of a new technology or its benefit for the city and the citizens, they create negative motives (based on poor past experiences) and develop an unwillingness to become vulnerable: “I do not really understand how this should help us and how we can benefit from it. Thus, what are the motives behind the introduction of this technology in our department?” [LA 2, representative of the transport planning department]. In some cases, the LAs failed to implement the new technology and the organisation moved
back to the old ways of working. Such negative experiences can strengthen the attributions of negative motives in the future and increase the likelihood that the unwillingness to become vulnerable emerges when it comes to the implementation of new technologies. Another example also provided evidence on the negative attribution towards motives. The majority of LAs avoided interaction with a service provider who offered a new tool to forecast air pollution or traffic peaks because they did not believe the suppliers’ business model. The supplier offered its’ service voluntary which the LAs perceived as less trustworthy as they suspected negative motives behind this model.

Table 2 summarizes some key examples from the interview and workshop data in line with the two identified indicators that increase the likelihood that users’ may not want to become vulnerable and thus, do not use a new technology in the long-run.

**Several hints for perceived value incongruence**

“I [LA 4 representative of the transport planning department] rather question whether this technology really works for us, you know, our LA is very traditional and citizens expect us to take responsibility for taking care of them [concerns when it comes to the use of e-skaters]”

“They [supplier] do not really listen to what we tell them – we provided them a lot of information but actually they did not come back to us – so I assume we are not on the same page” [employee of LA 3, transport planning department]

“We expect that we have little in common with the other and that the others intentions are different to ours in the long run. Maybe that can harm us sometime.”[LA 2, representative of the transport planning department].”

**Several hints for the attribution of negative motive**

“I do not really understand how this should help us and how we can benefit from it. Thus, what are the motives behind the introduction of this technology in our department? I suspect anything we really need.”[LA 2, representative of the transport planning department].
“they work for their own interest, they want to sell that technology, they are supportive now, as long as we show interest” [LA3, representative of the transport planning department]

Table 2. Indicators for an increased likelihood for the unwillingness to become vulnerable

Negative consequences of the unwillingness to become vulnerable in LAs

Two key indicative behaviours can be spotted when individuals do not want to use a new technology:

Avoidance of interaction. One of the key outcomes of the interviews has been evidence of avoidance of interaction – in particular some employee’s tried to avoid interacting with the new technology at all. This finding is in line with those in trust research (e.g. Bies & Tripp, 1996; Bijlsma-Frankema, 2004; March & Olsen, 1975). The interviewees referred to several examples that fostered their unwillingness to become vulnerable and thus, led to distrust towards new technologies. For example, when employees have been previously disappointed when their positive expectations towards new technologies were not fulfilled, they then became sceptical and tried to avoid interaction with it and the whole implementation process. “We tried not to be involved with the senior management that wanted us to test the new technology. You know last time we put so much effort in it and I still do not see the benefit for us.” [LA 1, representative of the mobility planning department]. Interestingly, in the end this may make them more vulnerable if their attitudes and behaviours are not shared by the rest of the organisation. These employees may become late adopters (shifting from early adopters to late adopters) or avoid adoption altogether, perhaps resulting in less employee satisfaction and reduced performance.
However, a new technology cannot be implemented by senior management alone as then the implementation is likely to fail. The top-down approach only works if it gets bottom-up support by the wider group of employees or stakeholders. For example, in our research, the city of Alba Iulia implemented new guidelines for municipal procurement, but without trust, this new process could not have been implemented. The transport and procurement departments worked closely together with an external supplier and were willing to become vulnerable towards each other – meaning they trust each other that no one will behave opportunistically - they were empowered to implement these guidelines successfully.

**Knowledge hiding.** Another negative consequence of the unwillingness to become vulnerable is an identified lack of knowledge sharing, mentioned by several LAs. West Midlands Combined Authority, a partner in the SUITS project, put this point on the top of their agenda as it is fundamental for organizational performance.

US organizations spend for example almost a trillion dollars annually to analyse, store, and retrieve knowledge (Lohr, 2002). The willingness of employees to share knowledge depends on the level of trust employees have with their organization, colleagues or other stakeholders (e.g. McAllister, 1995; Schewe and Nienaber, 2011). While technology is able to store explicit knowledge, tacit knowledge resides only in the minds of people and its availability to others depends upon individual decisions and behaviours (Nienaber and Schewe, 2011). Thus, when employees start to distrust a new technology, they are not willing to share their positive experiences with that technology, or their learnings and may start to talk very negatively about it. These aspects are very important for the future developments of new technologies.

Even worse is the negative culture that may evolve from the unwillingness to share information and knowledge. Employees may feel more isolated from the rest of
organisation and become less motivated which leads to lower levels of organizational performance (Nienaber, Romeike, Searle, and Schewe, 2015).

Table 3 summarizes some key examples for the two key consequences that follow the unwillingness of employees to become vulnerable.

Several hints for **avoidance of interaction**

“I am not really willing to provide any data. I am not sure what they will do with it in the future and thus, it is maybe better not to share anything.” [LA 2, representative of the transport planning department]

“We do not really meet each other as you know. Maybe we share not the same view.” [LA 1, representative of the mobility department]

“They always decide, so why should I try to ask them or provide feedback?” [LA 3, representative of the transport planning department]

Several hints for **knowledge hiding**

“I do not tell everything, sometimes I just think, you never know, maybe you need that information later […] and then it brings you in a better position [LA 1, representative of the mobility department].”

“They do not tell us, so why should I tell” [LA 5, representative of the transport planning department]

“In the end I told them but actually I do not tell everything, I mean for example we had some trouble with the technology once but we did not tell as you know then we are the stupid guys in the end, so we did not say anything and then yeah the implementation really failed. We all knew why… but nobody wanted to be guilty.” [LA 6, representative of the transport department]

Table 3. Negative consequences of the unwillingness to become vulnerable

Figure 2 shows the extended TAM developed from this analysis.
Figure 2. Extended and adopted framework on TAM distrust

**Guidelines**

The following section highlights the most important guidelines to avoid the emergence of unwillingness to become vulnerable and to cope with existent distrust. Herewith we want to support any organisation wishing to implement a new technology and as a result, change the working practices of its employees. The following guidelines will help senior management to recognize issues around the ‘human factors’ which may impede technological innovation at a very early stage to help them to be proactive in reducing the likelihood of a failure.

**Avoid the emergence of distrust**

**Identify the sources of distrust.** Our results highlighted that distrust can have several sources or referents. While employees may distrust a new technology, they can also distrust the supplier and their motivations. If senior managers want to reduce the likelihood that distrust emerges when new technologies are implemented, they first have to understand what employees distrust and to what or whom they are not willing to
become vulnerable in this context, e.g. is it the technology itself, the reputation of the supplier or brand. Furthermore, senior managers have to take into account that spill over effects from one source or referent to another are likely as distrust is pervasive (Bijlsma-Frankema et al., 2015), meaning that when individuals distrust a particular supplier (or decision maker), they will also distrust any technology associated with that supplier.

**Be aware of the users’ values.** When fostering the actual use of new technologies, it is important to understand a user’s values before trying to make him or her use it. It was important to understand the organisations’ values first, as the individuals in the organisation will match their values with those of the new technology to see whether they are congruent with each other or not. Thus, when a new technology shows values that are not congruent with the user’s values, usage will not happen. This means, senior management has to understand whether their employees’ values (as in the person-organisation-fit approach (e.g. O'Reilly, Chatman, and Caldwell, 1991) are in line with those of the organisation to ensure the success of a technological implementation process. When a mismatch exists between the technology and the organisational climate the likelihood is relatively high that the implementation will fail.

**Create a guiding coalition within the organisation that serves as role model.** A guiding coalition should comprise individuals that can be characterized as early adopters, have had previous positive experiences with new technology, and are also aware of negative consequences and potential obstacles to implementation. They should be well informed about the solution, have influential relationships with people at different levels of the organisations, be trusted by most and well respected for their competencies and come from diverse sections/represent different groups who will be effected by or use the technology. Their tacit knowledge can be matched alongside that
of more junior staff members, with high technical open-mindedness, who can help to motivate others and can serve as connectors for the younger and more diverse employees.

**Transparent and honest communication.** One learning from our work during SUITS has been the fact that senior management has to be very transparent when informing their employees of a new technology implementation. They also have to refer to potential obstacles and risks. They have to be honest about their concerns regarding the new technology. The literature shows that openness and honesty in communication helps employees trust in something they are not familiar with (Nienaber and Schewe, 2014). Furthermore, to show that for example expert knowledge is missing at senior levels, management may also motivate individuals to become indirectly part of the “guiding-coalition”, offering their experiences and skills to help the senior management. This will make such individuals to feel as real part of the whole implementation process and motivate them to function as role models for their colleagues in the organisation.

**Cope with the unwillingness to become vulnerable**

**Avoid increase of top-down monitoring.** According to the threat-rigidity theory when responding to demanding or crisis situations, organisations often constrain communication and assert more control, which ultimately makes them less flexible (Staw, Sandelands, and Dutton, 1981). Senior management may increase monitoring mechanisms if they feel that something is not working the way they intended, to understand what is happening. However, the trust-control literature demonstrates very clearly that most control mechanisms reduce the willingness to become vulnerable instead of increasing it (for an overview e.g. Long and Weibel, 2018; Bijlsma-Frankema and Costa, 2005). While Long and Sitkin (2006) emphasizes that formal controls can
foster trust when they reduce perceived levels of risk and uncertainty, or prevent authorities from encroaching on their personal freedom the majority of control mechanisms will lead to the opposite results (e.g. Long & Weibel, 2018). Close monitoring has been proven to foster distrust. Thus, even when the senior management recognizes that the likelihood for an implementation failure has increased, they have to avoid the implementation of micro-control mechanisms such as closer monitoring.

**Face-to-face communication.** Meeting face-to-face with those distrustful of the new technology may allow trust to emerge between the negotiating parties (individual level) which may in turn transfer to trust in the technology (human-technological level). It was said in the interview that face-to-face meetings are the best way to develop a trustful relationship with each other that will affect future decision-making. Face-to-face communication can mitigate the effects of perceived organisational rigidity, especially the ones resulting from the decreased quality of communication that characterises rigid organisations.

**Get a third party on board.** In order to address issues of developing trusting relationships within organisations, it may be helpful to gain external support from former suppliers or experts when implementation decisions have to be made. A third party could talk about experiences in the past and address particular concerns of the new technology from another perspective as the senior management or provider of the technology. Users may perceive those persons or institutions as “independent” and thus, be more likely to trust them. They can serve as mentor or mediator and help to overcome distrust towards the new technology and make individuals actual use it. Based on our results we can say that an educational institution or an individual dealing with similar technologies could serve as third party as these institutions and individuals are perceived usually as independent – different as consultancies.
Conclusion

This paper highlights the relevance of the employees’ (users’) willingness to become vulnerable when new technologies are implemented in LAs (organisations). As long as employees are not willing to become vulnerable when adopting a new technology and expect the new technology to be harmful, their introduction will be problematic. Based on comprehensive transcript material of interviews and workshops during the project SUITS, we are able to contribute decisively to existent research on TAM and trust by firstly, focusing on distrust and secondly, by shedding light on the users’ unwillingness to become vulnerable when using a new technology. We show two indicators for increasing the likelihood of non-use besides the perceived uneasiness of use and uselessness, i.e. incongruence of values and negative attributions towards motives. Both are decisive in implementing a new technology successfully. Furthermore, we show two behaviours that indicate the existence of distrust while implementing a new technology: a lack of knowledge sharing and the avoidance of interaction. Finally, we are able to provide practical guidelines to avoid the emerging of an unwillingness to become vulnerable which path the way to a successful introduction of a new technology in an organisation.

Acknowledgments. The data of this research was conducted during the SUITS project, which was funded by the European Union, Grant agreement ID: 690650, Programme H2020-EU.3.4. - Sociaetal challenges - Smart, Green and Integrated Transport, Topic MG-5.4-2015 - Strengthening the knowledge and capacities of LAs.
References


CIOMS. (2002), International ethical guidelines for biomedical research involving human subjects, Council for International Organizations of Medical Sciences (CIOMS), Geneva, CH.


Fugate, M. (2013). Capturing the positive experience of change: Antecedents, processes, and consequences. In S. Oreg, A. Michel, & R. By (Eds.), *The


Nienaber, A., Spundflasch, S., & Soares, A. (2019). Sustainable Urban Mobility in Europe: Implementation needs behavioural change. SUITS Policy brief X. SUITS funded from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 690650. Mobility and Transport Research Centre, Coventry University


Authors’ Biographies

Prof Ann-Marie Nienaber is specialist on trust challenges in and between organisations with emphasis on safety critical context, e.g organisational capability during crises and changes, mainly in the fields of public management, health, and transport. Her work has been published in journals such as Human Resource Management, Group and Organization Management, or Journal of Business Ethics.

Sebastian Spundflasch is a researcher at the Institute for Media Technology at Ilmenau University of Technology in Germany. Since 2011, he is in charge of different transport projects on a national and European level. His research focus is on the user-centered design of transport systems and services.

Andre Soares is an Assistant Professor with experience in HR&OB, and Business and Occupational Psychology in universities in Portugal, England and Poland. His research is about using social network analysis, team dynamics and positive psychology to increase the performance both in the industrial and in the sports context.

Prof Andree Woodcock is PI on the HS2020 CIViTaS SUITS, and H2020 TInnGO projects (focused on gender and transport). Both projects deal with inclusivity and capacity building. She was formerly PI of FP7METPEX project looking at the quality of multi modal end to end passenger journey experiences.