RISKS OF NEW TECHNOLOGY FOR STRUCTURAL HEALTH MONITORING OF BUILDING STRUCTURES

MOHD-RAHIM, F.A.*, CHUING, L.S., ABD-KARIM, S.B., AZIZ, N.M., ZAINON, N.

Centre for Building, Construction & Tropical Architecture (BuCTA), Faculty of Built Environment, University of Malaya, 50603 Kuala Lumpur.

*Corresponding author: azli@um.edu.my

Submitted final draft: 31 May 2021
Accepted: 25 June 2021

Abstract: Structural health monitoring (SHM) is a powerful monitoring method for assessing structural health in infrastructure, including damage detection and structural prognostics. The emergence of new monitoring technologies in sensing systems has been recognised for its potential in detecting various physical and chemical parameters related to structural health monitoring, but it also fraught with risks and unknown threats. This paper aims to investigate the risk factors that should be considered to decide whether to adopt a new monitoring technology. This research is based on preliminary identification of risks that could affect the adoption of new monitoring technology, focusing on the context of building and engineering structures. A content analysis approach that involves cross-referencing various sources of information was performed to identify the risks of new monitoring technology. The analysis revealed eleven main risks that influence the adoption of new monitoring technology in building and engineering structures. It emphasizes the importance of the risk assessment model for assessing the risk data for better structural health monitoring algorithm adoption decision, which considers technological risk and the external risks originating ed from the project environment.

Keywords: New monitoring technology, exogenous risk, endogenous risk, civil infrastructure, structural health monitoring

Introduction

Over the years, infrastructure development has received the largest share of public sector development expenditure in Malaysia (DoSM, 2019). The amount of funds allocated for infrastructure development has generally increased from one Malaysian Plan to the next and often significantly. According to the Capital Stock Statistics 2018 report (DoSM, 2019), the expenditure on structures, namely residential and non-residential buildings, and other construction, such as highways, has remained the largest contributor to Malaysia’s Net Capital Stock (NKS) with a share of 78.8% (Figure 1). Generally, civil infrastructure developments, such as bridges, tall buildings, power utilities, highways and dams are an important investment for any country, and usually becomes the most expensive asset. This is because all these structures have a long service life compared to other commercial products, and they are expensive to maintain and replace once they are established (Chong, 1998; Rice & Spencer, 2009).
Moreover, the civil structures are vulnerable to damage due to natural hazards (e.g., tornadoes, earthquakes, wind and humidity) and are subject to a variety of deteriorating mechanisms, including aging, environmental stressors and manufactured hazards (e.g., blasts, fires), during their service life (Frangopol et al., 2017). Therefore, it is crucial to continuously implement rational management strategies that continuously assess their health condition and structural integrity. Any damage identified early can be repaired economically, thus avoiding or minimizing potentially significant economic and human losses. Therefore, to ensure the integrity and security of the structures, they must be equipped with Structural Health Monitoring (SHM) of the infrastructure (Chang, 1999; Karbhari & Ansari, 2009).

Figure 1: Malaysia’s Net Capital Stock (NKS) by types of assets at constant 2015 prices (Source: DoSM, 2019)

While variations on the definition of Structural Health Monitoring (SHM) exist, generally, the term refers to the monitoring systems that can automatically acquire and process data to assess structural health, including damage detection and structural prognostics (Farrar & Worden, 2013). Basically, according to ISIS Canada (2004), it refers to the broad concept of assessing the ongoing and in-service performance of the structures by using a variety of measurement techniques. Structural health monitoring (SHM) provides a powerful method to reduce uncertainty, calibrate and improve structural assessment and performance prediction models (Gul & Catbas, 2011; Frangopol & Kim, 2014) by effectively capturing structural behaviour demands a structure. Many earlier studies have been undertaken to model the performance of in-service civil infrastructures over time (Glaser et al., 2007, Frangopol et al., 2008; Sousa et al., 2013; McRobbie et al., 2015). For example, Bush et al. (2013) presented an innovative approach to bridge management that guides the data collection, accuracy and precision required, the frequency of inspections, and the recommended SHM techniques used.

The SHM can be divided into three major components: damage detection/characterisation, prognostics, and risk assessment (Lynch et al., 2016). The key components of this SHM technology include sensing, signal processing, health assessment, and system integration (Rice & Spencer, 2009), wherein general all these technologies play an important role in monitoring various physical or chemical parameters associated with materials, design, fabrication, loading and operational conditions related to the structural health. Based on these inspections, the SHM data of one component in the civil infrastructures can be used to update the deterioration performance.
of other uninspected components of a structural system to reduce uncertainty (Frangopol et al., 2017).

With the advent of technologies, the field of SHM has grown rapidly. Even though SHM approaches offer civil infrastructure managers knowledge of actual behavior and demands on structural performance, the SHM techniques are ineffective in translating this information into actionable data for civil infrastructure managers. When new technology is used for the inspection, maintenance and management of existing infrastructure, one important factor to consider is the risk of adopting new technologies, especially in the context of the built environment, such as the realistic predictive view of cost, safety and condition of the infrastructure (Frangopol et al., 2017). The decision to adopt new technology or not in structural health monitoring depends not only on the benefits but also on the costs and risks involved. It involves many important factors such as technology, culture, economy, the environment, individuals and individuals’ organizations.

This research is centred on the early stage of the risk management process, which is risk identification. In this context, the objective is to investigate the risk factors that should be considered to decide whether to adopt a new monitoring technology for civil engineering infrastructure. It emphasizes the importance of a risk assessment model for assessing and quantifying risk data so that a better decision on adopting a structural health monitoring algorithm can be made, based on technological and external risks originating from the project environment.

Methods

This paper follows the literature review method proposed by Webster and Watson (2002). It attempts to analyze and synthesize literature regarding “risk management” and “new monitoring technology” in building and civil engineering structures. It will advance the knowledge base of risks that influence the adoption of new monitoring technology so researchers can use that to focus on important risks of new monitoring issues and by practitioners to develop an effective risk management strategy and approach. Although this paper emphasises the built environment context, the literature review is not limited to the built environment.

There is limited research on the risk management of new monitoring technology and perceived expectations compared with the actual usage of new monitoring technology in building and civil engineering structures. The keywords “risk of new monitoring technology”, “barrier in new monitoring technology”, “exogenous risk of new technology”, “endogenous risk of new technology”, and “challenges of implementing new technology infrastructure” returned 385 hits within the databases Scopus, Web of Science and JSTOR, with 301 of the hits were journal articles, 68 were conference papers, and 16 were books.

After filtering these results and a forward and backward search was performed to select relevant articles based on the criteria of whether they included a theoretical discussion on the use of new monitoring technology in the building and civil engineering structures. Eighty-five journal articles and conference proceedings were selected, and relevant principles from these sources were listed. The risks related to adopting new monitoring technology were then grouped according to concept based on the evidence from the literature review.
Literature Review

Risks of New Monitoring Technology

Innovations and new technologies occur when the need or opportunity presents itself. They have been referred to as “emerging”, including cloud computing, connected devices, mobile devices, robotic devices and blockers. The use of this new technology is critical to the success and survival of an organization. However, many are still trying to balance the need to adopt new technologies with speed and agility, with risk management.

Comprising six key phases, risk management is a systematic process for identifying, analyzing, and responding to project risks (Irimia-Diéuez et al., 2014). These risks, or threats, may come from various sources, including financial uncertainties, legal liabilities, strategic management mistakes, accidents, and even natural disasters. The six key phases of risk management as described by the Project Management Body of Knowledge are risk management planning, identifying risks, qualitative risk analysis, quantitative risk analysis, risk response planning, and risk monitoring and control (Berkeley et al., 1991 Flanagan, 1993; AS/NZS 4360, 2004; PMI, 2008; Dey, 2012)

Risk management is very crucial in helping organizations act on the ever-changing inventory of risks. Good risk management will facilitate and encourage the acquisition, analysis, and dissemination of current and future risk information, which will assist the organizations in making better decisions when dealing with the risks. One way of defining risk is a potential for unwanted or negative consequences of an event or activity (Rowe, 1975), a combination of hazard and exposure (Chicken & Posner, 1998).

Nevertheless, the previous research tends to emphasize the double-edged nature of risks, such as a threat and a challenge (Flanagan, 1993), by defining risk as to the chance of something happening that will have an impact on objectives; may have a positive or negative impact (AS/NZS 4360, 2004), the combination of the probability or frequency of occurrence of a defined threat or opportunity and the magnitude of the consequences of the occurrence (Association for Project Management, 2004). In general, risk of unexpected events occurring in projects may result in either positive or negative outcomes that deviates from the project plan (Ahmed et al., 2007). Risks, if they are not mitigated or managed properly, can result in project failure (Royer, 2000).

In the past two decades, technological advances have seen a trend in implementing structural health monitoring through the speed of wireless acceleration (Agbabian et al., 1991; Peter et al., 2003; Lynch et al., 2004; Brownjohn, 2006; Kim et al., 2007; Pakzad et al., 2008). The development of new monitoring technologies in sensing systems, such as fibre-optic (FOS) sensors, piezoelectric sensors, magnetostrictive sensors, and self-reinforcing fibre structure composites, has tremendous potential for detecting various physical and chemical parameters related to structural health (Sun et al., 2010; Meyer et al., 2010; Glisic et al., 2013; Leung et al., 2015; Spencer et al., 2016; Moreu et al., 2017; Noel et al., 2017). These new monitoring technologies have been recognised to bring many benefits to today’s structural engineering, but it also fraught with risks and unknown threats.
The 12th edition of the Global Risks Report by the World Economic Forum (2017) has highlighted 12 key areas of emerging technologies and their inherent risks and benefits. As shown in Figure 2, new technologies related to structural health monitoring, which are technologies that related to the “proliferation and presence of connected sensors everywhere”, have been reported as emerging technologies with the second-highest risk on the Internet of Things (IoT) (World Economic Forum, 2017). This is because, although this technology is designed to facilitate human work, for example, to remotely monitor engineering structures to ensure they are safe and functioning, it can also lead to unforeseen problems, for example, a misunderstanding in the system such as during interpretations of data, whether accidentally or intentionally, can cause many accidents, lead to property damage, injury and the possibility of death.

Figure 2: Perceived benefits and negative consequences of 12 emerging technologies (World Economic Forum, 2017)

Sakhardande et al. (2016) stated that IoT plays a significant role in the channeling and transmission of data through efficient use of technology. For example, an infrastructure monitoring network could be used to quickly assess damage to infrastructure so that maintenance procedures could be directed to areas that need immediate attention (Koo et al., 2015; Hentschel et al., 2016; Aono et al., 2016; Parkinson & Bamford, 2016, Brous et al., 2018). IoT is expected to improve the utilization of existing infrastructure (Koo et al., 2015; Hentschel et al., 2016) by providing
users with information on costs, time, environmental impact and perceived quality of services (Archetti et al., 2015).

Even though the communication between the IoT devices to surrounding objects and data infrastructure may benefit the management of civil infrastructures, by providing enough quality data required to make timely decisions (Brous & Janssen, 2015b), the quality of this data has been seen to vary greatly over time (Barnaghi et al., 2013). Trusted data is essential to aid the decision-making process in managing the civil infrastructures (Brous & Janssen, 2015a; Haider et al., 2006). Therefore, having trusted data is essential for organisations in which data-driven decision-making is widely recognised (Sicari et al., 2015). The IoT data can vary widely in format and representation; thus, it is crucial to determine the quality of data so that civil infrastructure managers can trust the IoT data, especially in use-case scenarios where the data is provided by many different providers (Barnaghi et al., 2013).

The notion of trust is often related to identity management and access control (Sicari et al., 2015); therefore, in the real world, the key concerns are the data related to people, privacy, and security (Barnaghi et al., 2013). The challenge is greater when the scale of the data and the number of different parties that can access and process the data is bigger, like in monitoring civil infrastructure. It is often believed that organizations involved in public projects are well equipped to handle big data, but this is not always the case (Thompson et al., 2015). It can be difficult to attribute the success or failure of data management projects to one or more specific factors due to the complexity of the data. According to Grus et al. (2010) and Brous et al. (2017), there is an interrelationship between data management’s sociological and technical dimensions. It is not easy to track cause-and-effect relationships.

**Identification of Risk Factors in New Monitoring Technology**

When discussing the risks in adoption of new technologies, the thing that needs to be concerned is not only about the technology itself (Thompson et al., 2015), but it also involves other relevant issues such as government regulations, natural hazards, labor abolition, legal risks, cash flow problems, safety issues and natural disasters (Archetti et al., 2015; Aono et al., 2016). As an integrative part of risk identification, risk classification plays an important role in shaping the various risks that affect the project (Zou et al., 2007). Nowadays, a variety of ways can be used to classify the risks associated with the projects. However, the reasons for choosing a particular method must meet the objectives of the investigation. Perry & Hayes (1985) provide a list of factors gathered from several sources and are classified in terms of risk retainable by contractors, consultants, and clients. Chapman (2001) grouped risk into four subsets: environment, industry, customer, and project, while Zeng et al. (2007) further classified risk factors as human, sites, materials, and equipment factors.

In this research, the risks of new monitoring technologies are classified by reference to the Project Management Institute (PMI), which classifies risks into two groups, namely external and internal risks (Tah & Carr, 2000; PMI, 2008; Rastogi & Trivedi, 2016). The external risks are those risks that are beyond the control of the project management team but may affect the direction of the project, while the internal risk may be under the control of the project manager, they cause uncertainty that may affect the project (Zou et al., 2007; PMI, 2008). In this research, all the issues
related to politics, social, cultural, economic, legal, logistical and natural catastrophes are classified as exogenous risks (Loo et al., 2013), and issues related to technological risks, such as data uncertainty, fit risk, changes in technology, design issues and operations/maintenance issues, are classified as endogenous risks (Ye et al., 2012).

Results And Discussion

Endogenous Risks of New Monitoring Technology

New technologies often involve risks and ambiguity, such as the probability of a different outcome is unknown (Barham et al., 2014); therefore, there is room for uncertainty (including risk and ambiguity) to play an important role in deciding to adopt new technology (Bryan, 2010; Brous et al., 2017; Zhou et al., 2019). According to Barham et al. (2014), risk occurs when the probability distribution of the random payoff is known while, ambiguity arises in situations where the probability distribution is not known with certainty by the decision-maker.

New technologies tend to be preferred when the expected yield is higher, the cost of avoiding the risk is lower and avoiding ambiguity is lower. For example, according to Aono et al. (2016), IoT infrastructure could reduce costs in terms of time and money as traditional methods of inspecting highway structures and bridges, because damage is often reactive and require significant amount of time and use of costly equipment to rectify. This is in line with previous studies that argue that higher probabilities contribute to adoption incentives, while newer technologies may have increased risk and lower adoption rates (Foster & Rosenzweig, 2010; Moreno et al., 2014; Howley et al., 2012).

Applying these arguments for structural health monitoring is of special interest. Civil engineering infrastructure is complex with a long service life, expensive to maintain and replace once it is established. New monitoring technologies are likely to expose projects to differing levels of uncertainty. Therefore, uncertainty (whether in the form of risk or ambiguity) is an important factor when deciding the use of new monitoring technology. However, if there is imprecise knowledge of the new technology, uncertainty can also affect adoption decisions (Barham et al., 2014).

Over the years, many researchers have used Technology Acceptance Model (TAM) to examine patterns of adoption of technology (Walczuch et al., 2007; Teo & Schaik, 2009; Sajjad et al., 2010; Abadi et al., 2012; Son et al., 2015; Park et al., 2019; Min et al., 2019). According to TAM, perceived usefulness and usefulness are key determinants of technology adoption in a project (Davis, 1989). Hassan et al. (2006) stated that the concept of perceived risk could be defined as the amount that will be lost if the outcome of an act is unfavorable and an individual’s subjective sense that the outcome will be unprofitable (Keat & Mohan, 2004; Lu et al., 2005). Perceived risk in customer behavior research is defined as any consumer’s action that may lead to unpleasant consequences (Lo´pez-Nicola´s & Molina-Castillo, 2008).

Previous studies have shown that risk perception is one of the key factors in the adoption of new technology, for example, Lima et al. (2005) explored the concept of ‘risk perception’ at the community level, and concluded that different risk perception patterns are important for the assessment and prevalence of technological growth. Bwalya (2009) found that perceived risk is
considered an important factor under user characteristics that may affect the use of technology in the conceptual model for e-government in Zambia.

Tanakinjal et al. (2010) found a significant direct effect perceived risk had on the intention decision for mobile phone users. Some previous studies have considered a perceived risk as a multi-dimensional construct and stated that perceived risk increased with ambiguity or to the extent of the associated negative consequences (Williams et al., 2003; Gerber & Neeley, 2005). Therefore, perceived risk has been considered an important factor in understanding an individual’s perception of the use of the new monitoring technology.

The adoption of new technologies is subject to various risks faced by different stakeholders in development projects. To adopt the new technology, it is important to select the technology that not only promotes its use in targeted projects but must also be compatible with the current state of the project, since the benefits of adoption mostly stem from the use of the technology (Parks et al., 2015). Ojo (2010) argues that a suitable and proper construction technology can be measured by locally manufactured plant and equipment, the level of utilization of the local construction resources, and locally skilled workforce. Technology marketers in developed countries recognize the important role of fit risk in adopting new technology. However, the concept of fit risk is still relatively new in the international development community. The concept of fit risk may be related to the quality of technology, but it is inherently different (Parks et al., 2015).

Archetti et al. (2015) indicated that for a new technology like IoT to be effective and efficient approaches in asset management planning, it must provide decision support functionalities that identify and address criticalities in civil infrastructure. The collected data must have significance for operations and services, such as inventory, usage, environmental management, and events. Likewise, the quality of the data must be considered in multiple aspects and dimensions. For example, the IoT data should be “fit-for-use” (Backman & Helaakoski, 2016; Cao et al., 2016).

Fit risk arises when potential users are unsure whether the technology meets their needs, lifestyle or capabilities (Heiman et al., 2001). The fit risk arises because technology providers and recipients do not know to whom the technology is appropriate. In a broader sense, the fit risk may vary across different populations for the same technology due to individual idiosyncratic differences in the population, such as socio-cultural factors, skills, economics, geography and environment. Technology that has been successful in some areas may not work in others. Improvements in the quality of technology can increase the potential for profit among the target population and increase, but not eliminate, the individual-level risk of whether the new technology suits one.

The literature agrees that often the key challenge with new technologies is not in the design or the innovation itself, but in the lack of policies and frameworks that can enable adoption, sustainability, and scalability (Pikkarainen et al., 2004; Lee et al., 2004; Yiu et al., 2007; Costa et al., 2016; Herrmann, 2016; Kim et al., 2016; Lidynia et al., 2017; Adler-Milstein et al., 2017; Greenhalgh et al., 2017; Meinert et al., 2018; Golizadeh et al., 2019). For example, previous studies on the adoption of e-banking have reported that users’ perception of the security and privacy risk (most of them under the notion of credibility) have become the inhibitors of internet
banking acceptance (Pikkarainen et al., 2004; Lee et al., 2004; Yiu et al., 2007). Although internet banking is recognised to facilitate transactions, users still refuse to adopt new technologies as they lack control over their behavior and system processes (Pikkarainen et al., 2004).

Golizadeh et al. (2019), in their study of the barriers to adoption of remotely piloted aircraft (RPAs) in construction projects, found that there was concern that unmanned aerial vehicles would affect the safety and privacy of residents. According to Lidynia et al. (2017), the public are concerned about breaches of privacy without their permission. The same thing has been reported by construction workers who feel uncomfortable being monitored by strangers (Costa et al., 2016; Herrmann, 2016; Kim et al., 2016). In general, the perceived risks of adopting new technologies can be attributed to consumer concerns about information system security and system confidence in managing user information and managing user assets (Giovanis et al., 2012). Security- and privacy-related challenges remain among the most significant concerns for creating a technology-led value-based monitoring technology.

When dealing with new technology, people are very concerned about potential security and privacy risks, such as losing their money during the transaction and perceived threats of privacy and personal information leakage. New monitoring technologies, such as structural survey and inspection tasks carried out by sensor technology, will produce large-scale images/videos and require reliable and efficient transfer and storage processing platforms (Irizarry & Costa, 2016, Han & Golparvar-Fard, 2017). However, one of the major challenges for organizations dealing with data storage is cyber-attacks. Cyber-attacks can occur when entities from outside or inside the system interrupt or disrupt the network to gain access, and are especially concerning if the whole system is affected; an example of such attacks is through the use of malware (Ulsch, 2014).

In addition, the common method of transferring real-time data to host base stations in monitoring technology using a wireless platform, is also risky (Kurata et al., 2005). According to Yang and Nagarajaiah (2017), losing a large amount of data is a major concern in wireless transferring platforms. The average data loss may vary between 30 and 50 per cent. Furthermore, data loss can also occur due to failures in the documentation process (Kim et al., 2016). Mass transfer of large amounts of data to offices in different locations is still vulnerable to security concerns due to the leakage of confidential data (Karpowicz, 2017). By effectively managing and analyzing various real-time data, it should be possible to create new services to achieve an efficient and sustainable civil infrastructure (Hashi et al., 2015; Backman & Helaakoski, 2016; Brous et al., 2017).

The other crucial challenge with the adoption of new technology is its workforces, particularly being able to operate at projected levels of the new technology (Ozorhon & Karahan, 2016; Jin et al., 2017; Brous et al., 2018; Tan et al., 2019). Adopting new technology introduces the need for new skills and staff to provide these skills and new organisational forms and processes (Brous et al., 2020). The availability and skills of workers also plays an important role in determining the intensity of the use of new monitoring technology (Ozorhon & Karahan, 2016; Jin et al., 2017). For example, Brous et al. (2020) stated that finding and employing qualified personnel can present enormous challenges due to shortages of skilled staff (Speed & Shingleton, 2012; Yazici, 2014), as well as limited training and educational options (Harris et al., 2015).
The implementation of new technology requires professional interactivity constantly and dynamically throughout a project. However, technical fields are universally known for their lack of professional interaction, especially in the building and construction industry (Ozorhon & Karahan, 2016; Jin et al., 2017; Tan et al., 2019). For new technology to succeed in a project, cooperation with the staff is very important (Arayici et al., 2012; Ozorhon & Karahan, 2016). Many researchers also stated that a reluctance to change or learn new technologies could be prevalent in many organizations (Reyes et al., 2012; Speed & Shingleton, 2012; Yazici, 2014; Brous et al., 2020). New technologies must be integrated into existing business processes to take full advantage of their potential (Yan & Damian, 2008; Lu & Korman, 2010; Elmualim & Gilder, 2014, Tan et al., 2019). Ideally, employees need to know the benefits of new technologies so that they are excited to leverage these technologies to generate revenue for the project.

After decisions are made to adopt new technologies, existing systems and procedures need to be adjusted to incorporate new technologies to limit the disruption and need for additional training while still benefiting from all the new technologies offered. When adopting new technology, stakeholders need to recognize the importance of training to ensure the smooth implementation of the technology (Suermann & Issa, 2009; Ozorhon & Karahan, 2016). However, previous studies have confirmed the stakeholders’ concerns on time and money spent training their workers (Eadie et al., 2014; Yan & Damian, 2008). In addition, stakeholders are also facing risks related to the potential decline in workers’ productivity due to the learning curve. Therefore, the cost and time required for training will be the risks that need to be considered when adopting new technologies. Table 1 summarizes the previous literature related to the endogenous risks in the adoption of new monitoring technology.

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk descriptions</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncertainty</td>
<td>The probability of a different outcome is unknown. (Barham et al., 2014)</td>
<td>Barham et al., 2014; Bryan, 2010; Howley et al., 2012; Foster &amp; Rosenzweig, 2010; Brous et al., 2017; Zhou et al., 2019</td>
</tr>
<tr>
<td></td>
<td>Include both risk and ambiguity (Bryan, 2010)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If there is imprecise knowledge of the new technology, then uncertainty can also affect adoption decisions. (Braham et al., 2014)</td>
<td></td>
</tr>
<tr>
<td>Fit Risk</td>
<td>Potential adopters of technology are uncertain whether the technology will fit their needs, lifestyles, or capabilities.</td>
<td>Ojo, 2010; Parks et al., 2015; Heiman et al., 2001; Li et al., 2016; Brous et al., 2017; Yan &amp; Damian, 2008; Lu &amp; Korman, 2010; Backman &amp; Helaakoski, 2016; Cao et al., 2016</td>
</tr>
<tr>
<td></td>
<td>May vary across different populations for the same technology due to individual idiosyncratic differences in the population.</td>
<td></td>
</tr>
<tr>
<td>Perceived risk</td>
<td>Based on Technology Acceptance Model (TAM)</td>
<td>Walczuch et al., 2007; Teo &amp; Schaik, 2009; Sajjad et al., 2010</td>
</tr>
</tbody>
</table>
- Defined as the amount that will be lost if the outcome of an act is unfavorable, and an individual’s subjective sense that the outcome will be unprofitable (Lu et al., 2005)
- Increased with ambiguity or to the extent of the associated negative consequences (Gerber & Neeley, 2005)
- Negative attitude towards data sharing

Security and privacy risk
- Due to the lack of policies and frameworks that can enable adoption, sustainability, and scalability
- Concerned about anonymity breaches of privacy without permission
- Perceived threats for privacy and personal information leakage
- Cyber-attacks (i.e., malware)

Technical difficulties
- A large volume of the generated data and data loss
- Confidential issues
- Technology complexity

Skilled workers risk
- Negative attitude towards working collaboratively
- Lack of professional interactivity
- Resistance to change

Exogenous Risks of New Monitoring Technology

The exogenous risk in this research is a risk emerging beyond new monitoring technology itself. The exogenous risks, also known as external risks, are those risks that are beyond the control of the project management team but may affect the direction of the project (Zou et al., 2007; PMI, 2008), such as government regulations, natural hazards, labour abolition, legal risks, cash flow.
problems, social and cultural issues, and natural disasters (Loo et al., 2013). Because these risks are beyond the organisation’s control, they are difficult to identify because there is no database available, and no structured methods are occurred to identify them (Rastogi & Trivedi, 2016).

When deciding to adopt new technology, one of the factors is the political risk, which has been recognised in the risk management literature as an important external challenge (Henisz & Zelner, 2003). According to Li and Liao (2007), political risk is about the changes in government laws of the legislative system, regulations and policy, and improper administrative system, etc. Previous literature has argued that the efficiency of political institutions affects the technology diffusion process (Comin et al., 2006; Erumban & De Jong, 2006; Galang, 2012; Arsyad & Hwang, 2014), highlighting the moderating role played by governance. The government’s efficiency and ability to control and enforce contracts is highly relevant to an organization’s technology purchases. It minimizes additional production costs and assists the dependence of exchange terms between firms based on inevitable circumstances (Rodriguez et al., 2005).

Social risk is increasingly important for any venture in risk allocation. The social risk can be defined as the situation where the social and political pressure from those who do not have an interest in a project but has a huge impact on the project greatly affects the outcomes (Kleijnen et al., 2009; Savas, 2017). Hence, the social risk is more likely to occur with services because of the service encountered (Murray & Schlacter, 1990; Mitchell & Greatotex, 1993). Murray & Schlacter (1990) defined social risk as the potential loss of user’s esteem, respect, and/or friendship offered by others (Laroche et al., 2004). For example, negative attitudes of family and friends or even a direct relationship with technology marketers on innovation will affect users’ adoption of the service innovation. Within the technology adoption process, social risk is one of the dimensions under perceived risk that affects users’ attitudes toward adoption intentions of new technology (Hirunyawipada & Paswan, 2006).

Culture is a difficult concept to define. A widely accepted definition by Hofstede (2001) characterizes culture as the collective mental programming of a people that distinguishes them from others. Culture influences individuals working in an organization, and can impact the adoption of technology in the organization. Users’ attitudes toward new technology may be shaped by their different values and lifestyles (Choi et al., 2014). In addition, national culture dimensions have been used extensively in different countries (Hofstede, 2001); for example, the difference in IT adoption between developed and developing countries (Baker et al., 2007).

Grover et al., 1994 have identified the national cultural differences in technology adoption within SME: technology spending, centralized versus decentralized environments, hardware, and telecommunications, innovation/risk-taking, IS and strategic planning integration, and information sharing (as cited in Beekhuyzen et al., 2005). Brettel et al. (2015) reported that all key dimensions of organizational culture (society, hierarchy and rationality) have a strong influence on innovation, proactiveness and risk-taking, with the focus on a firm’s entrepreneurial orientation (EO) at SMEs.

As referred to here, economic risk is a periodic economic threat when organizations are unable to evaluate their probabilities or cost implications. It is an economic condition or factors, inflation rate, interest rates, foreign exchange rates and economic growth patterns etc., which can negatively impact business operations or profitability and have long-term effects (Rastogi &
Trivedi, 2016). When considering how to adopt new technology, some factors need to be considered, for example, the actual total cost to the organisation and the range of desired organisational outcomes (the benefits of adopting the new technology, including tangible and intangible benefits) (Barlish & Sullivan, 2012; Jin et al., 2017; Zhang et al., 2018). The regulatory environment and governmental institutions more generally can have a powerful effect on technology adoption, often via the ability of a government to “sponsor” a technology with network effects (Hall & Khan, 2003).

Implementation of new technologies can bring new risks to stakeholders (Eadie et al., 2014). For example, construction companies are required to use Building Information Modeling (BIM) in their projects, but lack of BIM standardisation by the authorities is a common obstacle to BIM implementation (Tan et al., 2019). This puts shareholders in a precarious position as it requires them to spend extra time and money to address the potential risks. Errors in handling risks result in poor decision-making; thus, additional time and budget are required to address these unforeseen errors.

Legal risk covers all aspects of the law, such as consumer law, security standards, labor law, taxes, resources, imports and exports, etc. (Rastogi & Trivedi, 2016). A new legal contract is needed to avoid possible arguments associated with the new technology responsibilities and liabilities (Nawari, 2012; Bui et al., 2016). Moreover, appropriate legislation to protect the rights of intellectual property (IP) of new technologies, such as data ownership, is very important in the adoption of new technologies (Ozorhon & Karahan, 2016). Table 2 summarizes the previous literature related to the exogenous risks in the adoption of new monitoring technology.

Table 2: The exogenous risks in adoption of new technologies

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk descriptions</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political risk</td>
<td>● Government stability</td>
<td>Henisz &amp; Zelner, 2003; Li &amp; Liao, 2007; Arsyad &amp; Hwang, 2014; Galang, 2012; Erumban &amp; De Jong, 2006; Comin et al., 2006; Rodriguez et al., 2005</td>
</tr>
<tr>
<td></td>
<td>● Corruption, party in control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Regulation trends</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Tax policy and trade controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Government policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Likely changes to the political environment</td>
<td></td>
</tr>
<tr>
<td>Social risk</td>
<td>● Population growth and demographics</td>
<td>Savas, 2017; Archetti et al., 2015; Aono et al., 2016; Kleijnen et al., 2009; Mitchell &amp; Greatotex, 1993; Murray &amp; Schlacter, 1990; Laroche et al., 2004; Hirunyawipada &amp; Paswan, 2006</td>
</tr>
<tr>
<td></td>
<td>● User attitudes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● National and regional culture</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Lifestyle choices and attitudes to these</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Socio-cultural changes</td>
<td></td>
</tr>
<tr>
<td>Cultural risk</td>
<td>● Socio-cultural changes</td>
<td>Choi et al., 2014; Baker et al., 2007; Grover et al., 1994; Beekhuyzen et al., 2006</td>
</tr>
<tr>
<td></td>
<td>● National and regional culture</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Lifestyle choices and attitudes to these</td>
<td></td>
</tr>
</tbody>
</table>
The eleven risks of new monitoring technologies identified previously are used to develop the cause-and-effect model for structural health monitoring (Figure 3).

**Figure 3: Risks of new monitoring technology for structural health monitoring**

**Conclusion**

The urgent need for industry upgrading and the emergence of innovations and information technology provide a favorable opportunity for implementing new monitoring technology in structural health monitoring. However, the implementation of new technology in Malaysia’s structural monitoring project remains in its infancy. This study contributes to the body of knowledge by identifying eleven main risks affecting the adoption of new monitoring technology in the structural health monitoring context. Identifying risks in new technologies has been recognised as an important process to achieve project objectives in terms of time, cost, quality,
safety, and environmental sustainability. The identified risks are then used to develop the risk breakdown structure used for future development of risk assessment model for damage diagnostic technology adoption decision in structural health monitoring.

Acknowledgement

This study is funded through IIRG007C-2019, Risk Assessment Model for Smart Damage Diagnostic Algorithm to Assess Black Swan Events.

References


value-based healthcare system. *BMC Medical Informatics and Decision Making, 18*(1), 100.


