Association for Information Systems
AIS Electronic Library (AISeL)

GlobDev 2009

Proceedings Annual Workshop of the AIS Special Interest Group for ICT in Global Development

Winter 12-14-2009

# Contributing Factors in the adoption of RFID in Emergency Management: A Multiple Case study

Ashir Ahmed
*Monash University*, Ashir.Ahmed@buseco.monash.edu.au

Lyfie Sugianto
*Monash University*, Lyfie.Sugianto@buseco.monash.edu.au

# CONTRIBUTING FACTORS IN ADOPTION OF RFID IN EMERGENCY MANAGEMENT – A MULTIPLE CASE STUDY

**Ashir Ahmed**[1]
Ashir.Ahmed@buseco.monash.edu.au
**Lyfie Sugianto**[2]
Lyfie.Sugianto@buseco.monash.edu.au
Faculty of Business and Economics, Monash University, Australia

**ABSTRACT:** *By presenting emergency management organizations of developed countries as early adopter of RFID in emergency management, this paper aims to minimize the disastrous impacts of emergencies currently faced by mankind; especially in developing countries. We conduct a study in the context of RFID adoption in emergency management and seek to answer the question - What are the contributing factors in the adoption of RFID in emergency management? In order to answer this question, a research framework is proposed by using a rather loose interpretation of task-technology fit (TTF) model. Multiple case study method has been employed to explore the contributing factors of RFID adoption. It is anticipated that the findings of this research will not only enhance the research in technology adoption, but also assist the emergency management organizations to better plan the adoption of pertinent technologies such as RFID for emergency operations.*

**Keywords:** RFID, emergency management, task-technology fit, multiple case study, adoption model

## INTRODUCTION

Emergency is defined as a situation which has serious threats to human life and property (Parker 1992). Generally, emergencies are categorized under three categories including natural, manmade and hybrid (Eshghi et al. 2008; Kimberly 2003; Shaluf 2007). Although, it is not possible to prevent an emergency situation, especially the natural emergency, but the chances of its occurrence (emergency risk-ER) can be controlled to some extent. ADPC (2000) suggested that:

$$\text{Emergency Risk} = \frac{\text{Hazard x Vulnerability}}{\text{Capacity}}$$

Where:

**Hazard:** Hazard is an event, happening or human activity which has the chance for causing risk and danger to life or damage to properties and the environment.

**Vulnerability:** The term vulnerability is described as the physical, social, economic, cultural and environmental factors and conditions, which increase the community's feeling about disasters. In addition, inability of individuals, households and the community to prepare for and respond to hazards also increases their vulnerability against an emergency situation.

**Capacity:** Capacity is knowledge, skills, resources, abilities and strength, present in individuals, households and the communities, which enable them to prevent, prepare for, stand against, survive and recover from a disaster.

Although, risk of an emergency cannot be eliminated, but the equation mentioned above described that the capabilities of individuals or communities of coping up with emergencies can cause in minimizing the impacts of an emergency. Furthermore, it has been observed that the impact of emergencies on developing countries is far greater than on developed countries (Ayala 2002). The impact of emergencies generally depends on few factors. For instance, in case of natural disaster, most of the developing countries such as many Latin Americans and Asian countries are located in areas which are highly prone to natural hazards. Circum-Pacific Volcanic Belt as an example, where approximately 80% volcanism activities take place and result in emergences such as Nevado del Ruiz in Colombia, that caused 21,800 deaths(Ayala 2002). Similarly, Asia and Latin America share the highest concentration of flooding and associated risks due to hurricanes, cyclones, tropical storms, typhoons, and monsoons(Ayala 2002). In addition to the geographic locations of developing countries, their economical conditions also participate in escalating impact of emergencies (Anderson et al. 1992). For instance, more than 9000 people were died and about 11% (3.2 million people) of the total population in Central America was affected by the consequences of Hurricane Mitch. The impact was not homogeneous in all the countries. In Honduras the losses were equivalent to 80% of the 1997 GDP, whereas those in Nicaragua were almost 49% of GDP (Ayala 2002).

In short, the overall impact of emergencies on developing countries is much greater than the developed countries that require careful preparation and execution of emergency management plans.

Emergency management is a process that encapsulate all aspects of emergency situation including, risk, consequences, pre and post emergency activities such as prevention, mitigation, preparedness, response, recovery and rehabilitation (DPLG-1. 1998). Literature relevant to emergency management reported various models to conceptualize various types of emergency management phases. A significant body of literature is available which decomposed the emergency management life cycle in several phases such as three phases (ADPC. 2000; Atmanand 2003; Richardson 1994), four phases (Kimberly 2003; Tuscaloosa. 2003), six phases (Manitoba-Health-Disaster-Management 2002; Turner 1976), seven phases (Toft et al. 1994) and eight phases (Kelly 1999; Shaluf et al. 2003) of emergency management life cycle. In addition to the development of various models, research and practitioners have tested several technologies such as global information system (GIS), information technology (IT), satellites, global positioning system (GPS), global system for mobiles (GSM) and RFID (Derekenaris et al. 2001; Fry et al. 2005; Gunes et al. 2000; Marincioni 2008) in emergency management.

RFID is a term coined to use short to medium range of radio technology used to communicate between two objects without any physical contact. Objects on two sides of RFID link can be either stationary or moveable. A typical RFID system consists of (a) tag (b) reader/interrogator and (c) an antenna. Tags can be classified into active tags and passive tags. Active tags operate with a battery attached to them whereas passive tags are powered by the rectification of radio signals sent by the reader. Readers are comparatively complex device which is to send radio signals to the tags and locate them. These are connected with a host computer or a network. Antenna is connected with RFID tag and mainly responsible to absorb radio signals sent by the reader and pass them to RFID tag. A typical RFID system is able to communicate in a range of radio frequencies including low frequency, high frequency, ultra high frequency and microwave. The working principle of RFID technology is illustrated in Figure 1.

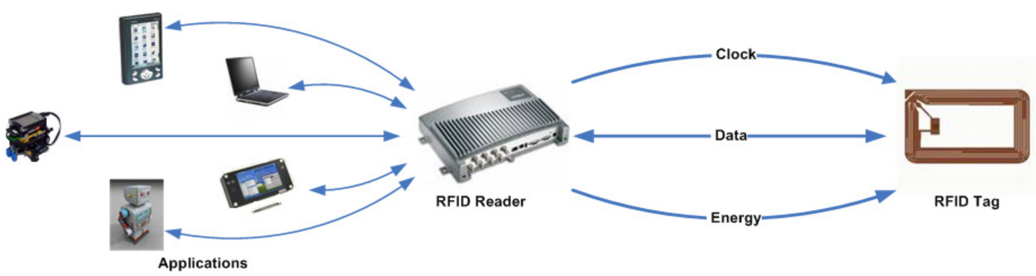


Figure 1: Working principle of RFID technology (Ahmed et al. 2008)

In order to examine the RFID adoption in emergency management, our previous work identified the common activities in existing emergency management models and segregated them into four major categories including authentication, automation, tagging/tracking and information management (Ahmed et al. 2008). Furthermore, these activities are used to elucidate the task characteristics of emergency management process. Although, such activities offer basic criteria to evaluate the feasibility of RFID in emergency management but the factors which influence the RFID adoption in emergency management were still unclear. Several technology adoption models are reported in the literature but their suitability to be applied in emergency management context is unexplored. Hence, our study aims to examine the suitability of existing technology adoption models in the context of emergency management. In facilitating the study, a framework is proposed as a means to identify various factors in RFID adoption process.

The rest of the paper is structured as follows. The following section presents the review of technology adoption models. Next, the proposed framework is described, followed by the research method and the strategy for data collection. Empirical findings obtained from the case studies are then discussed. The paper concludes with a brief summary outlining the empirical findings of this study.

## LITERATURE REVIEW

Generally, the relevant literature offered several different interpretations of the term 'adoption' such as 'pre-adoption', 'post-adoption', 'usage' and 'implementation' (Hoppe 2002; Karahanna et al. 1999; Sharma et al. 2007). Furthermore, the notion of 'adoption' was also found to be synonymously used with several other related terms like, 'decision to accept', 'tend to adopt', 'use', and 'utilization' (Rahim 2003). Consistent with this line of thinking, some IT adoption researchers for example, Lertwongsatien et al. (2003) used the term 'adoption' to refer to the decision making stage where an IT application or process was selected for subsequent use. Adoption was operationalized if an organization had a specific plan or intention to embrace or accept a new IT application or software process. Another group of researchers for example, Scupola (2003) and Runge et al. (2003) on the other hand described 'adoption' as the implementation stage in which adoption was operationalized as the actual level of IT use in an organisation. Similarly, Tornatzky et al. (1990) suggested a three stage process for technological adoption in organizations. These stages include initiation, adoption and implementation of technology. This paper looks at 'adoption' as the process before the actual implementation of

RFID in emergency management and examines the organizational intentions to adopt RFID technology from task-technology fit perspective. In short, the term 'adoption' used in this paper can be subject to follow the second stage of Tornatzky et al. (1990) model of the introduction of technological innovation process. The following discussion covers the TTF (task-technology fit) developed by Goodhue et al. (1995) and Zigurs et al.(1999) and used a rather loose interpretation of TTF for developing a framework for adoption of RFID in emergency management.

Two versions of TTF model have been reported in the literature (i) task technology fit model proposed by Goodhue et al. (1995) which examines the impact of "fit" between task characteristics and technology characteristics on individuals, whereas (ii) task technology fit model presented by Zigurs et al. (1999) explored the impact of task technology "fit" on group rather than individual. Both versions of TTF model agreed that the overall performance of an individual/group based on best fit of the technology characteristics and tasks undertaken by that individual/group. TTF models presented by Goodhue et al. (1995) and Zigurs et al. (1999) highlights the basic concept that a proper match between task and technology characteristics results in better performance impacts. This concept is used in this paper for development of a conceptual framework to examine the adoption of RFID in emergency management.

## CONCEPTUAL MODEL

In order to obtain a better understanding about the adoption of a technology such as RFID in emergency management, the concept of task-technology fit offers a suitable starting point and is, thus, applied in this research. By and large, this research use a rather loose interpretation of theories developed by Goodhue et al.(1995) and Zigurs et al. (1999) to develop a framework to predict the successful adoption of RFID in emergency management. Having its roots in the theory of task technology fit, Figure 2 depicts the key components of the conceptual model.

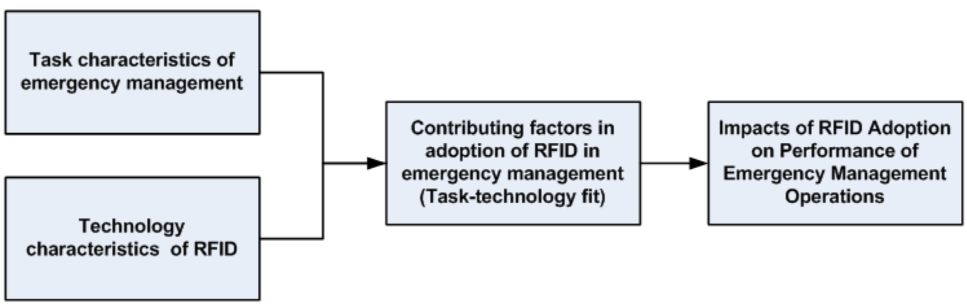


Figure 2: Conceptual model based on theory of task-technology fit

Following is the brief description of main components of the conceptual model:

***Task characteristics*** refer to the key activities of emergency management in the perspective of technological use.

***Technology characteristics*** refer to the features of RFID in context of task characteristics of emergency management.

***Task technology fit*** refers to the degree by which task characteristics matches with the technology characteristics. It also addresses the factors which influence the “fit” between task and technology characteristics.

***Performance impacts*** refer to the impacts of technological adoption on emergency management operations. (Beyond the scope of this paper)

Following discussion unfold various components of conceptual model presented in Figure 2.

**Task Characteristics of Emergency Management**

Significant volumes of literature haves been written on defining the emergency management process by decomposing it into several phases. The common objective to decompose emergency management process is to provide a basis and structure for segregating the problem into main areas and thus contribute to manage them successfully. According to Kelly (1999), the development of emergency management model can be useful for the following reasons (i) during the time-critical situations, a model can help in simplifying the complex events of an emergency by distinguishing between its critical elements (ii) a model can help in better understanding of the current situation and can thus facilitate the planning process and the comprehensive completion of emergency management plans (iii) a model can help in qualifying emergency event (iv) a model can help in establishing a common base of understanding for involved. It can help in the integration of the relief and recovery efforts. Table 1 provides an overview of existing emergency management models by segregating them according to the phases mentioned.

Table 1: Existing emergency management models

| Phases | Proposed by | Model Details |
|---|---|---|
| Three phases | Richardson (1994) | Consist of three stages (i) before disaster (ii) during disaster (iii) after disaster |
| | (ADPC. 2000; Atmanand 2003) | Three phases of this model such as (i) preparedness strand (ii) relief / response strand (iii) rehabilitation and recovery strand. |
| Four phases | Kimberly (2003) | This model consists of phases including (i) mitigation (ii) preparation (iii) response and (iv) recovery. |
| | Tuscaloosa (2003) | This model proposed four phases as (i) mitigation (ii) preparedness (iii) response and (iv) recovery. Mitigation is suggested as a starting and ending point of this cyclic model. |
| Six phases | Turner (1976) | This model consists of six stages: (i) notionally normal starting points, (ii) incubation period (iii) precipitating event (iv) onset (v) rescue and salvage and (vi) full cultural readjustment |
| | (MHDM 2002) | This model consist of six phases: (i) strategic plan (ii) hazard assessment, (iii) risk management (iv) mitigation (v) preparedness (vi) monitoring and evaluation |
| Seven phases | Toft et al. (1994) | Seven phases presented by this model: (i) the incubation period (ii) the operation-socio-technical system (iii) precipitating event (iv) disaster itself (v) rescue and salvage (vi) inquiry and report (vii) feedback. |
| Eight phases | Ibrahim M. Shaluf et al. (2003) | This model consist of eight phases: (i) inception of error (ii) accumulation of errors, (iii) warning, (iv) failure of correction (v) disaster impending stages (vi) triggering events (vii) emergency stage and (viii) disaster |
| | Kelly (1999) | Phases of this model include (i) warning (ii) preparedness (iii) mitigation (iv) disaster prevention (v) development (vi) reconstruction (vii) rehabilitation (viii) emergency response. |

Overview of the emergency management models presented in table 1 helps in qualifying various types of emergency events and offered a broad concept of activities involved in emergency management process. Although, all models reflects the emergency management life cycle, but they used different types of phases to represent it, which eventually caused the lack of standardization and uniformity among such models. In addition to that, the concept of phases offered least support for the technological adoption in emergency management. Therefore, this research introduced the concept of common activities involved in emergency management process and argued that a potential technology such as RFID should be evaluated on the basis of its capabilities to conduct such activities. These activities will further categorized based on the uniformity and will be used for developing an activity based framework for adoption of RFID in emergency management later in this paper.

Based on the commonalities, activities involved in emergency management life cycle are grouped together to form four major activities and are collectively known as AATI (authentication, automation, tagging/tracking and information management). In addition, various underlying activities cited in existing emergency management models were carefully studied and grouped together on the basis of commonalities involved in them and shown in Figure 3.

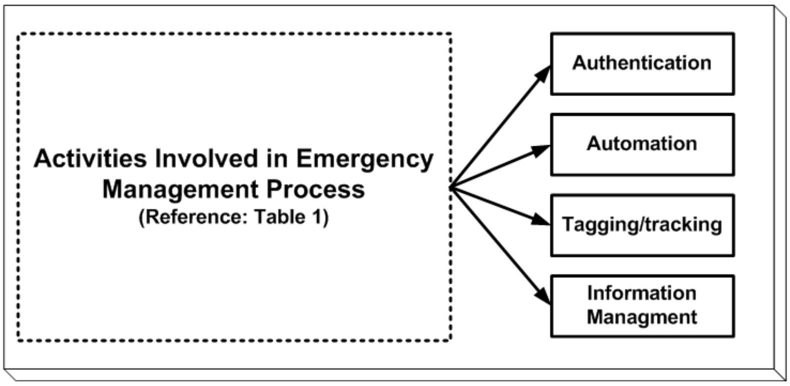


Figure 3: Classification of emergency management activities

Following is the brief description of these activities:

***Authentication*** can be defined as a process by which a system verifies the identity of a user who wishes to access it (M-Tech 2007). In the context of emergency management, authentication covers the following sub-activities (i) implementing authentication protocols (ii) assigning privileges to the users (iii) verification of access requests (iv) obstruct the unauthorized access/use of system.

***Automation*** is defined as a process of using control system such as computers to control machinery and processes; replacing human operators (Thomas 2002). Emergency related experiences suggest that in most emergency cases, the real barriers are not lack of data or insufficient technological capabilities. The real bottleneck is the automatically handling of information (Zlatanova et al. 2004). Automation in context of emergency management includes the following sub-activities (i) identification of tasks which can be done by control systems;

replacing humans (ii) automatic detecting of inputs using sensors (iii) automatic decision making based on the received data; using artificial intelligence (iv) using technology to assist in human decision making process.

***Tagging and Tracking*** is a process of capturing and maintaining the information of any moving object and it has been a real challenge for researchers and scientists. Most of the emergency management experiences show that during an emergency situation, one of the most important and urgent problems at the scene is the overwhelming number of patients that must be monitored, tracked and managed by each first responders (Barbara 2008; Fry et al. 2005; Killeen et al. 2006; Remko et al. 2005). Tagging/tracking is a group of following sub-activities of emergency management process (i) marking or tagging of humans and objects (ii) use these tags to track humans and other objects (iii) use these tags for human/object management before, during and after emergencies.

***Information Management*** is the collection and management of information from one or more sources and distribution to one or more audiences who have a stake in that information or a right to that information (Sagun et al. 2008). It is further argued that the lack of inadequate and incomplete information/communication is considered to be the main operational problem during emergency management (Wybo et al. 1998). Study of recent emergencies shows that at some level or another, information was available which could have prevented the emergency from happening (Chan et al. 2004; Lee et al. 2000; Mansouriana et al. 2006; Quarantelli 1988). Information management in emergency management is a collection of several other activities which comes under the umbrella of information management. Following sub-activities are grouped together to form information management (i) training/drills/exercises (ii) collect information from various resources (iii) broadcast warnings/alerts (iv) building and maintaining information pools (v) communication with other emergency management organizations.

**Technology Characteristics**

According to Goodhue et al. (1995) technologies are viewed as tools used by individuals in carrying out their tasks. Similarly, technology characteristics are the features offered by a technology to its users. Technological characteristics presented in conceptual model refer to the features offered by a technology in order to conduct the activities including authentication, automation, tagging/tracking and information management. Significant volumes of literature are available which reports the capabilities of RFID for conducting activities such as AATI (Estevez 2005; Fry et al. 2005; Kritzler et al. 2006; Lehtonen et al. 2007; Michael et al. 2005a; Mousavi et al. 2002; Wang et al. 2006; Xiao et al. 2006)

**Task-technology Fit:** ***(contributing factors in adoption of RFID in emergency management)***

Although, the factors presented by Goodhue et al. (1995) are specific to the adoption of information technology by its users (individuals), but, they provide some foundation, and hence some of them are borrowed in order to identify the contributing factors for adoption of RFID by emergency management organizations. Figure 4 shows the original factors presented in TTF, and how TTF was used to define the contributing factors of RFID adoption in emergency management.

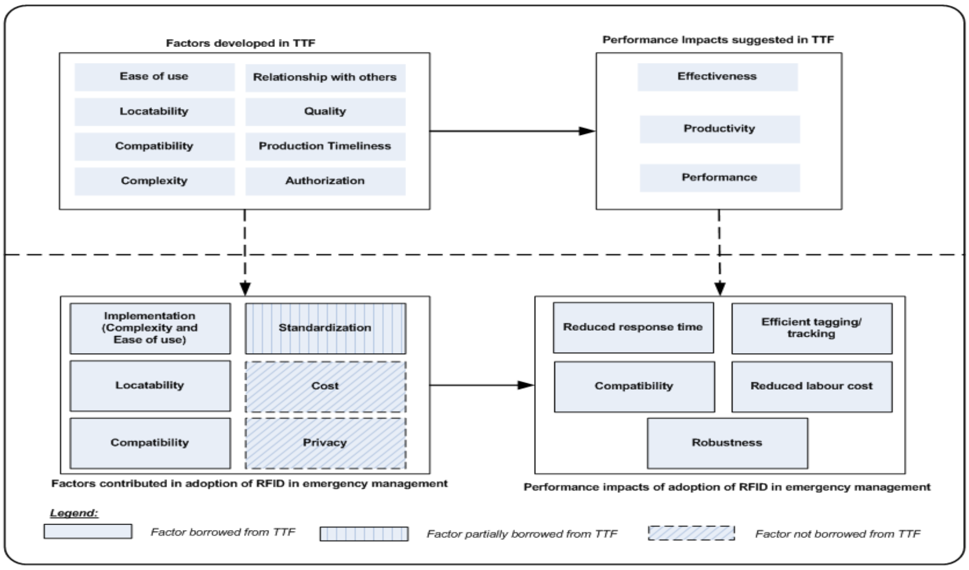


Figure 4: Contributing factors borrowed from TTF

As shown in Figure 4, key factors of technological adoption are borrowed from the theory of TTF and are then tailored to address the specific needs of RFID adoption in emergency management. Furthermore, the contributing factors are further amalgamated with the key concept of TTF and were used in the development of framework for RFID adoption in emergency management.

### Performance Impacts

It is anticipated that the successful adoption of RFID yields several impacts on the performance of emergency management organizations. However, the identification and significance of such performance impacts are beyond the scope of this paper.

## FRAMEWORK FOR RFID ADOPTION IN EMERGENCY MANAGEMENT

As mentioned earlier, the emergency management activities such as AATI offers basic criteria to evaluate the potential of RFID in emergency management, therefore, the framework presented in this paper is known as activity based framework for the adoption of RFID in emergency management and is shown in figure 5.

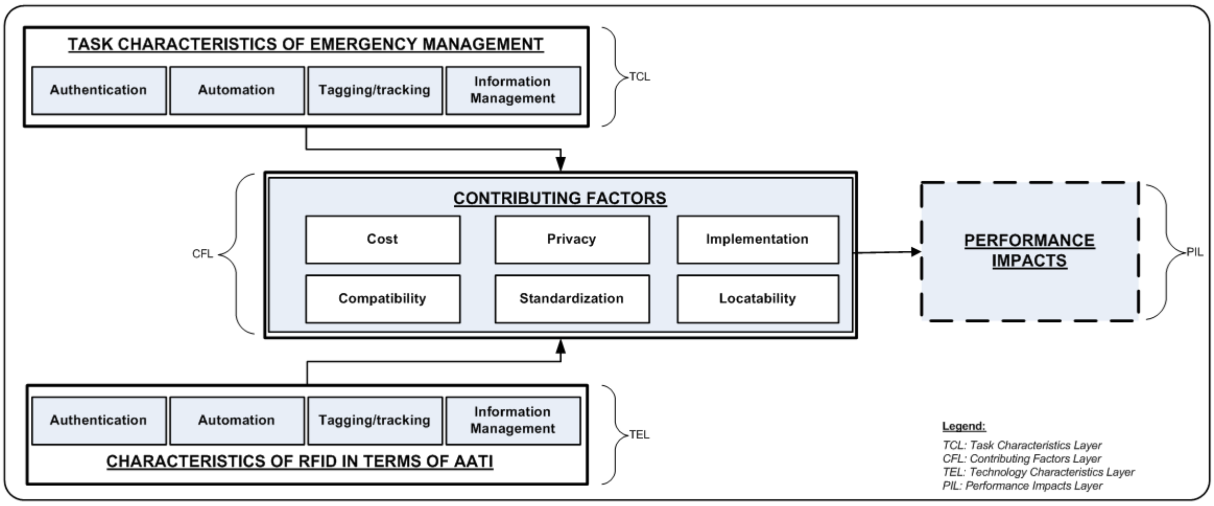


Figure 5: Activity based framework for RFID adoption in emergency management

The framework (shown above) consists of three main layers:

### Task Characteristics of Emergency Management Layer (TCL)

This layer represents the task characteristics of emergency management. Based on the discussion presented earlier in this paper, four key activities such as authentication, automation, tagging / tracking and information management and are used as task characteristics of emergency management.

### Contributing Factors Layer (CFL)

This layer refers to the factors contributed in RFID adoption in emergency management. Seven factors are identified in this layer and are discussed below:

***Cost:*** Higher cost of technology leads to lower intent to adopt (Saunders et al. 1991). The less expensive the innovation, the more likely it will be adopted (DiMaggio et al. 1983). On the other hand, Sharma et al. (2007) argued that the innovation cost relative to innovation benefits are more meaningful. Cost of technology refers to the purchase, setup, maintenance, up gradation and training costs required to use a technology. For instance, the cost of RFID plays a significant role in the decision of using this technology for conducting emergency operations. An Accenture survey found cost to be one of the two primary barriers to the implementation of RFID (Michael et al. 2005a). Therefore, the emergency management organizations must prepare a budget before they implement RFID. Lack of consideration of cost-related issues could potentially produce an ineffective and/or inefficient deployment of RFID. This can eventually lead the emergency management organizations straying away from their original goals of full implementation, or attempting cut some corners which may lead to a less than optimal implementation of RFID (Smith 2005). In conclusion, this factor encapsulates various cost-related matters that can be encountered during the deployment of technology such as RFID in emergency management**.**

***Privacy:*** During emergency or non-emergency situations, it is equally important to keep data and other resources private and secure. However, during emergency situations, where it is difficult to enforce security protocols, it becomes more critical to secure the important information. For RFID, privacy poses a huge barrier towards its use in all domains and it has received much attention in recent years as journalists, technologists, and privacy advocates who have debated the ethics of its use (Want 2006). It is further claimed that privacy issues loom as one of the biggest threats to the success of RFID. Privacy concerns have the potential to “stop a technology dead in its tracks”. In such circumstances, is RFID a suitable choice for emergency operations? This factor address this question and other privacy-related concerns associated with the use of RFID in emergency management.

***Implementation (Ease of use):*** This paper refers implementation factor as ease of use and the complexity involved in the use of RFID in emergency management. Rogers (1983), and Goodhue et al. (1995) agreed on the fact that the less complexity and more ease of use of technology plays a vital role in the successful use of technology. During emergencies, it can be foreseen that the technological infrastructures have to face extreme working conditions like harsh weather and insecure working environment. Inadequate time, human and other technological supports are also very common constraints while working in emergency situations. People working in emergency situations have the pressures to setup and implement the required technological infrastructure in the shortest possible time with minimum resources. Therefore, the setup and implementation requirements as well as ease of use of technology contribute in the decision of its adoption for emergency operations. For instance, with RFID as a technology to be used in emergency management, its easy implementation can result an extra ordinary performance in emergency situation. Overall, the implementation issues highlight the various types of implementation-related concerns like physical installation of technology (RFID devices), time and training required to setup technological infrastructure in an emergency situation, ease of use, human and technological support and maintenance requirements of that particular technological infrastructure**.**

***Locatability*: ** Originally, in task-technology fit model, locatability was referred as ease of determining what data is available and where. Due to varying nature of RFID from information technology, this thesis used the term locatability to address the issues related to physical location, accessibility and clear definition of use of RFID in emergency management and recommended that it as an important factor in the adoption of RFID in emergency management. Moreover, this factor underlines the significance of appropriate deployment of RFID at various physical locations and its easy access when required. Although, the locatability is considered as a complex and non-trivial task (Lorincz et al. 2004), it play a significant role in the successful adoption of technology (Goodhue et al. 1995).

***Standardization****:* Standardization refers to the process of developing and agreeing upon technical standards. It assures that the working of a technology follows some well defined standards which are globally recognized. Since, a standard technology is globally accepted and used, hence more technical support is generally available which in turn require less training in order to operationalize that technology. Deploying a standardized technology in emergency management guarantees the smooth operations of technology in varying working environments. Standardization is an important process in RFID deployment. It ensures the seamless working of different RFIDs regardless of their types and frequency bands. According to Michael et al. (2005b) there is an apparent lack of standards hindering the technology's adoption and its global use. Current IT EPC Global network (a member based organization) is working on RFID standardization, but its standard is yet to be backed by International Standard Organization (ISO). Authors further argued that there is no standard supported by all stakeholders that meets the need of all users. Therefore, the aim of this factor is to investigate and resolve the standardization issues involved in the use of technology such as RFID in a particular emergency scenario.

***Compatibility**:* As suggested by Rogers (1983) and Goodhue et al. (1995), compatibility play an important role in the successful use of technology. Therefore, this factor addresses the ability of a technology to work along with other technological infrastructures. In the perspective of emergency management, importance of this factor is vital. Technologies with the ability to work along with other supporting technologies and offer better compatibility are considered much as compared to the others. For instance, in order to achieve maximum benefits from RFID deployment in emergency management the support of some other technologies such as information technology, computer technology and bio-technology could be required.

**Technology Characteristics Layer (TEL)**

This layer encompasses different types/subtypes of RFID technology, features offered as well as the merits and demerits involved in the use of RFID. Moreover, the features offered by a technology are illustrated in terms of authentication, automation, tagging tracking and information management.

## METHODOLOGY

Multiple case study method is adopted to empirically validate the proposed framework. Selection of information-rich cases is significant for successful case studies (Paton 1990). As this study aims to investigate the factors involved in the technological adoption in emergency management several organizations have been identified, approached and invited to participate. The criteria in selecting the participating organizations are that they have already used or willing to use any technology in emergency management. The selection criteria are imposed to achieve analytical generalization for the emergency management organizations.

### Number of Cases and Their Selection

To improve the generalisability of the research findings and performs the theoretical replication across the cases, five organizations were selected. Although five cases may be too few to allow statistical validity, they allow reasonable range for acceptable theoretical replication. Similarly, many well-known case studies have been used on this number or fewer of cases (Dick 2002;

Eisenhardt 1989; Markus 1983; Orlikowski 1983). In order to maintain the privacy of participating organizations, they are assigned an alphabetic characters such as A, B, C, D and E. The following table (Table 2) lists the details of the participating organizations.

Table 2: Overview of participating organizations

| Case | Key Operations | Interviewee | Employees | Location |
|---|---|---|---|---|
| **A** | Responsible for state's disaster management arrangements and provide chemical hazard advice and emergency helicopter services. | Director Disaster Operations | 230 | Australia |
| **B** | Involved in activities such as drills, emergency management trainings and coordinating with other emergency management agencies. | Emergency Management Coordinator | 800-900 | Australia |
| **C** | Perform wide range of roles including planning for disasters (both natural and manmade) and involved in response and rescue operations. | Reg. Dir., Emergency Mgt. | 1600 (including volunteers) | Australia |
| **D** | Work with communities to reduce risk, mitigate the effects of, prepare to respond and recover from disasters. | Logistic Officer | 1661 | Switzerl-and |
| **E** | Maintain essential supplies and running a national disaster victim enquiry service, together with other emergency management activities. | Logistics Delegate | n/a | New Zealand |

**Strategy for Data Collection**

In-depth interviews were sought from following three types of informants (i) emergency managers (ii) senior executives and (iii) emergency coordinators. The interviews were conducted over 8 month period from October 2007 to June 2008. During this period of time, data from multiple sources, such as formal in-depth interviews with the key participants, organizational web sites, telephonic conversation and other relevant documents were collected. The case study conducted in this research mainly relies on formal in-depth interviews with key informants, whereas sources other than formal interviews were primarily used to assist in understanding and explaining the interviews material and results. Once all the data was collected, it was transcribed in full and sent back to the participants for data verification.

**Data Analysis**

In order to validate the framework for RFID adoption, an interview protocol was prepared. Aim of this interview protocol was to unfold the significance of several factors which contribute in decision of adopting RFID in emergency management. In addition, the participants of case study were also invited to record their feedback about the factors other than those identified by this research. Overall, the interview questionnaire consists of ten questions related to the contributed factors. Out of those nine questions, the first two questions were open-ended in nature, targeting the organizations' experience in adopting RFID for emergency operations. The next six questions were semi-structured and each question was targeted to address each individual factor. Following the recommendations of Rogelberg (2004), one catch-all (open-ended) question was asked at the end. The development of interview protocol is primarily based on the initial research questions. Pattern matching technique is used to analyze the empirical findings.

## RESEARCH FINDINGS

The following discussion summarizes the research findings by highlighting the empirical evidences from participating organizations.

**Cost Factor:** To investigate the importance of cost factor, the following question was asked from case participants:

*"How important is the cost of a technology/RFID in an adoption process in emergency management? Please explain."*

For this question, five responses were recorded; one from each participating organization. Empirical evidences collected from case organizations highlighted several aspects of cost factor in technological adoption process. For instance, according to the informant of case A, this factor was:

"*[…]very important, disaster management is always competing for resources with more mainstream disciplines[…]*".

On the other hand, an official document of case A reported that investment made during pre-disaster phases in terms of acquiring good technologies and establishing other means for preparedness actually saved money during and after disaster phases. It was reported as:

"*[…]every $1 spent on disaster mitigation saves at least $3 in economic and social recovery costs[…]."*

Consistent with the argument made by official document of case A, the respondent from case B clearly mentioned that the emergency management organizations had huge potential for new and pertinent technologies (irrespective of their costs) to be adopted and utilized. The following part of response collected from case B showed this fact:

"*[…]basically if there is good technology available the way we are operating our organization, we will pay more. So it is not all the matter of money, but if there is a good value of money then certainly we will pay for technology and bear the cost[…]*"

As mentioned by the response of case B, cost (dollar value) of the technology became relatively less important for emergency management organizations when compared to the associated benefits.

Similarly, response from case C also highlighted the fact that emergency management organizations were more interested in the benefits associated with the use of a technology and could pay cost for a good product or service. The following comments reflect this view point:

"*[…]we foresee the benefits which we will get against our investment on some technology. So, I think it would be primarily based on what we will get at the end of the day[…].*"

In contrary to the empirical evidences collected above, case D supported the importance of cost factor in technological adoption process. Case D informant stated as:

*"[…]it is highly important, generally in all disciplines and specifically in emergency management[…]".*

Although the comments reported above highlighted various aspects of cost factor, case E covered another aspect relating to the decision of adopting a new technology in emergency management. Performance or success rate of a particular technology in other fields (domains) was considered very important for securing or allocating finances for the adoption of a new technology in emergency management. Following part of case E highlighted this fact:

*"[…] it is very difficult in trying to get donors to get money for technology until they see the benefits after the operation […]."*

It was further stated that:

"*[…] the governments in the country really fund for an emergency and it is really very difficult to get money until it really shows the value […]*".

The above arguments also highlighted the association of cost and the benefits associated with the use of a technology in emergency management. Technologies offered more benefits to emergency organizations could secure more finances.

Based on the above findings, it is concluded that although, the cost of a technology is an important factor in the adoption and successful use of technology but for emergency management, the associated benefits of the technology overcomes the dollar value of technology.

**Locatability Factor:** To empirically validate the importance of locatability in emergency management, the following question was asked:

*"How important is the locatability of technology/RFID on specific task in emergency management? Please explain."*

Four out of five organizations agreed on the importance of this factor in technological adoption process in emergency management. Director disaster operations of case A stated that, although this is a time consuming but it is a very important task. It was stated as:

*"[…]defining the requirements of a technology and mapping current business practice is a time consuming but important task.[…]"*

Consistent with the case comments made by case A, case B also argued that right locatability of technology in emergencies makes huge impact. Failure in doing so could result in waste of time and other valuable resources. Moreover, a very comprehensive answer was recorded from case C. Regional director (emergency management), who was representing case C stated that:

*"[…] it is critical to place a technology at right place and should be easily accessible […]"*

Case D was uncertain about the role of locatability factor in the technological adoption process whereas, case E agreed on the significance of this factor but no detailed argument was made in this regard.

**Implementation Factor:** To ensure the importance of implementation and its role in the technological adoption process, the following question was added in the interview questionnaire.

*"How important is the proper implementation of a technology/RFID in emergency management? Please explain."*

Except case A (reported as *"not sure"*), the rest of the four cases: cases B, C, D and E supported the significance of physical implementation of technology during emergencies. Cases B, C and E agreed on the significance of this factor in the adoption of a technology in emergency management. According to emergency management coordinator of case B, the time required to deploy a technology in emergencies is the most critical factor in its implementation. It was further stated that the time-critical nature of emergency operations, only such technologies are desired which can be implemented quickly and easily. The following part of the empirical evidence reflected this view point:

*"[…]during the emergencies, time is the most critical thing. We need a technology which is easy and quick to implement[…]"*

Case C linked the implementation with the placement of the technology. It was further described that the proper and appropriate implementation or placement of technology makes a huge impact on the outcomes.

Similar to case B and C, case D argued that the technology to be selected for emergency operations should be quick and require fewer resources to implement. Implementation factor was also linked with the ease of use associated with the implementation of a technology. On the importance of implementation factor, it was stated as:

*"[…]The implementation process should be quick and simple. During emergencies, sufficient resources are not available, so if a technology itself needs many resources such as human and technical resources to implement and configure it[…]"*

Complexities in the implementation process curb the effective use of technology and hence cause the whole implementation process fail.

**Standardization Factor:** The question posed on the participating organizations was:

*"How important is the standardization among various sub-types of a technology/RFID used in emergency management? Please explain."*

Case A highlighted an important aspect of standardization. Director of disaster operations of case A suggested that standardization among various types and subtypes of a technology makes its adoption process easy and economical. Less time and expenses are required to train the staff if a technology meets a specific standard. It was suggested that standardization:

"*[…] helps in reducing the time and cost required familiarizing with the new technology […]*"

Similarly, emergency management coordinator of case B suggested that lack of standardization can cause the failure of system. If a system is not standardized, it is useless for the organization.

It is important to note that all five case organizations agreed on the significance of this factor especially case A, D and E rank this factor as very important whereas, case B and C rank it "important".

**Compatibility Factor:** In order to validate the significance of compatibility factor in adoption process, following question was asked from the interviewees of case organizations.

*"How important is the compatibility factor in the adoption of technology/RFID in emergency management? Please explain."*

All five cases reported that compatibility is one of the key factors in the technological adoption in emergency management. Responses recorded on this factor proved that neglecting this factor or adopting a technology with insufficient compatibility features will eventually caused additional overheads on emergency management organizations. Therefore, a technology is evaluated against its compatibility features and the one with better features attracts more attention from the emergency managers. Case A exclusively highlighted the significance of this factor as:

"*[…]the technologies with less compatibility with other technologies generally cause unnecessary overheads on the organization[…]*".

The abovementioned comments made by director disaster operations of case A showed that adopting a non-compatible technology causes technological islands and therefore organizations have to take extra measures and use extra resources in terms of technological and financial resources in order to interconnect the new technology with the existing technological infrastructure. This argument is also supported by the emergency management coordinator of case B. The significance of compatibility factor is clearly reflected in the following part of the comment made by the interviewee:

*"[…]if it is not compatible it will certainly not migrated easily[…]"*

This argument also highlights the fact that failing in adopting a compatible technology could cause additional efforts and resources in order to make it compatible and working along with the existing technological infrastructure. As most of the operations conducted by emergency management organizations are time and resources critical therefore, using a technology which cause additional overhead on organizational resources would be neither supported nor recommended.

In addition, the following statement made by case C further strengthens this argument:

*"[…] the technologies must be compatible with each other so that they can be used with the coordination and in place of each other […]"*

Consistent with the arguments of the first three case organizations, the remaining two case organizations, cases D and E also agreed on the key role of this factor. Both organizations claimed that compatibility was highly desirable in emergency operations and played an important role in technological adoption process.

**Privacy Factor:** To empirically validate the significance of privacy factor, the following question was added in the interview questionnaire.

*"How important is the privacy factor in the adoption of a technology/RFID in emergency management? Please explain."*

Overall, privacy factor is proved as an important adoption factor. The first two cases (case A and B) partially support this factor whereas the rest of three cases (case C, D and E) fully support this factor. The obvious reason for such support is the critical nature of emergency related information. Therefore, the organizations operate in this domain significantly consider the privacy-related features offered by a technology. For instance, according to the representative of case A:

*"[…] privacy concerns apply to disaster managers as they do to other sections of society. I mean, for us, the privacy of some of the information could be very critical whereas for some information, privacy couldn't be an issue […]"*

During the interview with the emergency management coordinator, it was observed that this organization critically considered the privacy related features of a technology while making a decision to adopt it or not. The following argument made by the representative of case B highlighted the significance of privacy factor and its role in the adoption of technology in emergency management:

*"[…] certain information is very important to keep private and our organization would always consider the privacy-related features offered by a technology […]"*

Similar to case B, case C also recommended that the privacy is an important factor in emergencies and is not limited to the victims only but also important to secure the information of emergency workers and emergency management agencies. The following part of the response collected from case C emphasizes on the significance of privacy in emergency management:

*"[…] in our organization where there are hundreds of volunteers who assists us during emergencies, we need to secure their information, and similarly there is lot of organizational factors which should remain private […]"*

Consistent with the above mentioned argument, the interviewee from case D also emphasized on the importance of privacy factor during emergencies. According to senior logistic officer of case D, it is very important not only to secure information but it is also required to take the precautionary measure in order to prevent the unauthorized use of information. The following statement from case D highlighted the importance of this factor as:

*"[…] It is extremely important that to keep all the information secure. It should be protected from any hacking chances […]"*

Overall, the significance of privacy factor was also supported by the representative of case E. Although, it was mentioned that this organization intentionally made some of its information public but, the significance of privacy and information security still remain vital. This point was clearly elaborated by comments made by the logistic delegate of case E. It was stated as:

*"[…]Our organization is fairly open. I mean you can find out easily where things have been donated and where these goods have been used, but to secure the data is increasable important […]."*

The empirical evidences collected from case organizations reveal that the privacy related features offered by a technology play an important role in its adoption.

In addition to questions (discussed above), one open-ended (catch-all) question was asked at the end of interview questionnaire. The purpose of this question was to make sure that all the relevant aspects about the adoption factors were covered and to explore the other factor if there is any. The question asked for this purpose was:

*"Apart from the above mentioned factors, do you think that there is any other important factor that plays an important role in the adoption of a technology in emergency management?"*

Answers from five case organizations to the above mentioned question were recorded. The importance of adoption factors mentioned earlier in this paper is further supported by the empirical evidences given below.

Case A: *"[…]robustness, simplicity and its impact on reducing time and resources[…]"*

Case B: *"[…]as mentioned earlier, the technology should be easy to use and easy to understand. And especially in emergency management you have cross sections of people with varying background and experience, so it should be something like that people can embrace, if it is too complex, people will shock, so I think it needs be easy to use[…]".*

Case C: *"[…]most the things have already been covered, but again I would like to emphasize on the quick implementation of a technology because time is very critical factor in emergency* *management therefore the technology to be used must be quick enough to respond in our emergency operations[…]"*

Case D: *"[…]actually it depends. As this organization is working in every country on the planet, It is an issue of giving training to people about the technology, like how it going to work in that country. If you are in a huge emergency, it is completely devastation. In short, during emergency, life is knock-off. It is fantastic to have a pretty good technology during emergency but in such scenarios it is extremely difficult to set up and use any technology […]"*

Case E: *"[…]training requirements must be low (many contexts, many languages, many levels of education and familiarity with technologies). Maintenance and support MUST be low – technical support is not available in the medium term in many operating environments […]"*

**Justification of "Other" Factors**

Important evidences were recorded for the question about "other" factors in the adoption of a technology in emergency management. These evidences further strengthen the factors proposed earlier in this paper; especially the implementation factor. This factor was exclusively emphasized by almost all the five case organizations. On the other hand, case A suggested "robustness" as another important adoption factor. This research placed "robustness" under the "performance impacts" and is out of scope for this paper. The reason behind placing robustness under performance impact is the fact that the considering the important factors during the technological adoption process and successfully deploying an appropriate and pertinent technology in emergency management yields several performance impacts like reduced response time, efficient tagging tracking, compatibility, reduced labor cost and robustness. Similarly, case D suggested that due to the adverse conditions of emergencies, it is quite difficult to set up and use any technology. No doubt, using a technology in emergency management is a non-trivial process, but significant progress can be made if an appropriate technology is available and the adoption process is carefully designed. Case D suggested that the training requirements should be low for adoption of technology in emergency. This argument was again in support of "implementation" factor which stated that the implementation or set up of a technology should be quick, simple and easy process.

## DISCUSSION

The factors presented in this paper highlight the important aspects which need to be considered during the adoption of technology in emergency management. All five case organizations supported these factors with a special emphasize on privacy, compatibility, standardization and implementation factors. In contrast to the initial hypothesis, it is revealed that the cost factor is not relatively significant for RFID adoption in emergency management. In fact, the emergency management organizations are more interested in the outcomes associated with the use of technology rather than its dollar value. Based on the empirical evidences collected from the participating organizations and the empirical findings reported above, importance of each adoption factor and presence of any other factor is depicted in Table 3. Table 3 concluded that standardizations and compatibility are the most important factors whereas, privacy is relatively less important. Moreover, implementation and locatability factors are less important than privacy factor whereas, costing factors is proved as least significant in the adoption of technology in emergency management.

Table 3: Empirical findings on the significance of contributing factors

| Contributing Factor | Case A | | | Case B | | | Case C | | | Case D | | | Case E | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | S | N | NS | S | N | NS | S | N | NS | S | N | NS | S | N | NS |
| Cost | | ✓ | | | | ✓ | | | ✓ | ✓ | | | ✓ | | |
| Privacy | | ✓ | | | ✓ | | ✓ | | | ✓ | | | ✓ | | |
| Compatibility | ✓ | | | ✓ | | | ✓ | | | ✓ | | | ✓ | | |
| Standardization | ✓ | | | ✓ | | | ✓ | | | ✓ | | | ✓ | | |
| Implementation | n/s | | | ✓ | | | ✓ | | | ✓ | | | ✓ | | |
| Locatability | ✓ | | | ✓ | | | ✓ | | | n/s | | | | ✓ | |
| Others | Robustness, Ease of use | | | Ease of use | | | Easy and quick implementation | | | Training | | | Require less resources | | |

*Legend: S= Supported, N= Neutral, NS=Not supported*

## CONCLUSION

This paper reported the empirical findings on significant factors that contribute in adoption of RFID in emergency management. It is anticipated that the framework presented in this papers will facilitate the adoption of RFID by emergency management organizations. Due to adequate accessibility of resources such as financial, technical and human, emergency management organizations of developed countries are presented as early adopter of RFID. Experiences and findings of such organizations could be further adopted by developing countries in order to reduce the impact of emergencies.

Although, the findings reported in this paper highlighted the significance of privacy, implementation, standardization and compatibility factors but, further research should be conducted for evaluating cost and locatability factors as they were not unanimously supported by all case organizations.

## REFERENCES


ADPC. "Community Based Disaster Management (CBDM): Trainers Guide Module 4: Disaster Management," *Asian Disaster Preparedness Center (ADPC) Bangkok, Thailand*) 2000.

Ahmed, A., and Sugianto, L. "RFID in Emergency Management " in: *RFID & Smart Technologies for Information Convergence,* J. Symonds, J. Ayoade and D. Parry (eds.), Information Science Reference, Hershey, USA, 2008, p. 350.

Anderson, J.L., and Decker, R.W. "Volcano Risk Mitigation Through Training," in: *Geohazards: Natural and Man-Made,* G.J.H. McCall, Laming, D.J.C., Scott, and S.C. (eds.), Chapman & Hall, London, 1992, pp. 7-12.

Atmanand " Insurance and Disaster Management: The Indian Context," *Disaster Prevention and Management* (12:4) 2003, pp 286-304.

Ayala, I.A. "Geomorphology, Natural Hazards, Vulnerability and Prevention of Natural Disasters in Developing countries," *Geomorphology* (47) 2002, pp 107–124.

Barbara, L.P. "Identifying and Tracking Disaster Victims: State-of-the-Art Technology Review," *The Journal of Health Promotion and Maintenance* (31:1), March 2008, pp 23-34.

Chan, C. Theodore , Killeen, J., Griswold, W., and Lenert, L. "Information Technology and Emergency Medical Care during Disasters," *Academic Emergency Medicine* (11:11), November 2004, pp 1229-1236.

Derekenaris, G., Garofalakis, J., Makris, C., Prentzas, J., Sioutas, S., and Tsakalidis, A. "Integrating GIS, GPS and GSM Technologies for the Effective Management of Ambulances " *Computers, Environment and Urban Systems* (25:3), May 1, 2001 2001, pp 267-278.

Dick, J.M. "The Benefits of Object Technology to Australian Software Development Organisations," in: *Faculty of Information technology*, Monash University, Melbourne, 2002, p. 300.

DiMaggio, J.P., and Powell, W.W. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," American Sociological Association, pp. 147-160.

DPLG-1. "White Paper on Disaster Management," 1998.

Eisenhardt, M.K. "Building Theories from Case Study Research," *The Academy of Management Review* (14:4), October 1989, pp 532-550.

Eshghi, K., and Larson, R.C. "Disasters: Lessons from the Past 105 Years," *Disaster Prevention and Management* (17:1) 2008, pp 62-82.

Estevez, A. "RFID Vision in the DoD Supply Chain," United States Army.

Fry, E.A., and Lenert, L.A. "MASCAL: RFID Tracking of Patients, Staff and Equipment to Enhance Hospital Response to Mass Casualty Events," AMIA Annual Symposium Proceedings, 2005, pp. 261-265.

Goodhue, D.L., and Thompson. "Task-Technology Fit and Individual Performance," *MIS Quarterly* (19:2) 1995, pp 213-236.

Gunes, A.E., and Kovel, J.B. "Using GIS in Emergency Management Operations," *Urban Planing and Developement* (126:3), September 2000 2000, pp 136-149

Hoppe, C.H. "The Timing of New Technology Adoption: Theoretical Models and Empirical Evidence," *The Manchester School* (70) 2002, pp 56-76.

Karahanna, E., Straub, W.D., and Chervany, L.N. "Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs," *MIS Quarterly* (23:2), June 1999, pp 183-213.

Kelly, C. "Simplifying Disasters: Developing a Model for Complex Non-Linear Events " *Australian Journal of Emergency Management [Aust. J. Emerg. Manage.]* (14:1) 1999, pp 25-27.

Killeen, P.J., Chan, C.T., Buono, C., Griswold, G.W., and Lenert, A.L. "A Wireless First Responder Handheld Device for Rapid Triage, Patient Assessment and Documentation during Mass Casualty Incidents," AMIA 2006 Symposium Proceedings, Washington, DC, 2006.

Kimberly, A.C. "Disaster preparedness in Virginia Hospital Center-Arlington after Sept 11, 2001," *Disaster Management and Response* (1:3), July 2003 2003, pp 80-86.

Kritzler, M., Lewejohann, L., Krüger, A., Raubal, M., and Sachser, N. "An RFID-based Tracking System for Laboratory Mice in a Semi Natural Environment," Pervasive Technology Applied: Real-World Experiences with RFID and Sensor Networks (PTA06), 2006.

Lee, J., and Bui, T. "A Template-based Methodology for Disaster Management Information Systems," 33rd Hawaii International Conference on System Sciences - 2000, Hawaii, 2000, p. 7.

Lehtonen, M., Staake, T., Michahelles, F., and Fleisch, E. "From Identification to Authentication – A Review of RFID Product Authentication Techniques " in: *Networked RFID Systems and Lightweight Cryptography*, Springer Berlin Heidelberg, 2007, pp. 169-187.

Lertwongsatien, C., and Wongpinunwatana, N. "E-commerce Adoption in Thailand: An Empirical Study of Small and Medium Enterprises (SMEs)," *Journal of Global Information technology Management* (6:3) 2003, pp 67-83.

Lorincz, K., Malan, D.J., Fulford-Jones, T.R.F., Nawoj, A., Clavel, A., Shnayder, V., Mainland, G., Welsh, M., and Moulton, S. "Sensor Networks for Emergency Response: Challenges and Opportunities," *IEEE Pervasive Computing* (3:4), Oct-Dec 2004, pp 16-23.

M-Tech "Identity Management Solutions," in: *Security Concepts*, 2007.

Manitoba-Health-Disaster-Management "Disaster Management Model for The Health Sector: Guideline for Program Development," 2002.

Mansouriana, A., Rajabifardb, A., Zoeja, M.J.V., and Williamson, I. "Using SDI and Web-Based System to Facilitate Disaster Management," *Computers & Geosciences 32 (2006) 303–315* (32:3), April 2006, pp 303-315

Marincioni, F. "Information Technologies and the Sharing of Disaster Knowledge: The Critical Role of Professional Culture," *Disasters* (31:4) 2008, pp 459-476.

Markus, M.L. "Power, Politics, and MIS Implementation," *Communications of the ACM* (26:6) 1983, pp 430-444.

MHDM "Disaster Management Model for The Health Sector: Guideline for Program Development," Manitoba-Health-Disaster-Management, 2002.

Michael, K., and McCathie, L. "The Pros and Cons of RFID in Supply Chain Management," International Conference on Mobile Business (ICMB'05) 2005 2005a, pp. 623-629

Michael, K., and McCathie, L. "The Pros and Cons of RFID in Supply Chain Management," *Mobile Business, 2005. ICMB 2005. International Conference*), 11-13 July 2005 2005b.

Mousavi, A., and Sarhadi, M. "Tracking and Traceability in The Meat Processing Industry: A Solution," *British Food Journal* (104:1) 2002, pp 7-19.

Orlikowski, J.W. "CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development," *MIS Quarterly, Vol. 17, No. 3 (Sep., 1993), pp. 309-340* (17:3), September 1983, pp 309-340.

Parker, D. *The Mismanagement of Hazards, Hazard Management and Emergency Planning Perspective on Britian* James and James Science, London, 1992.

Paton, M.Q. *Qualitative Evaluation and Research Methods* Sage publications, Newbury Park, 1990.

Quarantelli, E.L. "Disaster Crisis Management: A Summary of Research Findings " *Journal of Management Studies* (25:4) 1988, pp 373-385.

Rahim, M.M. "Understanding Adoption of Inter-organisational Systems (IOS): The Role of Organisational Motivations," in: *Department of Information Systems*, The University of Melbourne, Melbourne, 2003.

Remko, v.d.T., Beinat, E., Scholten, J.H., and Zlatanova, S. "Location Interoperability Services for Medical Emergency Operations during Disasters " in: *Geo-information for Disaster Management,* P.V. Oosterom, S. Zlatanova and M.E. Fendel (eds.), Springer Berlin Heidelberg, 2005.

Richardson, B. "Socio-Technical Disasters: Profile and Prevalence," *Disaster Prevention and Management* (3:4) 1994.

Rogelberg, S.G. *Handbook of Research Methods in Industrial and Organizational Psychology* Blackwell Publishing, 2004.

Rogers, E.M. *Diffusion of Innovations* Free Press, 1983.

Runge, J.B., and Lee, J. "Information Technology Adoption Among Small Retailers, Technical report," University of Nevada Las Vegas, USA, 2003.

Sagun, A., Bouchlaghem, D., and Anumba, J.C. "A Scenario-based Study on Information Flow and Collaboration Patterns in Disaster Management," *Disasters* (33:2), August 2008, pp 214-238.

Saunders, C., and Clark, S. "EDI Adoption and Implementation," *Information Resources Management Journal* (5) 1991, pp 9-19.

Scupola, A. "The Adoption of Internet Commerce by SMEs in the South Italy: An Environmental, Technological and Organizational Perspective," *Journal of Global Information Technology Management* (6:1) 2003, pp 52-71.

Shaluf, I.M. "An Overview on Disasters," *Disaster Prevention and Management* (16:5) 2007, pp 687-703.

Shaluf, I.M., Ahmadun, F.R., and Mustapha, S.A. "Technological Disaster's Criteria and Models," *Disaster Prevention and Management* (12:4) 2003, pp 305-311.

Sharma, A., Citurs, A., and Konsynski, B. "Strategic and Institutional Perspectives in the Adoption and Early Integration of Radio Frequency Identification (RFID)," Proceedings of the 40th Hawaii International Conference on System Sciences - 2007, Hawaii 2007.

Smith, A.D. "Exploring the Inherent Benefits of RFID and Automated Self-Serve Checkouts in a B2C Environment," *International Journal of Business Information Systems* (1:1-2) 2005, pp 149-181.

Thomas, B.S. *Humans and Automation: System Design and Research Issues* Wiley-Interscience 2002.

Toft, B., and Reynolds, S. *Learning from Disasters* Butterworth-Heinemann, Oxford, 1994.

Tornatzky, L., and Fleischer, M. *The Process of Technological Innovation* Lexington Books, NewYork, USA, 1990.

Turner, B.A. "The Organizational and Interorganizational Development of Disasters," *Administrative Science Quarterly* (21:3), September 1976 1976, pp 378-397.

Tuscaloosa. "Tuscaloosa County Emergency Management Cycle," 2003.

Wang, S., Chen, W., Ong, C., Liu, L., and Chuang, Y. "RFID Application in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital," (Volume: 8, On page(s): 184a- 184a) 2006.

Want, R. "An Introduction to RFID Technology," *IEEE CS and IEEE ComSoc*) 2006.

Wybo, J.L., and Kowalski, K.M. "Command Centers and Emergency Management Support," *Safety Science* (30) 1998, pp 131-138.

Xiao, Y., Shen, X., Sun, B., and Cai, L. "Security and Privacy in RFID and Applications in Telemedicine," in: *IEEE Communications Magazine*, 2006, pp. 64-72.

Zigurs, I., Buckland, K.B., Connolly, R.J., and Wilson, E.V. "A Test of Task-Technology Fit Theory for Group Support Systems " *The DATABASE for Advances in Information Systems* (30:3-4), Summer-Fall 1999 1999, pp 34-50.

Zlatanova, S., Oosterom, and Verbree. "3D Technology for Improving Disaster Management: Geo-DBMS and Positioning," XXth ISPRS congress, 2004.