Asia Pacific Journal of Information Systems
Vol. 24, No. 3, September 2014 http://dx.doi.org/10.14329/apjis.2014.24.3.345

An Empirical Investigation of Task-Technology Fit: Context of RFID in Disaster Management

Ashir Ahmed*

The notion of technological adoption such as Radio Frequency Identification (RFID) has been examined in various domains such as supply chain management, inventory management and health care. However, there are several unanswered questions surrounding how this technology is adopted in disaster management. This study attempts to explore the potential of RFID in disaster management. The notion of Task-Technology Fit (TTF) is deemed suitable for this purpose and thus used as the theoretical framework that is further validated by employing multiple case studies. The empirical findings indicate that there are six key factors influencing the decision to adopt RFID in disaster management. Some relate to aspects of RFID when it is put into practice, namely cost, compatibility, standardisation, implementation and locatability; while the other key factor relates to privacy and security aspect of information. It is hoped that the findings of this research will inform disaster management organizations to better plan the adoption of RFID for their operations.

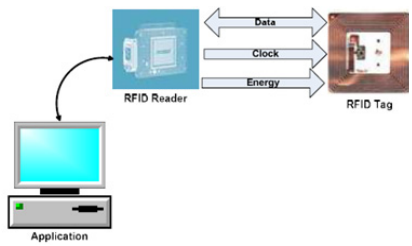
Keywords : Disaster Management, RFID, Technology Adoption, Task-Technology Fit

* Lecturer, Swinburne University of Technology, Australia

Ⅰ. Introduction

Research into technology adoption and diffusion has been carried out for many decades at user level or organization level. In the organizational context, the driver for technology adoption research has been to understand the technical-socio-organizational dimension as technology advances and converges with business processes, business models and governance practices [Han, 2013]. The influence of technology in society will be continues as technologies converge, evolve and emerge. Given that the nature of research tends to either be context specific or capturing the empirical data at a specific point in time, it implies that there will be a constant need for new theories to inform our understanding on technology acceptance and usage. In recent years, RFID technology in particular has drawn considerable attention from researchers and practitioners [Wang, 2010].

RFID is a term coined to use short to medium range of radio frequencies used to communicate between two objects without any physical contact. Objects at each end 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 are relatively simple devices and normally attached to the objects to be managed. 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 devices which send radio signals to the tags and locate them. These readers are connected to a host computer or to a network. Antenna is connected with RFID tag and mainly responsible to absorb radio signals sent by the reader and pass them to the RFID tag. The working principle of RFID technology is illustrated in <Figure 1>.



<Figure 1> Work Principle of RFID Technology

When the reader sends out the electromagnetic signals to couple with tag antenna, the tag gets electromagnetic energy from waves to power its circuits in the microchip. The chip located inside the tag then sends back electromagnetic waves to the reader, and the reader receives and coverts them into digital data. The data transmitted by the tag actually provide the metadata and information of the object, and the information can be processed in any information system or network connected to the reader [Shi Xinping, Chan Pui Yuk *et al*., 2005].

RFID has been successfully adopted in many sectors, including supply chain management, transportation, health, medicine and education. These exemplary cases serve as motivation for exploring the use of RFID in other domains-disaster management as an example.

According to Alexander [1997]:

"Disaster can be defined as a source of danger, and its consequences can adversely affect humans in terms of life, property and environment when the level of danger, and the consequences, exceed the ability of the affected society to cope using its own resources."

Similarly, the disaster management lifecycle

encapsulates all aspects of disastrous situations, including risk, consequences, pre and post disaster activities such as prevention, mitigation, preparedness, response, recovery and rehabilitation [DPLG-1, 1998]. According to DPLG-1 [1998], emergency management can be defined as:

"A collective term encompassing all aspects of planning for responding to emergency or disaster, including both pre and post disasters activities namely prevention, mitigation, preparedness, response, recovery and rehabilitation."

Currently there is a wealth of literature that examines the role of RFID in a particular phase of disaster management such as prevention, mitigation, preparedness, response, recovery and rehabilitation phase. However, there is a lack of significant study that extends the use of this technology and addresses its potential across all phases of the disaster management life cycle.

In order to address the above mentioned research gap, this study attempts to explore the potential of adopting RFID for disaster management by employing Task-Technology Fit (TTF) as the theoretical framework. TTF advocates that a match between business tasks and Information Technology (IT) is important to explain and predict the success of Information Systems [Goodhue and Thompson 1995]. The framework is also useful to help identify aspects that are critical to support a given business task, and thus, can contribute to the success of technology innovations [Junglas and Watson 2006]. For various scenarios of task and technology, statistical significance has been established for a positive association between TTF and Information Systems (IS); success measures such as use [Dishawa and Strong 1999], impacts on individual performance [Goodhue and Thompson, 1995] and on group performance [Zigurs, Buckland *et al*., 1999].

Considering the above line of argument, this study uses the concept of TTF to examine the 'fit' between the task characteristics of disaster management and the features offered by RFID. The original TTF model proposed by Goodhue and Thompson [1995] is thus adapted for this study.

Adapting TTF based on domain-specific requirements is supported in other studies [Benslimane, Plaisent *et al*., 2003; Wells, Sarker *et al*., 2003; Lee, Cheng *et al*., 2007; Gebauer and Tang, 2008; Cane and McCarthy, 2009]. In this study, the TTF components of task, technology and fit are modified according to the RFID and domain-specific requirements of disaster management. Overall this study attempts to add the following research questions:

i) What are the task characteristics of the disaster management life cycle?
ii) What are the technology characteristics of RFID?
iii) What are the contributing factors involved in the adoption of RFID in the disaster management?

<Table 1> presents a comparison of the TTF model and the conceptual model in this study. The rationale for adapting TTF is necessary because of the distinguishing characteristics of task domain (disaster management), technology (RFID), the technology adoption phase (pre-adoption) and the type of user (disaster management organizations).

The structure of the paper is as follows. The next section describes the conceptual model and its components, namely technology characteri-

<Table 1> Comparison of TTF Model with the Conceptual Model Proposed in this Study

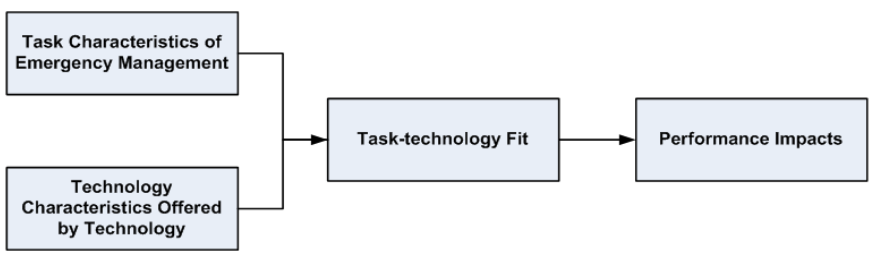
Construct	Task-Technology Fit Model by Goodhue and Thompson [1995]	Conceptual Model
Task domain	Using quantitative information in managerial tasks	Tasks performed in disaster management life cycle
Technology	Information technology	Radio frequency identification
User	Individual	Organization
Adoption phase	Post-adoption	Pre-adoption

stics and task characteristics. Systematic procedures to derive technology characteristics and task characteristics are also outlined in the next section. These procedures entail reviewing literature and using descriptive codes and analytical codes. This section also explains the four analytical codes used in this study: authentication, automation, tagging/tracking and information management. Next, the method for data collection and processing is described. The criteria for selecting participating organizations for multiple case studies are also outlined. This is followed by a section presenting the results and analysis of the multiple case studies. The last section concludes the paper with a discussion of the research findings and implication of this research.

Ⅱ. Conceptual Model

<Figure 2. shows the conceptual model proposed in this study. In <Figure 2>, Task Characteristics refer to the key tasks in disaster management that should be supported by the adoption of RFID. Technology characteristics refer to the features of RFID which are relevant and applicable to support disaster management activities. Task technology fit refers to the degree by which task matches with the technology characteristics. In other words, it is measuring how the technology support that fit requirement of a task. It is imperative to note that the focus of this study has been on the fit-focus, as opposed to utilisation-focus [Goodhue and Thompson, 1995]. Furthermore, while this notion of fit is borrowed from the original TTF model, the factors to measure this construct have been adapted to suit the context of this study.

In summary, this study addresses the three research questions (mentioned earlier) that are also reflected as the components of the conceptual model. The discussion on Performance impacts is out of focus for this paper. The next sections of the paper explain the components of the conceptual model in more details.



<Figure 2> Conceptual Model Based on Task-Technology Fit

2.1 Task Characteristics

Disaster management life cycle is generally described as a series of various phases or stages such as preparedness, mitigation, response and recovery [Kimberly, 2003]. Literature relevant to disaster management reported a number of models that describe various number of phases such as three phases [ADPC, 2000; Atmanand, 2003; Tuscaloosa, 2003], four [Kimberly, 2003; Turner, 1976], six [Toft *et al*., 1994a], seven [Shaluf *et al*., 2003a] or even eight [Kelly, 1999] phases which collectively form the disaster management life cycle. In depth analysis of these models reveals that they are comprised of various individual tasks. For instance, a task such as 'information sharing' is performed in different phases of disaster management including preparedness, mitigation, response and recovery. Similarly, an individual phase may include more than one task. For instance, response phase may include the tasks such as 'information sharing' and 'resource management.' In general, this paper agrees with the description of disaster management in terms of phases or stages. However, it advocates that the concept of phases does not facilitate the process of technological adoption. Furthermore, aligned with the recommendation of Goodhue and Thompson [1995b], this paper argues that the goal of adoption of technological process is to facilitate a particular task and not a phase. That being stated, disaster management operations entail a number of tasks that vary in context, nature and degree of complexity. Wells, Sarker *et al*. [2003] suggest that the overall classification of tasks is primarily based on the domain characteristics and context of that classification. Moreover the process of tasks analysis involves a hierarchical decomposition of autonomous tasks into lower-level sub-tasks [Hackos, 1998]. The nature of an autonomous task dictates the degree of variety, difficulty and interdependence of a particular task [Wells, Sarker *et al*., 2003]. In contrast to decomposing tasks into sub-tasks based on the variety, difficulty and interdependence, sub-tasks can be grouped together to form major tasks based on their commonalities of attributes.

In the context of RFID adoption, this study attempts to identify key tasks involved in disaster management to fit them into the TTF framework. Descriptive coding is applied on literature reviews in two domains, namely theoretical models of disaster management life cycle, and literature related to task characteristics of disaster management for adoption of information and communication technologies. The analysis process can be summarized as follows:

1. Review of literature that reports various theoretical models for disaster management
2. Identification of the key phases of disaster management in these models
3. Identification of the disaster management tasks reported in these models
4. Review of existing literature related to task characteristics of disaster management for adoption of information and communication technologies
5. Develop descriptive coding of tasks identified at step 3
6. Codes formed at Step 5 are further converted into analysis coding by analysing and categorizing into broader level of codes based on their commonalities. Use analytical codes as task characteristics of disaster management (in context of RFID adoption).
7. Repeat Steps 1-6 for various application domains.

As shown in <Table 2>, all disaster management tasks can be classified using four analytical codes, namely authentication, automation, tagging/tracking and information management.

<Table 2> Analytical Coding Leading to Identification of Task Characteristics

Disaster Management Model	Source	Tasks	Descriptive Codes	Analytical Codes
• Before disaster • During disaster • After disaster	Richardson [1994]	• Reducing/eliminating long-term risks of hazards and their effects • Assessing damage, communicating with all parties and initiating short-recovery attempts after an disaster • Detecting disaster signals and issuing warnings to public • People and victim management	• People management • Detecting disaster • Information sharing • Immediate response to emergencies	• Tagging/tracking of assets • Information management
• Preparedness strand • Relief and response strand • Rehabilitation and recovery strand.	ADPC [2000] Atmanand [2003]	• Establishing disaster plans by emphasizing on maintaining the inventories of resources, the training of people to management emergencies and taking immediate actions. • Communication among various disaster management agencies in response to a certain disaster	• Training • Communication • People management • Object management • Maintenance of inventories	• Information management • Tagging/tracking of assets
• Mitigation • Preparation • Response and Recovery	Kimberly [2003]	• Keeping the disaster plans up-to-date, conducting annual reviews, developing disaster management improvement projects, disaster training, maintaining records of drill activities, maintaining communication with participating parties, keeping and tracking adequate supplies.	• Training • Communication • People and object management	• Information management • Tagging/tracking of assets
• Mitigation • Preparedness • Response • Recovery	Tuscaloosa [2003]	• Establishing plans for disaster management, training of people, conducting drills and exercises. • Warnings of emergencies, evacuation, victim management, resource management and damage assessment	• Conducting drills • Issue warnings • People management • Object management	• Tagging/tracking of assets
• Notionally normal starting points • Incubation period • Precipitating event	Turner [1976]	• Preventing gross errors of perception, judgement and calculation that can lead to unfortunate disastrous consequences. • Preventing overlooking or misinterpreting data • Validating the identity of users before granting access to the system	• Information management • Manmade errors • System security by validating the authenticity of users	• Authentication • Information management

<Table 2> Analytical Coding Leading to Identification of Task Characteristics (cont.)

Disaster Management Model	Source	Tasks	Descriptive Codes	Analytical Codes
• Strategic plan • Hazard assessment • Risk management • Mitigation • Preparedness • Monitoring • Evaluation	Manitoba-Health-Disaster-Management [2002]	• Establishing disaster plans and communication channels among disaster service providers • Early assessment of damages caused by disaster assist in establishing better disaster response plans • Better preparation for upcoming disaster have potential to minimize the consequences of upcoming disaster	• Planning • Information sharing • Communication	• Information management
• The incubation period • The operation-socio-technical system • The precipitating event • The disaster itself • Rescue and salvage • Inquiry and report Feedback	Toft and Reynolds [1994]	• Communication among disaster management organizations • Planning • Authorized access to the system • Ensuring system security by validating the authenticity of users	• Communication • Access to the system • Authorized access to the system • Authenticity of users	• Authentication • Information management
• Inception of error • Warning • Failure of correction • Disaster impeding stages • Triggering events • Disaster stage • Disaster	Shaluf, Ahmadun *et al.* [2003]	• Errors that occur due to operation, maintenance and inspection negligence • Internal and external warnings • Automatic detection of disaster warnings and generation of appropriate responses against them • Automatic disaster response process	• Detecting disaster signals • Auto-detection of emergencies • Information sharing • Automation of warning system	• Automation • Information management
• Warning • Preparedness • Mitigation • Disaster prevention • Development • Reconstruction • Rehabilitation • Disaster response.	Kelly [1999]	• Planning, establishing the disaster plans, issue warnings, the immediate and automatic response to emergencies, communication amongst disaster management personal and taking long-term, step to minimize the consequences of emergencies.	• People and object management • Labelling or tagging of resources • Automatic disaster response process • Tracking of resources • Communication	• Tagging/tracking of assets • Information management • Automation

2.1.1 Authentication

Authentication refers to a process through which a system verifies the identity of a user wishing to access it [Randy, 2008]. As access control is normally based on the identity of the user who requests access to a resource, authentication is deemed essential to effective security [M-Tech, 2007]. Overall, reliable authentication is considered as the basis for protecting from a potential disaster. A rigorous and flawless authentication system is crucial in disaster management. Strong authentication assures that only valid users can interact with the system. This, in turn, minimizes the risks of various man-made emergencies, such as technological emergencies and terrorist attacks. Based on existing disaster management studies (see <Table 2>), this paper considers authentication in disaster management to encompass: implementing authentication protocols, assigning privileges to the users, verification of access requests and obstructing the unauthorized access or use of system.

2.1.2 Automation

Automation is defined as a process of using a control system, such as computers, to control machinery and processes and replacing human operators. Replacement of humans with control systems has some advantages, as well as disadvantages. A reduction in labour costs, being able to work in harsh climatic conditions, and consistent working hours are a few of the advantages of automation. The disaster management experiences indicate that although large amount of data is available during emergencies, data processing poses a huge problem [Zlatanova, Oosterom *et al*., 2004]. In addition, unfavourable working conditions further complicate the required working performance for human operators. In such situations there is a genuine need for systems that can automate the various procedures, and that can also ensure consistency, even in the hostile working environment of emergencies [Shaluf, Ahmadun *et al*., 2003; Zlatanova, Oosterom *et al*., 2004]. The following activities have been identified to be part of an automation process: identification of tasks which can be done by control systems, automatic detection of inputs using sensors, automatic decision-making based on received data using artificial intelligence, and using technology to assist in the human decision-making process.

2.1.3 Tagging and Tracking

Tagging and tracking refers to the process of capturing and maintaining information about any moving object, and this has been a real challenge for researchers and scientists [Gerald, Barbara *et al*., 2003]. The purpose of tagging and tracking is to identify the target object in a group of similar objects, as well as to keep real time information about its position. People and object management are the main objectives of this activity [Schulz, Burgard *et al*., 2001]. Most of the disaster management experiences show that during a disaster situation, one of the most important and urgent problems at the scene is the overwhelming number of victims that must be monitored, tracked and managed by each of the initial response organizations or individuals [Richardson, 1994; Tuscaloosa, 2003; Fry and

Lenert, 2005; Remko, Beinat *et al*., 2005; Killeen, Chan *et al*., 2006; Barbara, 2008]. The ability to automate these tasks could greatly relieve the workload for each responder. In disaster management, tagging/tracking encompasses: tagging of humans and objects, using these tags to track humans and other objects, and using these tags for human/object management before, during, and after emergencies.

2.1.4 Information Management

Information management refers to the process of collecting and managing information coming from one or more sources, and its distribution to one or more audiences who have a stake in that information or a right to that information. In disaster management, information management and communication play a vital role [Quarantelli, 1988]. Wybo and Kowalski [1998] argue that the inadequate and incomplete information/communication is considered to be the main operational problem during disaster management. A study of recent emergencies shows that, at some level or another, information was available that could have prevented the disaster from happening [Quarantelli, 1988; Toft and Reynolds, 1994; Kelly, 1999; Lee and Bui, 2000; Shaluf, Ahmadun *et al*., 2003; Chan, Killeen *et al*., 2004; Mansouriana, Rajabifardb *et al*., 2006]. Information management in disaster management is a combination of several other activities: training, gathering information from various sources/resources, broadcasting warnings/alerts; building and maintaining information pools, and communicating with other disaster management organizations.

2.1.5 Technology Characteristics

In this study, technology characteristics refer to the features of RFID which are relevant and applicable to support disaster management activities. <Table 3> presents an overview of RFID usage in other domains, including supply chain, assets management and healthcare and also reports a number of tasks performed by RFID in those domains. Data presented in <Table 3> is used to develop analytical coding. Subsequently, these analytical codes are referred as technological characteristics of RFID. The step by step procedure in developing descriptive coding and converting them into analytical codes is as follows:

1. Examine existing literature on the use of RFID in various domains
2. Identify technological characteristics (operations) performed by RFID
3. Develop descriptive coding of tasks identified at step 2
4. Convert descriptive coding into analytical coding based on the ideas and concepts reflected in descriptive codes
5. Use analytical codes developed at step 4 are used as technological characteristics of RFID adoption (in context of disaster management)
6. Repeat Step 1~5 for various domains.

Four analytical codes have been used to characterize RFID, namely authentication, automation, tagging/tracking and information management. These codes are also used in identifying task characteristics in disaster management. Descriptions of each of these analytical codes are provided in the later section of this paper.

<Table 3> Analytical Coding Leading to Identification of Technology Characteristics

Domain	Source	Tasks	Descriptive Codes	Analytical Codes
Assets Management, Warehouse Automation and Supply Chain Management	Michael and McCathie [2005] Xiao, Yu *et al.* [2006], Tajima[2007], Lehtonen *et al.* [2007]	• Tracking items and materials in the whole supply chain • Recording the locations and arrival time of products at warehouse • Processing and automating inventory • Automating non-line of sight scanning, enhancing visibility, asset tracking • Authenticating product at a single item level or over aggregated levels. Multiple similar units are authenticated simultaneously • Verification or validation of the claimed identity	• Control over inventory • Location awareness • Object tracking • Information management • Object Scanning • Automation • Information sharing • Non-line of sight scanning • Authentication • Validation of identity	• Tagging/tracking • Automation • Authentication • Information management
Defence Organizations	Estevez [2005]	• Managing the defence logistics • Automating logistics during the combat phase; benefits including improved in-transit and asset visibility, improved shipping/receiving/transportation timeliness and accuracy and reduced shrinkage.	• Managing logistics • Asset visibility • Automation • Object tracking • Improve accuracy	• Automation • Tagging/tracking • Information management
Healthcare/ hospitals	Wang, Chen, Ong, Liu and Chuang [2006]	• Minimizing the operational costs and improving patient safety.	• Patient management • Patient safety • Minimize operational cost	• Automation • Information management
Meat Industry	Mousavi and Sarhadi [2002], Staake, Thiesse and Fleisch [2005], Sarma, Weis and Engels [2003]	• Tracking in the meat industry • Tracing equipment, inject marking and tattooing. • Identifying and handling a meat product, and for gathering the information attached to it, throughout the production process.	• Enhance traceability • Object tracking • Object management • Information management	• Tagging/tracking • Information management
Laboratories	Kritzler, Lewejohann, Krüger, Raubal, and Sachser [2006]	• Tracking of location and movement of laboratory mice in a Semi Natural Environment • Tracking system for laboratory mice was to improve and extend the observations of their behaviour • Automatically tracked and analysed positional data of a large number of individual subjects over time	• Tracking • Automation • Improve the observations • Information management • Automatic tracking • Continuous observation	• Tagging/tracking • Automation • Information management

2.2 Task-Technology Fit

<Table 4> lists the contributing factors as the criteria for the level of 'fit' in the TTF model. Although the factors presented in <Table 2> are specific to the adoption of IT by its users, some of these factors are relevant in the adoption of RFID in disaster management. Based on (i) the thematic constructs identified in RFID literature, (ii) the domain-specific requirements of disaster management, (iii) variation of technical specifications of RFID from IT, and (iv) addressing the pre-adoption stage rather than the post-adoption stage, six factors have been proposed as determinants for RFID adoption in disaster management. These factors are: cost, privacy, implementation (ease-of-use), locatability, compatibility and standardization. A shift from IT to RFID technological practice implies that the notion of some of these constructs may have changed slightly. For example, *Cost* refers to the Total cost of ownership to adopt and use RFID. *Privacy* refers to the need of securing relevant information. *Ease* of use in the original IT application should be understood as RFID deployment; refers to as *implementation* in this study. Similarly, *locatability* refers to the installation of RFID equipment (tags and readers); *Compatibility* is the ability of RFID to work with other technological infrastructures such as IT and various types sensor networks. Finally the *Standardization* refers to the conformation to the standards of a particular industry.

<Table 4> Contributing Factors in the Adoption of IT [Goodhue and Thompson, 1995]

Components of Task-Technology Fit Model		
Contributing Factors	Quality	Data is used to store current and necessary elements in order to meet the requirements of the task. Moreover, the stored data is maintained at the right level of detail.
	Locatability	Each item of the data has a clear definition, where meaning of data is easy to find out.
	Authorization	The users are properly authorized to download data relevant to the task from corporate databases.
	Compatibility	The data is consistent with each other when it comes from two or more different sources.
	Ease-of-use/ training	It is easy to learn how to use the system and it is convenient to use the system to access data, including the ease-of-use of hardware and software, and easy of obtaining of relevant training.
	Production timeliness	The system can provide relevant information to the task in a timely manner.
	Reliability	The user can reliably depend on the system to complete the task without system problems and system breakdowns.
	Relationship with others	The system fits the users' daily requirements and corporate goals and provides maximum support to its users in order to perform their tasks.

Ⅲ. Data Collection and Analysis

To ensure generalizability and relevance of the research findings, this study uses multiple case studies involving various types of disaster management organizations as the conceptual population. Based on the task portfolios, 15 organizations were randomly identified as a result of Internet search. Further criteria were imposed to ensure the selection of case organizations involved in the complete disaster management life cycle and those which had used or were willing to use an appropriate technology for their operations. The additional criteria were:

- Case organization must be involved in the whole (complete) disaster management life cycle
- Case organization must have experience of being involved in real disaster situations
- Case organization must have used or be willing to use any pertinent technology, such a RFID, in disaster management
- Case organization should be willing to participate in this research.

Based on these criteria, 5 organizations were selected for this research. 3 of these organizations were based in Australia, 1 in New Zealand and 1 in Switzerland. Overview of the selected case organizations is given in <Table 5> below. It was decided that 5 cases would be sufficient to ensure theoretical replication based on organizational type and geographical location. As shown in <Table 5>, the participating organizations were mainly non-governmental organizations with differing size.

This study relied on the formal in-depth interviews with the key participants as the primary data source. For Australia-based organizations, the interviews were conducted (by the author of this paper) in-person at the premises of case organizations and each interview lasted for 1.5 to 2 hours. However, for organizations located overseas (in New Zealand and Switzerland), the interviews were conducted over the phone. With the consent of interviewees, all interviews were digitally recorded and ater transcribed in full for data analysis. It is important to note that representatives from different functional areas were interviewed as reported in <Table 6>. They comprised disaster managers, senior executive, or disaster coordinator/personnel involved in strategic planning for these organizations. These personnel had expertise in their specific roles in disaster management and they were involved in the overall strategic planning for their respective organizations. More importantly, they were involved in the decision making process regarding technological adoption for their respective organizations. By ensuring the involvement of representatives with different roles, all relevant aspects of the required information were covered. In order to minimize the bias in the data collection process from the organization representatives, several documents from the participating organizations were also considered. <Table 6> presents the overview of representatives of the participating organizations.

For data analysis, this study employed a pattern matching technique to compare the empirically-based pattern with the conceptual model. Pattern matching was applied to validate the contributing factors in RFID adoption decision.

<Table 5> Overview of Participating Organizations

Case	Overview of Organization	Type	Total Staff	Location
A	• Responsible for State's disaster management arrangements—the core staffing of the state disaster coordination center and state emergency services.	Public	230	Australia
B	• Maintains an emergency coordination centre that provides necessary information to different agencies and Involved in different types of activities including fire drills, training and coordinating with other disaster management agencies in Melbourne, Australia.	Public	800~900	Australia
C	• Performs a wide range of roles, including planning for and responding to floods, severe storms, earthquakes, road accident, victim search and rescue.	Public	90 (1,500 volunteers)	Australia
D	• Improving the local, regional and international capacity to respond to disasters and public health emergencies and renewing the advocacy on priority humanitarian issues, especially fighting intolerance, stigma and discrimination, and promoting disaster risk reduction.	NGO	1,661 (number of staff can vary on project bases)	Switzerland
E	• Provides emergency social services in times of trouble. These include maintaining essential supplies and running a national disaster victim enquiry service, together with other activities set out in their emergency management policy.	NGO	Number of staff can vary on project bases	New Zealand

Legend: NGO = Non-government organization.

<Table 6> Overview of Participating Interviewees

Case	Job Title	Key Job Responsibilities	Work Experience
A	Director, Disaster Operations	• Manage the corporate function of Disaster Operations to enhance and develop the operational performance levels of the organization through innovation and identification of best practice strategies. Provide strategic advice to top management of State Government Agencies regarding disaster management arrangements and operations.	25 years
	Executive Manager, Disaster Operations	• Involved in key disaster operations performed by this organization. • Responsible for managing State's disaster coordination centre and involved in building better strategies to coordinate amongst several agencies during emergencies.	15 years
B	Coordinator, Emergency Management	• This person is one of the few people in the organization who has a dedicated disaster management role. Responsible for coordinating the disaster management responses across the organization and working closely with other people who have a disaster management function.	8 years
	Team Leader, Spatial Systems	• Working as a spatial systems team leader in business information services. • Involved in building better strategies to coordinate amongst several agencies during emergencies.	13 years
C	Regional Director, Emergency Management	• This role also includes the deployment to operations within the State, or national deployment to disaster activities, such as storms and floods, and also the support role to other organizations. • Involved in running disaster management courses in collaboration with other agencies.	6 years
	Director, EMC	• Responsible for all disaster planning, disaster management training and disaster management capacity building. • Responsible for community education, media and public relations related to disaster management.	8 years
D	Senior Logistic Officer	• Project Management - focusing on development of global infrastructure and response capacities to the major disasters anywhere in the world.	10 years
E	Logistics Delegate	• Responsible for managing sub-regional warehouse that will be available to respond to emergencies and disasters in pacific region and disaster response unit that respond to any disaster in the world.	15 years

Ⅳ. Analysis and Results

4.1 Cost

Intuitively, cost of a particular technology is often considered as a dominant factor to adoption decision. Surprisingly, the empirical data on cost is rather contradictory. Cost is often perceived as the main constraint for adopting new technology in Case A:

"Anything we do is constrained by DOLLAR and PUBLIC POLICY… If we don't have funding than we cannot adopt a technology, no matter how important it is?" [Executive Manager, Disaster Operations–Case A]

Consistent with the evidence from Case A, the representative of Case B clearly stated that disaster management organizations have huge potential for the adoption of new and pertinent technologies irrespective of their cost. The following portion of Case B's response highlighted this fact:

"If there is good technology available, the way we are operating our organization, we will pay more. So it is not all a matter of money, but if there is good value for money, then certainly we will pay for technology and bear the cost." [Coordinator, Emergency Management–Case B]

As mentioned by the representative of Case B, the cost (or dollar value) of the technology becomes relatively less important (for disaster management organizations) when it is compared with the associated benefits. However, another respondent from the same organization implied that cost is only 60% of the criteria used to evaluate the potential of technology in Case B; but at the same time the representative also acknowledged that there were some problems and concerns regarding this criterion. For instance, the cheaper solutions often end up with more running costs such as training cost and maintenance cost.

The Director, Emergency Management and Communication of Case C highlighted a very important aspect related to the cost of technology. It was stated that the cost should not be considered as a single factor. The need and objectives of adopting a technology should also be evaluated with the cost (dollar value) of the technology. The following is a portion of the feedback on the cost factor:

"Just to identify the cost as a single entity is not quite right because it related to the budget that we have and the objectives and need behind adopting that technology." [Director, Emergency Management and Communication–Case C]

The empirical evidence indicates that although the cost of the technology is important however, the decision for adopting a technology is not solely based on the dollar value of the technology. The potential benefits associated with the technology are crucial in influencing the adoption decision. The representative from Case E drew attention to another aspect that relates to the adoption decision. The performance or success rate of a particular technology in other fields (also referred as 'observability') was considered very important for securing or allocating finances for the adoption of a new technology in disaster management. The following portion of Case E highlights this fact:

"It is very difficult to get donors to give money for technology until they see the benefits after the operation ⋯ 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." [Logistics Delegate−Case E]

Contrary to the support witnessed for cost factor, the representatives from the other three cases claimed that the cost of technology is not critical in the adoption decision. Most of the organizations operating in the disaster management domain perform cost-benefit analyses and appraise the outcomes of the adoption of technology rather than solely considering its dollar value. Furthermore, financial feasibility of a technology is also based on the available budget. If a sufficient budget is available, the cost of the technology would not be a constraint. In addition it was also argued that the cost of technology should not be treated as a single entity but that it should be considered along with the budget, the perceived benefits and the actual need to adopt a technology.

4.2 Privacy

Literature suggests that disaster management organizations endeavour to guard the privacy and security of their information. Empirical evidence collected for this factor shows that some organizations consider the technology characteristic that can ensure information security is an important factor to adoption decision. Representative of Case B highlights the significance of the privacy factor and its role in the adoption of technology in disaster management:

"Certain information is very important to keep private and our organization would always consider the privacy-related features offered by a technology." [Coordinator, Emergency Management−Case B]

Further adding to the above argument, representative from Case C stated that privacy is an important factor and that it is not limited to victim-related information only, but that is also important to secure the information of disaster workers and disaster management agencies. It was stated as:

"In our organization, where there are hundreds of volunteers who assist us during emergencies, we need to secure their information, and similarly there is lot of organizational factors which should remain private." [Regional Director, Emergency Management−Case C]

The Director of Emergency Management and Communications from Case C also stated that the nature of this factor varies from situation to situation depending on the type of information being dealt with. In some situations they need to keep information private, whereas in other cases they do not worry about the privacy of information.

The significance of the privacy factor was also supported by the representative from Case E. Although it was mentioned that this organization intentionally makes some of its information public, the significance of privacy and information security still remain vital. This point was clearly elaborated in the following comment.

"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 increasingly important." [Logistics Delegate–Case E]

Based on empirical evidence, it is concluded that the entire disaster management process contains two types of information: (i) information which need to be secured and remain private at all times; and (ii) information for which privacy is not an issue. In order to secure the required information, the technology should offer the features that ensure the security and privacy of critical information. In short, in relation to privacy, the findings of this research are threefold: (i) not all the information in disaster management needs to be secured; (ii) RFID is a suitable technology for dealing with information where privacy and security is not a main concern; and (iii) as not all the information in disaster management is required to be secured and made private, the privacy-related feature of a technology was shown to be less attractive for disaster management organizations.

4.3 Implementation(Ease of Use)

The emergency management coordinator of Case B stated that the time required to deploy a technology during emergencies is one of the most critical factors of the implementation process. It was further stated that the time-critical nature of disaster operations allowed the adoption of only those technologies that could be implemented quickly and easily. The following paragraph reflects this view:

"During emergencies, time is the most critical thing. We need a technology which is easy and quick to implement during disaster situations." [Coordinator, Emergency Management–Case B]

Consistent with the above argument, representative from Case C stated that the time-critical nature of disaster operations demanded only time and resource efficient technologies to be used; otherwise the technology itself might yield more problems than benefits. The Director, Emergency Management and Communication from Case C stated that a technology that was easy to use, and that required less training and maintenance not only suited the unfavourable working conditions of emergencies, but also encouraged people to use that technology. An important issue was raised by the Senior Logistics Officer of Case D, who stated that the improper implementation of a technology was worse than useless. The following portion of Case D's response highlights the significance of the implementation factor in the technology adoption process:

"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, then it would be an unnecessary overhead for the disaster management team." [Senior Logistics Officer–Case D]

The empirical findings of this research showed tremendous support for implementation factor. RFID in disaster management must be implemented quickly and easily. For instance, Executive Manager, Disaster Operations from Case A argued that easy-to-use technologies not only

encouraged the users to use that technology but also helped in minimizing the operational costs required to use that technology. The representative from Case D argued that adopting a technology in disaster management that was not easy to use and required more resources would actually be an unnecessary overhead for a disaster management team. In short, the empirical evidence suggested that implementation factor had a huge impact on the decision of technology adoption.

4.4 Locatability

A majority (seven out of eight) participants agreed on the importance of locatability as a key factor in technological adoption process. For instance, the Director, Disaster Operations from Case A stated that, although locatability was time-consuming, it was a very important task:

"Defining a complete access plan and deploying the technology at proper access points makes a huge impact on outcomes of our disaster related operations." [Director, Disaster Operations–Case A]

Consistent with the above comments, the Coordinator, Emergency Management of Case B argued that this factor had a huge impact on the expected outcomes of technological adoption. Failure to deploy a technology at the appropriate site could result in a waste of time and other valuable resources. Adding to that, the Team Leader, Spatial Systems from Case B stated that the correct location of a technology in an emergency not only minimized the likelihood of an extension of the emergency's impact but also assisted in responding to an emergency situation. Similarly, the Regional Director from Case C, stated that:

"It is really a very important question and we do prepare the actual locatability plans of technologies for different sorts of emergencies … we plan based on our available options and implement a technology at certain points from where it is not only easily accessible but can also return maximum outputs." [Regional Director, Emergency Management–Case C]

Based on the empirical evidence, this research concludes that locatability is an important factor in the decision to adopt a technology in disaster management and considerable attention is given to what exactly a technology will do and how it would be placed and accessed during emergencies. By taking RFID as a potential technology to be adopted in disaster management, this research also concludes that this technology offers easy and clear mechanisms for placing and accessing it during emergencies. Therefore, from the locatability point-of-view, RFID can be considered a pertinent technology for disaster management.

4.5 Compatibility

For disaster management organizations, compatibility of their technologies with other technologies used in their disaster management operations is critical. The empirical evidence also shows that neglecting this factor, or adopting a technology with insufficient compatibility features, will eventually cause additional overheads for disaster management organizations. Therefore a technology is evaluated against its com-

patibility features and the one with better features attracts more attention from disaster managers. Representative from Case A exclusively highlighted significance of this factor as:

"Technologies with less compatibility features generally cause unnecessary overheads for the organization." [Director, Disaster Operations, Case A]

The above comment shows that adopting a non-compatible technology can cause technological islands, and therefore organizations have to take extra measures and use extra technological and financial resources in order to interconnect a new technology with their existing technological infrastructure. This argument was further supported by the participants as well. For instance, representative from Case A explained the two reasons for adopting compatible technologies, such as:

"There are two reasons to adopt compatible technologies. The first reason is the cost, because if you take on a number of technologies, the cost associated with those technologies will go higher because you have to have different platforms to run these technologies, whereas the second reason is the interpretability." [Executive Manager, Disaster Operations −Case A]

The Emergency Management Coordinator of Case B also supported the significance of compatibility factor, as clearly reflected in the following comment:

"If it is not compatible it will certainly not migrate easily." [Coordinator, Emergency Management−Case B]

Similarly, the Team Leader of Spatial Systems from Case B stated that adopting incompatible technologies caused several integration issues that created operational problems for organizations. In addition, the following statement from Case C strengthens this argument:

"The technologies must be compatible with each other so that they can be used in coordination and in place of each other." [Regional Director, Emergency Management−Case C]

Based on the findings drawn from the empirical evidence, this research concludes that compatibility is a key factor in adopting a technology in disaster management. Therefore, compatible technologies are more likely to be adopted for this domain. Furthermore, it is also concluded that RFID could be a suitable and reliable technology for disaster operations where capability is highly desirable.

4.6 Standardization

Standardized technologies make the adoption process easy and economical. Less time and financial resources are required to train staff if a technology meets a specific standard. It was suggested that standardization

"Helps in reducing the time and cost required for familiarizing with the new technology." [Director, Disaster Operations−Case A]

Consistent with the above arguments, representative from Case B highlights the role of standardization within recent disaster management experiences. The interviewee stated that

during the recent Australian bush fires, people from different areas (interstate and overseas) arrived at the disaster scene (bush fires) to work with local agencies. Similarly, several fire fighters from Australia were sent to the US to assist in emergencies. In such situations, only standardized technologies allow different technological infrastructures to work in collaboration. The comment made by the interviewee is as follows:

"If you got standardized technology, different people and agencies can work together and know what they are doing… I think it [standardization] is very important. Also, with disaster management in this organization we are looking at the standards if our people have to work in other parts. They can go there and help people in other areas." [Team Leader, Spatial Systems–Case B]

In addition to the aforementioned factors, this research also attempted to address any additional factor that might contribute to the adoption of RFID in disaster management. For instance, an important factor i.e. 'observability' emerged from the empirical findings of this research. The term was used to refer the overall reputation and the knowledge of capabilities of a technology by other organizations.

In conclusion, the above discussion serves two purposes: (i) it unfolds the role and significance of various factors that contribute to the adoption of technology (RFID in this case); and (ii) it reveals the potential of RFID to be adopted in disaster management. It is anticipated that the empirical findings of this research also assist organizations operating in disaster management to foresee the most significant adoption factors, along with their influence on technological adoption process.

In order to summarize the role of the contributing factors suggested by the case study participants, <Table 7> depicts the significance of these factors in the adoption of RFID in disaster management.

On the basis of the data shown in <Table 7>, it is concluded that implementation, locatability, compatibility and standardization are the most important factors in the decision of adopting RFID in emergency management. The significance of the privacy factor comes after these factors and, finally, the cost factor proves to be the least significant factor in the adoption of technology/RFID in emergency management.

<Table 7> Analysis of Empirical Findings on Contributing Factors

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		√		√				√		√			√		
Implementation		√		√			√			√			√		
Locatability	√			√			√				√		√		
Compatibility	√			√			√			√			√		
Standardization	√			√			√			√			√		
Others	Robustness, ease-of-use, observability			Observability, ease-of-use			Observability, easy and quick implementation			Less training requirements			Require less resources, observability		

Legend: S = Supported, N = Neutral, NS = Not supported, N/s = Not sure.

Ⅴ. Discussion

This study exemplifies the use of TTF model to understand the potential of RFID in disaster management. Distinctive characteristics (referred as *task characteristic*) of disaster management and technological features offered by RFID (referred as *technology characteristics*), led the adaption of original TTF model and resulted in the development of a conceptual model that specifically dealt with the 'fitness' between task and technology characteristics. Initially, the review of disaster management literature was conducted to identify the key task characteristics of this domain. Findings of the literature review reported various disaster management models suggesting varying number of phases and stages to describe disaster management life cycle. Though, the significance of such phases was invaluable, they were beside the point to understand the nature of activities (task characteristics) of disaster management. Descriptive and analytical coding was then employed in order to derive task characteristics from various disaster management models (as reported in <Table 4> above). Consequently, four unique characteristics (namely authentication, automation, tagging/tracking, and information management) were identified that characterize disaster management activities in the context of RFID adoption.

Subsequently, the potential of RFID for facilitating disaster management was examined by analysing the relevant literature on RFID adoption in various domains such as supply chain, warehouse automation, transportation and healthcare. This formed the basis for the conceptual model proposed in this study <Figure 1>. Task and technology characteristics derived by the analytical coding were further validated by interviewing the key informants from five disaster management agencies. The findings of this study suggest that in the perspective of technological adoption in disaster management, the technology needs to be supportive in the areas of authentication, automation, tagging/tracking and information management. It is believed that that the identification of these task characteristics (as mentioned above) played a critical role in examining the potential of a pertinent technology in disaster management and hence is considered as one of the key contributions of this study.

Further to the above discussion, this study also relied on TTF model to examine the key factors that contribute in the 'fitness' and the adoption of RFID in disaster management. Six factors have been identified for this purpose (namely Cost, Privacy, Implementation, Locatability, Compatibility and Standardization). Though the factors that believed to be critical for RFID adoption in disaster management are somehow comparable with others suggested in majority of the literature on technological adoption, the empirical findings of this study reported the unique nature of the degree of significance of these six contributing factors in particular context of RFID adoption in disaster management. For instance, the majority of the literature on technology adoption suggests that the cost of the technology is a dominant factor in technology adoption decisions. However, the empirical findings of this study suggests otherwise. It was found that the decision to adopt a technology such as RFID in disaster management is not solely based on the dollar value but in fact based on the benefits associated with the technology.

Similarly, this study contrasts the literature that suggests that all information in disaster management needs to be protected. This study assisted to explain this phenomenon and took an extra step by elucidating that not all the information in disaster management is of the same nature and hence can be categorized into two distinct types (i) information which need to be secured and remains private at all times; and (ii) information for which privacy is not an issue. In order to secure the required information, the technology should offer the features that ensure the security and privacy of critical information. This distinct contribution is believed to be valuable in order to examine the potential of a technology in disaster management.

Though the remaining four factors such as implementation, compatibility and locatability do support the relevant literature, the findings of this study suggested another critical factor, named as, 'observability' that has its unique significance in RFID adoption in disaster management. It was revealed that organizations operating in disaster management domain cautiously consider the success and reputation of a technology in other organizations and domains before they decide to try them in their own organizations.

In summary, this study has examined the potential of RFID throughout the disaster management life cycle. By employing rather flexible interpretation of TTF, a conceptual framework is proposed that brings task characteristics of disaster management together with technological characteristics of RFID. This study does not claim that RFID is the only (and the best) technology for this domain rather it successfully examines the 'fitness' between task and technology characteristics. Moreover the identification of various contributing factors is expected to facilitate disaster management organizations in their decisions to adopt RFID for their operations.

〈References〉

[1] Atmanand, "Insurance and Disaster Management: The Indian Context," *Disaster Prevention and Management*, Vol. 12, No. 4, 2003, pp. 286-304.

[2] Barbara, L.P., "Identifying and Tracking Disaster Victims: State-of-the-Art Technology Review," *The Journal of Health Promotion and Maintenance,* Vol. 31, No. 1, 2008, pp. 23-34.

[3] Benslimane, Y. and Plaisent et al., Applying the Task-Technology Fit Model to WWW-based Procurement: Conceptualization and Measurement, Proceedings of the 36th Hawaii International Conference on System Sciences, Hawaii, USA, 2003.

[4] Cane, S. and McCarthy, R., "Analyzing The Factors That Affect Information Systems Use: A Task-technology Fit Meta Analysis," *Journal of Computer Information Systems,* Vol. 50, No. 1, 2009, pp. 108-123.

[5] Chan, C.T. and Killeen et al., "Information Technology and Emergency Medical Care During Disasters," *Academic Emergency Medicine*, Vol. 11, No. 11, 2004, pp. 1229-1236.

[6] Dishawa, T.M. and Strong, M.D., "Extending the Technology Acceptance Model with Task Technology Fit Constructs," *Information and Management*, Vol. 36, 1999, pp. 9-21.

[7] Estevez, A., RFID Vision in the DoD Sup-

ply Chain. Acquisition Process Improvement, United States Army, 2005.

[8] Fry, A.E. and Lenert, A.L., MASCAL: RFID Tracking of Patients, Staff and Equipment to Enhance Hospital Response to Mass Casualty Events. AMIA Annual Symposium Proceedings, Washington, D.C., 2005.

[9] Gebauer, J. and Tang, Y., "Applying the Theory of Task Technology Fit to Mobile Technology: The Role of User Mobility," *International Journal of Mobile Communications*, Vol. 6, No. 3, 2008, pp. 321-344.

[10] Gerald, K.L. and Barbara et al., "What Is Tracking? Cultural Expectations in the United States, Germany, and Japan," *American Educational Research Journal*, Vol. 40, No. 43, 2003, pp. 43-89.

[11] Goodhue, D.L. and Thompson, R.L., "Task-Technology Fit and Individual Performance," *MIS Quarterly*, Vol. 19, No. 2, 1995, pp. 213-236.

[12] Han, J., Kang, S., and Moon, T., "An Empirical Study on Perceived Value and Continuous Intention to Use of Smart Phone, and the Moderating Effect of Personal Innovativeness," *Asia Pacific Journal of Information Systems*, Vol. 23, No. 4, 2013.

[13] Goodhue, D.L. and Thompson, "Task-Technology Fit and Individual Performance," *MIS Quarterly*, Vol. 19, No. 2, 1995, pp. 213-236.

[14] Hackos, J.T. and Redish, J.C., User and Task Analysis for Interface Design, New York, Wiley Computer Publishing, 1998.

[15] Junglas, I. and T.R. Watson, "The U-Constructs: Four Information Drives," *Communications of the Association for Information Systems*, Vol. 17, No. 1, 2006.

[16] Kelly, C., "Simplifying Disasters: Developing a Model for Complex Non-Linear Events," *Australian Journal of Emergency Management*, Vol. 14, No. 1, 1999, pp. 25-27.

[17] Killeen, P.J. and Chan et al., "A Wireless First Responder Handheld Device for Rapid Triage," Patient Assessment and Documentation during Mass Casualty Incidents. AMIA 2006 Symposium Proceedings, Washington, DC, 2006.

[18] Kimberly, C., "Disaster preparedness in Virginia Hospital Center-Arlington after Sept 11, 2001," *Disaster Management and Response*, Vol. 1, No. 3, 2003, pp. 80-86.

[19] Kritzler, M. and Lewejohann et al., "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.

[20] Lee, C.C. and Cheng et al., "An Empirical Study of Mobile Commerce in Insurance Industry: Task-Technology Fit and Individual Differences," *Decision Support Systems*, Vol. 43, No. 1, 2007, pp. 95-110.

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

[22] Lehtonen, M. and Staake et al., "From Identification to Authentication-A Review of RFID Product Authentication Techniques Networked RFID Systems and Lightweight Cryptography," Berlin Heidelberg, 2007, pp. 169-187.

[23] M-Tech, "Identity Management Solutions," Security Concepts, 2007.

[24] Manitoba-Health-Disaster-Management, "Disaster Management Model for the Health Sector: Guideline for Program Development,"

2002.

[25] Mansouriana, A. and Rajabifardb et al., "Using SDI and Web-Based System to Facilitate Disaster Management," *Computers and Geosciences*, Vol. 32, No. 3, 2006, pp. 303-315.

[26] Michael, K. and McCathie, L., The Pros and Cons of RFID in Supply Chain Management, International Conference on Mobile Business (ICMB'05) 2005 Sydney, Australia, 2005.

[27] Mousavi, A. and Sarhadi et al., "Tracking and Traceability in The Meat Processing Industry: A Solution," *British Food Journal*, Vol. 104, No. 1, 2002, pp. 7-19.

[28] Quarantelli, E.L., "Disaster Crisis Management: A Summary of Research Findings," *Journal of Management Studies*, Vol. 25, No. 4, 1988, pp. 373-385.

[29] Randy, J.O., Data Center Industry Terms, The Data Center Journal, 2008.

[30] Remko, v.d.T. and Beinat et al., Location Interoperability Services for Medical Emergency Operations during Disasters Geo-information for Disaster Management. P.V. Oosterom, S. Zlatanova and M.E. Fendel. Berlin, Heidelberg, Springer, 2005.

[31] Richardson, B., "Socio-Technical Disasters: Profile and Prevalence," *Disaster Prevention and Management*, Vol. 3, No. 4, 1994, pp. 41-69.

[32] Richardson, B., "Socio-Technical Disasters: Profile and Prevalence," *Disaster Prevention and Management*, Vol. 3, No. 4, 1994, pp. 41-69.

[33] Sarma, E.S. and Weis et al., RFID Systems and Security and Privacy Implications Cryptographic Hardware and Embedded Systems - CHES 2002. Berlin/Heidelberg, Springer 2523/2003, pp. 1-19.

[34] Schulz, D. and Burgard et al., Tracking Multiple Moving Objects with a Mobile Robot IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR' 01) Hawaii, USA, 2001.

[35] Shaluf, I.M. and Ahmadun et al., "Technological Disaster's Criteria and Models," *Disaster Prevention and Management*, Vol. 12, No. 4, 2003, pp. 305-311.

[36] Staake, T. and Thiesse et al., Extending the EPC Network: The Potential of RFID in Anti-counterfeiting. 2005 ACM Symposium on Applied Computing, Santa Fe, New Mexico ACM New York, USA, 2005.

[37] Tajima, M., "Strategic Value of RFID in Supply Chain Management," *Journal of Purchasing and Supply Management*, Vol. 13, No. 4, 2007, pp. 261-273.

[38] Toft, B. and Reynolds, S., "Learning from Disasters," Butterworth-Heinemann, 1994.

[39] Toft, B. and Reynolds, S., Learning from Disasters Oxford, Butterworth-Heinemann, 1994.

[40] Turner, B.A., "The Organizational and Interorganizational Development of Disasters," *Administrative Science Quarterly*, Vol. 21, No. 3, 1976, 378-397.

[41] Tuscaloosa, "Tuscaloosa County Emergency Management Cycle," Retrieved June 4, 2007, from[http://www.tuscoema.org/cycle.html, 2003.

[42] Wang, S. and Chen et al., RFID Application in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital. 39th Hawaii International Conference on System Sciences, Hawaii, USA, 2006.

[43] Wang, Y.M., Wang, Y.S., and Yang, Y.F., Understanding the determinants of RFID adoption in the manufacturing industry, *Technological forecasting and social change*, Vol. 77, No. 5, 2010, pp. 803-815.

[44] Wells, D.J. and Sarker et al., Studying Customer Evaluations of Electronic Commerce Applications: A Review and Adaptation of the Task-Technology Fit Perspective. Proceedings of the 36th Hawaii International Conference on System Sciences Hawaii, USA, 2003.

[45] Wells, D.J. and Sarker et al., Studying Customer Evaluations of Electronic Commerce Applications: A Review and Adaptation of the Task-Technology Fit Perspective. 36th Hawaii International Conference on System Sciences, Hawaii, USA, 2003.

[46] Wybo, L.J. and Kowalski, M.K., "Command Centers and Emergency Management Support," *Safety Science*, Vol. 30, No. 1-2, 1998, pp. 131-138.

[47] Xiao, Y. and Yu et al., "Radio Frequency Identification: Technologies, Applications, and Research Issues," *Wireless Communications and Mobile Computing*, Vol. 7, No. 4, 2006, pp. 457-472.

[48] Zigurs, I. and Buckland et al., "A Test of Task-Technology Fit Theory for Group Support Systems," *The DATABASE for Advances in Information Systems*, Vol. 30, No. 3-4, 1999, pp. 34-50.

[49] Zlatanova, S. and Oosterom et al., 3D Technology for Improving Disaster Management: Geo-DBMS and Positioning, XXth ISPRS congress, 2004.

[50] Zlatanova, S. and Oosterom et al., 3D Technology for Improving Disaster Management: Geo-DBMS and Positioning. XXth ISPRS congress, 2004.

◆ About the Authors ◆

Ashir Ahmed

Ashir Ahmed is a lecturer of Information Systems at Swinburne University of Technology, Australia. He earned his PhD degree in information systems from Monash University, Australia. His research interests focus on the role of social media in various context including Disaster Management and Small and Medium Enterprises (SMEs). He has published his research in the area of technology adoption (such as Radio Frequency Identification) in Disaster Management that appeared in (PAJAIS), International Conference on Information Systems (ICIS), European Conference on Information Systems (ECIS), Hawaii International Conference on System Sciences (HICSS) and Pacific Asia Conference on Information Systems (PACIS).

Submitted : April 23, 2014
1st revision : September 08, 2014
Accepted : September 11, 2014