A networking solution for disaster management to address liaison failures in emergency response

A. V. Singhal[1], A. Jha[1] & A. Gairola[2]
[1]*Department of Metallurgical and Materials Engineering, Indian Institute of Technology, India*
[2]*Center of Excellence in Disaster Mitigation and Management, Indian Institute of Technology, India*

Abstract

A huge loss of life and property takes place during disasters due to the lack of organization, coordination and effective communications in disaster response. To address these issues an automated IT based networking solution named e-ICS has been proposed in this paper. The need and the utility of such a system has also been highlighted through case studies of the Bhuj earthquake 2001, the Mumbai attacks of 26.11.2008 and a pilot study during the anti-ragging mock drill. This paper also introduces the innovative Confirmation Net for the authentication of information and reports during an emergency situation.
Keywords: automated disaster response, multi-organizational coordination, incident command system, e-ICS, confirmation net, open source.

1 Introduction

Population growth, environmental changes, global warming, and terrorism are the key factors in making mankind increasingly prone to both natural and man-made disasters (Mayhorn and McLaughlin [1]). The occurrence of disasters is usually beyond human control, especially natural disasters. Their effects can merely be mitigated and managed for minimizing the loss of life, human suffering and property loss. Coordination among various jurisdictions and organizations is important for planning and execution of disaster response and recovery (Emmanuel and Dewald [2]).

WIT Transactions on Information and Communication Technologies, Vol 47, © 2014 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/RISK140341

Communications should not be taken for granted as it plays a key role in mobilizing resources, disseminating strategic information, delivering commands and assessing risk in any disaster situation. Fast, accurate, precise and sometimes confidential communications are a cost-effective means of curbing loss of life and property, and increasing public awareness (Regenie [3]). However, providing effective communication during disaster situations is a challenging task (Nelson *et al.* [4]). Generally, disaster managers and responders have to cope with incomplete, unavailable and/or outdated information in a disaster scenario (Helsloot [5]).

This paper discusses the need, the structure and the development of an automated networking system hereby named e-ICS for improving coordination and communication in disaster response. This system can be an effective tool in the management of an emergency situation in a disaster which is discussed in Section 2. Thereafter, in Section 3 liaison failures during the Bhuj Earthquake (2001), and the Mumbai Attacks of 26/11 (2008) have been reviewed so that modern needs of disaster response mechanism are precisely highlighted. Further, Section 4 explains the Incident Command System, a well-accepted organizational framework for disaster response and its success and adoption in India. Finally, Section 5 provides a detailed insight into the structure, technology and the working mechanism of the e-ICS.

2 Anti-ragging mock drill

According to the University Grants Commission (UGC) [6], Government of India ragging is an incident involving any conduct by any student or students which can cause physical, psychological, mental, sexual or financial harm to any fresher or student. Due to increasing incidents of student suicides and depression cases; as per the directives of the Supreme Court of India, ragging is completely banned in all academic institutions. Yet, incidents of ragging continue to occur, therefore to curb such incidents and to test the GSM Interface of the e-ICS a team from the Center of Excellence in Disaster Mitigation and Management (CoEDMM), Indian Institute of Technology, Roorkee undertook a pilot study within which a prototype of the e-ICS was tested in an Anti-Ragging Mock Drill organized on 31st of August, 2012 within the IIT Roorkee campus. The participants enacted a mock Ragging Incident at a hostel room from where a SMS reporting the incident was sent to the e-ICS emergency number following which the Server analysed the message, and the authorities were alerted. Deputy Incident Commander (playing the role of the Dean of Discipline) and Operation's Section Chief (playing the role of Hostel Warden) successfully raided the room within 18 minutes and 13 seconds. The information regarding the incident was disseminated to the authorities within a minute, however the major part of the response time was elapsed in reaching the incident location as the participants playing the role of the Incident Commanders were new to the hostel and had to undertake the legal procedure before they could finally raid

the room. A comparative study highlighting the benefits of e-ICS in the above mock drill has been summarized in table 1. The drill clearly highlighted the benefits of such a system in incident management.

Table 1: Comparison of salient features of the Anti-Ragging Mock Drill.

e-ICS	Conventional System
▪ Informer has a single memorable emergency number	▪ Uncertainty of getting a response from a large list of contacts
▪ All responsible authorities are informed in one go	▪ May require multiple trials for informing even a single authority
▪ Structured flow of information	▪ Structuring is absent
▪ Quick deliverable response	▪ Response delayed or none at all
▪ Anonymous reporting	▪ Informer's identity may be revealed

3 Case study

This section analyses and summarises the findings of the Bhuj Earthquake 2001 (a natural disaster) and the Mumbai Attacks of 26/11, 2008 (a man-made disaster) case studies to effectively understand the role of communication and Information Systems in disaster management especially in relief and response. These disasters involved multi-organizational coordination which highlights the role of IT and communications in disaster management. Moreover, these events have occurred during the span of almost a decade which helps us to analyse the changes in the Disaster Management Framework in India and the effects these changes had on overall relief and response or in other words, how effective were these changes.

3.1 Bhuj earthquake 2001

As the national program of the Republic Day, 26th January of 2001 commenced Indians experienced one of the most devastating earthquake of the era which began at 08:46 am IST with its epicentre near Bhuj in the Kutch District of the state of Gujarat and lasted for more than a minute. Based on the reports by the National Institute of Disaster Management, Ministry of Home Affairs, Government of India [7] and by the World Seismic Safety Initiative and the Earthquakes and Megacities Initiative [8], although, the tremors were felt all over the Indian sub-continent yet Gujarat was the most affected state with 13,805 deaths and around 167,000 severely injured. Table 2 shows the assessment of the relief and response during the aftermath of the Bhuj Earthquake.

Table 2: Assessment of the relief and response process. Column 1 contains elements vital for coordination in crisis response (Dorothy *et al.* [9]).

Elements	Description with reference to Bhuj Earthquake 2001
IT infrastructure	Satellite phones backed by police wireless were the only available IT infrastructure
Leadership	Commendable leadership and initiation were shown by the surviving government officials, NGO's and other volunteers available in the region despite a lack of resources and communication facilities
Collaborative network	Officials tried to develop and manage an in situ collaborative network of officials, NGO's, Indian Army and other national and international organizations to facilitate relief and response
Ability to build and apply IT	Absent. Even the available satellite phones were not used in every district
Ability to see the big picture	Government of India and the state of Gujarat took concrete steps which enabled the creation of GSDMA and a review of the initiatives of NCMC for better control over the situation
Resolute informing	Absent. Due to failure of communication links
Agile mobilizing	Absent. The mobilization of people and resources could not be done in a timely fashion due to lack of pre-designated resources, their inadequate availability and proper coordination channels
Coordination structure	Absent. Although response was quick, but there were duplication and inefficiency due to lack of a proper coordination structure
Crisis Response organizational structure	Absent. By that time ICS was not incorporated into the Indian Disaster Management Framework and officials had to be assigned responsibilities on site which lead to delays and chaos as people acted in the way they felt best
Informational structure	Absent. There was a complete lack of a protocol for information gathering, sharing and transparency across various stakeholders
IT structure	Modern IT resources and network were absent and there was no alternative for the conventional communication links

Based on the above assessment the following conclusions can be drawn from the relief and response phase of the Bhuj Earthquake of 2001:

- availability of alternative communication networks is excessively essential due to the possibility of a complete breakdown of conventional telecommunication networks,
- requirement of an effective system for emergency communications which can integrate the existing systems and facilitates flexible response,
- up gradation of search and rescue capabilities and equipment,
- a need for an inventory of available resources, equipment, response teams and lists of contact persons which has already been initiated in the form India Disaster Resource Network (IDRN) and State Disaster Resource Networks (SDRN),
- need of an organizational framework to prevent chaos and confusion during response phase, providing detailed guidelines for protocols to be followed, and the roles and responsibilities of various personnel,
- development of a networked Early Warning System for effective dissemination of timely and precise warnings.

3.2 Mumbai attacks of 26/11, 2008

During the Mumbai attacks of 26th November, 2008 several new features were witnessed, although the number of casualties was less as compared to earlier such incidents, yet the psychological damage and panic were widespread. Quite unexpectedly, armed terrorists invaded India via the sea route, with active combat continuing for 68 long hours. Major innovations were witnessed in the methodology of the terrorists including the use of modern IT technology and the use of the country's free electronic media to coordinate their actions. The major issues that these attacks raised include ignorance of intelligence alerts, inadequate training, lack of coordination, scarcity of resources and designated combat forces and most importantly the leakage of critical information through the electronic media (Balachandran [10]).

4 Current scenario of disaster management in India

The concept of Incident Command System (ICS) was developed by the Fire fighting Resources of California Organized for Potential Emergencies (FIRESCOPE) program of the state of California, USA in 1980's for responding to disastrous wild land fires [11]. However, various agencies and entities have accepted and evolved ICS to facilitate systematic and planned coordination across various stakeholders at different levels of the government, non-government organizations and the private sector working towards disaster management and mitigation; regardless of the cause, size, location or complexity of the incident [12]. Major features of ICS include manageable span of control, unity of command, common terminology and specified incident objectives. The entire structure of ICS is based on three networks (1) Command/Information Net

(strategic functions) (2) Tactical Net (execution) and (3) Support Net (medical teams, fire fighters, etc.). For professionals and strengthen the disaster management framework ICS was adopted in India after 2003 as practiced by the USFS (US Forest Services), Sinha [12]. The Indian structure identifies the Central Relief Commissioner (CMC) in the Ministry of Home Affairs [13] as the nodal officer for coordinating all forms of disaster related issues. The National Crisis Management Committee (NCMC) headed by the Cabinet Secretary is the national body undertaking policy making while the Crisis Management Group (CMG) headed by the CMC takes care of the execution of these policies at the national level. At the State Level, State Disaster Management Authorities undertake these activities, with hierarchy extending up to the district as well as the municipalities and village levels with a coordinating body at each level. Although, the introduction and adoption of ICS in India and elsewhere have addressed the organizational issues with clarification of roles and domains of various stakeholders, yet ICS is found to be a failure in most of the post disaster assessment reports due to lack of proper coordination and communication structure [15].

5 e-ICS, the proposed system

Due to the complexity, uncertainty and uniqueness, disaster situations differ considerably and require custom management approaches, however the impact and influence of disasters on human life and behaviour remains similar (Othman and Beydoun [15]) thus while dealing with issues of coordination and communication a generalized system can provide an effective response without delays. e-ICS stands for Electronic Incident Command System. This section illustrates as to how the e-ICS system developed by the authors can strengthen the conventional Incident Command System discussed in Section 4 in terms of multi-organizational coordination and integrated communication which is shown in fig. 1.

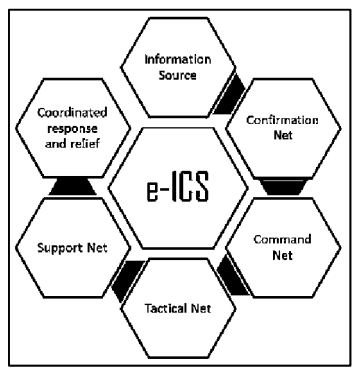

Figure 1: Overall function of e-ICS: to serve as a medium of information flow across ICS structural networks for coordinated response and relief.

5.1 e-ICS structure

e-ICS is designed to be compliant with the Indian ICS Team Structure and involves the use of Modern Telecommunication Technologies like GSM, GPS, 3G, Wi-Fi, etc. along with conventional technologies like UHF, VHF, HF and standard web access tools to facilitate information sharing through the mediums of text, voice, image and video. e-ICS follows pre-determined channel of information as developed into its code with a constant feedback mechanism for improving responsiveness at each stage. It has been so designed that structurally similar but functionally different channels are triggered corresponding to variations in incidents. It ensures unification of Command, Tactical and Support Nets with vertical and horizontal flow of commands and information through the system. The entire e-ICS structure involves four components (1) the Partners (2) the Six Interfaces (3) the Early Warning System, and (4) the Server. Fig. 2 shows the block diagram of e-ICS, highlighting the various components and the flow of information through the system.

5.1.1 Confirmation net

Apart from the Command, Tactical and Support Nets or Networks of the conventional ICS structure an innovative Confirmation Network has been introduced and presented in this paper; for authentication of the varied information that pour in from various sources and are often of questionable tangibility. The Confirmation Net is headed by the Information Officer and provides confirmation of the genuineness of the available information. It comprises of the lower level staff deployed in the target area connected to e-ICS through either the wireless or the GSM interface. It promotes efficiency and avoids wastage of resources and time in dealing with false information. Confirmation Net is designed to prevent triggering of false alarms which is essential to ensure the trust of the partners in the system. However, the response may be slightly delayed due to an additional step.

5.1.2 Partners

The personnel involved in the Command, Tactical, Support and Confirmation Nets as well as the beneficiaries (people of the affected community) constitute the partners of e-ICS. The primary objective of e-ICS is to facilitate coordination and communication among its partners and to build their trust in the system, so that protocols can be executed religiously to provide a satisfactory response.

5.1.3 e-ICS interfaces

The entire coordination and communication among the partners is an outcome of the complex network of the six interfaces namely (1) Wireless Interface (2) GSM Interface (3) Smartphone Interface (4) Satellite Interface (5) Web Interface and (6) GPS Interface of e-ICS and their link with the partners and the server. Depending upon the level and type of communication required different partners are connected to the system through unique combinations of these interfaces which is explained in fig. 2.

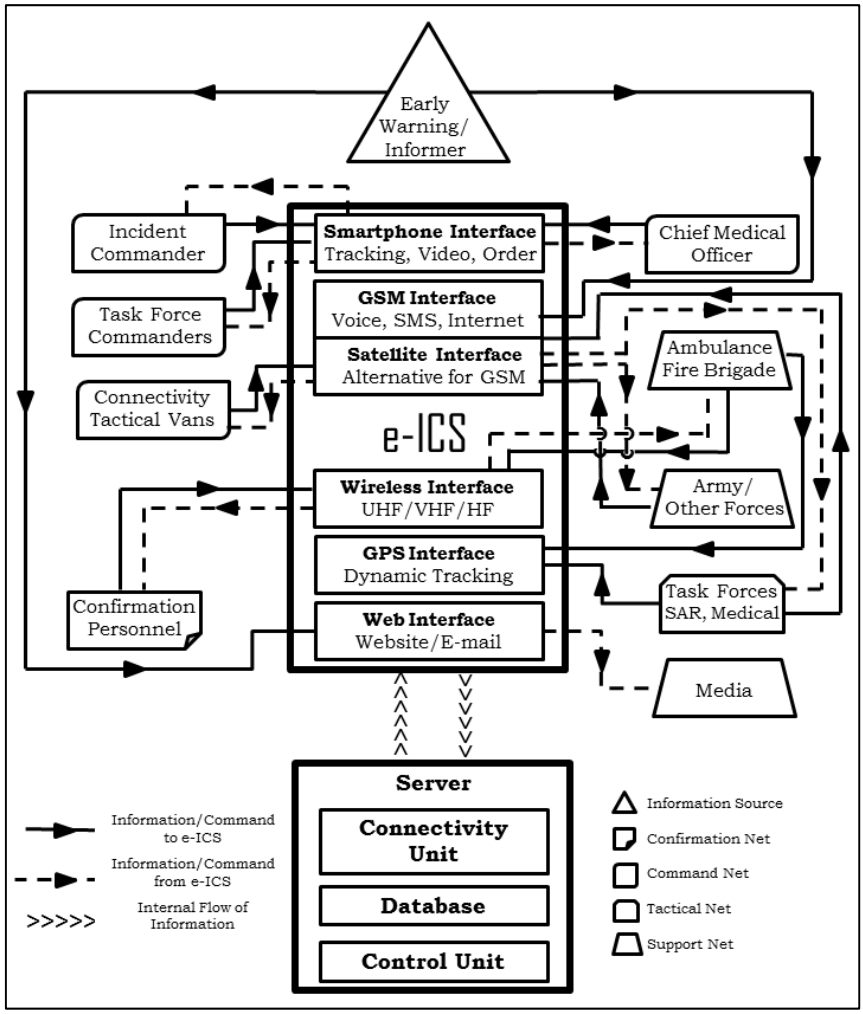

Figure 2: Block-diagram showing the structure of e-ICS.

5.1.4 The early warning system

According to the Ministry of Home Affairs [13], currently, early warning systems are in place only for Tropical Cyclones and Floods in India. e-ICS is designed to receive early warnings for tropical cyclones from the Indian Meteorological Department (IMD) and for floods from the Central Water Commission (CWC). The warnings thus received are immediately updated on the website and forwarded to the media for public information. Also, the responsible authorities are alerted to be prepared for the possibilities of an impending disaster. The system is also designed to allow the incorporation of protocols for early warning systems for other disasters as and when they are incorporated in the Indian framework.

5.1.5 The server

The Server is the brain of the e-ICS located at the Emergency Operations Centre. It is basically a high performance computer providing communication links and channelizing flow of vital information in a disaster situation with constant logging of events. The server is the centre for all information collection and dissemination. The codes on the server ensure that proper channels are triggered and that protocols are strictly followed. The server has three basic components based on the functions it performs:

5.1.5.1 Connectivity unit It is the nodal point for all communications and includes facilities for various interfaces of the system. It links the different access points (the partners) of the e-ICS communication network. Connectivity Unit controls all the communication channels and ensures that the communication links are uninterrupted.

5.1.5.2 Database The e-ICS database is a vast inventory of pre-designated resources such as fire fighting units, emergency medical teams, facilities like hospitals, dispensaries, fire stations, police stations, etc., and policies of the response mechanism. Policies here include protocols to be followed, structure of command, and authorities, roles and the domains of various response personnel, agencies and organizations.

5.1.5.3 Control unit This unit of the Server is the central processing unit of e-ICS and it is the place where the entire computational and logical codes are stored. As the name suggests the Control Unit controls the entire functioning of the system by setting priorities, providing notifications, receiving and disseminating information and conveying orders while providing dynamic situational awareness to the partners.

5.2 Special features

e-ICS offers some special features which add to its utility and acceptability. It has been developed keeping in mind the needs, capabilities and knowledge of the common man and the people involved in response processes. Also, it has been designed to deal with any disaster situation irrespective of the kind, location, size and span of the incident.

5.2.1 Open source

Considering the software aspect of e-ICS it is to all extents an open source code allowing custom modifications to meet the needs of the target community. It allows changing codes of priorities, protocols and channels with ease. Thus, e-ICS is meant to earn greater trust and acceptability with lesser user frustration. Also, e-ICS automatically adjusts to the scale of the emergency and triggers only appropriate channels for efficient response.

5.2.2 Uninterrupted connectivity

As is evident from the case studies analysed in this paper, conventional telecommunication networks often break down in the aftermaths of a disaster. Thus, to ensure communication link at different levels of the Incident Command System presence of an alternative communication network is vital. e-ICS ensures that communications among various partners is uninterrupted in any scenario. Even in case of a failure of the entire telecommunications network e-ICS provides complete textual, audio and visual connectivity between the site and the control room through its strategic Connectivity and Tactical Vans. These mobile units are connected to the Server through a satellite link which in turn facilitate on site connectivity through Wi-Fi routers, thus enabling the Smartphone, Web and GPS Interface to function properly.

5.2.3 Closed loop and cyber security

As we have learned from the case of the Mumbai Attacks of 26/11 (2008) that leaking of critical information can be detrimental to the entire response process, lowering commitment and motivation of the involved personnel. e-ICS ensures that a closed loop of information is formed among the designated personnel and only approved information is passed for mass communication thus maintaining the secrecy of such responses and avoiding misuse of critical information. This is made possible by using a private portal thus lowering the hacking threats. Also, e-ICS can offer varied levels of security through retina scans, fingerprint scanning or smartcard scanning according to the requirements.

5.2.4 Dynamic inventory

With the onset of the disaster response, e-ICS provides constant real time situational awareness to all commanders at the scene, as well as en route for better control over the resources. Live feed of the positioning and availability of various mobile resources like fire fighting units, medical teams, search and rescue teams, connectivity and tactical vans and other task forces is provided to the commanders through the Smartphone interface. This dynamic inventory of available resources ensures effective and efficient deployment of the resources.

5.2.5 Graphics user interface (GUI)

Designed for users unfamiliar with the Information Technology protocols e-ICS offers a user friendly GUI for easier understanding and usage. e-ICS GUI facilitates greater belief in the system with increased acceptability without anxieties.

5.3 Working

Although, the e-ICS has been so designed that structurally similar but functionally different channels are triggered corresponding to variations in incidents, yet it is possible to explain its basic working mechanism in a generalized manner by highlighting the sequence of triggering of various segments of the system along with their functions. The system can be triggered by two methods either by an early warning or through incident reporting. In case

of the reporting of an incident, the information is confirmed through the Confirmation Net using either the wireless interface or the GSM interface. Once, the occurrence of the incident is confirmed the Chief Incident Commander (IC) is informed of the situation through the Smartphone interface along with an instant mobilization of the Immediate Response Team. Further, decisions and commands are initiated by the commander. Assessing the level of the incident, the IC decides the grade of response and the number of personnel to be deployed. Following which the respective commanders are informed of the situation who can command for mobilization of other resources. During the entire process, the Commanders have access to the real time status of the mobile resources and also back-up resources in case the available resources are exhausted. e-ICS also enables the commanders to coordinate among themselves as well as the dispatch and operations centres either through textual, audio or visual mediums incorporated into the Smartphone interface. The robust connectivity provided by e-ICS ensures synchronization of response by sharing of information among various units while each unit can focus on its assigned tasks. Constant logging of process is a vital function of the Server for post-disaster analysis and assessing failures. Further, the necessary warnings and incident related information is passed to the public via the media and the website through the web interface. Thus, e-ICS is a completely automated IT based solution to ease coordination and communications in disaster response.

6 Conclusions

e-ICS is a twenty-first century solution to address liaison failures in incident management incorporating the use of modern telecommunication technologies. The purpose of communication and decision support systems like e-ICS is to reduce human errors, chaos and confusion during emergency response. However, errors in incident management will continue to occur owing to the factors of stress, pressure, hurry and incompleteness of information prevailing in such situations (Hoogendoorn *et al.* [16]). The success of system like e-ICS depends on relevance and accessibility of information and response timeliness provided by the system. Whereas, the acceptability is governed by behavioural tendencies of the users in terms of perceived task support, group coordination and personal biases (Lee *et al.* [17]). Therefore, applicability and feasibility of e-ICS needs to be further studied by applying it in realistic scenarios.

References

[1] Mayhorn, C.B. & McLaughlin, A.C., Warning the world of extreme events: A global perspective on risk communication for natural and technological disaster. Safety Science, In Press, Corrected Proof, Available online 7 June 2012. http://www.sciencedirect.com/science/article/pii/S0925753512001014.

[2] Emmanuel, R. & Dewald, V.N., Intra-governmental coordination for sustainable disaster recovery: A case-study of the Eden District

Municipality, SA. International Journal of Disaster Risk Reduction, 4, pp. 92-99, 2013.
[3] Regenie, F., Communicating Effectively In A Disaster Situation. Presented at the CARILEC Conference, Managing Tropical Storms: Challenges Faced and Lessons Learnt in 2004, http://www.canto.org/document_center/conference-presentations/communicating-effectively-in-a-disaster-situation.
[4] Nelson, C.B., Steckler, B.D. & Stamberger, J.A., The Evolution of Hastily Formed Networks for Disaster Response: Technologies, Case Studies, and Future Trends. Global Humanitarian Technology Conference, eds Boutillon, E., Britto, R. & Chavez, D., IEEE: Seattle, pp. 467-475, 2011.
[5] Helsloot, I., Bordering on reality: findings on the bonfire crisis management simulation, Journal of Contingencies and Crisis Management, 4, pp. 159-169, 2005.
[6] What constitutes ragging? University Grants Commission, Government of India. https://antiragging.in/upload/Infopack/what_constitues_ragging.pdf.
[7] Mishra, P.K., The Kutch Earthquake 2001: Recollections, Lessons and Insights, National Institute of Disaster Management, Ministry of Home Affairs, Govt. of India, pp. 4-16, 192-219, 2004.
[8] Mistry, R., Dong, W. & Shah, H., Interdisciplinary Observations on the January 2001 Bhuj, Gujarat Earthquake, World Seismic Safety Initiative & Earthquakes and Megacities Initiative, pp. 7-28, 2001.
[9] Dorothy, E.L., Gary, P. & Shan, L.P., The role of IT in crisis response: Lessons from the SARS and Asian Tsunami disasters. Journal of Strategic Information Systems, 18(2), pp. 80-99, 2009.
[10] Balachandran, V., Dealing with Aftermath of Attacks: Lessons from Mumbai and elsewhere on what to do and what not to do. Presented at the Pluscarden Programme conference on The Future of International Cooperation in Countering Violent Extremism, Oxford University, 2010. www.sant.ox.ac.uk/centres/Balachandranpaper.pdf.
History of ICS, Incident Command System, National Training Curriculum, U.S.A. National Wildfire Coordinating Group website. www.nwcg.gov/pms/forms/compan/history.pdf.
[11] National Incident Management System, U.S. Department of Homeland Security website. www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.
[12] Sinha, J.K., Concept Note, Thematic Session on Incident Command System. Proc. of Second India Disaster Management Conference, NDMA, New Delhi, pp. 138, 2009.
[13] Disaster Management in India, Ministry of Home Affairs, Government of India, pp. 5-24. http://nidm.gov.in/PDF/DM%20in%20India.pdf.
[14] Williams, A., Liability Issues in Emergency Response (Chapter 10). Disaster Medicine, ed. G.R. Ciottone, Elsevier Health Sciences: Philadelphia, pp. 71, 2006.
[15] Othman, S.H. & Beydoun, G., Model-driven disaster management. Information & Management, 50(5), pp. 218-228, 2013.

[16] Hoogendoorn, M., Jonker, C.M., Treur, J. & Verhaegh, M., Agent-based analysis and support for incident management. Safety Science, 47(8), pp. 1163-1174, 2009.
[17] Lee, J., Bharosa, N., Yang J., Janssen, M. & Rao, H.R., Group value and intention to use – A study of multi-agency disaster management information systems for public safety. Decision Support Systems, 50(2), pp. 404-414, 2011.