Applications of RFID in Incident Management

Amir N. Shamdani
IT Department, School of Technology
Purdue University Calumet, USA
ashamdan@purdue.edu

Barbara J. Nicolai
IT Department, School of Technology
Purdue University Calumet, USA
bnicolai@purduecal.edu

***Abstract* – This paper surveys the applications of Radio Frequency Identification (RFID) in incident management to improve the accurate resource tracking and tracing functionalities in disaster situations. The paper started with an initial discussion on what the possible goals working with the active RFID kit (FFID Reader + RFID Tags), to provide a solution to monitor an object for the purpose of identification and tracking using radio waves. Afterwards, Incident Management and its role in specifying the response process and resource management from the Network Centric approach will be determined with an applied approach. It is concluded that what would be the process of monitoring at any time for Dynamic Information Collection to provide a real-time scalable decision support framework built on rapid information collection using RFID technology.**

Keywords – RFID; Incident Management; Command and Control; Network Centric Paradigm

I. INTRODUCTION

Radio Frequency Identification (RFID) is defined as a set of technology that provides network delivered information services dependent on physical object identification captured by radio waves. A typical RFID system consists of four main components, a tag (transponder), a reader (interrogator), an antenna and middleware (Computer) [1]. When the tag is in the electromagnetic field of RFID antenna the tag's presence is detected by the reader. The reader is interfaced to the middleware using a network cable which displays the number of reads on a screen. This entire process can be completed with no human intervention hence RFID system can be truly automatic. Hence this is the most preferred methodology of tracking and tracing objects within and beyond the organization's borders.

In incident management, RFID is the use of an object (typically referred to as an RFID tag) applied to or incorporated into patients, responders, or emergency transport vehicles involved in disasters to identify their locations and status [1]. RFID is a technology that offers huge potential for incident management activities by automating processes and providing accurate, trusted data. Its unique features include giving each physical object a globally unique digital identity read from a distance without requiring line-of-sight capability, and often without using a battery. These features provide new ways of measuring and integrating the real world into information systems. The two most talked-about components of a RFID system are the tag, which is the identification device attached to the item one wants to track, and the reader, which is a device that can recognize the presence of RFID tags and read the information stored on them. The reader can then inform another system about the presence of the tagged items [1], [2].

Disaster response and recovery efforts require timely interaction and coordination of emergency services in order to save lives and property. Decisions about the selection of new technologies such as RFID to track patients, equipment and staff during the response to a disaster require significant investment and can provide a real-time scalable decision support framework built on rapid information collection and accurate resource tracking functionalities. The purpose of this paper is to improve managerial decision making about the adoption of RFID in incident management. It discusses the use of this technology from a managerial viewpoint for disaster managers. This paper contains the following subjects:

At first, the RFID Applications and the necessity of attention to this technology are defined. Then differences in scope and leveling between the terms incident response, incident handling, and incident management are determined. Section IV introduces resource management concepts. The complexity of information age and disaster missions are described in section V. Section VI discusses the RFID tag readability and Section VII concludes the paper.

II. RFID APPLICATIONS

The two major areas of significant where this technology is used are financial services for IT asset tracking and healthcare with more than 60% of the top medical device companies using passive ultrahigh-frequency (UHF) RFID in 2010. RFID use in product tracking applications begins with plant-based production processes, and then extends into post-sales configuration management policies for large buyers. On the other hand, logistics and transportation are important areas of implementation for RFID technology. For example, yard

 ISBN: 978-1-61208-202-8

management, shipping and freight and distribution centers are some areas where RFID tracking technology is used. Locomotives and rolling stock are equipped with two passive RFID tags (one mounted on each side of the equipment); the data encoded on each tag identifies the equipment owner, car number, type of equipment, number of axels, etc. Aerospace applications that incorporate RFID technology are being incorporated into Network Centric Product Support Architecture [2]. This technology serves to help facilitate more efficient logistics support for systems maintenance on-board commercial aircraft.

RFID could also be used to mitigate a wide array of logistical challenges such as monitoring evacuees and managing the flow of medical supplies in the immediate aftermath of major disasters, like an earthquake, to help save lives. Researchers found there is a 72 hour 'golden' rescue period following an earthquake during which the efficiency of emergency response procedures is key to the rescue operation [3]. Particularly challenging, is knowing how many people are present in a damaged building or structure that needs to be evacuated. In these scenarios, RFID can facilitate the dispatch of rescue personnel and provide real-time information that could be used to organize search and rescue missions.

A real-world example of the value that RFID can provide in emergency situations was realized immediately following the 7.0 earthquake that struck Port-au-Prince, Haiti on January 12th, 2010. As detailed in an RFID Journal report, the U.S. Department of Defense leveraged its In-Transit Visibility (ITV) network to track shipping containers as they moved to and from the island. Lieutenant Colonel Ralph Riddle, the commander of the 832nd Transportation Battalion, in Jacksonville, FL described the benefits of ITV network: "From a commander's point of view, I'd say that the ITV was critical to the recent aid operations in Haiti. This was a very complex mission, with a rapid deployment. It's something we don't do every day, but we prepare for every day, and the ITV network was absolutely critical to its success" [3].

As an engineering solution, RFID is best understood as technology cluster within the auto ID group of technologies (which also includes, for example, barcode and optical character recognition). Unlike auto ID, however, RFID has no line-of-sight requirement, which means it provides wireless unique identification at the item level that can be seamlessly retrieved at the group level. RFID systems can operate on a stand-alone network of RFID readers and collectors or can be imbedded into responder centers' WiFi.

The following illustration, Fig. 1, shows how the RFID Software modules connect RFID devices and generic sensors with business applications.

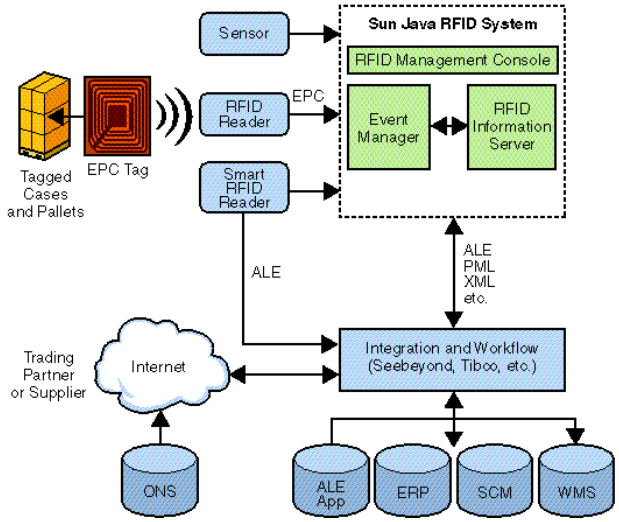

Figure 1. Layers of RFID systems.

The RFID Software consists of the RFID Event Manager, the RFID Management Console and the RFID Information Server modules. The RFID Event Manager gathers information from RFID readers, filters the information, and provides the processed information to the RFID Information Server module or to a third-party ERP system. The integration layer is optional as business applications can obtain RFID sensor events through an integration layer or directly through dedicated connectors [2], [3].

III. INCIDENT MANAGEMENT

Historically, people have used the term "incident response" and "incident handling" to define the activities for tasks and projects of a disaster responder. Consider those phrases also too narrow in scope to adequately address the wide range of work and services a responder might provide. It is shown that although incident handling and incident response are part of that work, the range of work that can be done actually encompasses a larger set of activities that we refer to as incident management [4]. There is a defined difference in scope and leveling between the terms incident response, incident handling, and incident management. We define incident handling as one service that involves all the processes or tasks associated with "handling" events and incidents. Incident handling includes multiple functions:

- **Detecting and reporting:** the ability to receive and review event information, incident reports and alerts.
- **Triage:** the actions taken to categorize, prioritize, and assign events and incidents.
- **Analysis:** the attempt to determine what has happened, what impact, threat, or damage has

 ISBN: 978-1-61208-202-8

resulted, and what recovery or mitigation steps should be followed. This can include characterizing new threats that may impact the infrastructure.

- **Incident response:** the actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to prevent the incident from happening again.

Incident response, as noted in the list above, is one process, the last step in incident handling. It is the process that encompasses the planning, coordination, and execution of any appropriate mitigation and recovery strategies and actions.

The term "incident management" expands the scope of this work to include the other services and functions that may be performed by disaster responders, including vulnerability handling, artifact handling, security awareness training, and the other services outlined in the service management procedures. The definition of this term to include this expanded set of services is important because incident management is not just responding to an incident when it happens. It also includes proactive activities that help prevent incidents by providing guidance against potential risks and threats, for example, identifying vulnerabilities in software that can be addressed before they are exploited. These proactive actions include training end users to understand the importance of computer security in their daily operations and to define what constitutes abnormal or malicious behavior, so that end users can identify and report this behavior when they see it [4].

Usually as part of the wider management process in private organizations, incident management is followed by post-incident analysis where it is determined why the incident happened despite precautions and controls. This information is then used as feedback to further develop the security policy and/or its practical implementation. In the USA, the National Incident Management System, developed by the Department of Homeland Security, integrates effective practices in emergency management into a comprehensive national framework [4].

Fig. 2 illustrates the relationship between the terms incident response, incident handling, and incident management. Incident response is one of the functions performed in incident handling; incident handling is one of the services provided as part of incident management [5].

Information Technology and technological systems provide supporting capabilities essential to implementing and continuously refining the disaster domains. These include voice and data communications systems, information systems (i.e., record keeping and resource tracking), RFID technology and display systems [6]. These also include specialized technologies that facilitate incident operations and incident management activities in situations that call for unique technology-based capabilities. Ongoing development of science and technology is integral to continual improvement. Strategic research and development (R&D) ensures that this development takes place. Each system should rely on scientifically based technical standards that support the nation's ability to prepare for, prevent, respond to, and recover from domestic incidents [5].

Maintaining an appropriate focus on science and technology solutions as we relate to incident management will necessarily involve a long-term collaborative effort among nation's partners. Effective communications, information management, and information and intelligence sharing are critical aspects of domestic incident management. Establishing and maintaining a common operating picture and ensuring accessibility and interoperability are principal goals of communications and information management. A common operating picture and systems interoperability provide the framework necessary to [4], [5]:

- Formulate and disseminate indications and warnings.
- Formulate, execute, and communicate operational decisions at an incident site, as well as between incident management entities across jurisdictions and functional agencies.
- Prepare for potential requirements and requests supporting incident management activities.
- Develop and maintain overall awareness and understanding of an incident within and across jurisdictions.

Prior to an incident, entities responsible for taking appropriate pre-incident actions use communications and information management processes and systems to inform and guide various critical activities. These actions include mobilization or pre-deployment of resources, as well as strategic planning by preparedness organizations, multiagency coordination entities, agency executives and jurisdictional authorities. During an incident, incident management personnel use communications and information processes and systems to inform the formulation, coordination, and execution of operational decisions and requests for assistance [5]. Their goal is to restore a normal service operation as quickly as possible and to minimize the impact on responder operations, thus ensuring that the best possible levels of service quality and availability are maintained.

 ISBN: 978-1-61208-202-8

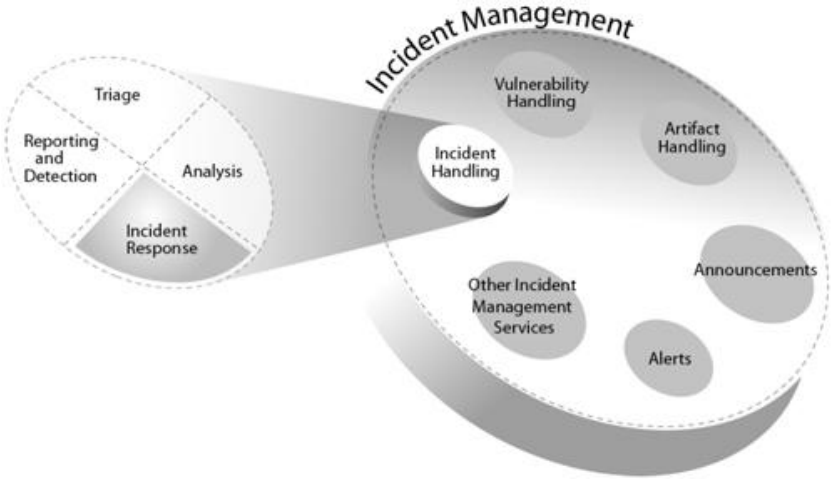

Figure 2. Defining the relationship between incident response, incident handling and incident management.

IV. RESOURCE MANAGEMENT

Resource management involves coordinating and overseeing the application of tools, processes, and systems that provide incident managers with timely and appropriate resources during an incident. Resources include personnel, teams, facilities, equipment, and supplies. Resource management involves four primary tasks:

- Establishing systems for describing, inventorying, requesting, and tracking resources;
- Activating these systems prior to and during an incident;
- Dispatching resources prior to and during an incident; and
- Deactivating or recalling resources during or after incidents.

The basic concepts and principles that guide the resource management processes allow these tasks to be conducted effectively. By standardizing the procedures, methodologies, and functions involved in these processes, resources move quickly and efficiently to support incident managers and emergency responders. The underlying concepts of resource management are that [5]:

- It provides a uniform method of identifying, acquiring, allocating, and tracking resources.
- It uses effective mutual-aid and donor assistance and is enabled by the standardized classification of kinds and types of resources required to support the incident management organization.
- It uses a credentialing system tied to uniform training and certification standards to ensure that requested personnel resources are successfully integrated into ongoing incident operations.

Generally, preparedness organizations work together in advance of an incident to develop plans for managing and employing resources in a variety of possible emergency circumstances [7]. Resource managers use standardized processes and methodologies to order, identify, mobilize, dispatch, and track the resources required to support incident management activities. Resource managers perform these tasks either at a customer request or in accordance with planning requirements. Resources are categorized by size, capacity, capability, skill, and other characteristics. This makes the resource ordering and dispatch process within jurisdictions, across jurisdictions, and between governmental and nongovernmental entities more efficient and ensures that incident management receive resources appropriate to their needs.

V. INFORMATION AGE AND DISASTER MISSIONS

The most effective consequence of Information age paradigms is deep changes in various fields including the disaster environment. Growing complexity and diversity of recent disaster missions, tasks and also methods have affected deeply Command and Control (C2) structure [8]. In fact, various missions in the disaster atmosphere require faster and more flexible plans where the traditional central and hierarchical C2 structure is not suitable. It is obvious that without dynamic information collection and resource tracking there is no guarantee for a smart response to the environment change. Also, there is neither agility nor fast movements and it is hard to plan complex operations in the right place and at the right time. These facts necessitate a new paradigm for the C2 and the main decision maker in the disaster [8], [9]. The Network Centric approach using RFID technology is a good substitution for the traditional C2. In this way, various aspects of disaster environments such as power transferring to the edge, self-similarity, sense making, agility and effectiveness can be achieved more easily [10], [11]. Concurrent planning and execution is one

 ISBN: 978-1-61208-202-8

of the most fundamental subjects in which there is always the opportunity to change, modify and/or heal the plans, therefore complex missions can be done. Active RFID is now being used to track and trace victims in a disaster situation. Each tag generating a message each time when passing a reader may be a desired outcome. Some RFID tags can be read from several meters away and beyond the line of sight of the reader. The application of bulk reading enables an almost-parallel reading of tags. Data can be collected in real time and made available to emergency workers immediately, saving precious hours. Crisis management teams, hospitals and other emergency personnel have access to the information via a computer database. Hospitals, for instance, can start planning for the arrival and treatment of disaster victims. The combination of these components will result in the creation of a mobile, scalable tool that can be rapidly deployed at a disaster scene to enable an offsite commander to visualize the location and triage condition of the casualties as well as the available resources. This information will improve the coordination of the response to better match supply (care providers, ambulances, medical equipment) with demand (number of patients, level of acuity) [12], [13].

VI. RFID TAG READABILITY AND OPTIMIZATION OF RFID SYSTEMS

For an incident commander, keeping track of resources, equipment and products at the scene of an emergency is vital. Current performance of RFID systems is highly application dependent: tag-reader combinations behave differently for different target applications, as well as under variations of the environment for a given application. In general, successful data transaction between tags and a reader with a maximum reading range, and tag read rates (as specified by the existing standards EPC Class 0 & 1, ISO 18000-6A/B, ISO 15693, etc.) with unrestrictive tag orientations are the key aspects that measure performance of an RFID system [14]. Currently, low frequency and high frequency technologies perform reliably, but for ultra-high frequency RFID the deployment needs careful tag, reader, protocol and environment selection to achieve acceptable tracking reliability. The main factors that effect the tag readability are type of antenna, height of tag from the ground, displacement of tag and distance of tag from antenna. RFID system implementation always requires that the system be optimized to every application. For optimizing the RFID system experiments need to be performed to identify the placement, location, orientation of tag antenna and other factors which interact with the system. The importance of optimization is explained by Ammu [14]. He identifies the effect of distance between tag and antenna and performs design of experiments to analyze the resulting data. The main measurement is the number of reads for every experiment and its repetitions. The difference between the levels of each factor is also analyzed using statistical analysis software. The placement and location of the tag is identified using the factorial approach. This approach gives an application specific optimization. The RFID system is used as a trigger mechanism to a vision system which determines whether the object is moving towards or away from a particular position. Another similar invention is the integration of video surveillance system with the RFID tracking system. The calibration of RFID tracking system is enhanced by the use of information provided by the video surveillance system. Moreover, the calibration of the vision system is enhanced by the information of the RFID system. RFID systems are calibrated by placing RFID tags at visually apparent locations to determine appropriate correction factors for use in subsequent RFID locations. This invention provides the advantages of RFID tracking system and the video surveillance system to overcome the disadvantages of either systems or both [14].

VII. CONCLUSION

The demand for effective and expediently-made decisions is always in vogue. This is not surprising since making correct decisions is essential for successful operations in many places such as disaster environments. Decisions require data to be processed for quality, concept and context [13]. The goal of information gathering and processing is focused on existing or arising problems. The main conclusion of this paper is expanding the network-centric paradigm allows for access to additional, previously unreachable sources of information in addition to physical and informatics scopes [15]. One the main points in this conclusion is the development of security as well as quality of services rendered by trust networks and reliability systems using RFID technology. RFID is a non-line-of-sight (capable of communicating remotely even when obscured) and contact-less (without direct contact between the transacting elements) automatic identification technology. The identification data is stored on chips that can be attached or embedded into products, animals or even humans. The tag can be active (with on-board power source) or passive (with no power source). These enable robots and humans to use passive RFID tags and GPS devices to map out a disaster area and send information to a command center. While there is a benefit of getting more information, the time spent to weigh information for quality, to fuse information into concepts, and to package for contextual relevance is also increasing.

VIII. REFERENCES

[1]. Takizawa, O., “RFID-based Disaster-relief System”, National Institute of Information and Communications Technology, Japan, 2005.

[2]. Kitayoshi, H. and Sawaya, K., “Technical Conditions for High-power Passive Tag Systems Using the 950 MHz Band (partial report from Information and Communications Council)”, Ministry of Internal Affairs and Communications, Tokyo, Japan, 2004.

 ISBN: 978-1-61208-202-8

[3]. Shibayama, A. and Hisada, Y., "An Efficient System For Acquiring Earthquake Damage Information In Damaged Area", The 13th World Conference on Earthquake Engineering, No.1121, Vancouver, Canada, August 2004.

[4]. Chertoff, M., "National Incident Management System (NIMS)", Federal Emergency Management Agency, U.S. Department of Homeland Security, Washington DC, USA, March 2010.

[5]. Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., and Zajicek, M., "Defining Incident Management Processes for CSIRTs: A Work in Progress", USA, October 2004.

[6]. Gadh, R. and Prabhu, B. S., "Radio Frequency Identification of Katrina Hurricane Victims", USA, 2010.

[7]. Atkinson, S. R. and Moffat, J., "The Agile Organization: From Informal Networks to Complex Effects and Agility". Washington D.C, USA, CCRP 2005.

[8]. Alberts, D. S. and Hayes, R. E., "The future of command and control", Washington DC, USA, CCRP 2007.

[9]. Alberts, D. S. and Hayes, R. E., "Power to the Edge: Command Control in the Information Age", Washington DC, USA, CCRP 2003.

[10]. David, A. S., Garstka, J. J., and Stein, F. P., "Network Centric Warfare: Developing and Leverage Information Superiority", Washington DC, USA, CCRP 1999.

[11]. Dekker A. H., "A taxonomy of Network Centric Warfare Architectures", Systems Engineering/Test and Evaluation Conference, Brisbane, Australia, November 2005.

[12]. Ling, M. and Selvestrel, M., "An Organisation-Oriented Agents Approach to Modelling Network-Centric Warfare". SimTecT 2004, Canberra, Australia, 2004.

[13]. Shamdani, A. N., "Intelligent Net Centric Command and Control Architecture Using Cognitive Approach", The World Congress on Engineering and Computer Science (WCECS 2008), San Francisco, USA, 22-24 October 2008.

[14]. Ammu, A., "Effect of Factors on RFID Tag Readability – Statistical Analysis", USA, 2009.

[15]. Shamdani, A. N., "The Effect of Avicenna's Philosophy on the Development of Cognitive Architecture for the Network Centric Command and Control", The International MultiConference of Engineers and Computer Scientists (IMECS 2010), Hong Kong, 17-19 March 2010.

 ISBN: 978-1-61208-202-8