TOWARDS A FRAMEWORK FOR CRISIS INFORMATION MANAGEMENT SYSTEMS (CIMS)

Renato Iannella

NICTA, Australia[1]

Karen Robinson

NICTA, Australia[2]

Olli-Pekka Rinta-Koski

NICTA, Australia[3]

Keywords

Crisis Information Management Systems, Frameworks and Architectures, Interoperability, Standards, Emergency Management Systems, Incident Management Systems

Abstract

After a number of recent major natural disasters (eg Boxing Day Tsunami, Hurricane Katrina, and Cyclone Larry) the sector stakeholders are moving towards efforts to define and exploit greater ICT utilisation during the response and recovery phases of major incidents. The focus has moved from just improving voice-data-network-level technologies for communication into harnessing new information-level technologies to cover all phases of crisis management. This includes information infrastructure for incident message routing and standard languages for conveying the semantics of emergency warnings and resource and task management. In this paper we review some of the emerging requirements for Crisis Information Management Systems (CIMS) and look at the current and future technologies that will need to address these requirements. A CIMS needs to also address the sharing of information across emergency agencies and any stakeholders involved in the response and recovery. A CIMS will also be required to follow any number of emergency response models and provide technologies to match and support the policies and rules that govern these human-oriented models. Also, based on our own CIMS demonstrator, we propose a starting framework to support CIMS functionality and identify the key interoperability opportunities.

Introduction

With the recent impact of natural and other disasters, the emergency management community has focussed energy on defining greater requirements for ICT support during and post these incidents. There has also been an expectation that ICT should be providing such support. However, emergency management is not a discipline that follows well behaved rules nor allows itself to be modelled sufficiently well that all contingencies can be catered for a priori. In essence, emergency management is still in its infancy when utilising ICT solutions.

[1] NICTA, 300 Adelaide St, Brisbane QLD, 4000 AUSTRALIA <renato@nicta.com.au>
[2] NICTA, 300 Adelaide St, Brisbane QLD, 4000 AUSTRALIA <karen.robinson@nicta.com.au>
[3] NICTA, 300 Adelaide St, Brisbane QLD, 4000 AUSTRALIA <ola.rinta-koski@nicta.com.au>

Crisis Information Management Systems (CIMS) is a new concept now entering the vocabulary of the emergency and disaster sector. Its aim is to provide a complete suite of ICT functions addressing the many requirements from the emergency management community. There are other terms, such as Disaster Management Interoperability System, and Critical Incident Management System, but CIMS is emerging as the preferred term for major crisis needs across multiple agencies and across multiple jurisdictions, where there is a need to exchange information for coordinated action and capability sharing.

Recent work on frameworks for CIMS has shown a broad scope in findings. Kim *et al* (2006) define 12 underlying factors that need to be supported, such as information sharing, resource allocation, secure and reliable communications, coordination with national resources, integrating information, and privacy issues. Dwarkanath & Daconta (2006) outline an "enterprise framework" for CIMS and argue that no single entity can be responsible for the entire management of a crisis which a shared services platform across many enterprises could support.

Ryoo & Choi (2006) argue that modularity is critical for CIMS to maintain their flexibility in adapting to disasters of different magnitude. They also present a classification framework that includes high level functions of: collection, distribution, presentation, and processing for CIMS frameworks. Wang & Belardo (2005) present a crisis management framework where the information management strategies differ depending on the state and type of the disaster.

The Institute for Security Technology Studies (2004) found many challenges facing the CIMS community, including:

- Supporting a wide range of functional areas,
- Supporting the Critical Infrastructure community,
- Supporting a broadly accepted vocabulary of technical terms, and
- Promoting the interoperability of CIMS.

We propose that a CIMS Framework needs to capture and categorise the functions and services of CIMS to enable a common terminology to evolve with shared meanings. Additionally, the interoperability between CIMS must be based on open information standards developed by the community to enable flexibility in the systems architectures and deployment of CIMS.

This paper is organised into three sections covering the aims and scope of CIMS (as shown in Figure 1).

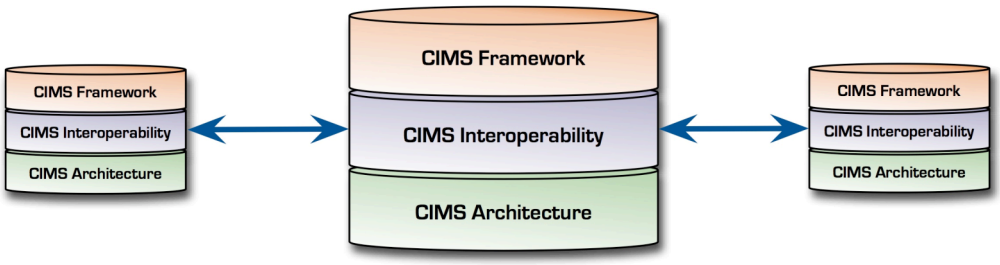

Figure 1 – CIMS Scope

Firstly, the CIMS Framework will be presented that covers the high-level functionality and services provided by CIMS systems. Secondly, CIMS Interoperability covers the sharing of information between CIMS systems in a consistent and standardised manner. This will focus on current information standards related to emergency management. And thirdly, the CIMS

Architecture will cover some of the underlying technical issues for deploying CIMS systems, and will be based in a demonstrator CIMS system.

CIMS Framework

The functionality of a CIMS will vary greatly. This will be reflected in the both the needs of the crisis team using the CIMS and the level of expertise and reporting structures. Figure 2 presents some of the core functionality for CIMS services across three horizontal layers. Layer one functions include functions that provide direct crisis control and management. Layer two provides support functions to layer one services, and Layer three provides core system-wide services.

Figure 2 – CIMS Framework

The Operational Methodology Management function is one of the critical functions of a CIMS and operates across all layers. This supports the processes used in crisis coordination centres which are governed by Incident Management Systems (IMS), which vary across jurisdictions, but fundamentally provide a structured and hierarchical "command and control" framework. For example, in Australia the common IMS is the Australian Inter-service Incident Management System (AIIMS), which governs the roles and relationships between the local, district, and state level disaster coordination centres, and disaster management groups. The Operational Methodology Management would provide overall concepts that would need to be supported across all the other layers and functions, based on the terms, structures, and semantics defined in the IMS.

The layer one Incident Management supports the high-level recording of individual incidents. Since a CIMS will be used for multiple incidents over time, there is need to manage a crisis as a single event. All other layer one and two functions would be related to one or more incidents. People Management supports the management of defined roles, teams, tasks and duties of individuals and organisations.

Resource Management supports the management of resources during a crisis. This involves all stages (discovery, commitment, deployment, return, extension, etc) for resources involved in the recovery and response phases of a crisis.

Notification Management supports the management of outgoing and incoming information messages. This includes broadcast messages to large groups, even community wide, and routing of messages to the right people who need to be informed of the content.

Situational Awareness Management supports development of a "picture-of-operation" that encapsulates the current crisis, based on all the information currently held or made available to the CIMS. Typically, this would be aggregated situational reports or geo-spatial images with multiple layers showing current status of the incident and allowing planning operations.

The layer two Document Management supports the effective categorisation of the documents created and deposited into the CIMS. Report Management supports the automated creation of incident reports, based on the CIMS repository of information, such as status reports etc.

Financial Management supports budgets, expenditures, and reconciliation of financial transactions. Assessment Modeling Management supports planning and modelling functions of the incident, such as damage assessment, or storm-tide surge modelling.

The layer three Authentication and Authorisation Services support users to gain access and be authorised to perform secure functions in the CIMS. Directory Services supports a single view of users across the CIMS including federated identity services. Geospatial Services support mapping of incident data to various map sources, such as road networks or satellite maps.

The aim of this framework is not to present an extensive functional map of CIMS services, but to focus on the core functions, and their interoperability challenges across CIMS.

CIMS Interoperability

When designing CIMS, it should not be assumed that they will operate in isolation. Although some systems have been designed in this way in the past - including a variety of standalone Web-based and client/server solutions, such as WebEOC (ESi, 2007) and L-3 CRISIS (Ship Analytics, 2007) - the requirement for all parties involved in crisis management to use a single (and often centralised) system has hindered their uptake. Crisis management is typically a complex activity involving distributed teams of people from a variety of organisations; therefore, requiring everyone to adopt and log on to a single system is extremely challenging in terms of conflicting organisational policies and procedures (e.g., security policies), differing IT setups and system scalability. In order to be successful, interoperation based on common standards should be supported, both between different implementations of CIMS, as well as between CIMS and other types of software used by the emergency management community. As discussed earlier, many countries have standardised their terminology, principles and command structures for crisis management by developing their own IMS (such as AIIMS in Australia); however, there has been limited adoption of standard formats for information sharing between information systems such as CIMS. Despite this, some work on the standardisation of information formats has begun – particularly in the US, driven by problems highlighted by recent disasters such as Hurricane Katrina and 911.

The most relevant standards for CIMS are being developed by the OASIS consortium's Emergency Management Technical Committee (OASIS Emergency Management TC, 2007). The Common Alerting Protocol (CAP) (OASIS Emergency Management TC, 2005) was the first standard to be sanctioned by this group. CAP defines an XML format for interoperability in alerting and public warning systems. The intention is to promote consistency in the information produced by all kinds of sensor and alerting systems, thereby reducing confusion and helping to get crucial warning information to the public faster. CAP messages carry message identifiers; information about the sender and the time sent; message status, type and scope; and the event category, urgency, severity and certainty. In addition, the messages can carry other optional information, such as instructions for the recipients and a description of the target area. CAP has had good early uptake in the US – e.g., in the Department of Homeland Security and the National Weather Service (Botterell, 2006) – and is emerging as the common information standard for general incident messages.

The next generation of information standards are being developed as part of the Emergency Data Exchange Language (EDXL) family of standards. This family includes one completed standard – the EDXL Distribution Element (OASIS Emergency Management TC, 2006) – and two further specifications that are nearing completion – EDXL Resource Messaging (OASIS

Emergency Management TC, 2007b) and the EDXL Hospital AVailability Exchange Language (OASIS Emergency Management TC, 2006b).

The EDXL Distribution Element (EDXL-DE) captures information required to enable routing of XML (and other) payloads, in order to facilitate information exchange between the various organisations involved in emergency management and response. This routing information includes elements such as the target area for a message (in order to support location-based message delivery); information about the sender; the target address for the message, if applicable; keywords describing the message content; and the type and "actionability" of the message (actual, exercise, test, etc.). The Distribution Element can be used as an envelope/container to support dissemination of other EDXL components, such as resource messages, hospital availability information, or CAP payloads. It can underpin all forms of information exchange in CIMS (including interoperability with other software), as it is designed to carry any form of emergency-related data, and can serve as one of the standards underpinning the Notification Management function of the CIMS framework described in the previous section.

The Hospital AVailability Exchange Language (EDXL-HAVE) enables hospitals to exchange information about their bed availability, status, services and capacity. EDXL-HAVE can partially support the Situational Awareness function outlined previously – that is, it can be used to support emergency logistics and resource-related decisions, but requesting specific hospital resources is outside its scope. This is covered by EDXL Resource Messaging (EDXL-RM), which aims to provide a comprehensive set of message formats for resource management across all areas of the emergency sector. EDXL-RM provides a set of 16 message types for purposes such as requesting resources and responding to resource requests; requisitioning and committing resources; offering unsolicited resources; requesting and reporting resource deployment status; and releasing resources. Although the standard is reasonably complex, it is comprehensive and will provide a good basis for the Resource Management functionality of CIMS. Both EDXL-HAVE and EDXL-RM are expected to be approved as OASIS standards in the first half of 2007.

Figure 3 shows the relationship between the EDXL and other interoperability standards in terms of their roles for underlying communications, routing infrastructure, and incident-specific information messages.

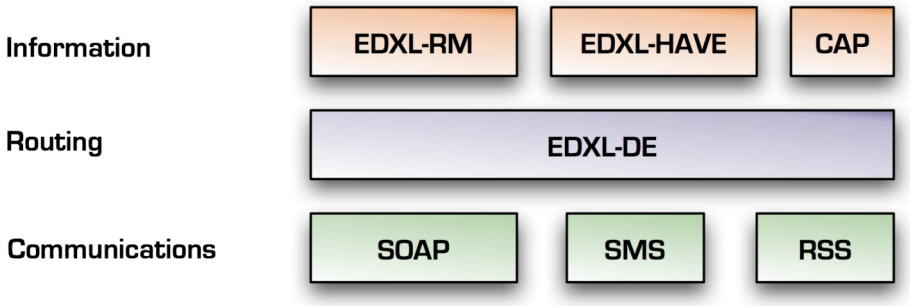

Figure 3 – CIMS Interoperability Layers

These current and emerging standards are a good step in the right direction for interoperability, but are far from covering the full scope of CIMS functionality. Further standardisation efforts will be required to close the gaps. In addition to participating in the development of OASIS specifications such as EDXL-RM, we have been developing information models and XML formats for cyclone/hurricane warnings, tsunami warnings and situation reports. Some of this work is described in our earlier publications (Iannella, 2006; Iannella and Robinson, 2006; Sun *et al.*, 2006).

CAIRNS: A CIMS Architecture

Because CIMS systems come under heaviest load when a disaster occurs, they have to operate in challenging external conditions. Network connections might be intermittent, network nodes have to be able to join and disconnect at will, and information has to be accessible to end user terminals with limited resources, such as PDAs and mobile phones.

CAIRNS (Cooperative Alert Information and Resource Notification System) is a demonstrator of technologies that can be used to construct a resilient, fault-tolerant CIMS architecture. Currently, CAIRNS is focussed towards an interoperable architecture for incident notification.

On the most basic level, CAIRNS is a collection of independent nodes that can join and drop out of the network at will (see Figure 4). Messages between nodes are passed using peer-to-peer (P2P) technologies similar to those used in file sharing networks. There is no central node, which means there is no single point of failure that would bring the whole system down. Each node caches the messages it receives and is able to forward them even if the original sender can no longer be reached. A message is purged from the cache when an update arrives or its expiration time is reached.

Interoperability with other systems is achieved by using a standards-based message format. CAIRNS message traffic is based on SOAP, a standard protocol for exchanging XML-based messages over networks. Each node acts both as a SOAP server and a SOAP client, so that any node can initiate the message transfer without the need to poll. Routing information is attached to the message using EDXL-DE.

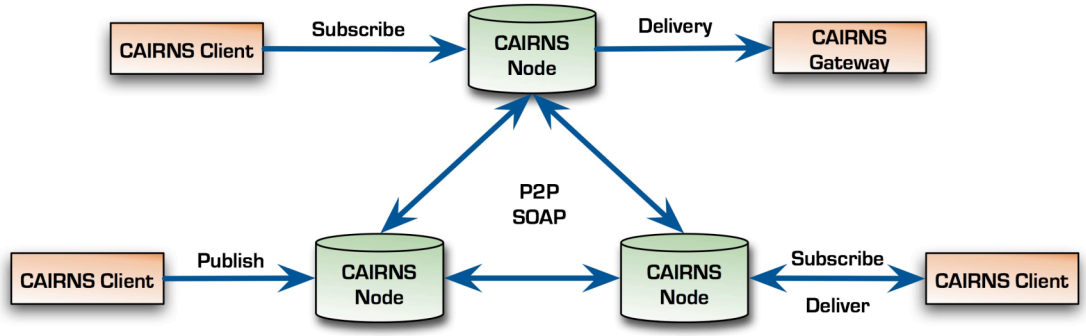

Figure 4 – CAIRNS Architecture

End users can connect to a CAIRNS node with a standalone client or through a Web interface. Each user registers their interest in a particular type of message by specifying subscriptions containing rules such as type of incident, geospatial area affected, sender role, severity and so on. Whenever a new message matching the subscription arrives, the user will get a notification by appropriate gateways to delivery mechanisms (eg SMS, email, SOAP) which can be selected according to rules such as "if it's past 5pm, I want a brief summary by SMS, otherwise send the full message by email". The messages can contain information about the intended recipient roles, so that fire incidents will be relayed to all users with the "fire chief" role specified in their profile even without a matching subscription. By specifying roles instead of specific email addresses, the messages will reach the appropriate persons regardless of their actual identities.

All the information available through CAIRNS is provided by Publishers. At the most basic level, their role is to receive information through other channels (for instance, an ocean buoy that transmits sea level data) and transform it into CAIRNS messages. In practice, a Publisher

amalgamates information from different external sources and publishes conclusions based on this data (eg a Tsunami warning). Subscribers are directly connected to the CAIRNS network and can access information either by subscribing or through direct queries. Consumers receive CAIRNS information through one-way gateways that transform CAIRNS messages to a format more suited to the distribution channel. An example of a Consumer could be a member of the general public who receives a tsunami warning as an SMS cell broadcast to his or her mobile phone, or an Emergency Manager responsible for evacuating people.

The next phase of CAIRNS is to extend the architecture to support Resource Management functions from the CIMS Framework utilising the EDXL-RM standard for interoperability. This will also test a number of the related CIMS Framework functions, such as Notification (for routing message) and Situational Awareness (show me the current locations of my resources).

Conclusion

We have presented findings on evaluating the functional requirements for CIMS and developed an initial framework. This has highlighted the key requirement of interoperability for CIMS to enable collaborative sharing of critical information. Our CAIRNS demonstrator is the first step in realising this CIMS framework and technical interoperability architectures.

There is no doubt that information is critical during catastrophic disasters. The emergency sector is now moving towards common CIMS solutions as a result of recent major disasters that have highlighted ongoing challenges across the community. As the community works towards addressing these challenges with CIMS, we need common tools, frameworks, and terminologies for consistency and interoperability.

References

Botterell, A. (2006). The Common Alerting Protocol: An Open Standard for Alerting, Warning and Notification. In *Proceedings of the 3rd International ISCRAM Conference*, pp. 497-503, Newark, NJ, USA.

Dwarkanath, S., Daconta, M. (2006) Emergency Services Enterprise Framework: A Service-Oriented Approach. Proceedings of the 3 International ISCRAM Conference (B. Van de Walle and M. Turoff, eds.), Newark, NJ (USA), May 2006,

ESi. (2007). *WebEOC overview*. <http://www.esi911.com/esi/products/webeoc.shtm> Last accessed 21 February 2007.

Iannella, R. (2006). Modeling and Integration of Severe Weather Advisories for Situational Awareness. In *Proceedings of the 9th International Conference on Information Fusion*, Florence, July 2006.

Iannella, R. and Robinson, K. (2006). Tsunami Warning Markup Language (TWML), version 1.0. *NICTA Technical Report*. <http://xml.coverpages.org/TsunamiWarningML-V10-20060725.pdf>

Institute for Security Technology Studies (2004) Crisis Information Management Software (CIMS) Interoperability: A Status Report. Technical Analysis Group, Dartmouth College.

Kim, J K., Sharman, R., Rao, H R., Upadhyaya, S. (2006) Framework for Analyzing Critical Incident Management Systems (CIMS). Proceedings of the 39th Hawaii International Conference on System Sciences.

OASIS Emergency Management TC. (2005). Common Alerting Protocol, v. 1.1. *OASIS Standard CAP-V1.0* October 2005.

OASIS Emergency Management TC. (2006). Emergency Data Exchange Language (EDXL) Distribution Element, v. 1.0. *OASIS Standard EDXL-DE v1.0*, 1 May 2006.

OASIS Emergency Management TC. (2006b). Emergency Data Exchange Language (EDXL) Hospital AVailability Exchange (HAVE). *OASIS Public Review Draft 02*, 2 November 2006.

OASIS Emergency Management TC. (2007). *OASIS Emergency Management Technical Committee Website*. <http://www.oasis-open.org/committees/emergency/> Last accessed 21 February 2007.

OASIS Emergency Management TC. (2007b). Emergency Data Exchange Language Resource Messaging (EDXL-RM) 1.0 (01). *OASIS Committee Draft 01*, 20 February 2007.

Ryoo, J., Choi, Y B. (2006) A comparison and classification framework for disaster information management systems. International Journal of Emergency Management, Vol. 3, No. 4, pp. 264-279.

Ship Analytics. (2007). *L-3 CRISIS overview*. <http://www.shipanalytics.com/EMSS/L-3CRISIS.asp> Last accessed 21 February 2007.

Sun, S., Iannella, R. and Robinson, K. Cyclone Warning Markup Language (CWML), version 1.0. *NICTA Technical Report*, December 2006.

Wang, W-T., Belardo, S. (2005) Strategic Integration: A Knowledge Management Approach to Crisis Management. Proceedings of the 38th Hawaii International Conference on System Sciences.

Acknowledgements

National ICT Australia is funded by the Australian Government's Department of Communications, Information Technology, and the Arts; the Australian Research Council through Backing Australia's Ability and the ICT Research Centre of Excellence programs; and the Queensland Government

Author Biography

Renato Iannella is Principal Scientist at the National ICT Australia (NICTA) and leads the Smart Applications For Emergencies (SAFE) project. His research covers policy-aware information architectures and standards in trusted information and rights management. Renato has extensive experience in the development of Internet, Web, and Mobile technologies and standards and was a former member of the World Wide Web Consortium (W3C) Advisory Board. Renato also is an Adjunct Associate Professor at the University of Queensland, Visiting Associate Professor at the University of Hong Kong and was previously the Chief Scientist at LiveEvents Wireless, IPR Systems and Principal Research Scientist at the Distributed Systems Technology Centre (DSTC).

Karen Robinson is a researcher in the SAFE project at National ICT Australia (NICTA). Her current research focuses on information modelling for emergencies, with an emphasis on standards. Her background is in the field of pervasive and mobile computing, and she received a PhD in this area from the University of Queensland in September 2004. She has previously worked as a Research Fellow at the University of Queensland and a Research Scientist at the Distributed Systems Technology Centre (DSTC).

Olli-Pekka Rinta-Koski is a Research Engineer in the SAFE project at National ICT Australia (NICTA). His work is focused on incident management ICT infrastructure design, with an emphasis on standards and interoperability. He has previously worked on software development in the fields of derivative trading, mobile communication and bioinformatics. He holds a MSc (Tech) in Computer Science from the Helsinki University of Technology.