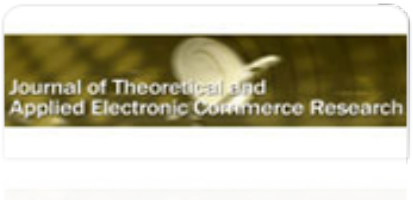

Journal of Theoretical and Applied Electronic Commerce Research
E-ISSN: 0718-1876
ncerpa@utalca.cl
Universidad de Talca
Chile

Kuehn, Andreas; Kaschewsky, Michael; Kappeler, Andreas; Spichiger, Andreas; Riedl, Reinhard
Interoperability and Information Brokers in Public Safety: An Approach toward Seamless Emergency Communications
Journal of Theoretical and Applied Electronic Commerce Research, vol. 6, núm. 1, abril, 2011, pp. 43-60
Universidad de Talca
Curicó, Chile

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

Interoperability and Information Brokers in Public Safety: An Approach toward Seamless Emergency Communications

Andreas Kuehn[1], Michael Kaschewsky[2], Andreas Kappeler[3], Andreas Spichiger[4] and Reinhard Riedl[5]

[1] Syracuse University, School of Information Studies, Syracuse, NY, United States, ankuhn@syr.edu
Bern University of Applied Sciences, Competence Center Public Management and E-Government, Bern, Switzerland,
[2] michael.kaschewsky@bfh.ch, [3] andreas.kappeler@bfh.ch, [4] andreas.spichiger@bfh.ch, [5] reinhard.riedl@bfh.ch

Received 16 August 2010; received in revised form 21 November 2010; accepted 22 December 2010

Abstract

When a disaster occurs, the rapid gathering and sharing of crucial information among public safety agencies, emergency response units, and the public can save lives and reduce the scope of the problem; yet, this is seldom achieved. The lack of interoperability hinders effective collaboration across organizational and jurisdictional boundaries. In this article, we propose a general architecture for emergency communications that incorporates (1) an information broker, (2) events and event-driven processes, and (3) interoperability. This general architecture addresses the question of how an information broker can overcome obstacles, breach boundaries for seamless communication, and empower the public to become active participants in emergency communications. Our research is based on qualitative case studies on emergency communications, workshops with public safety agencies, and a comparative analysis of interoperability issues in the European public sector. This article features a conceptual approach toward proposing a way in which public safety agencies can achieve optimal interoperability and thereby enable seamless communication and crowdsourcing in emergency prevention and response.

Keywords: Communication, Coordination, Crowdsourcing, Emergency response, Events, Information broker, Interoperability, Public safety

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

1 Introduction

When severe damage occurs in disasters or catastrophes and large-scale public safety is threatened, close collaboration between emergency workers and government agencies is essential. At these times, resources and information – both governmental and non-governmental – must be integrated in order to enable seamless, ad-hoc interaction of otherwise independent, self-organized emergency response units. In such circumstances, collaboration and coordination across organizational and jurisdictional boundaries cannot be achieved without interoperable technologies that are based on standards and arrangements agreed upon in advance.

Interoperability plays a major role in enabling collaboration among government, public safety agencies and their rescue teams to prevent disasters and protect the general public from significant danger in the event of an emergency. Cutting-edge technology, including applications, devices, and networks, can support public safety departments to prevent catastrophes and respond quickly when one occurs. Mobile technology enables access to, and the exchange of, vital information (1) among emergency response units, (2) between emergency response units and the affected public, and (3) among the affected public. This is possible regardless of where emergency personnel reside. Furthermore, new technologies are not restricted to voice; information in the form of video and data from heterogeneous, public and private sources can be integrated to provide emergency response units with a better understanding of the situation and the scale of the disaster [19]. Ultimately, this access to real-time information can save lives.

In a perfect world, the aforementioned outlined use of technology aimed at seamless interaction between organizations and people would function perfectly every time [39]. In reality, though, communication and sharing of vital information across agencies of different jurisdictions are often hindered by the lack of interoperable systems, the lack of contractual agreements, and legal incompatibilities (i.e., different responsibilities and range of authority as barriers). Current technology only satisfies specific, local uses within particular agencies. Notification systems are often outdated and do not adequately inform and warn the public about emergencies. The gathering and sharing of information from people directly affected by the emergency has not yet been envisaged; even though they are at the center of the crisis and could provide critical first-hand information [3]. The challenges that public safety agencies face today far surpass technology. In addition to legal and organizational challenges, there is a great need for a comprehensive plan to enhance public safety [19]. We can observe a number of bottom-up initiatives that have attempted to improve this; some of them failed [19], but standards are slowly emerging. From a bird's eye perspective, however, the landscape for interoperability in public safety looks scattered and fragmented. Clearly, a coordinated approach is essential to bring together piecemeal solutions for a closer, more effective and efficient collaboration among public safety agencies from different jurisdictions and governmental levels.

In this paper, we focus on the notion of interoperability – in its technical, semantic, organizational, legal, and political aspects – in public safety with a particular emphasis on communication during an emergency. We consider the notion of interoperability as a necessary prerequisite to achieving seamless communication among public safety units and the public for collaborative and coordinative purposes. Under the term ‘emergency communications’, we understand all the bi-directional communication that takes place in an emergency among three groups: (1) public safety agencies, such as police agencies, fire departments, and emergency medical services (EMS) that are in the thick of the disaster; (2) affiliated organizations, such as hospitals, municipal services, telecommunications, logistics, and utilities (e.g., electricity, gas, water) as well as media or schools and other public or private institutions or companies; and (3) the concerned and/or affected public who have been injured, are in imminent danger of injury, or are able to provide critical information about particular situations. The underlying assumption is that these three groups would benefit from greater information sharing in an open communication system.

1.1 Objectives and Structure

The objectives of this paper are threefold. First, we introduce a general architecture that describes an information broker for emergency communications. An information broker enables the gathering and analysis of large-scale, up-to-date data in a timely fashion across organizational and jurisdictional boundaries, helping public safety agencies and emergency response units to communicate and collaborate more effectively. Second, based on this general architecture, we identify and reflect upon interoperability issues in a public safety environment. Third, we discuss how the public may become an important actor in emergency communications by using the information broker as a means to enable crowdsourcing in disaster prevention and response.

To achieve these objectives, we draw upon ongoing and recently concluded research in which we were involved. In the second section, we provide a brief overview of related domains to help identify some key challenges involved in achieving close collaboration in emergency situations. Here, we do not claim to provide a comprehensive literature review, but instead outline areas for further consideration. In the third section, we introduce the notion of an information broker as a metaphor and concept in emergency communications; we also describe its major components and functions. This research was part of a government-mandated preliminary study for a future emergency communications and alert system in a European country. The conceptual findings provide a basic understanding of the elementary components and functions of an open communication system. The fourth section

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

examines the conceptual foundations of event-driven processes. This section makes use of an ongoing research project investigating different approaches to manage and utilize large-scale data through complex event processing in emergencies. The fifth section draws on related research on interoperability and ICT standardization to outline different levels of interoperability, and it identifies objectives, trade-offs and resource requirements, particularly in regard to organizational and semantic interoperability. In the sixth section, the previously outlined notions are integrated into a coherent general architecture describing a holistic view of emergency communications. Further, some reflections on implementation, crowdsourcing, and coordination are included that reference related work. Finally, in the conclusion, premises and design principles by [68] are briefly discussed relating to the information broker, and a brief outlook is given on emerging technologies and their possible effects on crowdsourcing in emergency communications.

1.2 Methodology

This paper follows a design-oriented research approach that seeks a feasible solution for problems we identified together with our research partners in previous research projects [24]. The relevance of the research emerged from public sector ICT practice that focuses on interoperability and public safety, with a particular focus on emergency communications. The research process followed a generic approach that considers real-world requirements to satisfy applicability. The process consisted of (1) eliciting meta-requirements and requirements, (2) validation of requirements through interviews and scenario testing, (3) developing conceptual alternative solutions, (4) assessment of the solutions, (5) development of the proposed solution, (6) validation through interviews and scenarios, and (7) reflection and discussion with practitioners.

Requirements for emergency communications were elicited in expert interviews with federal authorities in charge of modernizing the alerting system currently in use. A related ongoing research project uses real-world scenarios to investigate the use of information from multiple actors and heterogeneous sources for disaster management. In these case-based scenarios, the focus is on the utilization of large-scale data through complex event processing and on the identification of trade-offs and resource requirements. The result is evidence-based knowledge of information management for disaster prevention, preparedness, response, and recovery. A literature review was undertaken to identify the challenges of emergency communications. For the section on interoperability in the public sector, a comparative study was conducted that compared the interoperability frameworks of three European countries and the European Union [35]. This conceptual work is not a comprehensive empirical evaluation, but rather identifies key challenges in emergency communications and ways in which these issues may be addressed.

2 Background

In order to achieve close collaboration in emergency response, as a prerequisite, interoperability is required on a technical, semantic, organizational, legal and political level. Thus, we first address relevant work on the topic of interoperability and related standards. Then, based on our literature review, we elaborate upon three broad categories of factors that enable or hinder collaboration in emergency response.

2.1 Interoperability

With reference to [16], we define ‘interoperability’ for emergency response as the ability of disparate and diverse public safety agencies and their emergency response units to interact in emergency situations towards common goals, involving the sharing of information and knowledge between involved organizations and the public via defined or ad-hoc processes to achieve coordinated actions, by means of the exchange of data between their respective information and communication systems.

Emergency response may benefit from existing frameworks that have been established to enable interoperability in (e.g., [12], [15], [32]) and between national states (e.g., [16], [45]) as well as specific requirement analysis for public safety (e.g., [13], [68]). Even though the benefit from interoperability in the form of enhanced information sharing is obvious, it is seldom achieved. According to [7], on-demand sharing of maps, situational reports, and the status of medical resources is essential in critical situations; however, comprehensive standards that could enable the exchange of such vital data – with the exception of voice – do not exist yet. Such standards would need to address the sharing of devices, information security, control over resources and robustness to continue availability in uncertain and dynamic conditions. Such systems are heterogeneous and interdependent, and the broad range of required standards is complex [7].

To give a few examples of the interoperability challenge, [30] identified 266 different systems in use for public safety purposes in the United States. This example is particularly eminent for the United States as it mirrors an underlying challenge for public safety agencies that affects the ability to act cooperatively: overlapping responsibilities and jurisdictions, decentralization, and a lack of unitary command or control [66]. The sheer number of public safety agencies in the United States makes the complexity clear: 17,000 law enforcement agencies, 30,000 fire departments, and 15,000 emergency operation centers [13]. Hence, the variety of incompatible software and hardware sounds more like a logical inference, given these circumstances [8]. Public safety radio systems are

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

assigned different frequencies in order to avoid interference with neighbouring departments; hence, it is hardly astounding that public safety radio systems lack basic interoperability [19]. In the past, efforts to build an interoperable public safety network in the United States have failed [19]. Projects and related standards on digital radios for emergency communications (e.g., "Project 25" in the U.S. and TETRA in Europe) have successfully started to bridge this gap, but are limited to voice. Overall, the cost for fragmented public safety communication is significant, as special equipment to overcome the communication gap is up to ten times more expensive than conventional public safety communication equipment [44]. Consequently, there is a strong and explicitly stated need for interoperable systems that allow collaboration across organizations, jurisdictions, and even nation states in both public safety and other areas of the public sector [34]. Projects that attempt to implement interoperability become difficult and expensive and are often challenged before they are completed.

Given this analysis, interoperability remains a critical issue for public sector entities that must access information from diverse information systems and sources. To use an analogy from the private sector, 'unified communication' is needed in public safety where the entire communication of an organization is integrated with different networks, devices, and applications through a universal platform. Worldwide access to such a platform allows the decentralization of command and control structures, enables the efficient sharing of information, and quickens the flow of communication. Third parties can access this universal platform as needed; however, this analogy may not satisfy the particular requirements for public safety information systems in terms of availability in remote locations and the ability to withstand disasters. Nonetheless, it remains a valuable metaphor for what the development of emergency communications could become. In terms of interoperability, research and practice should focus primarily on semantic and organizational interoperability [49].

2.2 Information Systems, Technology and Infrastructure

Information systems for public safety (including emergency management information systems (EMIS) and emergency response information systems (ERIS)) must satisfy requirements for high standards of reliability, resiliency, security, and availability that guarantee access to sufficient capacity on a day-to-day and emergency basis. These requirements apply to networks, devices, and applications that are involved in collecting data from different sources, joining, analyzing in real-time, and distributing this information to the involved parties and to the public over the appropriate channels. The same level of requirement must be ensured for related systems, such as actuator systems that control the environment (e.g., systems that regulate the water level in reservoirs). Such systems must respond in a timely manner and provide an appropriate user interface for any given situation. Even if segments of the networks are compromised, adequate service must be continued [58]. These requirements impact the design of public safety emergency systems; [68] formulates a set of nine premises that consider these implications and that are concerned with training and simulation, information focus, crisis memory, exceptions as norms, scope and nature of the crisis, role transferability, information validity and timeliness, free exchange of information, and coordination.

Innovative technologies offer new approaches to facilitate interoperability. One such technology, wireless grids, is defined as the ad-hoc dynamic sharing of physical and virtual resources among heterogeneous devices [41]. Software for wireless grid connectivity utilizes open specifications, allowing ad-hoc, distributed resource collaboration for devices and applications on a new scale, and enabling greater interoperability across networks, devices, applications, services, and content. According to [65], a wireless grid has the capacity to solve the problems of trust, access and control over resources and thus constitutes an approach toward tackling urgent issues of information and resource sharing.

Public safety information systems are part of the overall government infrastructure that must withstand natural and man-made disasters. Government infrastructure provides robust networks that enable the exchange of structured information between networks [27]. This infrastructure provides a range of generic functionalities upon which other systems can build and which are used by a large number of users [27]. All considerations previously mentioned must be considered in planning next-generation digital government infrastructure. During the financial crisis that lasted from 2007 to 2010, significant investments in technology were enacted to stabilize tumbling national economies [22], [52]. Emergency response infrastructure, as part of the next-generation infrastructure, benefits from investment in wireless and wired broadband technology. Along these lines, the United States is planning a nationwide interoperable public safety broadband wireless network [19].

2.3 Information Sharing, Trust and Security

Increasingly, studies have begun to focus on information sharing in emergency response settings. For example, [1] investigated secure information sharing in emergency management, and others, such as [72], used rational choice and institutional theories to examine information sharing across organizational boundaries in public safety networks. In practice, though, information sharing remains a challenge. Scientific case studies (e.g., [28], [48]) and government reports (e.g., [40]) have concluded that a problem still exists with sharing information and knowledge within public sector inter-organizational networks and that coordination among public safety agencies is less than optimal, and is hindered by disparities between jurisdictions and overlapping responsibilities.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

Another barrier to information sharing is the lack of understanding on how to utilize a third-party system to which one may gain access. Without prior training, one's ability to use a foreign system to retrieve information may be limited [73], and variations in terminology or nuances in metaphors may lead to misinterpretations [39]. Consequently, access to a third-party system is of minimal use without semantic knowledge of its representation. Thus, semantic interoperability remains a critical issue [49].

As a prerequisite, trust must be established among emergency response agencies before they share information. A lack of trust may impede information sharing in a collaborative system [31]. In addition, social and personnel issues that involve security concerns may also hinder the effective processing of information across organizational borders. A public safety information system must address a difficult trade-off between security and the sharing of information in emergencies. On the one hand, there is a compelling need to cooperate and share information. On the other hand, security and privacy must also be ensured. Unauthorized access, modification and disruption must be avoided. Without guaranteeing classic information security characteristics (e.g., confidentiality, integrity and availability), information providers in an inter-organizational network will be reluctant to share. As a prerequisite for trust, control of the information flow is important; systems must be capable of monitoring and tracking the dissemination of information [51]. Otherwise, emergency agencies may be unwilling to use or adopt it [64].

2.4 Cognitive Factors

The advent of integrated information processing systems is providing public safety agencies and emergency response units with more and more information; however, information overload is a recognized problem for these individuals [67]. This has an impact on the design of such systems and the way in which filters and searching processes are applied to retrieve relevant data to make accurate decisions. There is neither time nor tolerance for non-relevant information [68].

3 Information Broker for Emergency Communications

As outlined above, the Information Age demands more effective communication between public safety agencies, emergency response units, and the public before, during and after an emergency occurs. To achieve this, information and communication systems must be able to handle data integration, data management, data analysis, data visualization, and the dissemination of information to public safety forces.

More and more, data acquisition in disaster management is tapping into networked and computerized systems, websites, and social networking platforms. More and more, the public is becoming a valuable information source of its own, passively by carrying mobile devices (e.g., movement profiles of the masses) and actively by communicating with peers and reporting to authorities (e.g., messaging). Besides coordinating disaster response and recovery, data about mass behavior has great potential for the early recognition of trends and anomalies [37].

Utilizing vast amounts of data and transforming it into valuable information for disaster management requires intelligent storing and analyzing of mass data. In the near future, emergency response units will increasingly utilize crowdsourcing – the outsourcing of tasks to the public – as their central paradigm for disaster management. Furthermore, using multiple decentralized channels adds beneficial redundancy to help overcome potential blackouts of some communication structures during disaster situations. The capability to create ad-hoc networks that incorporate voice, messaging, graphics, and video enables command and control personnel to have much richer information resources for decision making and coordination [10]. Improvisational orchestration of heterogeneous information sources – what [42] called "a structured approach to real-time mixing and matching of diverse ICTs to support individuals and organizations" – calls for emergent interoperability in emergency response activities.

In order for first responders and decision makers to receive the information they need and to communicate that information with the public, we propose the use of an information broker, which meets the requirements of a dynamic emergency response management information system (DERMIS) as introduced in [68]. Generally, a broker is defined as "the named resource that executes the business logic defined in the message flows. Applications send and receive messages to and from a broker. The broker routes each message using the rules defined in message flows and message sets, and transforms the data into the structure required by the receiving application" [54]. In [3], we introduced the notion of an 'information broker' in the context of public safety to describe a generic concept which aims for seamless communication among multiple heterogeneous groups. Ideally, in an emergency, close cooperation between humans and adaptive systems takes place, and information and knowledge are shared across organizational boundaries and physical distances. This includes both pre-existing information and run-time generated information.

The information broker consists of two components – a communication push broker and an information pull broker – which can be realized in different stages. This allows a separation between information pull, which involves integration and continued processing of information, and a communication push, which deals with bi-directional information delivery. For both, well-defined responsibilities and interfaces are prerequisites.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

3.1 Functions of the Communication Push Broker (Information Dissemination)

The communication push broker receives messages that are to be distributed and delivered through standardized interfaces. The broker monitors the communication channels, their availability, their bandwidths and further characteristics, and takes over the entire communication propagation. The broker has current and detailed information about the communication channels, including information about disturbances of these channels. In addition, the communication push broker collects information about targeted receivers of the information. It is thus able to select the appropriate communication channels based on (a) information about which channels serve the targeted receivers best and (b) which of these channels are actually available.

Seen from an abstract point of view, messages are target-independent when they are fed to a communication broker. It is then the task of the broker to translate them into target-specific messages. This is a concept well known from system software – the format of the original messages fed to the broker corresponds to device-independent formats there. The key is to translate the formats only at the periphery, where information about the receivers is available. By eliminating the necessity of a central storage for distributed information and a central planning for the distribution of information, critical resources are saved.

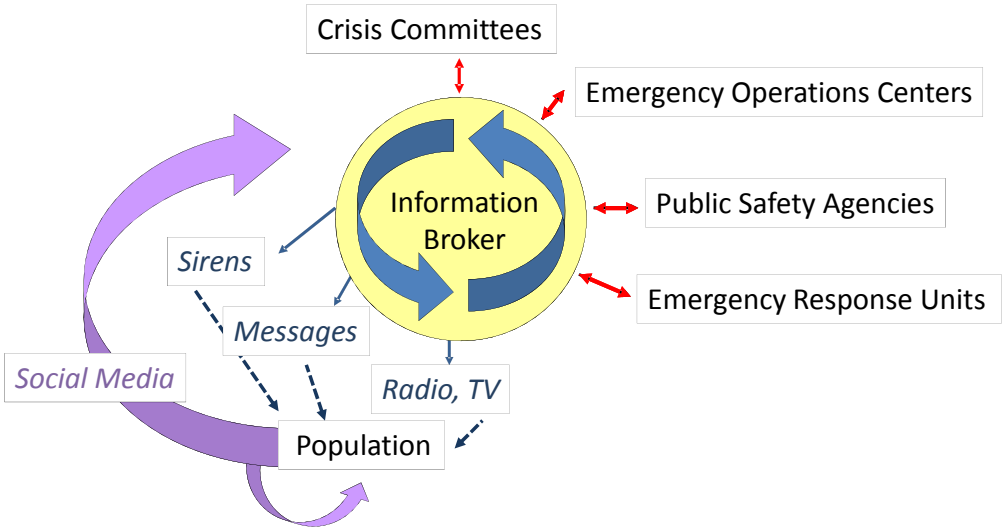

Figure 1: Conceptual representation of pull and push brokers for emergency communications

In order to select the appropriate delivery channels, it is necessary to have several conceptual models at hand for the following:

- Communication patterns (quality and method);
- Sets of receivers (characterization of the sets, identification and characterization of its members);
- Communication channels and channel performance classes; and
- Channel-to-receiver affinity (for individuals and sets of receivers).

The principal idea is to infer from the estimated actual situation (localization) of intended receivers and the estimated actual performance of channels – with respect to the situated receivers and their channel-to-receiver affinity – to the targeted set of receivers.

As the communication push broker takes charge of the dissemination of information, public safety authorities are enabled to focus on the emergency itself. The broker monitors all critical performance indicators of the communication channels, such as their availability, bandwidths and further characteristics, and takes command of all communication propagation. In an emergency, the broker has current and detailed information on the statuses of the channels and the areas in which some of the channels are affected by the event. The broker can link the availability status with the communication channels in such a way that, if a channel is unavailable, it automatically suggests alternative routes.

We identified two functions that are particular to a communication push broker:

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

- **Individualized Information:** Information can be individualized towards a targeted individual, group, or organization. First, one-to-one, one-to-many, many-to-one, and many-to-many information dissemination from sender to receiver is supported either by the information broker or associated but independent information systems (e.g., social network sites). Second, new types of information may be integrated that become available through the communication push broker (e.g., geographic location data of smart devices by mobile, platform, or application providers).

- **Bi-Directionality:** Information flow is bi-directional. First, the information broker supports communication of emergency response units across different organizations and jurisdictions. Second, the public is part of the information creation and feeds situational information back to the public authorities. Third, an individual may exchange situational information with others via social network sites (e.g., Twitter, Facebook). Bi-directionality is a key function that allows the integration of various resources and actors across multiple boundaries and thus enables crowdsourcing in an emergency.

3.2 Functions of the Information Pull Broker (Information Processing)

The information pull broker gathers and processes various forms of pre-existing information to describe regular settings, and it continuously integrates new information. Using predefined conditions, it can indicate an impending emergency to the crisis committee and generate situation reports for public safety authorities. Possible damage areas utilizing cadastral maps, risk maps, and other information (e.g., information gained from previous disasters) can be computed and used to provide decision support and preliminary warning. It also allows easy recognition of important correlations between different kinds of events. In a crisis, a comprehensive presentation of all concerned domains (e.g., electricity, water supply and transport infrastructures) is offered. As a result, correct information is available for authorities to protect a population in advance, or to provide them with assistance if a disaster occurs.

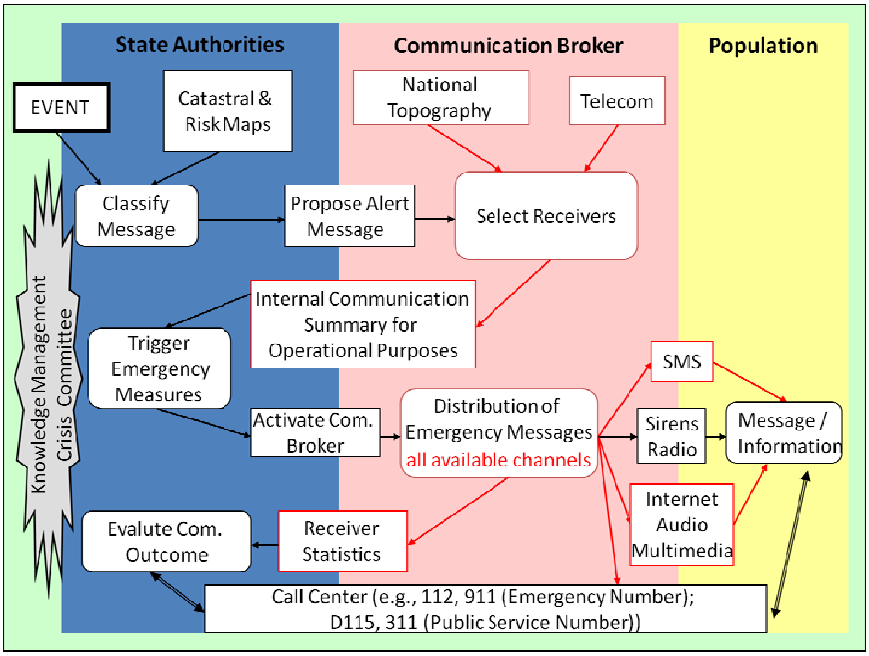

Figure 2: Communication push broker (process) [3]

The key challenge is to integrate all available information and to process it in such a way that it can be used in a straightforward manner by various receivers. The information broker thus resembles a large real-time processing system whose information pieces are not created by sensors only, but by human beings as well. As with other real-time systems, preprocessing of information at the periphery is advantageous as it helps to avoid information flooding of the central computing resources and the decision-makers.

Information may be picked up by the information pull broker in several ways: it may be directly addressed, it may be picked up from monitored information channels, it may be requested from information sources and measurement points, or it may result from observational analyses of the situation. It is then packaged into messages, which are associated a-priori observables (e.g., source, destination, content summary). Based on these observables, information pull brokers preprocess the messages, possibly creating new messages or dismissing them. Then, it assigns receiver sets and delivers the messages to the communication push broker.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

If intermediary receivers are introduced that correspond to logical entities rather than physical ones, then the information preprocessing may be divided into an internal information delivery to logical entities (performed by the communication push broker) and a simple aggregation of information at the logical delivery points. Therefore, at its heart, the information pull broker deals with the dual problems of resource allocation and information integration. The resource allocation problem is to identify message delivery points based on a-priori observables (allocation). This means that the information pull broker classifies incoming information pieces (integration). Then, based on the actual values of the classification, the messages are routed to the receivers. In order to improve the quality of this process, the routings are evaluated and the results are fed back to the process. Figure 2 provides an overview of how the communication push broker process is executed. The process consists of three steps: (1) message creation, (2) communication execution and (3) communication evaluation.

We identified four functions that are particular to an information pull broker:

- **Interdependency:** As a support to decision making, the information pull broker gathers and integrates information to provide a comprehensive view of a situation, taking into account complex interdependencies with adjacent events. This information may be used for an actual emergency as well as for prevention and warning.

- **Simulation:** Simulations may be used for preventive scenario and risk calculations, as support for real-time decision making in an emergency, and for training purposes. Instruction in the use of an emergency response information system is critical for effectiveness in an actual disaster [68].

- **Location:** In a disaster, information on geographic location is vital. Based on such information, emergency response units may deduce the whereabouts of people through aggregated information of mobile devices or observe the collective behavior of people. To use such data, cooperation with service providers is required.

- **Event Integration:** Resources and information of affiliated organizations (e.g., hospitals, schools, utilities), as defined in Section 1, need to be integrated in the information broker; this is achieved via events and event-driven processes (see Section 4). The management and integration of these events takes place in the information pull broker.

3.3 Practitioner Workshop on Alerting and Communication in Emergencies

In a stakeholder workshop in 2008 where participants included several federal departments, military, broadcast networks, meteorological services, utilities, telecommunication and transportation companies, four shortcomings were identified in the current alerting and communication system: (1) reduced capacity of emergency power stations, (2) lack of system redundancies and lack of interoperability between systems, (3) limited stress resistance of equipment during emergencies, and (4) lack of coordinated disaster preparedness planning. These concerns relate to the concept of an information broker, which was introduced for discussion as an alternative model to the existing alerting approach, as follows:

- The dependency of power supply to run the infrastructure of information brokers.

- The vulnerability of the complex communication schemes with respect to disturbances. Set up properly, though, the brokers can indeed protect communication against disturbances.

- The large computation workload of information brokers, which might result in performance issues.

- The brokers could be used routinely as a government information system. Through application in everyday life, the users would gain familiarity with the system that would become useful in the case of emergency. It was generally assumed, however, that such highly sophisticated information brokers would bear a high failure risk.

The workshop participants agreed that future action should be targeted at increasing the capacity of emergency power stations, enhancing system redundancies and safety precautions, improving disaster preparedness planning and resource management during emergencies, and introducing change management and controlling measures.

4 Events and Event-driven Processes in Emergency Response

In an emergency situation, data about events are actively or passively retrieved from machine and human sources and are received by many people and systems that are often separated by legal and organizational barriers. With an information broker architecture, these events are registered from data sources (e.g., sensor, RFID, and social networks) and are fed across an event bus to applications used by the corresponding and responsible entities or by involved citizens and organizations. The information broker detects critical events based on inferences from multiple

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

data streams, aggregates them, and publishes and distributes this information according to the needs of various stakeholder groups.

4.1 Event-driven Processes

To cope with the growing complexity of business processes [57], event-driven processes have been proposed. Event-driven architectures are commonly regarded as the "next big thing", enabling the production, detection, consumption of, and reaction to business-critical events [25]. For example, in activity-based processes, after completion of an activity, the task is routinely pushed (published) to the next step (subscriber). In an event-based process, though, the event handler (consumer) proactively acts on an event based on a real-time matching of event characteristics and consumer profiles. Hence, there is no need to draw out in detail the activities involved in completing a task which, in complex scenarios, may be impossible; however, event-based processes make it crucial to define the syntax and concepts so that real-time matching of event characteristics and event consumers can be achieved [60].

An 'event' is defined as "a significant change in state," while 'event consumers' are those entities responsible for acting on these changes [11]. Event consumers include, for example, information workers, visualization tools or automated response systems. From this perspective, a business process is "a collection of interconnected events which are purposively conceived, planned, designed, implemented, executed and controlled" [9]. In other words, the business process is viewed not primarily as a set of activities but as a set of changes in the state of an organization.

Applications based on event processing encompass software for automatically or semi-automatically filtering data and highlighting information based on emerging relationships and patterns as well as calculating inferences and visualizing trends. These immediate analytical results are made available via dynamic reports indicating possible courses of action. Involved stakeholders can highlight issues (i.e., flagging) for in-depth analysis and human attention, to comment on issues, and to interrelate diverse issues.

Examples of existing Web-based software applications are PAGER (Prompt Assessment of Global Earthquakes for Response), WAPMERR (World Agency of Planetary Monitoring and Earthquake Risk Reduction), "Did you feel it" App (which generates seismic intensity maps based on shaking and damage reports from citizens), SAHANA (which manages resources and information in disaster response, but lacks integration of external data sources), HOUDINI (which provides integration and visualization of heterogeneous data sources for disaster management based on Semantic Web technologies RDF and a push/pull approach), EEW System (Earthquake Early Warning), and SmartWeb Vehicle (mobile information system that interacts with drivers in natural language, e.g., for requesting data analysis over voice dialog systems).

4.2 Event-driven Computing Platform

The key to an efficient event-driven approach is proper computing of the consumers associated with the event. This computing of event consumers is referred to as "matching" and is a distributed process [47]. Complex event processing makes it possible to process hundreds of nearly simultaneous occurrences and to determine how to proceed in the most efficient and optimized way. It is at this intersection of human and automated activity where the event-driven approach outperforms linear activity-based processes. In this case, no linear process has been defined ex ante. Rather, event consumers act on notifications based on the unique constellation of hundreds of occurrences, and many event consumers are not human beings but rather computing agents.

On top of the matching that takes place between events and event consumers, there runs a concurrent analysis and visualization of the continuous event stream to monitor the frequency and relationships between entities and to identify patterns. In the case of extreme and unforeseen events, such as natural or technological disasters, an event-driven approach for decision-support systems can provide cognitive support for determining how to best respond and improvise in an unforeseen situation [43]. In order to deal with the information overload in decision-support systems, methods of data reduction have been used to reduce the effects of excessive data while preserving patterns and surprises in the data [53]. The nonlinear matching between events and event consumers, together with the continuous monitoring of the event stream and ad-hoc critical incidence detection and propagation, constitutes the main advantage of an event-based, as opposed to an activity-based, process.

The computing platform involves a solution stack with complex event processing and modeling capabilities for interpreting information for decision making, coordination and dissemination (e.g., filtering, modeling, simulation, visualization and evaluation in real-time). Complex event processing is distinguished from the actual solution stack comprising the operating system, middleware and databases. It involves technologies for the detection of complex events (e.g., interrelated events) in the data streams as well as the evaluation of events from the different application parts. With backward discovery, incoming events are checked against multiple event histories to detect interrelations, while forward discovery detects complex events in stages [55]. A rule and execution model is required for defining complex events and their set of responses.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

5 Interoperability in Emergency Response

Interoperability on various levels is a prerequisite for effective collaboration and communication. The interoperability levels discussed here establish multiple perspectives for a comprehensive understanding of what issues may enable or hinder interoperability in the context of emergency response.

5.1 Interoperability Framework

An interoperability framework consists of a set of rules and agreements describing how organizations should best interact with each other. It also provides policies and guidelines for how standards should be selected and used [16]. According to its scope and applicability, the interoperability framework must be adapted to a specific situation; in our case, public safety constitutes the context at hand. A comprehensive interoperability framework gives an indication of the direction in which interoperability and corresponding standards might develop in the near future.

To achieve interoperability among diverse public safety agencies, there must be consensus on the objectives of interoperability, discussed and agreed upon by the larger public safety community. Generally, such objectives address agility, availability, cost effectiveness, extensibility, flexibility, maintenance, multiple use, openness, performance, scalability, and security (e.g., [16], [32]). These objectives are often stated in the form of guidelines and principles to determine what should (and should not) be achieved with interoperability; they provide guidelines for decision making in implementations, and serve as compliance checks for post-implementation purposes [34]. Binding objectives that are in accordance with statutory and architectural provisions support the coordinated development of distributed, interoperable solutions.

5.2 Interoperability Levels

Stated objectives and guidelines alone are hardly enough to address the complex challenges that interoperability presents. A conceptual framework is needed to investigate different facets of this challenge that are not only technical and semantic, but organizational, legal and political as well. To establish interoperability, [16] considers the following five facets as levels that must be addressed:

- **Political Context** – Collaboration and cooperation across boundaries require political support. On a political level, in order for collaboration to work, the vision and goals of the involved actors must be aligned. Consequently, sufficient priority and resources must be available on an ongoing and timely basis to address the political context.

- **Legal Interoperability** – Legality is a precondition for collaboration across jurisdictional and organizational units. An alignment of diverse legislation may be required. Interoperability can be affected in numerous ways, such as differences in administrative law, intellectual property rights, privacy and data protection, public administration transparency or the re-use of public sector information. Exchanged data need to be in accordance with the law of its place of origin. Furthermore, data originated in another jurisdiction must be mutually recognized.

- **Organizational Interoperability** – To achieve collaboration on an organizational level, interoperability must address the integration of business processes and the exchange of information across organizational boundaries. This includes a broad set of elements of interaction, particularly business processes management and the design of interfaces that enable seamless interaction among different organizational units.

- **Semantic Interoperability** – On the semantic level, cooperating organizational units have to process information from their partners in a meaningful way. This requires agreement on the meaning and format of the exchanged information (e.g., agreement on data structure, data elements, protocols). Thus, sector-specific, semantic standards play an important role.

- **Technical Interoperability** – On the technical level, interoperability covers technical aspects of interconnecting systems and services to include interfaces, interconnection services, data integration, middleware, and security services.

From an analytical point of view, these five levels offer helpful insights as to "where" and "what" interoperability issues may arise as well as "which" actor may respond to them (e.g., a legally non-compliant transaction on the organizational level that needs to be addressed by a legislative function). Establishing open, non-proprietary protocols for emergency response communication and information systems would allow systems to evolve more readily and incorporate more intelligent and robust capabilities that would make them more effective.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

In [16], the interoperability framework addresses information security implicitly, as part of the technical, organizational, and legal level. An information broker may handle a variety of sensitive information that needs to be protected accordingly; thus, information security should be an explicit issue in this context. Finally, governance is an issue that addresses all levels of interoperability [17]. Governance is concerned with maintaining and improving the maturity level of interoperability. As such, governance assures that interoperability is preserved when standards are further developed. As outlined in the brief literature review above, the organizational and semantic levels constitute a primary challenge, and the following subsections focus on these issues.

5.2.1 Organizational Level

Regarding organizational interoperability, organizations involved in disaster prevention and response are only gradually beginning to work together more closely. There are organizational and technical barriers that inhibit closer cooperation. Interoperability in organizational terms means closely aligned processes and activities for operation and communication. For over half a century, the functional organization has been criticized for rigidity and inflexibility [5]. For more than 20 years now, computer-supported cooperative work (CSCW) has been available to overcome functional barriers [21]. Since information and communication technology (ICT) was designed to bypass functionally organized information and communication channels, the need for organizational redesign ensued [23]. As business processes are becoming increasingly complex and heterogeneous, organizations are undergoing a shift from functionally organized bureaucracies to networked teams across processes [56]. In contrast to traditional definitions of the business process as a set or collection of activities [14], [23], [29], we define the business process as "a collection of interconnected events which are purposively conceived, planned, designed, implemented, executed and controlled" [9]. Events are defined as "a significant change in state" [11]. Organizing around events thus builds flexibility into organizational processes. In changing environments, it becomes less important to follow a fixed set of predefined activities correctly than to respond to changes in a timely and appropriate fashion.

Strategic Direction. The first step towards organizational interoperability is the strategic intent to cooperate more closely with other organizations involved in disaster prevention and response. This strategic intent must be addressed in the political context and the legal level of the interoperability framework. A strategy requires a vision and a willingness to act. The definition of a strategy means that the development of an organization is not left to itself, but that there is willingness to lead. Effective leadership consists of creating structures, steering goal-setting and developing potentials. The process of goal formulation and implementation planning leads to awareness of the implicit goals and different perceptions among involved stakeholders. In the present context, the challenge is to align the ICT potential with (inter-)organizational processes as well as to redefine processes to exploit the full ICT potential. Success in this regard depends on how effectively the information management during the cooperation processes can be improved. Important objectives are as follows:

- Direct information access within the organization, across involved organizations and with the affected population;
- Ubiquitous digitalization of information for seamless exchange and processing of information;
- Improved data governance through elimination of uncontrolled data redundancy and increased data quality;
- Shared applications and computing resources across involved organizations;
- A workflow management system for support of information and coordination processes; and
- Process monitoring for optimization of workflows.

Interoperability on the organizational level requires two distinct strategic directions. First, there should be a strategy for ICT infrastructure aimed at optimizing the ICT infrastructure's level of technical maturity. Second, there should be a strategy for ICT exploitation aimed at optimizing the ability of ICT use. This strategy determines which concrete ICT applications are implemented and operated around the organizational capabilities of involved organizations. These two types of strategies are reciprocally interlinked. If a certain level of maturity is to be obtained in the use of ICT, then an appropriate level of maturity in the IT infrastructure is a prerequisite. The adjustment of the ICT infrastructure must, in turn, follow the strategy for ICT use.

5.2.2 Semantic Level

Semantic interoperability is closely related to organizational interoperability. Cooperation improves if a common understanding of processes and activities exists among involved organizations. Interoperability in semantic terms refers to this common understanding and to shared concepts and approaches. From a more technical perspective, semantic data enables optimized service queries, through the automatic selection and interoperation of individual services (i.e., service composition), to deliver targeted and precise information via personalized composite services. At least three building blocks can be identified – knowledge representation, data extraction, and decision support. The following section outlines some research directions within each of these three areas.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

Knowledge Representation. A common language and a shared understanding of concepts and objects are prerequisites for semantically enabling electronic information flows in the context of disaster prevention and response. Developing a common understanding is complicated by the fact that it must be coordinated across all involved stakeholders, ranging from government to emergency response units to the public [69]. The definition of a common vocabulary, therefore, constitutes just one step in this direction [59]. Based on this vocabulary and its categories, communities of interest can be organized, for example, concerning the coordination of tasks or the provision of specific emergency services. Service providers can then identify the community of interest and register their services with it, which includes mapping the generic operations defined by the community with those defined in the service [6].

The major obstacle, thus far, has been low interoperation and connectivity among various actors involved in disaster prevention and response. The cooperation plans in emergency cases were drafted at a time before today's complexity and potential for managing complexity had become evident. In addition, providing information and services requires aggregation from several different actors, thereby compromising transparency and accountability. Studies suggest that information and coordination can be improved through more accurate and flexible semantic-based search engines and query languages for interrogating standardized Internet content. In addition, information and service aggregation is enhanced through dynamic semantic linking to automatically consolidate diverse and heterogeneous sources related to a particular issue or piece of information [62].

Data Extraction. The tedious task of assigning classifications to new data can be vastly reduced through several means. First, information often already provides a number of qualified metadata. Second, text-based information can be analyzed using natural language processing techniques for extracting labeled class instances [50]. Based on logic rules, existing classifications from established vocabularies can thus be automatically assigned to text-based information passed along activities around disaster prevention and response. Third, information extraction based on machine learning and Object-Relation-Object descriptions (e.g., School <has> Fire Alerting System) are techniques to identify logical tuples in data that can be combined with a community approach to supervise the accuracy of results [71].

The fact that, in principle, metadata is extractable and analyzable offers not only great opportunities for quickly accessing information from multiple heterogeneous sources but also poses challenges concerning the protection of the privacy of involved parties. The concept of the economics of privacy is therefore a useful approach for assessing the trade-off between two goods – privacy and the quality of online services [33]. Often, issues of personal privacy are addressed from the perspective of restricting access to information; however, limiting access to data becomes increasingly difficult as it becomes easier to aggregate data from multiple information sources and to make inferences based on these aggregations [70]. The emphasis of effective privacy protection therefore shifts from restricting access to data towards enabling users to manage their own.

Decision Support. Arguably, there are clear benefits to making existing data and information actionable by aggregating it over multiple sources and by using these aggregations to make inferences to support decision making in disaster prevention and response. For example, biosurveillance utilizes health data to identify outbreaks of disease. The process typically requires daily counts of regional emergency department notifications (e.g., coughing), daily sales of relevant remedies (e.g., cough medicines at pharmacy stores), and daily counts of school absences. Combining or mashing these various data sources can pinpoint problems much earlier than waiting for each single data stream to pass a critical threshold. Data is aggregated and relationships and patterns are analyzed, ultimately leading to the conclusion that a disease is spreading. The goal is to alert public officials early and create an opportunity to combat the outbreak as promptly as possible [36].

In addition, reasoning and simulation can be used to assess decisions and compare decision alternatives. Typically, these approaches involve calculating the value function of a specific policy, based on modeling the transition and observation probabilities, and the reward functions [6]. Simulations can be used to make policy implications more tractable and to furnish stakeholders with a better grasp of decisions. The area of foresight and simulation in disaster prevention and response, therefore, provides one of the most interesting and promising applications of intelligent and semantically enriched information management.

6 General Architecture for Emergency Communications

In this section, we propose a general architecture for seamless emergency communications that integrates the aforementioned concepts: (1) information broker, (2), events and event-driven processes, and (3) interoperability. The general architecture establishes a comprehensive view that considers an end-to-end information process – from the collection or use of information to its distribution, processing and storage, and vice versa. The alignment of the various segments of this chain of information is crucial, but it is often done poorly, which may lead to fragmented local architectures and standards that are difficult to integrate.

The general architecture consists of two dimensions: (1) interoperability and (2) an information broker. The benefit of bringing together these two dimensions is the effective, bi-directional propagation of information in a distributed, heterogeneous emergency response information system with diverse actors. The proper characteristics and the

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

appropriate alignment of these two dimensions constitute the necessary preconditions that information in the form of events and event-driven processes disseminates effectively end-to-end in all directions. The two dimensions are depicted in Figure 3.

6.1 Interoperability Levels

Interoperability in the general architecture consists of five levels – technical, semantic, organizational, legal, and political – as described in Section 5. To achieve consistent interoperability, these interoperability levels must align with each other in a meaningful way. In practice, many initiatives and programs – whether they bear the notion of interoperability in their name or not – are barely or sometimes just loosely coupled to other levels of interoperability that they may affect. We do not advocate a centralized coordination of interoperability initiatives and programs, as this is barely achievable given the magnitude of political initiatives and programs that directly or indirectly state interoperability as a main objective; however, a mechanism is needed that ensures a basic alignment among the various levels of interoperability. As a point of reference, shared interoperability goals can serve the function of a simple alignment mechanism. Furthermore, the continuous monitoring of national and international interoperability initiatives helps to anticipate developments in related areas that need to be taken into account earlier or later [34]. From our observation in practice, we conclude that such mechanisms are not in place, leading to locally constrained interoperability on individual levels, instead of a consistent interoperability across all levels. This may occur when initiatives focus on separate levels of interoperability (e.g., organizational vs. semantic interoperability) with diverse objectives due to different political mandates.

6.2 Information Broker Layers

Orthogonal to the interoperability dimension in the general architecture for emergency communications is the information broker, conceptualized as a four-layered model, consisting of (1) an actor layer (sender/receiver), (2) a distribution layer (communication push broker), (3) a production layer (information pull broker), and (4) a registry layer (heterogeneous databases) –which together describe the provision of emergency response services. This model represents a slight extension of the information broker introduced in Section 3; an actor layer and a registry layer have been added to improve the conceptualization of actor-system interaction (actor layer) and data access and storage (registry layer). In this stratification, a distinction is made between the actors (request or delivery of information), the distribution (presentation and propagation of information), the production (processing of information), and the registry (access and storage of information). This separation distinguishes between the responsibilities of different roles, as the various layers may fall into distinct local and national powers. However, the concept of roles is not elaborated here. For an extended discussion of the concept of roles in emergency response, see [68].

The **actor layer** describes actors that may be human (first responders, emergency response units, public safety agencies, command and control centers, experts, companies) or non-human (sensors, smart devices) and may be part of trained emergency response units (police agencies, fire departments) or not (volunteer aid workers, concerned or affected public). All of these actors receive events based on specific needs for their local operation and decision making and/or send events to the information broker to inform other actors. Depending on the degree of involvement, an actor is either fully responsible, partially involved, or only informed in the processing of information. Large numbers of events are concurrently delivered to, or received from, the **distribution layer** (communication push broker) that covers the presentation of the information, filter logic, and routing information. In the distribution layer, decisions are made about preferences and availability of communication channels; this layer simulates a uniform access to emergency information for the actors in the emergency operation. All the collected events are then continuously processed in the **production layer** (information pull broker), to make analyses, inferences, and visualizations (e.g., anticipated environmental development of the damage area) to be sent to actors and/or to update registries. The **registry layer** describes public or private heterogeneous, distributed databases (e.g., public registries on citizens, residence information, health information, geographic information, weather information) that, in order to be effective, must be integrated with the production layer. Triggers, neural networks, and data mining produce events based on the information in the registry layer that lead to automated processing in the production layer. The events go back and forth in the four layers of the information broker and may skip one or more layers while these events are disseminating throughout the system (e.g., an event of a sensor that is directly connected to a registry). As a side note, to illustrate the collaboration between two actors – in particular, organizations – the layers may be symmetrically mirrored at the actor layer, which then would serve as an interface.

6.3 General Architecture

Bringing the two dimensions together, the general architecture constitutes a grid of 5 (interoperability levels) x 4 (information broker layers) fields. Thus, in total, the grid offers 20 fields – one at each intersection of the two dimensions – that constitute an individual perspective on architectural and operational issues. Since a discussion of the 20 individual perspectives is beyond the scope of this article, three perspectives will be discussed as examples. In practice, however, some of these perspectives may melt together horizontally or vertically and thus constitute broadened perspectives.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

[Distribution *x* Political Context]: The distribution of events in an emergency response information system requires an infrastructure that enables communication between the actors and the information processing units. The channels that provide this kind of communication must satisfy particular requirements for an emergency context and are subject to technological change and deterioration. This, among others, makes the distribution of events costly and requires a strong political will to establish such infrastructure as a prerequisite for interoperability. In practice, the political will is often nourished by bottom-up demand. For instance, after 9/11, the demand for an interoperable emergency response communication infrastructure grew massively. The political context was set according to these events. Evidence for this political will are plans for a 4G Wireless Public Safety Network in the United States that, depending on its deployment, may cost between USD 6.5 to 15.7 billion over a 10-year span [19]. Further evidences of such political will are the consideration of Next-Generation 911 (NG 911) networks and emergency alert systems and the establishment of the Emergency Response Interoperability Center (ERIC) [19]. Once the political context is set for interoperability, it is expected to affect the legal level of interoperability. Evidence for this are proposed bills and laws, such as the ICOM Act (federal funding for interoperable communications programs), the SAVE LIVES Act (program for public safety communications potentially funded by frequency spectrum sales) or the Public Safety Interoperability Implementation Act in the United States.

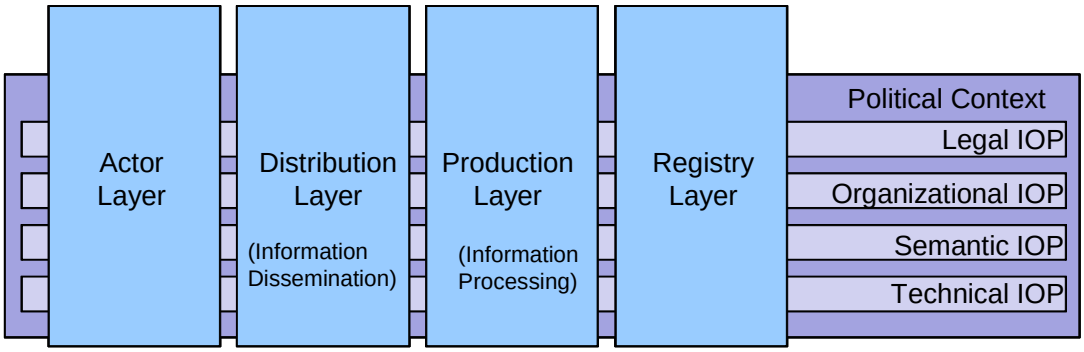

Figure 3: General architecture for emergency communications

[Actor *x* Legal Interoperability]: In the field, emergency response units can access personal and medical information on their mobile devices to facilitate decisions about treatment for injured individuals. Access to this information is regulated by law and may constitute an obstacle for emergency response units in administering care. There are examples where legal regimes prevent appropriate medical actions (e.g., in cases where children are affected and their parents are unavailable to provide consent for medical treatment). Accordingly, a legal basis is required to enable first responders to act and to access necessary information [61]. However, as regulations are often compartmentalized, it is necessary to review dependent elements in other layers, as when legal interoperability of the same information must be met for the distribution layer ("Is it allowed to disseminate this information on this particular communication channel?"), the production layer ("Is it allowed to process this information and to share it across organizational and/or jurisdictional boundaries?"), and the registry layer, where the medical information is stored and the ownership, access, and format is determined ("Is it allowed to access this information for this particular purpose?"). This example shows that, in order to enable effective event propagation, legal interoperability must be met across all four layers of the information broker.

[Production *x* Organizational and Semantic Interoperability]: In order to establish effective information processing for data analysis, integration and visualization, various public safety agencies need to share information across organizational and jurisdictional boundaries. This requires organizational and semantic interoperability that would enable business processes to cross organizational boundaries and establish a shared understanding of meaning and format of the processed information. For example, end-to-end security (ingrained in the organizational as well as in the technical level) must be assured when information is processed across multiple public agencies on different federal levels (e.g., local, state, federal). The integrated information across different domains (e.g., fire departments, police agencies, medical services) is a particular challenge that is addressed – among others – by the Emergency Response Interoperability Center (ERIC) (operational procedures), Semantic Interoperability Centre Europe (SEMIC.EU) (semantic data model, XML schema for public administration and e-government), Organization for the Advancement of Structured Information Standards (OASIS), Common Alerting Protocol (CAP), Emergency Data Exchange Language - Distribution Element (EDXL-DE), Emergency Data Exchange Language - Resource Messaging (EDXL-RM), and Emergency Data Exchange Language - Hospital Availability Exchange (EDXL-HAVE) and is subject matter for several governmental agencies equivalent to the Federal Emergency Management Agency (FEMA) and the Department of Homeland Security (DHS) in the United States.

Overall, the proposed general architecture identifies distinct areas where interoperability issues and corresponding standardization issues may arise. In [34], such areas are covered with bundles of standards that constitute an 'interoperability element'. These interoperability elements describe a generic function that can be used abstractly in various emergency settings. In practice, these elements cover one or more levels and layers in the general architecture; identified gaps indicate a potential need for further interoperability elements, but not necessarily standards.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

6.4 Reflections: Implementation, Crowdsourcing and Coordination

There exist a number of interoperability frameworks that address particular areas, such as national interoperability in the public sector (e.g., SAGA in Germany [32], eGIF in the United Kingdom [15], FEAF in the United States [12]), interoperability among different nations and their institutions (e.g., EIF in the European Union [16], NAF in the NATO [45]), national response (e.g., National Response Framework in the U.S. [20]), and requirements for national interoperability in emergency response (e.g., in the U.S. [13]). Our proposed general architecture for emergency communications must not be seen as independent but rather as complementary to these interoperability frameworks. In concrete implementation, the general architecture may draw from other frameworks: (1) adapt architectural viewpoints (enterprise, information, computation, engineering, technology) of the reference model of open distributed processing (RM-ODP) [32], [26]; (2) review elicited requirements (e.g., compare with [13], [68]); (3) incorporate standards that are established in this context (e.g., from [32] or the W3C Emergency Information Interoperability Framework Incubator Group); and (4) incorporate concepts for roles and responsibilities (e.g., from [20], [68]). In summary, the general architecture for emergency communications provides a model to implement an information broker; likewise, related frameworks may be brought in for a specific instantiation.

The conceptual approach by which the information broker integrates crowdsourcing in emergency communications holistically – from actors (which constitute the crowd) to the distribution of messages, the processing of information, and the integration of registries, and back – is novel. The general architecture introduced here advocates an ad-hoc and open communication system where everyone – whether professional or private – can participate meaningfully according to their group affiliation (as defined in Section 1). As such, those who participate – the crowd – are not assigned in advance with specific roles or access rights, which is the case in most distributed emergency management information systems (see also the design principles in [68]). Connectivity to the crowd is conceptualized by the actor layer. Related literature that examines the use of mobile devices, social media, and social networking sites in the context of disasters and emergency response is growing. [46] provided a vision for the use of technology in disasters to encourage the involvement of the public as a powerful, self-organizing, and collectively intelligent force. Others have examined the use of social media, such as Twitter [63] and Wikis [2], in recent catastrophes. The information broker expands upon these works and illustrates how the proposed system could be connected to other emergency management information systems in use. However, with the concept of crowdsourcing in emergency response, new challenging issues arise that are beyond the scope of the information broker. An open communication system is used by both professional and volunteer safety workers (group 1 and 2), but also by untrained people (group 3) who find themselves caught up in the disaster. Thus, the question arises as to how the interaction of these different groups is to be designed after the public has been empowered to participate in emergency communications. Furthermore, there is a need for a mechanism to ensure information quality and reliability, in order to validate the collected information for decision making. With the new empowerment of the public and the abundance of information, these two questions become central to achieving an effective and efficient outcome in emergency response.

Coordination is the crucial underlying problem in emergency response [68]. Coordination theory [38] provides insight into what enables multiple actors to coordinate ad-hoc in a dynamic environment. Crises possess the characteristics of such an environment, and [68] proposes that technology (e.g., wireless grid technologies [65]) will address the coordination problem and enable people to self-organize accordingly. The information broker as such does affect the coordination problem in two ways: (1) directly, crowdsourcing is enabled through bi-directionality and open communication; and (2) indirectly, since the alignment of interoperability levels and information broker layers in the general architecture is a prerequisite to enabling different actors in an emergency to form groups ad-hoc and dynamically.

7 Conclusion and Outlook

Existing emergency management information systems lack the capacity to share vital information and resources. Thus, they hinder the coordination of emergency response units to save lives and prevent further damage in a crisis; opportunities are missed for innovation that would make public safety more effective. The organizational and technological fragmentation comes at high cost. In practice, this loose patchwork of technologies and solutions is a real concern for public safety managers; no one wants to buy into a solution that may or may not continue to rise as an accepted standard. The need to integrate technologies and to coordinate further development among public safety stakeholders has been recognized in various initiatives, such as the Partnership for Public Warning in the United States and the Public Safety Communication Europe Forum. We believe that, in order to satisfy this need, mechanisms must be created to promote interoperability of networks, devices and applications, across organizational and jurisdictional boundaries. Therefore, there must be funding and research initiatives that explore solutions in this field.

Based on our case studies, workshops with public safety agencies, and a literature review, we propose a general architecture for emergency communications to include three district concepts: (1) an information broker for information dissemination and processing, (2) events and event-driven processes to address complexity in the end-to-end information flow holistically, and (3) interoperability in public safety. The general architecture for emergency communications is, overall, in alignment with the premises and design principles for an emergency management

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

information system as stated in [68]. However, an open communication system that enables bi-directionality and empowers the public to participate via crowdsourcing needs to examine the first and second premises of [68]. Premise 1, in order to be used effectively in a crisis, requires training and simulation for an emergency management information system. Such training is an integral part of the overall instruction for public safety forces; however, how might the general public be prepared to use such a system in the case of an emergency? A simple and intuitive design of the system's human-computer interface may be one approach [13]. Others argue that an effective inclusion of the public at large during an emergency is contingent upon the existence of groups or communities prior to a disaster's occurrence. Premise 2 requires that information for decision making be presented with specificity to the crisis at hand. The information broker may provide a rich, comprehensive view of events; but, if filter mechanisms are not applied effectively, it may also lead to information overload. The premises and design principles in [68] address relevant further issues of training, roles, and accountability that are not covered in the general architecture but must be addressed in a concrete implementation.

We see the conceptual inclusion of crowdsourcing via the information broker as a contribution to the emergency management information system literature, particularly because it addresses elements of the coordination dilemma, but at the same time raises new questions about the reliability, quality and volume of such information once the public has been empowered to participate. The concept of information broker and crowdsourcing in emergency response still needs to be tested in practice. Furthermore, the proposed general architecture may be used as a reflective tool (e.g., for comparative studies on public safety interoperability), or as a framework in practice to identify future fields of action (e.g., standardization).

Emerging technologies will enable new dimensions of information processing and their use in emergency communications. Within the next two or three years, it is estimated that more individuals will be connected to the Internet via mobile devices than by traditional personal computers. These technologies will cause a disruptive transformation and affect the entire public safety lifecycle, including emergency prevention, precaution response, and damage control and recovery. Integrating these technologies comprehensively while maintaining interoperability will present an even greater challenge than it does today. The call for close collaboration and civic participation in emergency response will only become more pressing.

References

[1] N. R. Adam, V. Atluri, S. A. Chun, J. Ellenberger, B. Shafiq, J. Vaidya, and H. Xiong, Secure information sharing and analysis for effective emergency management, in Proceedings of the 2008 International Conference on Digital Government Research, Montreal, Canada, 2008, pp. 407-408.
[2] D. Bedford and L. Faust, Role of Online Communities in Recent Responses to Disasters: Tsunami, China, Katrina, and Haiti. Panel at the ASIS&T 2010 with I. Bakri, T. Wang, Y. Qu, D. Yates, E. Pryor. Pittsburgh, PA, October 2010.
[3] Bern University of Applied Sciences, InfoBev Krisen, Report to the Federal Chancellery, Bern, Switzerland, 2008.
[4] N. Bharosa, J. Lee, M. Janssen, and H.R. Rao, A case study of information flows in multi-agency emergency response exercises, in Proceedings of the 10th Annual International Conference on Digital Government Research: Social Networks: Making Connections between Citizens, Data and Government, Digital Government Society of North America, 2009, pp. 277-282.
[5] P. M. Blau and W. R. Scott, Formal Organizations: A comparative approach. San Francisco CA: Chandler, 1962.
[6] A. Bouguettaya, D. Gracanin, Q. Yu, X. Zhang, X. Liu, and Z. Malik, Ubiquitous Web Services for E-Government Social Services, presented at the 2006 AAAI Spring Symposium Series, Stanford, CA, March 27-29, 2006.
[7] D. G. Boyd, Testimony of David G. Boyd, Ph.D., Director Command, Control and Interoperability Division Science and Technology Directorate, Department of Homeland Security before the U.S. House of Representatives Committee on Science and Technology, Subcommittee on Technology and Innovation. Washington, D.C.: Government Printing Office, 2010.
[8] P. Bulman, Communicating Across State and County Lines: The Piedmont Regional Voice over Internet Protocol Project | National Institute of Justice, NIJ Journal NCJ 224087, no. 261, 2008.
[9] F. Butera, Design and Strategic Management of Networked Enterprises and Network Enterprises, presented at the CEFRIO Conference, Montréal, May, 21-22, 1994.
[10] L. Carver and M. Turoff, Human-computer Interaction: The human and computer as a team in emergency management information systems, Commun. ACM, vol. 50, pp. 33-38, 2007.
[11] M.K. Chandy, Event-Driven Applications: Costs, Benefits and Design Approaches, presented at the Gartner Application Integration and Web Services Summit, San Diego, CA, 2006.
[12] Chief Information Office Council, Federal Enterprise Architecture Framework (version 1.1), United States, September 1999.
[13] Commercialization Office, National Emergency Response Interoperability Framework and Resilient Communication System of Systems, Department of Homeland Security, February 2009.
[14] T.H. Davenport, Process Innovation: Reengineering Work Through Information Technology, Harvard Business Press, 1993.
[15] e-Government Unit, e-Government Interoperability Framework (version 6.1), Cabinet Office, United Kingdom, March 2005.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

[16] European Communities, European Interoperability Framework, 2nd ed. (draft), European Commission, Brussels, Belgium, Document for Public Consultation, 2008.
[17] European Public Administration Network eGovernment Working Group, Key Principles of an Interoperability Architecture, 2004.
[18] M. M. Fard, J. Pineau, and P. Sun, A variance analysis for POMDP policy evaluation, in Proceedings of the 23rd National Conference on Artificial Intelligence – vol. 2, Chicago, Illinois: AAAI Press, pp. 1056-1061, 2008.
[19] Federal Communications Commission, Connecting America: The National Broadband Plan, Washington, D.C., U.S., Governmental Report, 2010.
[20] Federal Emergency Management Agency, National Response Framework, NRF Resource Center, 2008.
[21] J. Grudin, Why CSCW Applications Fail: Problems in the design and evaluation of organizational interfaces, in Proceedings of the 1988 ACM Conference on Computer-supported Cooperative Work, Portland, Oregon, United States: ACM, pp. 85-93, 1988.
[22] D. Guellec and S. Wunsch-Vincent, Policy Responses to the Economic Crisis: Investing in Innovation for Long-Term Growth, OECD, Directorate for Science, Technology and Industry, 2009.
[23] M. Hammer and J. Champy, Reengineering the Corporation: A manifesto for business revolution, Harper Business, 1992.
[24] A. R. Hevner, S. T. March, J. Park, and S. Ram, Design Science in Information Systems Research, MIS Quarterly, vol. 28, no. 1, pp. 75-105, 2004.
[25] M. Ibrahim and O. Etzion, Workshop on Event-driven Architecture, Companion to the 21st ACM SIGPLAN Symposium on Object-oriented Programming Systems Languages, and Applications, Portland, Oregon: ACM, p. 624, 2006.
[26] ISO/IEC 10746-3: Information Technology – Open Distributed Processing – Reference Model: Architecture, Geneva, 1996.
[27] M. Janssen, S. A. Chun, and J. R. Gil-Garcia, Building the next generation of digital government infrastructures, Government Information Quarterly, vol. 26, pp. 233-237, 2009.
[28] F. Jing and Z. Pengzhu, A case study of G2G information sharing in the Chinese context, in Proceedings of the 8th Annual International Conference on Digital Government Research: Bridging Disciplines & Domains, Philadelphia, Pennsylvania: Digital Government Society of North America, pp. 234-235, 2007.
[29] H. J. Johansson, Business Process Reengineering: Breakpoint strategies for market dominance, Wiley, 1993.
[30] JRSA, Information Sharing Systems: A Survey of Law Enforcement, Survey Report, Justice Research and Statistics Association, Washington, D.C., July 31, 2006.
[31] M.V. Karahannas and M. Jones, Interorganizational systems and trust in strategic alliances, in Proceedings of the 20th International Conference on Information Systems, Charlotte, North Carolina, United States: Association for Information Systems, pp. 346-357, 1999.
[32] KBSt, Standards and Architectures for e-Government Applications (version 4.0), Federal Ministry of the Interior, Germany, March 2008.
[33] A. Krause and E. Horvitz, A utility-theoretic approach to privacy and personalization, in Proceedings of the 23rd National Conference on Artificial Intelligence – vol. 2, Chicago, Illinois: AAAI Press, pp. 1181-1188, 2008.
[34] A. Kuehn, A. Spichiger, and R. Riedl, Interoperabilität und Standards im E-Government, in Proceedings of the 12th Int. Rechtsinformatik Symposions, Vienna, Austrian Computer Society Press, 2009.
[35] A. Kuehn and A. Spichiger, eCH Interoperabilitätsansatz: Vergleichsstudie 2008, Federal Strategy Unit for IT, unpublished study, 2009.
[36] T. H. Lotze and G. Shmueli, Ensemble forecasting for disease outbreak detection, in Proceedings of the 23rd National Conference on Artificial Intelligence – vol. 3, Chicago, Illinois: AAAI Press, pp. 1470-1471, 2008.
[37] R. Magoulas and B. Lorica, Big Data: Technologies and Techniques for Large-Scale Data, Release 2.0, vol. 11, 2009.
[38] T.W. Malone and K. Crowston, The interdisciplinary study of coordination. Computing Surveys, vol. 26, no. 1, 1994, pp.87-119.
[39] B. Manoj and A. H. Baker, Communication challenges in emergency response, Commun. ACM, vol. 50, pp. 51-53, 2007.
[40] R. McFee, The DHS National Biosurveillance Integration Center – Ready or Not, Opening September 30th, Family Security Matters, 2008.
[41] L. W. McKnight, J. Howison, and S. Bradner: Wireless Grids – Distributed Resource Sharing by Mobile, Nomadic, and Fixed Devices, IEEE Internet Computing, vol. 8, pp. 24-31, 2004.
[42] D. Mendonça, T. Jefferson, and J. Harrald, Collaborative adhocracies and mix-and-match technologies in emergency management, Commun. ACM, vol. 50, pp. 44-49, 2007.
[43] D. Mendonça, Decision support for improvisation in response to extreme events: Learning from the response to the 2001 World Trade Center Attack, Decis. Support Syst., vol. 43, pp. 952-967, 2007.
[44] L. K. Moore, Public Safety Communications: Policy, Proposals, Legislation and Progress. CRS Report for Congress. Library of Congress, 2005.
[45] NATO C3 Board, NATO Architecture Frameworks (version 3), NATO, November 2007.
[46] L. Palen, K. M. Anderson, G. Mark, J. Martin, D. Sicker, M. Palmer, and D. Grunwald, A Vision for Technology-Mediated Support for Public Participation & Assistance in Mass Emergencies & Disasters, in Proceedings of ACM-BCS Visions of Computer Science, 2010.
[47] S. Pallickara and G. Fox, On the Matching of Events in Distributed Brokering Systems, in Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC '04) – vol. 2, IEEE Computer Society, pp. 68-76, 2004.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 1 / APRIL 2011 / 43-60

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000100005

[48] T. A. Pardo, A. M. Cresswell, F. Thompson, and J. Zhang, Knowledge sharing in cross-boundary information system development in the public sector, Inf. Technol. and Management, vol. 7, pp. 293-313, 2006.
[49] J. Park and S. Ram, Information Systems Interoperability: What lies beneath?, ACM Trans. Inf. Syst., vol. 22, pp. 595-632, 2004.
[50] M. Pasca, Turning Web text and search queries into factual knowledge: Hierarchical class attribute extraction, in Proceedings of the 23rd National Conference on Artificial Intelligence – vol. 2, Chicago, Illinois: AAAI Press, pp. 1225-1230, 2008.
[51] D.A. Powner, Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks, Washington, D.C.: GAO-08-607, June 26, 2008.
[52] S. Roberts, The Impact of the Crisis on ICTs and their Role in the Recovery, OECD, Directorate for Science, Technology and Industry, 2009.
[53] S. Russell, A. Gangopadhyay, and V. Yoon, Assisting decision making in the event-driven enterprise using wavelets, Decision Support Systems, vol. 46, pp. 14-28, 2008.
[54] C. Sadtler, B. Crabtree, D. Cotignola, and P. Michel, Patterns: Broker Interactions for Intra- and Inter-enterprise. IBM International Technical Support Organization, Redbooks, 2004.
[55] M. Schaaf, A. Koschel, S. Gatziu Grivasy, and I. Astrova, An Active DBMS Style Activity Service for Cloud Environments, in Proceedings of the Intl. Conf. Cloud Computing 2010, IARIA, Portugal, Nov. 2010.
[56] T. Schael, Workflow management systems for process organisations, Springer, 1998.
[57] A.-W. Scheer, O. Thomas, and O. Adam, Process Modeling Using Event-Driven Process Chains, in Process-aware information systems: bridging people and software through process technology (M. Dumas, W.V.D. Aalst, and A.T. Hofstede Eds.). John Wiley and Sons, 2005.
[58] B. L. Schooley, Inter-organizational systems analysis to improve time-critical public services: The case of mobile emergency medical services, dissertation, School of Information Systems & Technology, Claremont Graduate University, Claremont, CA, 2007.
[59] N. Shadbolt, T. Berners-Lee, and W. Hall, The Semantic Web Revisited, IEEE Intelligent Systems, vol. 21, pp. 96-101, 2006.
[60] G. Sharon and O. Etzion, Event-processing network model and implementation, IBM Syst. J., vol. 47, pp. 321-334, 2008.
[61] D.C. Sicker, L. Palen, D. Grunwald, K. Anderson, L. Blumensaadt, Policy Issues Facing the Use of Social Network Information During Times of Crisis, presented at the 38th Research Conference on Communication, Information and Internet Policy, Washington, D.C., October 2010.
[62] T. Sidoroff and E. Hyvönen, Semantic E-government Portals – A Case Study, presented at the ISWC Workshop on Semantic Web Case Studies and Best Practices for eBusiness SWCASE05, Galway, Ireland, 2005.
[63] K. Starbird and L. Palen, Pass It On?: Retweeting in Mass Emergency, in Proceedings of the 7th International ISCRAM Conference, Seattle, WA, May 2010.
[64] K. Tierney and J. Sutton, Cost and Culture: Barriers to the adoption of technology in emergency management. RESCUE Research Highlights, June 2005.
[65] J. Treglia, L.W. McKnight, A. Kuehn, and A. Ramnarine-Rieks, Interoperability by 'Edgeware': Wireless Grids for Emergency Response, unpublished document, 2010.
[66] J. V. Treglia and J. S. Park, Towards trusted intelligence information sharing, in Proceedings of the ACM SIGKDD Workshop on Cyber Security and Intelligence Informatics (CSI-KDD '09), New York, NY, 2009.
[67] M. Turoff, Past and future emergency response information systems, Commun. ACM, vol. 45, pp. 29-32, 2002.
[68] M. Turoff, M. Chumer, B. D. Walle, and X. Yao, The Design of a Dynamic Emergency Response Management Information System (DERMIS), Journal of Information Technology Theory and Application (JITTA), vol. 5, Jan. 2004.
[69] C. Wagner, K. S. Cheung, R. K. Ip, and S. Bottcher, Building Semantic Webs for e-government with Wiki technology, Electronic Government, an International Journal, vol. 3, pp. 36-55, 2006.
[70] D. J. Weitzner, H. Abelson, T. Berners-Lee, C. P. Hanson, J. Hendler, L. Kagal, D. L. McGuinness, G. J. Sussman, and K. Krasnow Waterman, Transparent Accountable Data Mining: New Strategies for Privacy Protection, in Proceedings of AAAI Spring Symposium on The Semantic Web meets eGovernment. AAAI Press, Stanford University, Stanford, CA, March, 2006.
[71] D. S. Weld, F. Wu, E. Adar, S. Amershi, J. Fogarty, R. Hoffmann, K. Patel, and M. Skinner, Intelligence in Wikipedia, in Proceedings of the 23rd National Conference on Artificial Intelligence – vol. 3, Chicago, Illinois: AAAI Press, pp. 1609-1614, 2008.
[72] C. B. Williams, M. Dias, J. Fedorowicz, D. Jacobson, S. Vilvovsky, S. Sawyer, and M. Tyworth, The formation of inter-organizational information sharing networks in public safety: Cartographic insights on rational choice and institutional explanations, Info. Pol., vol. 14, pp. 13-29, 2009.
[73] H. Zimmermann, Availability of technologies versus capabilities of users, in Proceedings of the 3rd International ISCRAM Conference, Newark, NJ, May 2006.