3B2v8.07f XML:ver:5.0.1 5/12/06 08:08 HIS – V002 : 2014 Prod.Type: pp.329–353(col.fig.:NIL) ED:Sharan PAGN:BMP SCAN:

Chen, Santanam, Ramesh, Vinze & Zeng, Eds., *Handbooks in Information Systems, Vol. 2*

Chapter 14

Government Agency Interoperation in Security Applications

Nabil R. Adam, Aabhas V. Paliwal and Vijay Atluri
RUTGERS University, CIMIC, Ackerson Hall, Newark, NJ 07102, USA

Soon Ae Chun
City University of New York, Staten Island, NY 10314, USA

Jim Cooper and John Paczkowski
Operations and Emergency Management, Port Authority of New York and New Jersey, USA

Christof Bornhövd, Ike Nassi, Joachim Schaper and John Ellenberger
SAP Labs, LLC, Palo Alto Research Center, 3475 Deer Creek Road, Palo Alto, CA 94304, USA

Abstract

Incident management for homeland security requires the accurate up-to-date situational awareness for rapid engagement of first responders at state and local levels. Major challenges for agile and effective responses include: (1) identifying and visualizing the right type of information that is relevant to the incident to see the coherent picture of the incident, (2) identifying resources to handle the incidents, including agencies, specialists, other personal and resources specific to a given alert type (e.g., fire, hazmat spills), (3) disseminating appropriate information and tasks to the right level of responders and to the public in an appropriate format to their available devices. We present a semantic incident management framework which uses a common incident ontology that captures the concepts of different incident types and their relationships among different incidents. The concepts are tied to the information resources such as textual description of incidents, audio and video clips from the incident scene. This framework allows: (1) dynamic composition of customized information, relevant resources, reports, and models based on the nature and location of the alert; (2) automated manifestation of the modality and format of the information based on the recipient's role and device, and (3) automated composition of alert components and models through Semantic Web and Semantic Web Services (SWS). The composition and dissemination adheres to the National Incident Management System (NIMS) and the National Response Plan (NRP) protocols and has been implemented using the Common Alerting Protocol (CAP) and the Ontology Web Language for Services (OWL-S).

1 Introduction

Government agencies need to form an ad hoc global virtual organization and collaborate in order to handle homeland security-related incident management. This virtual security team consists of people from executive level, management level, and responder level from different organizations that are geographically and functionally distributed. The executive people may include political and government leaders, agency and organization administrators and department heads, incident commanders for either a specific area and single incident or multi-agency coordination. The management level personnel often includes unit leaders, technical specialists, strike team and task force leaders, single resource leaders, and field supervisors. Finally, the responder level emergency response providers and disaster workers include emergency medical service personnel, firefighters, medical personnel, police officers, public health personnel, public works/utility personnel, and others.

This team-oriented virtual "agency" needs to make accurate decisions in a timely manner for an effective incident management to reduce the severity and damage. Decision on facilities may include the selection of facilities and sites for command post, evacuation, casualty collection sites, and transportation sites (e.g., heliports). Decisions on the resources usually rely on resource needs and available resources in the incident areas and the resource capacities of local agencies that are specified in the emergency operations procedures. The incident management also needs to consider current incident situations, objectives, hazard types, and hazard severities. These decision-making tasks related to homeland security are highly decentralized given the apparent diversity of agencies and information sources. A key challenge for the virtual government entity for effective decision-making for rapid responses to threats to homeland security is to consider data from diverse sources in different formats. Effective assimilation, exchange, and dissemination of information are vital for homeland security wherein it is important for agencies to communicate in a way where information can be fused and exchanged in a more efficient manner.

Second, command and control of incident management is based on incident commander's situational observations, the situational reports by different agencies, or the incoming data from sensors, if any. The data volume from various sources can be overwhelming and the interpretation of data and information needs to be done efficiently. Thus, another challenge is a rapid analysis and interpretation of voluminous real-time data from different sources. In order to achieve this, the data from different sources needs to be shared, fused, and analyzed as it becomes relevant without a prior data-sharing agreement among different agencies.

Finally, the decisions made may call for some actions (tasks) by various team members. The proper tasks, agencies (representative person) that can accomplish the tasks, and the information needed for tasks have to be identified and disseminated to each agency. Putting the information and tasks together manually jeopardizes the timely response to an incident. Thus, there should be an automated way to identify and compose tasks and to disseminate these tasks and relevant information to be executed by different team members.

Therefore, information interoperation in homeland security application is required to support complex decision-making process that involves multi-agencies (horizontal coordination) that may encompass several jurisdictions, multi-layer (vertical coordination) that may involve the executive team, objectives, special forces team, resources, and services within an agency. In order for each individual agency to work toward the common goal of stabilizing the incident and protect life, property and the environment, it needs to have the right type of information and services at their hands. To illustrate these challenges, consider the following scenario of an incident.

> Scenario: *At 9:30 am, it was reported that a truck carrying a chemical substance on route to NY Lincoln tunnel is missing. At 10:01 am, a truck accident on highway was reported and an unknown chemical spill was reported. A hazmat team needed to be brought in. At 10:17 am, the chemical spill is identified as toxic chlorine and immediate area residents needed to be alerted for evacuation. The police department needed risk assessment information and how the wind may carry the chemical to identify immediate risk areas, evacuation facilities, and hospitals. Also, volunteer information is needed.*

As seen in this scenario, the incident management has the following characteristics:

- The incident characterization is continuous and dynamic as more information is available throughout the management of the incident.
- As the situations change constantly, the information needs and resource requirements are changing as well. The agency and participants to handle the incident change as time progresses, and the resource requirements also change as the situation of the incident develops.

- There should be an efficient dissemination of incident messages that include incident-related information, services, and tasks.
- The devices of responders may be diverse and heterogeneous. Thus, the incident information and services need to be portable and sharable.

The key to achieving success and breakthroughs in homeland security lies in effective team communication, resourceful knowledge management, consistent coordination of team processes, and timely dissemination of relevant information; all ensured within a structured collaborative decision environment.

In this paper, a collaborative framework for information interoperation is proposed as a critical provider of a distributed information and decision-making backbone for homeland security. We identify data mining based information filtering as the first key step for effective decision-making. The objective here is to filter the vast information base so that relevant and important situational awareness information is accessible quickly to key decision makers. Most of the current filtering systems provide minimal means to classify documents and data. A common criticism of these systems is their extreme focus on information storage, and their failure to capture the underlying metadata. As a consequence, our proposed approach employs an ontology framework, which allows specifying domain-level context that enables users to attach rich domain-specific semantic information and additional annotations to situational awareness information and services and to employ the meta-information for effective response analysis and execution.

Second, our approach uses Semantic Web Services (SWS) to achieve complex tasks to automate the discovery of the necessary information services (tasks) and compose these services for a particular incident situation in accordance with the national, regional, or local incident management protocols (policies). The final step involves disseminating appropriate information and tasks to the right level of responders and to the public in an appropriate format to their available devices.

This chapter is organized as follows. Section 2 provides the overview of current incident management efforts. Section 3 describes an overall framework of our approach and its components. Section 4 presents our semantic incident management approach using incident ontology and how it is utilized for semantic filtering of information and the identification of Web Services. It shows the SWS and how these are automatically discovered and composed to achieve desired functionalities to added value services. Section 5 presents the dissemination of the information and services customized to fit to the agency and responder's roles, and devices. Section 6 addresses the prototype implementation followed by the description of our conclusion and on-going and future work in Section 7.

2 Incident management

An Incident of National Significance (INS) is "an actual or potential high-impact event that requires robust coordination of the federal response in order to save lives and minimize damage, and provide the basis for long-term community and economic recovery" (NRP, 2004). According to Homeland Security Presidential Directive-5 (HSPD-5) issued by President Bush in 2003, the Secretary of Homeland Security is directed to develop and administer a National Incident Management System (NIMS) to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. NIMS serves as a single, consistent nationwide template to enable all government, private sector, and non-governmental organizations to work together during domestic incidents (NIMS, 2004).

Six major components of the NIMS are:

1. Command and management that defines standard incident command systems, multi-agency coordination systems, and public information system. These standard incident command structures define the operating characteristics, interactive management components, and structure of incident management and emergency response organizations, and processes for communicating timely and accurate information to the public during crisis or emergency situations.
2. Preparedness that involves an integrated combination of planning, training, exercises, personnel qualification and certification standards, equipment acquisition and certification standards, and publication management processes and activities.
3. Resource management that defines standardized mechanisms and establishes requirements for processes to describe, inventory, mobilize, dispatch, track, and recover resources over the life cycle of an incident.
4. Communications and information management that identifies the requirement for a standardized framework for communications, information management (collection, analysis, and dissemination), and information-sharing at all levels of incident management.
5. Supporting technologies that include voice and data communications systems, information management systems (i.e., record keeping and resource tracking), and data display systems. Also included are specialized technologies that facilitate ongoing operations and incident management activities in situations that call for unique technology-based capabilities.
6. Ongoing management and maintenance component that establishes an activity to provide strategic direction for and oversight of the NIMS, supporting both routine review and the continuous refinement of the system and its components over the long term.

HSPD-5 requires all federal departments and agencies to adopt the NIMS and to use it in their individual domestic incident management and emergency prevention, preparedness, response, recovery, and mitigation programs and activities, as well as in support of all actions taken to assist state, local, or tribal entities. The directive also requires federal departments and agencies to make adoption of the NIMS by state and local organizations a condition for federal preparedness assistance (through grants, contracts, and other activities) beginning in FY 2005. The participation and integration of all state, territorial, and community-based organizations, including public, non-governmental, and private organizations, such as private sector emergency medical and hospital providers, transportation systems, utilities, and special facilities such as industrial plants, nuclear power plants, factories, military facilities, stadiums, and arenas. Full NIMS implementation is a dynamic and multi-year phase-in process with important linkages to the National Response Plan (NRP), the HSPD-8 (i.e., the "National Preparedness Goal"), and the National Infrastructure Protection Plan (NIPP).

The NIMS provides a comprehensive national framework to incident management by representing a core set of doctrine, concepts, principles, terminology, and organizational processes to enable effective, efficient, and collaborative incident management at all levels. On the other hand, the NRP is an operational incident management or resource allocation plan. The NRP specifies how the resources of the federal government will work in concert with state, local, and tribal governments and the private sector to respond to Incidents of National Significance. It specifies various centers and officers in charge of incident management, e.g., joint field office, joint information center, federal coordinating officer, resource officer, and defines supporting resources such as transportation, communication infrastructure as well as interact with the state, county, and local Emergency Operations Centers and Incident Command Post that provides tactical level incident management operations.

The NRP

1. Describes the structure and processes comprising a national approach to domestic incident management designed to integrate the efforts and resources of federal, state, local, tribal, private sector, and non-governmental organizations. It includes planning assumptions, roles and responsibilities, concept of operations, incident management actions, and plan maintenance instructions.
2. Provides detailed supporting information, including terms, definitions, acronyms, authorities, and a compendium of national interagency plans.
3. Details the missions, policies, structures, and responsibilities of federal agencies for coordinating resource and programmatic support to states, tribes, and other federal agencies or other jurisdictions and entities during Incidents of National Significance.
4. Provides guidance and describes the functional processes and admin-

istrative requirements necessary to ensure efficient and effective implementation of NRP incident management objectives.

In order to have a successful implementation of these national directives, guidelines, and operational procedures, the information technology can be utilized to enhance incident management capabilities for different levels of incident responders from different organizations.

The high-quality, accurate, and timely information affects the quality of decisions and more effective incident management tasks. The information technology research in incident management focuses on gathering, processing, managing, using, and disseminating information as well as training incident-related personals.

The 2002 National Research council recommended development of a threat-based 3-D simulation models and visualization tools for Emergency Operation Center training. To achieve this, a network of consortium called Homeland Defense Center Network was formed to develop reusable and standard-based simulation and modeling tools that can be easily shared and integrated to another systems, and to support federal, state, and local response teams, including decision makers and first responders (Corley and Lejerskar, 2003; NIST, 2003). These tools include graphical display of the unfolding of the simulated disaster event and response actions for decision makers to increase the situation awareness, and to make high-level decisions such as deploying and coordinating multi-organizational units of first responders in different areas impacted by the disaster. The first responder training tools include immersive virtual reality, stereo displays, 3-D sound, hand and tracking control to make the disaster responders to feel the disaster zone.

These simulation tools are used not only for training of emergency management teams but also for planning such as location of police, fire, and hospital facilities, defining evacuation procedures and designing communication infrastructure. These are also used to assess vulnerabilities in action plans and strategies such as city emergency plans. The simulation tools are also useful for determining the likelihood of disaster event and identifying potential targets, and for real-time situation updates to project current and future impact of the incidents. The simulation-based incident training and management research areas within the HDC organizations include urban assessment, surveillance, sensor simulation, critical infrastructure, firefighting, and HAZMAT dispersal predictions. Similar 3-D visualization and human-interaction reasoning with artificial intelligence tool (DEFACTO) is developed for training the incident commanders to gain the experience and evaluate tactics in real disaster incidents (Schurr et al., 2005).

Crisis management utilizes the geospatial data that can be located on a map. GIS is a useful tool in all aspects of emergency management from planning to mitigation to response by combining hazards data with other geospatial data. For example, GIS facilitates planning the mitigation and response needs, and identifying and assessing the real and potential damage levels on lives, property, and environment from potential disasters. GIS can provide real-time monitoring for emergency tasks and early warnings, and it can identify resource selection and routing for quick responses for crisis management (Johnson, 2000). A series of research work in Rauschert et al. (2002), Fuhrmann et al. (2003), and Cai et al. (2004) recognize the limitation of the current GIS technologies to support group collaboration as required by the crisis management and propose GeoCollaborative Crisis Management (GCCM) where the maps play a role as visual mediator of communication and collaboration among distributed team players. This group collaborative GIS allows the natural, multi-modal (i.e., two or more combined user input modes such as speech, gesture, gaze, or body movements), multi-user dialog-enabled interfaces using large screen displays. The geo-collaborative crisis management is based on a distributed multi-agent system that captures the mental states of participants and reasons about the role of maps in order to determine its contents, presentation format, and sharing requirements.

An interdisciplinary RESCUE project (RESCUE, 2004, 2005) assumes humans as sensors collecting data from the incident scenes, in addition of other device driven sensors. Four major research areas to enhance the ability of emergency response focus on information collection, information analysis, information sharing, and information dissemination. Research areas in information collection include speech recognition and event extraction from voice signals, video analysis to track multiple people and recognition of license plates, sensing technologies including remote sensing and bridge sensing, robust networking systems to support information gathering in unpredictable situations, adaptable data collection including cell phone sensors and cellular-based location tracking, privacy protecting data collection.

Topics in information analysis cover information and event extractions from text, video, and multi-modal speech, event awareness such as event database systems or event reasoning, spatial awareness to locate the events from reports, people awareness such as vehicle tracking and peoples location, decision support tools such as loss estimation, emergency vehicle routing and Bayesian analysis of informant reports, etc.

In information sharing area, research goal is to share the information across different organizational boundaries with trust building and controlled access to preserve privacy. Thus, topics include network analysis of the incident command system, trust management in crisis network such as trust negotiation schemes, storing and managing credentials in a mobile environment, encryption of sensitive credentials for limiting access, security, and privacy management such as secure XML publishing or secure processing of queries, distributed peer-based data sharing in crisis-response organizations using overlay networks, peer-based sharing and searching, GIS-based search, etc. Information dissemination areas includes research topics such as establishing responder networks and data sets by analyzing communications among responders in disaster scenes, modeling information flow through networks, customizable dissemination, navigation support for users with disabilities, targeted dissemination, flash dissemination of critical information to a large number of recipients in a very short period time, audio-cued location-based orientation and maintenance to safe paths, etc.

While RESCUE project is comprehensive in terms of research topic areas, the focus is to improve the situation awareness of the first responders by collecting and analyzing communication data from the first responders, and providing distributed network infrastructure. It does not address important issue of filtering data for incident commanders to identify the real threats from superfluous ones. The incoming sensor data, either from surveillance devices or humans, should be integrated and direct the command officers for a set of information and response tasks. To this end, our approach focuses on the semantics of data to identify real threats, identify tasks and resources for composite tasks as SWS to manage the incidents. Like other dissemination research projects mentioned, our approach focuses on location-, device-, security credential-aware customization of information.

3 Our approach and architecture

With the support of technology, we provide a framework for semantic incident management in homeland security applications to support the automatic data and information filtering, identification of relevant information and resources, dissemination of customized information to the needs of agencies and responders. This provides the responding virtual government team with the right information relevant to the incident type and location, adhering to communication and other collaborative protocols among participating agencies as well as adhering to the individual agencies business policies. Challenges in developing this framework include: (1) identifying the right type of information that is relevant to the incident and visualize them to see the coherent picture of the incident, (2) identifying resources to handle the incidents, including agencies, specialists, other personal and resources specific to a given alert type (e.g., fire, hazmat spills), (3) disseminating appropriate information and tasks to the right level of responders and to the public in an appropriate format to their available devices. Our approach achieves automatic filtering of alert information and data using an incident knowledge base represented as an semantic graph (ontology). The semantic graph captures the concepts of different incident types and their relationships among different incidents. The information resources such as textual description of incidents, audio and video clips from the incident scene are tied to the concepts. Our approach for semantic incident

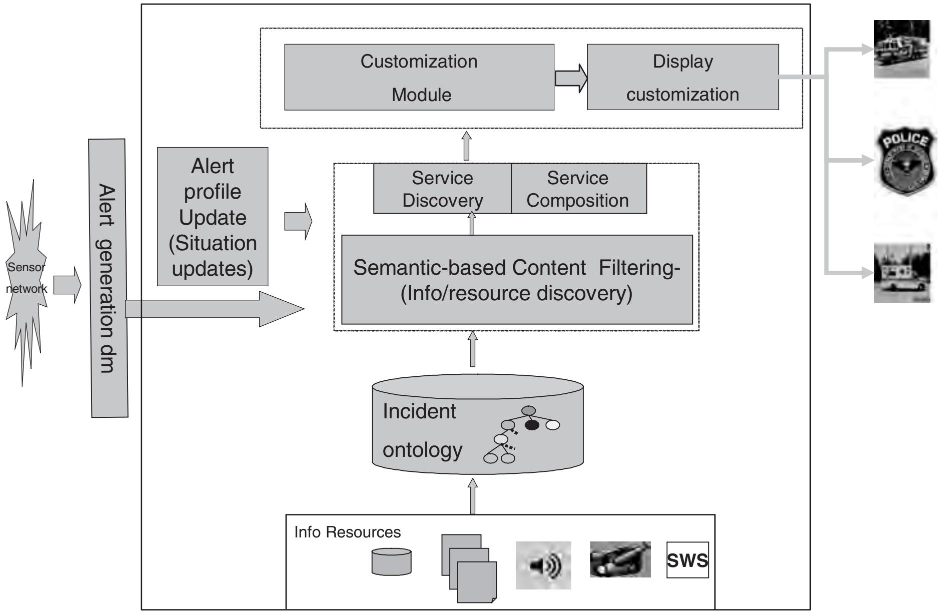

Fig. 1. Semantic incident management for homeland security.

management is to construct a knowledge base (ontology and relational knowledge base) and to utilize it to automatically identify the relevant incident management multi-media component information and services related to an incident type. The knowledge base is constructed based on each agency's Emergency Operations Plan (EOP). Figure 1 shows the overall framework and its components. A brief description of the components is given below.

3.1 Alert profile update and alert generation data mining

These two modules capture the incident/alert profile from the situation reports or by automatic data mining components from the data in the sensor network (Adam et al., 2005). Alert profiles include alert types, location, severity, casualties, etc. (Janeja et al., 2005a).

3.2 Semantic-based content filtering

The necessary resources, services, and information for handling the incident are automatically discovered. This module uses a knowledge base of incident ontology (concepts, types) and incident relationships (incident RDF/semantic graphs) to discover resources (Sheth et al., 2002). Each of the resources is described using concepts and relationships defined in the ontology. For instance, the semantic description of the resources takes into account the type of incidents (fire, radiological, or chemical, etc.), severity, and human casualty levels. Individual agencies are also considered as resources, and they are described with the concepts from the incident ontology. Thus, the types of the incidents may determine which agencies need to be involved and which resources are required.

3.3 Service discovery and service composition

Some of the information resources are not static, for instance, the map of coordinate (x, y) needs to be generated using a map generation software. Thus the map generation Web services are described as a part of information resource. In order to plan an evacuation, a host of information is required. First the evacuation plan should identify a hazardous material spreading modeling tool to assess where may be most severely affected, and a map of potential evacuation sites and hospitals are needed around the incident site (Chandrasekaran et al., 2002). Thus decision on the evacuation plan may require a complex set of information and service resources composed together, e.g., hazard spread modeling with wind directions from the weather forecasting service. Then the plan will require determining the number of volunteers based on the size of the evacuation. This requires the volunteer lookup service. The SWS and Service Composition modules are to discover available services and compose them for complex information needs. These services are also described in terms of the incident ontology to be discovered automatically via semantic concepts (McIlraith et al., 2001; McIlraith and Martin, 2003).

3.4 Customization

The alert information and services discovered from the semantic filtering stage now can be disseminated to each agency and group of responders. However, not all the semantically related incident information is needed for every agency. The fire department and medical organization's information needs are different and a particular responder's role may further restrict information based on the need-to-know access authorization, thus further role-based filtering is conducted to customize the alert-related information for each agency and responder.

3.5 Display customization

This module determines the device-specific content filtering and spatial and temporal display preferences and constraints are considered to provide the customized display of alert/incident information. A PDA display and a PC display may contain similar information, but the PDA may not be able to play video and only text or audio can be selected while a PC may display the audio, video, and text components. The spatial arrangement and temporal synchronization of information from different sources are to be considered.

4 Incident ontology

An ontology can be understood as a graph whose nodes and edges represent concepts and the relationships between those concepts. Ontologies are used for the conceptualization of the application domain in a human understandable and machine-readable form (Gómez-Pérezet al., 2003). We have developed an incident ontology to represent different incident types as shown in Fig. 2. National Research Council (NRC, 2002) identified nine critical areas of terrorism-related threat and incident areas: nuclear and radiological incidents; human and agricultural health threats; incidents on toxic chemicals and explosive materials; information technology and telecommunication attacks; incidents on energy systems; incidents on transportation systems; threats on cities and fixed infrastructure; human response-related incidents; and complex and independent systems incidents.

Similarly, we have organized incidents with several situational types, such as accidents, natural disaster types, or hazardous materials. Each of these subtypes has finer incident types. For instance, the hazardous material-related incidents can be radiological, chemical, or biological incidents. These hierarchical type and subtype incidents are related via "is–a" rela-

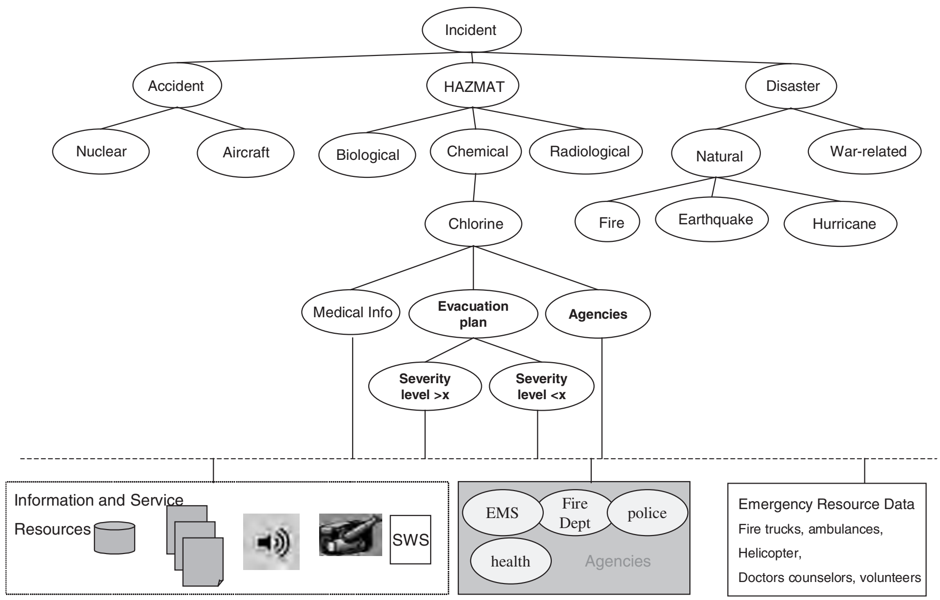

Fig. 2. Incident ontology.

tionships (Kokla and Kavouras, 2001). The information resources (database, Web pages, audios, videos) and Web services as well as IM resources (agencies, equipment, facilities) are described using these semantic incident concepts from the ontology showing its relevance to an incident/alert type. These incident concepts augment the NIMS National Incident Management Resource Typing Protocol (NIMS)] where resources (personnel, teams, facilities, supplies, and major items of equipment) are described by common category, kind, components, metrics, and type data in order to avoid confusion in crisis management.

4.1 Semantic filtering for incident information discovery

Our approach to identify and discover relevant information and resources uses semantic filtering. Alert/incident profiles (alert type, location, severity, etc.) are generated from either situation reports or a sensor alert generation module (Janeja et al., 2005b). They are specified in CAP (Common Alerting Protocol) compliant format. An alert profile is matched against the concepts in the ontology using either exact match or approximate matching techniques. Then the resources that are described with the same semantic labels or the subcategories of the concept label are searched, and put into the candidate information pool. For example, the chlorine spill incidents may require medical information on chlorine effects on health. The following step involves looking for medical information described with chlorine health effects. The resources may be either in textual, audio, or visual format. The agencies to treat the chlorine hazards can be discovered. The evacuation plan depends on the severity levels. There are different resource requirements for different levels of severity. The severity level is also specified in the resources. These will be discovered. Equipment and facilities to manage the spill are also described. Thus the semantic labels can be used for identifying these.

Our approach allows the incident-specific information and resources to be discovered in ad hoc manner dynamically as needed, rather than in a predefined and static manner, providing more flexible incident information discovery and management. This information can be optionally composed into complex multi-media objects. Similarly, services also need to be automatically discovered and composed to provide required functionalities. This is discussed in the following sub-section.

4.2 Semantic web services and web service composition

In incident management, often not only information and resources but also services (e.g., to support the adequate response to an incident) are needed. These services can be made available via the Web, thus called Web Services (Harris et al., 2003). Using the incident ontology, we describe the semantics of the Web Services to achieve their automated discovery

(Kulvatunyou and Ivezic, 2002). We call such services SWS. Unlike other information, SWS can be described not only regarding their semantics (behavior) but also their operational (syntactic) characteristics such as input, output or service bindings (Sollazzo et al., 2002). We use WSDL and OWL-S [OWL-S 1.0 Release] to describe properties and capabilities of SWS which support the automated discovery and Composition of Web Services. Using the Process Ontology, for parts of the OWL-S specifications, Web Services are considered to provide simple or complex actions with pre-conditions and effects. To provide information rich resources that form a part of the overall alert, we consider both simple services that are independent, self-reliant services implementing the task functionality and composite services that are a combination of services providing the task functionality. We discover relevant simple Web Services using concepts from our Incident ontology. For composite Web services, we use Semantic Web Service Composition and selection based on service pre-conditions and post-effects.

4.2.1 Semantic web service composition

WS Composition involves the process of selecting, combining, and executing WS to achieve the purpose of a user request (Wu et al., 2003). This involves match making of constraints between Web Service inputs, outputs, preconditions, and effects (IOPEs) along with the outputs and effects (OEs) of a user request. In addition to matching IOPEs, the automated WS Composition problem also can involve the selection from alternative Web Services that match the IOPE constraints of the composition problem (Martin et al., 2004).

In our approach, we first require an OWL-S description of that service that more fully represents the inputs and outputs of the service, i.e., constructing a composite process model that links the various operations provided by the Web Service into semantically meaningful message patterns, e.g., checking responder identification before displaying traffic details (Chun et al., 2005). We make use of capability matching as described in (Martin et al., 2004) that compares the capabilities provided by any of the advertised services in UDDI with those needed by the requester. The goal is to find the service provider that produces the results required for the requester. In general, it is unrealistic to expect that the capabilities offered by a service will exactly match the request. For example, the request may be for traffic information based on location, and the task of the matching engine is to decide whether it can be accomplished by a service that accepts zip codes (Martin et al., 2004; Akkiraju et al., 2003). Our matchmaking algorithm determines how likely it is that each capability advertisement indicates that the service will accomplish the particular function specified in the request.

The matchmaking algorithm initially maps the composite Web Service operations to a set of specialized UDDI TModels that store the corresponding OWL-S information. Next, each calling operation of the composite service is mapped to one or more operations of the existing service.

The algorithm looks for the composite Web Services description so that the purpose and category are compatible with that of the available services. Then the algorithm verifies that interacting services are binding composable.

For example, Web services for a chemical HAZMAT incident related to chlorine may include Traffic Status and Plume Modeling. A typical scenario would be of a responder, at the executive level or at the site of the incident, using the associated services for better decision-making. The responder would feed in the environment parameters to the chosen services to obtain specific information. For example, the executive responder may want to view the traffic conditions for the site including the surrounding areas (based on the address in terms of the city and state) whereas the on-site responder may want to view the traffic status at a specific geo-coordinate. One of the (pre) conditions for the TrafficStatus operation of TC is validLocation and service constraints are the access control privileges accorded to the user to view generateTrafficReport. Preconditions are logical formula that need to be satisfied by a service requestor prior to the execution of the service, e.g., check for the validity of responder identification to view the details of the requested information. Effects are logical formula that state what will be true on the successful execution of the service, e.g., displayTrafficEventTag, for the retrieval of a related traffic event. OWL-S effects are the side effects of the execution of the service (Martin et al., 2004).

The following steps describe the mapping of the submitTrafficArea operation of the TrafficStatus service according to our matchmaking algorithm (Paliwal et al., 2004).

- Map the composite Web Service operations to a set of specialized UDDI TModels that store the corresponding OWL-S information of the Traffic Service.
- Identify the component services (e.g., Traffic Service) supporting the SOAP protocol so that submitTrafficArea's purpose and category are compatible with the service purpose and category.
- Determine operations of the Traffic Service that are composable with submitTrafficArea. Since submitTrafficArea is a solicit-response type of operation it shall map to a corresponding request–response operation getLocationInfo.
- Test the operations for message composability. The input of submitTrafficArea is compared with the output of getLocationInfo. All of getLocationInfo output's parameters are mapped to the corresponding parameters of submitTrafficArea's. Since we can determine such a mapping, the two operations are message composable.
- Insert a "plug-in" between the operations in the layout, since both operations are syntactically and semantically composable.
- Perform iterations for all other service operations required by the composite service.

5 Customization and dissemination

For alert message filtering and delivery, especially in an emergency situation, we have to consider the inter-organizational relationships across entities such as responding agencies. Some information distributed along with the alert is situation-specific while other information is agency-specific. The alerts should be disseminated based on the recipient's different credentials on the agency level as well as the hierarchical level within the same agency. For example, the information required by the police department is different from the information required by the fire department; in addition the information required by the chief of the fire department is different from the information needed by a fireman.

The customization module receives the alert information from the semantic filtering and service composition module. It then starts filtering the alert based on (1) the recipients' role and (2) the recipients' devices and preferences. The role filtering of the alert is to select the relevant components to the related agencies as well as the role of the recipient's role in each agency.

After selecting the related components for each agency, we adapt the components' spatial layout and rendering format based on the recipient's devices characteristics (e.g., monitor size, Operating System), and the recipient's preferences (e.g., audio format instead of text) (Atluri et al., 2003).

For the underlying protocol in the customization module, we adhere to the NIMS and the NRP protocols. NIMS has been developed and administered by the Department of Homeland Security to provide a consistent nationwide template to enable all government, private sector, and non-governmental organizations to work together during domestic incidents. The NRP focuses on prevention, preparedness, response, and recovery within the life cycle of an incident by establishing incident monitoring and reporting protocols. One way to allow different agency's information systems to communicate is CAP. CAP is an XML non-proprietary data interchange format that can simultaneously transmit emergency alerts through different communication networks. The Organization for the Advancement of Structured Information Standards, an international standards body, has adopted CAP as a standard. Once the policy for manifesting the alerts is determined, the alert format is presented using CAP that provides a digital message format for all types of alerts and notifications (Common Alerting Protocol v 1.0, 2003).

CAP defines the alert message structure which includes four main segments. (1) The <alert> segment, which provides the message identifier, purpose, source, and status. It may contain one or more segments. (2) The <info> segments which describe the urgency, severity, certainty, actions to be taken, and related parameters of an anticipated or actual event. Each <info> segment may include one or more resource segments. (3) The <resource> segment provides a reference to additional information such as video, image, text, or audio file and one or more area segments. (4) The <area> segment describes one or more geographic areas related to the <info> segment.

5.1 Role filtering

The role filtering of the alert message is based on the jurisdiction policies, agency policies, and the role policies. Based on the NIMS and NRP, certain protocols need to be followed in an emergency scenario. A jurisdiction policy determines which agencies should coordinate the emergency management based on the alert magnitude and area. An agency policy determines the access to certain components based on the access rights of the agency. It is used to identify which information resources should be accessed from an alert message by which individual. A role policy determines which resources to be accessed based on the role within an agency.

5.2 Personal preference and device filtering

Based on the individual accessing the alert, we start our second stage filtering to best convey the alert to the recipient. In this filtering stage, instead of creating separate style sheets to layout the XML information for each role in each agency based on each device, and individual preference, we automatically select the components modalities that match the recipients' device characteristics and then reconstruct the layout of the alert accordingly (Gomaa et al., 2005).

6 Prototype implementation

We have developed a prototype based on our semantic incident management framework for Emergency Management Office of New York and New Jersey Port Authority with multi-media contents and interfaces that includes maps with basic location information and other thematic layers (e.g., available evacuation facilities), video feeds from the incident site, video-conference interface for communication with various partner agencies in incident management, status of situation report, etc. The multimedia information gives a comprehensive view of the incident situation and interaction interface. Figure 3 shows the alert/incident information view where a truck with radiological material is missing on route to the normal course described in the bill of lading. Continuous situation reports come in and are summarized in the form of text headlines (in the lower left corner), a map and a video feed from the highway with suspicious truck (upper-right corner) are displayed, and a set of Web services to assess the risk model (lower-right side) are shown with links. The video-conference interface is shown as well (upper-right corner).

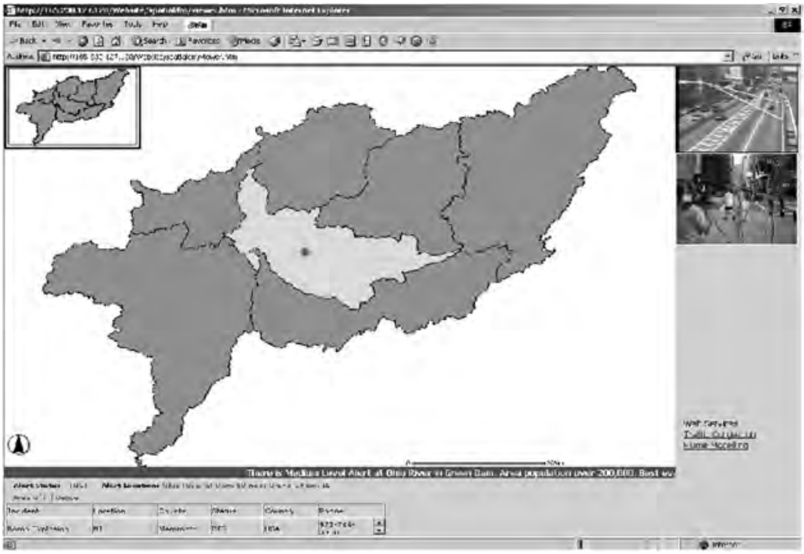

Fig. 3. Multi-media incident/alert information presentation.

Alert messages from situation reports and information components (such as video feeds) identified from the semantic filtering are encapsulated in CAP compliant XML format. The use of XML facilitates the portability and sharing of information among different agencies and responders. XML messages are customized according to the roles and policies, user device properties as well as user preferences. We implement the role filtering by using jurisdiction, agency, and role policies.

On user access, the system retrieves the user role, preferences, and used device properties (Gomaa et al., 2005). The prototype then selects the relevant formats for the alert components. It then decides the spatio-temporal layout of the alert components to finally send the alert to the user based on his role, device, and preferences. For the customized view implementation we use a web interface using Java Servlets. The alert is associated with location coordinates to be presented on a map in a GIS interface, along with the information to be presented to all the relative agencies. When a member of a related agency logs in to the system, he receives the alert related to his department. The received alert is associated with a generated XSL style sheet based on the alert and the receiving device. The general alert is represented as shown in Fig. 4. It is then customized for each agency so that only relevant information is displayed. Figure 5 shows the customized XML for a specific agency.

The adjustment of the layout changes according to the receiving device. For example, Fig. 6 shows the view for a normal PC monitor and Fig. 7 shows the corresponding view on a PDA. We detect the monitor resolution and send it to our server to apply the changes to the layout.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <alert>
   <identifier>43b080713727</identifier>
   <sender>ems@dhs.gov</sender>
   <sent>2005-01-02T14:39:01-05:00</sent>
   <status>Actual</status>
   <msgType>Alert</msgType>
   <scope>Restricted</scope>
 - <info>
     <category>Security</category>
     <event>Homeland Security Advisory System Upda
     <urgency>Immediate</urgency>
     <severity>Severe</severity>
     <certainty>Likely</certainty>
     <senderName>U.S. Government, Department of Ho
     <headline>Sensor genreated alerts</headline>
     <description>sensor generated alert indicates a te
     <instruction>A High Condition is declared when the
       previous Threat Conditions, Federal department
       their existing plans.</instruction>
     <web>http://www.dhs.gov/dhspublic/display?th
     <parameter>HSAS=ORANGE</parameter>
   - <fireresource>
       <fireresourceDesc>Plume Modelling service</firer
       <fireuri>http://cimic.rutgers.edu/~vandy/plum
       <fireuri>http://cimic.rutgers.edu/~ahgomaa/vi
       <fireuri>http://cimic.rutgers.edu/~ahgomaa/vi
     </fireresource>
   - <policeresource>
       <policeresourceDesc>Traffic Congestion service</
       <policeuri>http://www.buckeyetraffic.org/otis/
       <policeuri>http://www.buckeyetraffic.org/otis/
       <policeuri>http://www.buckeyetraffic.org/otis/
     </policeresource>
   - <healthresource>
       <healthresourceDesc>Traffic Congestion service<
       <healthuri>http://www.buckeyetraffic.org/otis/
       <healthresourceDesc>Plume Modelling service</h
       <healthuri>http://cimic.rutgers.edu/~vandy/pl
     </healthresource>
```


Fig. 4. Alert with all related agencies.

Web services discovery and composition are implemented with WSDL and OWL-S based on SAP's NetWeaver and Auto-ID Infrastructure (AII) (Bornhövd et al., 2004).

7 Conclusion

In this chapter, we have presented an approach for semantic incident management for homeland security that supports the provisioning of incident-related information, resources and service discovery, composition, customization, and dissemination. We have presented incident/alert ontology to capture the semantics and situations of the different incidents and threats including those for homeland security. Ontology concepts are used

```
<?xml version="1.0" encoding="UTF-8" ?>
- <alert>
    <identifier>43b080713727</identifier>
    <sender>ems@dhs.gov</sender>
    <sent>2005-01-02T14:39:01-05:00</sent>
    <status>Actual</status>
    <msgType>Alert</msgType>
    <scope>Restricted</scope>
  - <info>
      <category>Security</category>
      <event>Homeland Security Advisory System Update</event>
      <urgency>Immediate</urgency>
      <severity>Severe</severity>
      <certainty>Likely</certainty>
      <senderName>U.S. Government, Department of Homeland Security</senderName>
      <headline>Sensor genreated alerts</headline>
      <description>sensor generated alert indicates a terrorism attack </description>
      <instruction>A High Condition is declared when there is a high risk of terrorist attacks
        previous Threat Conditions, Federal departments and agencies should consider age
        their existing plans.</instruction>
      <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
      <parameter>HSAS=ORANGE</parameter>
    - <healthresource>
        <healthresourceDesc category="private">Traffic Congestion service</healthresourceD
        <healthun category="private">http://www.hqmc.usmc.mil/health.nsf</healthun>
      </healthresource>
    - <area>
        <areaDesc>Ohio River at Dam 53 near Grand Chain, IL</areaDesc>
        <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,- 12
        <geocode>fips6=006109</geocode>
        <geocode>fips6=006009</geocode>
        <geocode>fips6=006003</geocode>
      </area>
    </info>
  </alert>
```


Fig. 5. Customized alert for one agency.

to describe information and service resources. The incident management-related resources and information are discovered through a semantic filtering process where the alert profile information is used to match the semantic descriptions of the information and services. Web services are also described with concepts from the incident ontology and are discovered similarly. The added functionalities can be achieved through Web Service Composition. The discovered information and services are further customized according to the roles and preferences of responders and agencies. Then the dissemination and display of information is customized according to the device and display preferences such as spatial and temporal layout

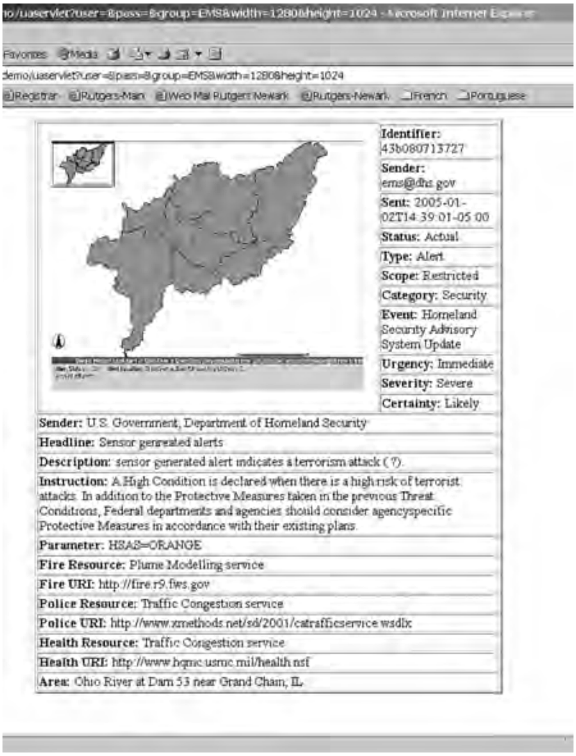

Fig. 6. PC monitor view.

constraints. Our prototype system is implemented in the domain of NJ–NY Port Authority Emergency Management Office where the situation reports are used to capture the alert profiles in an XML-based CAP format. Information and service discovery and composition is implemented using SAP's NetWeaver platform, and customization and dissemination are implemented for various devices, like Laptops, PCs, and PDAs. We are in the process of developing comprehensive incident ontology and we are planning to incorporate the consideration of dynamic situations in the incident information and process management. From the recent experiences, incident management requires quantum transformation.

To achieve this, quantum or rapid advances in information technologies is necessary. Data gathering from static surveillance devices are changing to data streaming from ad hoc networks of devices and humans that move around. The key research challenges include to measure the quality and relevance of the heterogeneous data coming from a particular situation and context, interpret, process, and construct the emergency situation in rapid manner to be useful in decision-making and response task execution. The manual textual interface to access data is changing to multi-modal inter-

Fig. 7. PDA view.

face. The combined speech, gesture, and visual interface will be a normal rather than an exception. We foresee IT advances in the intuitive multimodal data access and interface. Another critical area to advance is ‘‘flexible’’ information protection and controlled access. The ad hoc coalition of multi-agency and multi-organization incident management network generates temporary roles to play. The information access needs to be determined according to not only the roles, but also contexts, including time, location of incidents, and time and location of the responders. The accountability of temporary roles in dynamic incident management still needs to be investigated. The protection of sensitive data and privacy protection of data access are critical. The dynamic data fusion is required rather than static one for seamless access to data. To this end, the service-oriented approach has potential as seen in our approach. The mobile collaborative tools have to be devised. The incident management opens up these opportunities and many other challenges for emerging technology areas.

8 Questions for discussions

1. Discuss the major characteristics and differences between incident management for man-made such as 9/11 terrorist attacks and natural disasters such as Tsunami incidents or Hurricane Katrina. What are some of available information technology tools to prevent and prepare for these incidents, and what are the challenges facing information technology research?
2. Illustrate an example of resource identification process in a multi-agency incident management, and that of a single/local agency incident management. Discuss the differences and commonalities.
3. The incident management involves dynamic "coalition" of multiple organizations ranging from federal, state, and local agencies to non-governmental organizations, depending on the needs and the jurisdictions involved in the incident. Discuss the NIMS specifications on the different roles for incident command, how the chain of commands are established, and what conflicts may arise?
4. Discuss available evaluation criteria and schemes to measure effectiveness of incident management.
5. Often incident management requires decision-making with real-time data streaming from sensor data including human (responders as well as observers). Discuss the challenges that the current decision-making technologies may face. Specifically, discuss the issues of data quality and available tools and approaches to identify and prioritize the critical data in decision-making.
6. Information sharing in multi-organizational incident management requires responders of different levels to access data owned by different organizations. Discuss the possible approaches to render the temporary access to data, and how to protect the sensitive data?
7. Mobile devices used by responders form a distributed network among responders. The peer-to-peer communication among responders is used for situation awareness. Discuss different ways mobile devices are used in incident management, and what the challenges are?
8. Discuss how the location and context information can be used in information collection, sharing, and dissemination. What are the research challenges to consider the context in each stage of incident management?

Uncited References

Gómez-Pérez et al., 2004; NIMS, National Incident Management Resource Typing System.

References

Adam, N., et al. (2005). Semantic graph based knowledge discovery from heterogeneous information sources, in: *Proceedings of Working Together: Research and Development Partnerships in Homeland Security, April*, Boston, MA. QA :1

Akkiraju, R., R. Goodwin, P. Doshi, S. Roeder (2003). A method for semantically enhancing the service discovery capabilities of UDDI, in: *Proceeding of IJCAI-03 Workshop on Information Integration on the Web (IIWeb-03)*, Acapulco, Mexico, August 9–10, 2003.

Atluri, V., N. Adam, A. Gomaa, I. Adiwijaya (2003). Self-manifestation of composite multimedia objects to satisfy security constraints, in: *Proceedings of the 2003 ACM SAC*, pp. 927–934.

Bornhövd, C., T. Lin, S. Haller, J. Schaper (2004). Integrating automatic data acquisition with business processes, experiences with SAP's auto-ID infrastructure, in: *Proceeding of the 30th VLDB Conference*, Toronto, Canada, August 29/September 3, 2004.

Cai, G., A.M. MacEachren, L. Bolelli, GCCM. (2004). Map-mediated collaboration among emergency operation centers and mobile teams, in: *Proceedings of GIScience 2004*, Adelphi, MD, USA.

Chandrasekaran, S., G. Silver, J. Miller, J. Cardoso, A. Sheth (2002). Web Service technologies and their synergy with simulation. *Winter Simulation Conference (WSC'02), December*, San Diego, CA, USA.

Chun, S.A., V. Atluri, N.R. Adam (2005). Using semantics for policy-based Web Services composition, a special issue on Web Services. *Journal of Distributed and Parallel Databases* 18(1), 37–64.

Common Alerting Protocol v 1.0, OASIS Emergency Management TC [OASIS 200402], 12 August 2003.

Corley, J., D. Lejerskar (2003). Homeland defense center network—captializing on simulation, modeling and visualization for emergency preparedness, response and mitigation, in: *Proceedings of the 2003 Winter Simulation Conference*. QA :2

Fuhrmann, S., I. Brewer, I. Rauschert, A. MacEachren, G. Cai, R. Sharma, H. Wang, L. Bolelli, B. Shaparenko (2003) Collaborative emergency management with multimodal GIS, in: *Proceedings of ESRI User Conference*, San Diego, CA, USA.

Gomaa, A., N.R. Adam, V. Atluri (2005). Adapting spatial constraints of composite multimedia objects to achieve universal access, in: *IEEE International Workshop on Multimedia Systems and Networking (WMSN'05)*, Phoenix, AZ, USA.

Gómez-Pérez, A., M. Fernández-López, O. Corcho (2004). *Ontological Engineering*. Springer-Verlag London Ltd, London, UK.

Harris, S., N. Gibbins, N. Shadbol (2003). Agent-based semantic Web Services, in: *World Wide Web Conference (WWW2003)*, Budapest, Hungary.

Janeja, V.P., V. Atluri, J.S. Vaidya, N. Adam (2005a). Collusion set detection through outlier discovery, QA :3
in: *IEEE Intelligence and Security Informatics*, Springer, Berlin, Germany. QA :4

Janeja, V.P., V. Atluri, A. Gomaa, N. Adam, C. Bornhoevd, T. Lin DM-AMS (2005b). Employing data mining techniques alert management, in: *NSF National Conference on Digital Government*, Atlanta, GA, USA.

Johnson, R. (2000). *GIS Technology for Disasters and Emergency Management: An ESRI White Paper*, http://www.esri.com/library/whitepapers/pdfs/disastermgmt.pdf

Kokla, M., M. Kavouras (2001). Fusion of top-level and geographical domain ontologies based on context formation and complementarity. *International Journal of GIS* 15(7), 679–687. QA :5

Kulvatunyou, B., N. Ivezic (2002). Semantic web for manufacturing web services, in: *World Automation Congress Eight International Symposium on Manufacturing with Applications, June,* Orlando, FL, USA.

Martin, D., M. Paolucci, S. McIlraith, M. Burstein, D. McDermott, D. McGuinness, B. Parsia, T. Payne, M. Sabou, M. Solanki, N. Srinivasan, K. Sycara (2004). Bringing semantics to Web Services: The OWL-S approach, in: *Proceeding of the First International Workshop on Semantic Web Services and Web Process Composition*, San Diego, CA, USA, July 6–9, 2004.

McIlraith, S., D. Martin (Jan/Feb, 2003). Bringing semantics to web services. *IEEE Intelligent Systems.* QA :6

McIlraith, S., T. Son, H. Zeng (2001). Semantic web services. *IEEE Intelligent Systems* 16(2), 46–53. QA :7

NIMS National Incident Management Resource Typing System: http://www.nimsonline.com/nims_3_04/national_incident_management_resource_typing_system.htm#purpose QA :8

NIMS (National Incident Management System) Homeland Security, http://www.nimsonline.com/docs/NIMS-90-web.pdf, 2004.

NIST. (2003). *Conference on Modeling and Simulation for Emergency Response*, http://www.mel.nist.gov/div826/msid/sima/simconf/mns4er.htm

NRC. (2002). *Making the Nation Safer — The Role of Science and Technology in Countering Terrorism*, Committee on Science and Technology for Countering Terrorism, Division on Engineering and Physical Sciences, National Research Council, National Academy Press, Washington, DC, 2002.

NRP. (National Response Plan) Homeland Security, http://www.dhs.gov/dhspublic/interweb/assetlibrary/NRPbaseplan.pdf, December 2004.

OWL-S 1.0 Release. At http://www.daml.org/services/owl-s/1.0/

Paliwal, A.V., N. Adam, C. Bornhövd, J. Schaper (2004). Semantic discovery and composition of Web Services for RFID applications in border control, in: *Proceeding 1st. Intl. Workshop SWS'2004 at ISWC 2004, Hiroshima*, Japan, November 8, 2004, CEUR Workshop Proceedings, ISSN 1613-0073.

Rauschert, I., P. Agrawal, S. Fuhrmann, I. Brewer, H. Wang, R. Sharma, G. Cai, A. MacEachren (2002). Designing a human-centered, multimodal GIS interface to support emergency management, in: *Proceedings of the 10th ACM International Symposium on Advances in Geographic Information Systems*, pp. 119–124.

RESCUE, First Year RESCUE Progress Report (2004). *Responding to Crises and Unexpected Events*, http://www.itr-rescue.org/bin/pubdocs/rescue%20docs/2004%20RESCUE%20annual%20report.pdf

RESCUE, Second Year RESCUE Progress Report (2005). *Responding to Crises and Unexpected Events*, http://www.itr-rescue.org/bin/pubdocs/rescue%20docs/2005%20RESCUE%20annual%20report.pdf

Schurr, N., J. Marecki, M. Tambe, P. Scerri (2005). Demonstration of DEFACTO: training tool for incident commanders, in: *Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'05)*

Sheth, A., C. Bertram, D. Avant, B. Hammond, K. Kochut, Y. Warke (2002). Managing semantic content for the web. *IEEE Internet Computing* 6(4), 80–87.

Sollazzo, T., S. Handschuh, S. Staab, M. Frank, N. Stojanovic (2002). Semantic web service architecture—evolving web service standards toward the semantic web, in: *FLAIRS 2002*.

Wu, D., B. Parsia, E. Sirin, J. Hendler, D. Nau (2003). Automating DAML-S Web Services composition using SHOP2, in: *Proceeding of 2nd International Semantic Web Conference (ISWC2003), October*, Sanibel Island, FL, USA.

AUTHOR QUERY FORM

ELSEVIER	**Book : HIS-V002** **Chapter : 2014**	**Please e-mail or fax your responses and any corrections to:** **E-mail:** **Fax:**

Dear Author,

During the preparation of your manuscript for typesetting, some questions may have arisen. These are listed below. Please check your typeset proof carefully and mark any corrections in the margin of the proof or compile them as a separate list*.

Disk use
Sometimes we are unable to process the electronic file of your article and/or artwork. If this is the case, we have proceeded by:
- Scanning (parts of) your article
- Rekeying (parts of) your article
- Scanning the artwork

- *Uncited references*: This section comprises references that occur in the reference list but not in the body of the text. Please position each reference in the text or delete it. Any reference not dealt with will be retained in this section.

Queries and / or remarks

Location in Article	Query / remark	Response
AQ1	Please provide all author names in reference Adam et al. (2005).	
AQ2	Please provide the venue of the proceedings for the references (Corley and Lejerskar, 2003; Rauschert et al., 2002; Schurr et al., 2005; Sollazzo et al., 2002).	
AQ3	Since there are two publications by Janeja et al. (2005), we have inserted 'a' and 'b' only in the reference list. Please go through each mention in the text and indicate by comparing with the list as either '2005a' or '2005b'.	
AQ4	Please check the inserted publisher and publishing location for reference Janeja et al. (2005a).	
AQ5	Please check the inserted volume number and page range for reference (Kokla and Kavouras, 2001).	
AQ6	Please provide the volume number and page range for reference (McIlraith and Martin, 2003).	
AQ7	Please check the inserted page ranges for references (McIlraith et al., 2001; Sheth et al., 2002).	
AQ8	Please provide the year of publications for references (OWL-S 1.0 Release; NIMS) and update in text also.	

Thank you for your assistance

*In case artwork needs revision, please consult http://authors.elsevier.com/artwork