Supporting Physical and Logical Communication in Emergency Management Virtual Distributed Teams

Daniel Sanz, Patricia Gómez Bello, Paloma Díaz, Fausto J. Sainz and Ignacio Aedo
DEI Laboratory, Computer Science Department, Carlos III University of Madrid
Avda. de la Universidad 30, 28911 Leganés (Spain)
{dsanz|pgbello|pdp|fsainz}@inf.uc3m.es, aedo@ia.uc3m.es

ABSTRACT

Virtual Distributed Teams (VDT) need to face physical and logical communication challenges during emergency response. Physical problems include heterogeneous technology infrastructures, ubiquitous accessibility, alternative media communication or real-time interaction. Logical problems are related to the accomplishment of a coordinated activity, such as the need for a common place accessible by all where digital artefacts are available, spontaneous communication, real-time interaction, and emergency awareness. We present an integration framework that addresses the physical and logical communication requirements in emergency management for VDTs. The framework provides a ubiquitous mobile infrastructure that supports physical communication, proposes a generic role-based organizational structure for VDT, and outlines an integration strategy that allows to define logical communication channels by means of information flow and access control policies based on the VDT structure.

Keywords

Virtual Distributed Teams, Communication, Role Based Access Control, Information Flow, Ubiquitous Mobile Infrastructure.

INTRODUCTION

A Virtual Distributed Team can be defined as a group of people geographically scattered that cooperate across time, space and organizational boundaries to achieve a goal, using information and communication technologies to coordinate their work. Emergency Management Virtual Distributed Teams (VDT henceforth) have the goal of managing the emergency situation and providing assistance, in a potentially hostile environment, usually with the help of mobile technology. In this paper we will focus on problems concerning computer mediated communication amongst VDT members. Roughly speaking, while a part of the VDT is displaced to the emergency area to provide assistance by means of one or more mobile help units, other VDT members stay at the operation center, providing a variety of services to displaced members. The term operation center denotes a department of any organization that supports and manages the response to an emergency. The term mobile help unit (HU henceforth) refers to any kind of help unit, regardless of the organization the unit belongs to, displaced to the emergency area.

VDTs need to face physical and logical communication challenges such as those mentioned in (Steinfield, Jang and Pfaff, 1999). Physical problems include heterogeneous technology infrastructures, ubiquitous accessibility, alternative communication media, monitoring interesting actions or real-time interaction. Logical problems are related to the achievement of a coordinated activity, such as the need for a common place accessible by all, where digital artefacts, spontaneous communication, real-time interaction, and awareness (what actions are being undertaken by other members, or the VDT, availability of people, alerting users…) are available.

Emergency management frameworks such as (AIIMS, 2004; ICS, 2005; NIMS, 2005) address a variety of issues related to communications in emergency management. The goal of AIIMS (Australia) is the seamless integration of activities and resources of multiple agencies when applied to the resolution of any emergency situation. The goal of ICS (United States, Canada, and United Kingdom) is to standardize on-scene incident management concept designed specifically to allow responders to adopt an integrated organizational structure equal to the complexity and demands of any single incident or multiple incidents without being hindered by jurisdictional boundaries. The goal of NIMS is to respond to natural disasters and emergencies, such as acts of terrorism, including a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid and resource management. However, AIIMS, ICS, and NIMS do not support physical and logical communication among teams that are near to the emergency area. By analyzing these frameworks we can identify some challenges that require still a proper solution, including: 1) To improve the information flow among VDT members, helping with the communication, coordination and cooperation of operational efforts; 2) Efficient and effective use of networks resources; 3) Accessibility to the VDT member's software applications; 4) Mobility of VDT members without communication technology's disruption.

In this paper we present an integration framework that addresses physical and logical communication requirements in emergency management for VDTs. We propose a solution based on a combination of Role-Based Access Control and mobile technology that has three main elements: 1) a role-based organizational structure with three broad levels: directive (strategic functions), tactic (communications, logistics and deployment), and operative functions (help providers); 2) a ubiquitous system meta-architecture supporting ubiquitous mobile office; 3) a flexible integration strategy between the organizational structure and the technological architecture. This framework must facilitate the information flows required to mitigate an emergency by taking advantage of the underlying technology. An *ubiquitous mobile office* (detailed later) provides mobility and accessibility to communicate between different VDT members, even in limited conditions. *Information flow* mechanisms can be used to provide VDT members a degree of transparency[1] regarding who to communicate with, and which messages may be interchanged, both within the VDT and between different VDTs. We are focusing on vertical and horizontal communication between VDT members. We have improved the information flow between operation centers and mobile help units (vertical communication); between mobile help units of the same organization (vertical communication); and between mobile help units from different organizations (horizontal communication). In this context, VDTs are made up in two ways. Firstly, members belonging to different organizations must cooperate to improve the response, as suggested in (Bui and Sankaran, 2006). Secondly, members can be scattered in different emergency locations and operation centers, as mentioned in (Meissner, Wang, Putz and Grimmer, 2006). Moreover, information overload can also be mitigated by means of *access control* mechanisms based on the roles taken by different VDT members, so that each member only receives the information required to accomplish his tasks. To set up such mechanisms, it is crucial to determine who is responsible for each task.

The proposed framework is intended to serve as a basis for emergency management systems design. We do not address in this paper how the framework may be integrated in existing or new emergency management systems, such as incident command systems. The solution must be independent of, and adapted to, the procedures established by the organizations responsible of emergency management and intervention.

The remainder of the paper is organized as follows. We present the integration framework in Section 2. We describe a use case to illustrate the ubiquitous mobile infrastructure in Section 3. Finally, we sum up with some conclusions and future lines of development.

INTEGRATION FRAMEWORK TO SUPPORT VIRTUAL DISTRIBUTED TEAMS COMMUNICATION

We assume some premises that help in the design of the framework and are useful to elicit some requirements. Firstly, no two emergencies are equal, so the solution must be general and adaptable to each situation. Another assumption is simplicity: technology is useless if it is not correctly used, coordinated and accepted by the people that will use it. We focus on communication and coordination issues during the emergency, and not on the "before" (prevention) nor "after" (recovery). We also assume a common type of assistance deployment hierarchy in response to an emergency, as well as the existence of a minimal communication and information infrastructure.

Organizational Structure

Our solution proposes the use of Role-Based Access Control to model the VDT organizational structure. RBAC is an access control model that has been proved to be a natural means of capturing organization's lines of authority and responsibility in an intuitive way (ANSI, 2004). Instead of granting privileges directly to users, permissions are assigned to roles, and users are made members of adequate roles, acquiring its permissions. The role concept represents a set of permissions and a set of users allowed to use them, so it is used to capture job positions, qualifications or responsibilities. In terms of permissions, a role is much more stable than a user: while user's responsibilities change over time, the notion of role usually requires fewer changes. This flexibility is one of the most valuable features of RBAC: a change in user membership will affect available permissions for that user, without changing the permissions assigned to any role and other users´ permissions, allowing to precisely define

[1] We use the term transparency to denote that users do not need to be aware of certain details that may disrupt the course of their work, such as technical issues like network selection, channel availability verification, determination of who has to be contacted.

which are the privileges granted to each user. RBAC is widely used in a variety of computer systems, including emergency management systems (Aedo, Díaz, Sanz, 2006; Chen and Dahanayake, 2006; Zhu and Zhou, 2006), for which special care must be taken: a user should be previously trained in order to gain the required skills and qualifications to hold a concrete role. RBAC is considered to be policy-neutral, in the sense that it does not impose any specific access policy, allowing to be configured to enforce mandatory as well as discretionary policies.

The solution proposed in this paper integrates different technologies and uses unstructured and semi-structured information. In this scenario, RBAC must be judiciously used in order to provide the required improvisation to face unexpected situations, while guaranteeing a certain degree of control. In general terms, we assume a rule of thumb: physical communication such as voice (unstructured information provided by the ubiquitous platform) is unconstrained, but logical communication is subject to RBAC (semi and structured information provided by distributed information systems used in emergency management). Improvisation is desirable, however a certain degree of control is required in order to support accounting as well as the development of an institutional memory that will help to learn from own experiences. Accountability can benefit from the fact that the framework assumes RBAC: since decisions are taken by users holding roles, intervention results may be recorded using roles, so that no concrete user identities are undisclosed. This approach may reduce users' reluctance to use the system in presence of accounting mechanisms.

Several roles are identified to capture the structure of the organizations that participate in emergency mitigation and management. Since there are substantial differences amongst them, we have adopted a general function-driven approach similar to the one suggested in (Aedo et al., 2006), so the structure is defined according to the different responsibilities required to face the emergency. It is important to note that our proposal is not intended to substitute any existing structure. The idea is to provide a loosely-coupled structure made up by different roles that use the system, which should be mapped to proper organizational entities, or directly assigned to trained people according to their positions within the organization. This approach provides the required flexibility to adapt to different contexts where the emergency is happening, such as cultural or local context. From a logical communications point of view, the proposed structure can fit in different organizations, such as public services, NGO and others: one person may hold several roles, depending on his capabilities, and roles are dynamic in the sense that they may be held by different people at different times. Moreover, a user can delegate his/her role to other user for a specific period if required, thus allowing the new user to hold that role. Aspects such as who is assigned to each role in a given moment are managed by one or more system administrators according to organizational policies. This flexibility allows organizations to tailor the framework, particularly user-to-role assignments, to their specific social, organizational and/or structural needs. This is especially useful for highly structured organizations, where procedures are predefined and clearly established.

For each organization involved in an emergency there are strategic, tactic and operative function levels. Our proposal focuses on tactic (communications, deployment and logistics) and operative (help provision) levels, for which several functions, represented by roles, may be identified. The following roles are based on the idea of VDT deployment as an operation center and one or more displaced HUs:

- Responder: this role represents the basic function of each organization. Usually, users holding this role are frontline helpers in touch with affected people, and they are a valuable resource in order to evaluate the situation and estimate the required help. They have a specific ability depending on the organization they belong to (i.e a firefighter), although there may be different types of Responder. For instance, a physician or a nurse have the same function for the purposes of the system usage, so there is no need for a further decomposition of this role. Each responder belongs to a given HU where has a precise function.
- Help Unit Coordinator (HUC): this role coordinates all the people belonging to a HU, for each HU there is one coordinator. HUs usually use a single vehicle and equipment (for instance, an ambulance, a police patrol or fire truck), which include technology for communication with other HU of the same service, and with the operation center. The HUC, often also a responder, communicates with the responders to gather information and resource needs.
- Deployment Coordinator (DC): this role coordinates all deployed HUs of a given type. Communicates with HUC to make a precise evaluation of the situation, and gathers all resource requests made by HUCs in order to prepare a single resources request and send it to the operation center. DCs are also responsible to keep themselves informed about where are the HUs, what are they doing and what their needs are. According to this information, DC may request HU or resource movements, as well as set delivery points for resource delivery. For small emergencies there should be one DC, which is also an HUC and possibly a responder.

- Communication Manager (CM): this role represents a communications responder usually located at the operation center. He receives help requests and provides a response according to the needs. The way this response is orchestrated among the different resource providers is not covered by our framework, as these decisions are taken far away from the emergency area, where our solution is designed to work, and may be based on political decisions that lay outside the scope of this paper. Depending on this, the CM work may range from forwarding the request to other management role (such as a Director) to organize and send the help to the emergency area. From the system's viewpoint, the CM acts a communication point able to receive help requests and provide responses.

Since several roles overlap, we use the inheritance relation to define a role hierarchy. If role A and role B are related through the inheritance relation, the permissions of B are also permissions of A, while users of A are also users of B. Then, it is said that B is senior of A. Figure 1 shows the proposed role hierarchy, where arrows denote inheritance, i.e Deployment Coordinator inherits permissions from HU Coordinator. The Director and Organization Member roles are not further elaborated, due to we focus on communications between mobile HUs and operation centers.

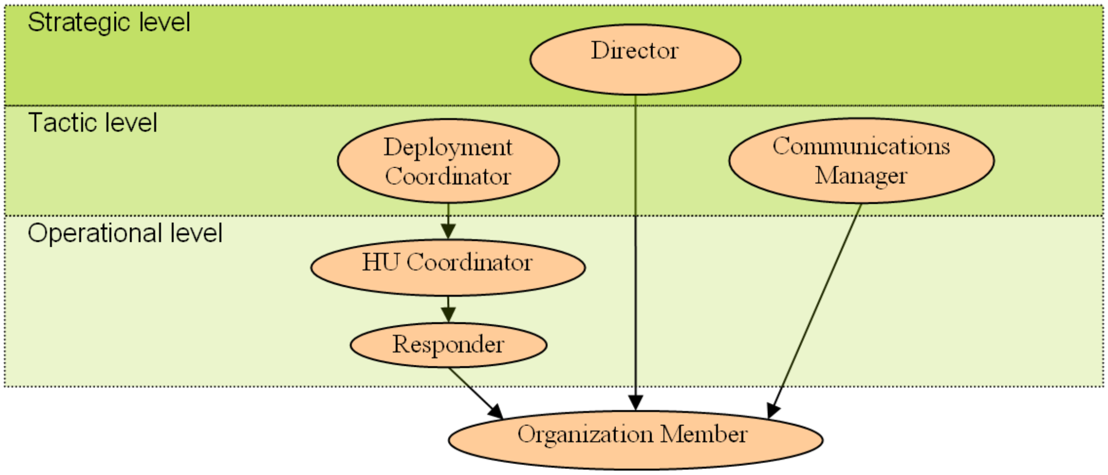


Figure 1. The proposed generic role hierarchy

This structure facilitates the logical communication as it can be used as the basis for access control and information flow policies. Once authenticated, each user is automatically assigned the roles he can take. Authentication mechanisms are not concerned with access control itself, as users are assumed to be authenticated before any role is assigned to them. We do not cover directly authentication issues in this paper; however ubiquitous framework (discussed in next section) provides the infrastructure to achieve single sign-on and session management. If that user requires additional roles, they may be reassigned by the system administrator or delegated by senior roles. In this paper we do not address administrative issues, such as the number of administrators, which administration privileges they have, or which procedures are used to contact administrators and request role memberships. Each user only has access to pertinent information and functionality, as the user interface is automatically built according to the RBAC policy. Moreover, information flow guarantees that messages only arrive to the right users, and no message will be sent by, or delivered to, unauthorized roles. Each role can send/receive a specific set of messages, so that it is not necessary to identify the specific person to send a message: the information access policy establishes who must/can/cannot receive what type of message. Although some information is of interest for all emergency managers (ground zero maps, weather reports, etc.), each organization deployed in the emergency area will have different information needs, so the concrete message contents are different in each case.

For example, when several firefighters HUs are mitigating a fire, a firefighter acting as HU Coordinator may inform other HU Coordinators about the fire extent in his area. This information may help to foresee fire behavior. If needed, HU Coordinators may communicate with its Deployment Coordinator to inform about the estimated fire evolution, which in turn can decide to move some HUs or even request more units to the firefighter Communications Manager. The framework allows to define all these information flows and subject them to RBAC according to each organization access policy, so that each user does not need to identify who is the person to communicate with: each possible type of message codes the receiver role and the contents.

Ubiquitous System Meta-Architecture

In order to assure physical communication among VDTs, we have developed a ubiquitous mobile office based on ubiquitous system meta-architecture.

The ubiquitous mobile office's goal is to support the emergency management thorough data transmission. Ubiquitous mobile offices are nodes situated in outdoor areas near to an emergency, where services are provided to VDT members. Ubiquitous mobile offices integrate mobile technologies, such as PDAs, laptops, wireless modems, radio WLAN antenna, batteries, GPS receivers, wireless, cellular, GPS and satellite networks (Gómez Bello, Aedo, Sainz, Díaz, Munnelly and Clarke, 2007).

The meta-architecture consists of mobile devices and different networks. This meta-architecture is focused on resolving the following physical challenges: the integration of heterogeneous mobile devices, ubiquitous accessibility, and real-time interaction. Ubiquitous system meta-architecture offers transparent communication to VDT members resolving these physical challenges. The ubiquitous mobile office is part of this meta-architecture. It uses a PDA that can connect to any network to transmit information, and a laptop, which acts as server to the client (PDA). The design of ubiquitous mobile office is based on ubiquitous computing.

UILE (Fritsch, Munnelly, and Clarke**,** 2006) is the ubiquitous computing framework used by our ubiquitous mobile office. UILE identifies concerns that should be taken into consideration when incorporating mobility and context-awareness into software applications. Using UILE guidelines, ubiquitous mobile office should provide communication that addresses mobility concerns such as those mentioned in (Fritsch et al., 2006):

1. `Service discovery` dynamically discovers and acquires access to the necessary services for the software application.
2. `Quality of service assurances` is a mechanism for ensuring network resources to the software application.
3. `Network rooming` ensures that an appropriate network is available to the software application at all times.
4. `Location` is the user's position with respect to the context.
5. `Ad-hoc networking` is a collection of smaller distinct concerns such as service discovery, proximity, and reliability.
6. `Limited connectivity` detects disconnections in a timely manner, as well as providing the facility for specifying contingency plans for use, when disconnections occur in the software application.
7. `Transaction management` provides quality assurances with respect to data integrity.
8. `Security` protects a software application against attacks on network resources by malicious entities.
9. `Software roaming` is an agent that reduces the quantity of network calls to overcome network latency problems on slow networks.
10. `Proximity` is the ability to communicate with other entities.
11. `Distribution` facilitates communications between multiple system components.

In addition, many contextual concerns should be addressed in the software application. It should be developed including contextual concerns such as those described in (Fritsch et al., 2006):

1. `User context` relates to all the knowledge pertaining to the user that the software application requires to function correctly.
2. `Social context` refers to user's data against his environment.
3. `Device context` determines the maximum physical capacity of the device, and how much data can be displayed on the device at any given point in time.
4. `Location related context` acquires user's physical location.
5. `System context` refers to the architectural semantics of the software system.
6. `Environmental context` is the context of the physical world in which the software application is running; for example, light, temperature, etc.
7. `Temporal context` allows the software application to adapt according to the notion of time both physical and relative.
8. `Application specific context` refers to the gathering of all knowledge with respect to a particular user's interaction with the system.
9. `Mobility` makes explicit references to user's interactions with mobile context.
10. `Proximity` plays a vital role in how interaction may occur between different components in a system.

Any user can access to any mobile device (radio, mobile phone, PDA, and laptop), as they are part of the ubiquitous system meta-architecture. However if he accesses a PDA, he can get mobility and context concerns when he registers a software application assuring reliability and trust on the communication. Both a PDA and a laptop are part of the ubiquitous mobile office. A PDA could be configured by the next concerns: software [User context, Social context, Device context, Location related context, System context, Environmental context, Temporal context], network [Service discovery, Quality of service assurances, Network rooming, Location, Ad-hoc networking], and hardware [Limited connectivity, Transaction management, Security, Software roaming, Proximity, Distribution]. PDA and laptops could get connection from WLAN, Cellular, GPS and Satellite networks.

Mobile devices such as radio, mobile phone, PDA, and laptop could be used by any user on the response to an emergency. However, if a user wants to access to the ubiquitous mobile office, he needs to use a PDA or laptop, and he can access to any emergency software application. Mobile devices could get connection from any network such as radio signals, cellular, WLAN, and satellite. Radio and mobile phones are part of the ubiquitous system meta-architecture. They are used by any role, but they are not part of the ubiquitous mobile office solution.

Communication is transparent to VDT members. They do not need to worry about the network connection or software application availability. PDA's social context includes the use of Role Based Access Control (RBAC) described above. When a VDT member logs into the software application, the VDT member's role is identified and the correct context for that VDT member is loaded, so the PDA interface is built according to VDT member' roles. PDA's service discovery is used to connect to a mobile office. Before the call to register a VDT member, the service discovery module is triggered. A VDT member cannot be registered until the software application service has been discovered and his mobile device is a node in the WLAN. The software application multicasts a request for a service discovery and the mobile office returns a response with its IP address.

Resource Management

A key aspect to achieve an effective communication is the existence of common information repositories accessible by all VDTs. In the case of emergency management systems, these repositories may include weather report services, or geographical information systems, however the existence of a resource catalogue is a key requirement. The resource catalogue is one of central parts for emergency planning and response, so this repository has to be quickly and reliably accessed, as well as contain multilingual information in order to avoid misunderstandings about what is exactly required, which measurement unit is used, etc.

Integrating Physical and Logical Communications

This section proposes a strategy for integrating the ubiquitous platform and the organizational structure, thus providing the basis to develop distributed information systems for emergency management. The framework allows to define the communication needs for each role in a given organization, which serves as a basis for information flow policy, access control policy and technology deployment for help units.

The framework assumes the existence of many organizations that participate in the emergency, from public services (such as firefighter, police, health, or civil protection organizations) to non-profit private services (NGOs). Each organization has a different nature and may have different structure, but a common set of function types may be identified, as shown in the section Organizational Structure. For each organization there is at least one operation center, and one or more HUs, each one having a mobile office and more mobile devices.

The framework defines a set of components required to integrate the physical and logical communication, as illustrated in Figure 2:

- Role-based organizational model instantiation: the organizational structure proposed above has to be instantiated for each organization that participates in an emergency response. This instantiation process requires the identification of responsibilities for each VDT members and subgroups to determine which roles are available for each unit. Then, specific roles for that VDT can be created, such as *firefighter HUC*.
- Tasks: different categories of emergency management tasks can be identified; such as logistics, response tasks management, technical assistance, and resource management. Each VDT should be trained for a specific tasks subset. Each task requires a set of physical and logical resources, such as mobile devices, information flows or information sources.

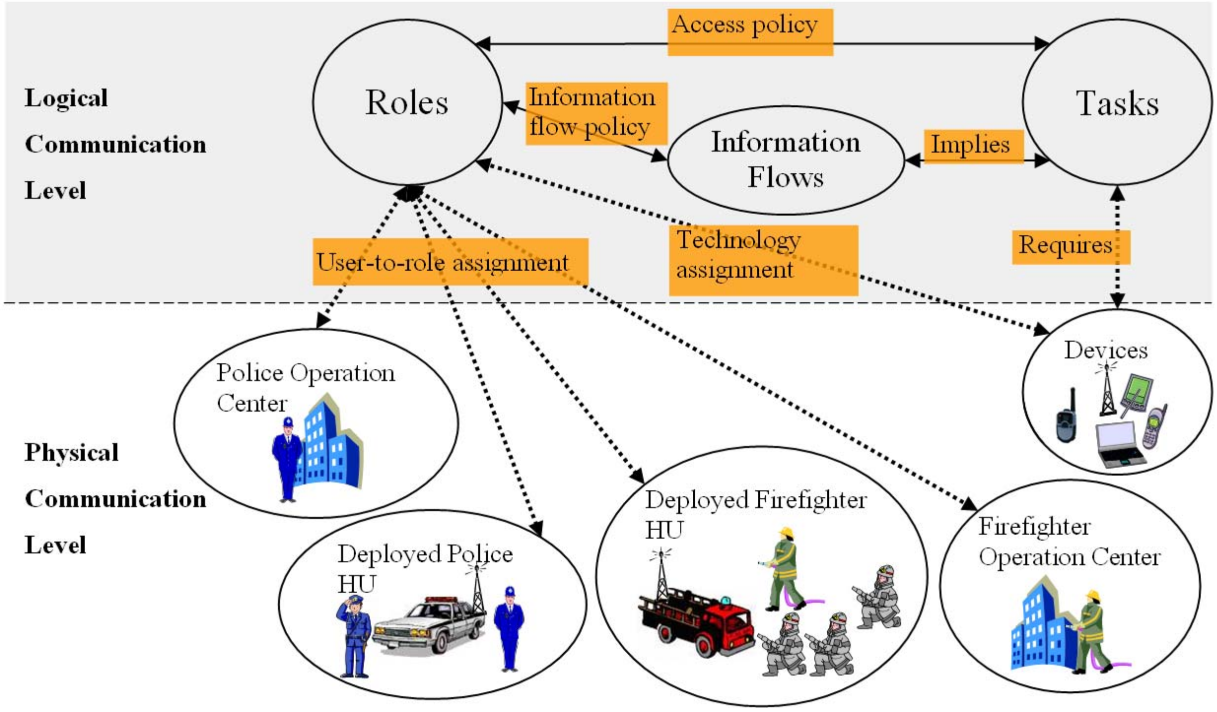


Figure 2. Integration framework overview

- `Information flows`: from a logical communications point of view, each task requires a set of message interchanges in order to be accomplished. It is worth mentioning that these flows imply the usage of different mobile devices and networks.
- `Access control policy`: defines the task-role assignment, what roles have access to which information resources. This includes access to information repositories (such as resource catalogues) as well as access to common information.
- `Information flow policy`: given the task-role assignments and the information flows required by a task, the set of messages that a role can send/receive is computed.
- `Technology assignment`: once information flows are established from/to each role, technological needs are identified, according to the nature of the VDT. This includes mobile devices as well as software/user interfaces required for each role to accomplish the assigned tasks, taking into account the location and mobility needs of each member.
- `Assignments of VDT members to proper roles`: finally, the equipment and configuration for each VDT member is defined according to the user-to-role assignments.

The proposed framework facilitates communication in a number of ways: horizontal flows allow to keep VDTs updated about the emergency status as well as other VDTs important information; vertical flows help to clarify the needs from affected people and determine which resources have to be requested and where to deliver them. Since these flows are regulated through RBAC, the framework respects the existing organization's structure, procedures and practices. Unnecessary resource usage and information overload are minimized: only pertinent data is transmitted to the right person according to what has been established in the information flow policy.

USE CASE

Now we present a use case that involves deployment and coordination of VDTs in a building on fire in a town (small emergency), it also illustrates how our solution may be used in bigger emergencies. The example assumes that the emergency could be mitigated using resources managed by the administrative area where the situation is taking place (i.e city or region resources), so no external resource requests are required. Figure 3 depicts the disaster scenario for the use case. Numbers represent the order in which information flows take place, and dashed lines represent flows that our framework does not address.

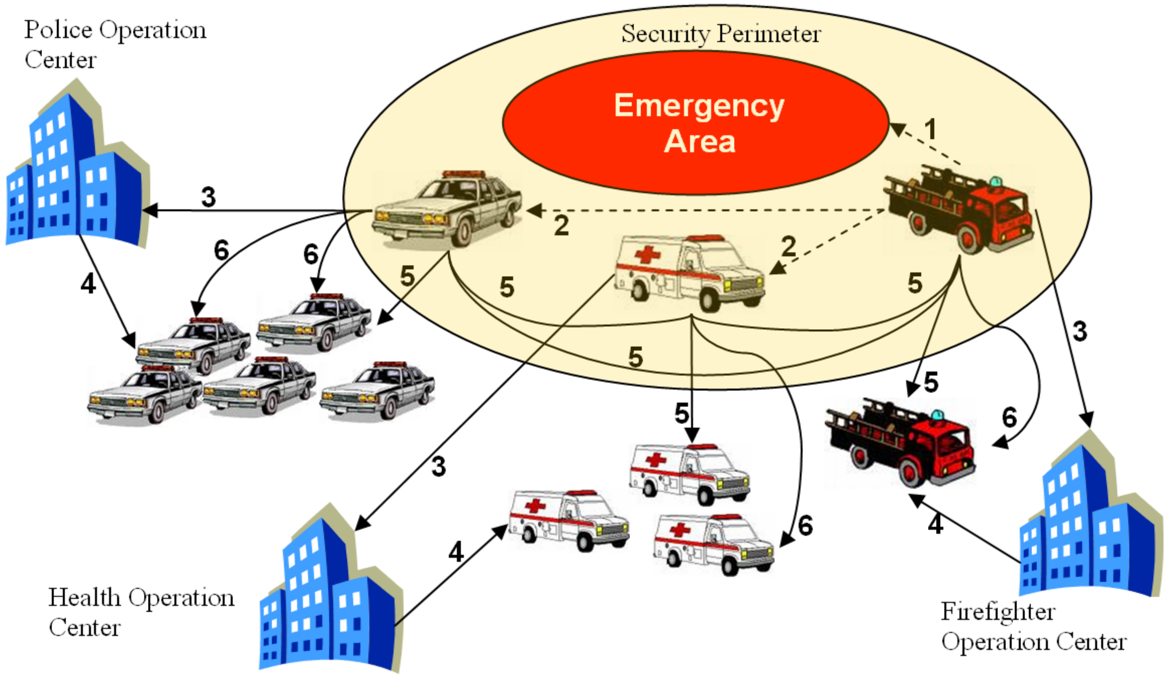


Figure 3. A fire emergency use case. Dashed lines represent flows not managed by the framework.

The scenario develops as indicated in the following paragraphs, numbered according to information flows depicted in figure 3:

1. Some units come into the emergency area. We assume three initial HUs, corresponding to firefighter truck, police patrol and ambulance. Since the emergency is a fire, firefighter unit starts the evaluation of the situation, which implies entering the building and determining the fire extent, location of affected people, exits, and so on. These responders communicate with the firefighter HUC, which is also inside the building. In turn, HUC keeps informed the firefighter DC, which is outside the building.

2. Firefighter DC informs police and health DCs about the situation, through voice communication. The fire affects the 9th floor and is propagating upwards. There are about 20 injured and lower floors need to be evacuated quickly. Now, each HU may take decisions according to the type of service: 1) police unit sets a security perimeter around the area; 2) ambulance locates inside the perimeter to receive the injured.

3. The three DC determine that they need more resources to address the emergency. Using the ubiquitous mobile office, they communicate with each CM, located usually at an office in the corresponding operation center (police station, fire station or hospital). The police DC requests five more patrols, one to reinforce the perimeter, one to manage the surrounding traffic, and three to evacuate the people not injured. The ambulance DC considers that the injured may be attended in place or moved to city hospitals, and estimates that three more ambulances are required, and requests them. Firefighter DC requests one more truck to extinct the fire from two sides of the building and more responders to evacuate the injured.

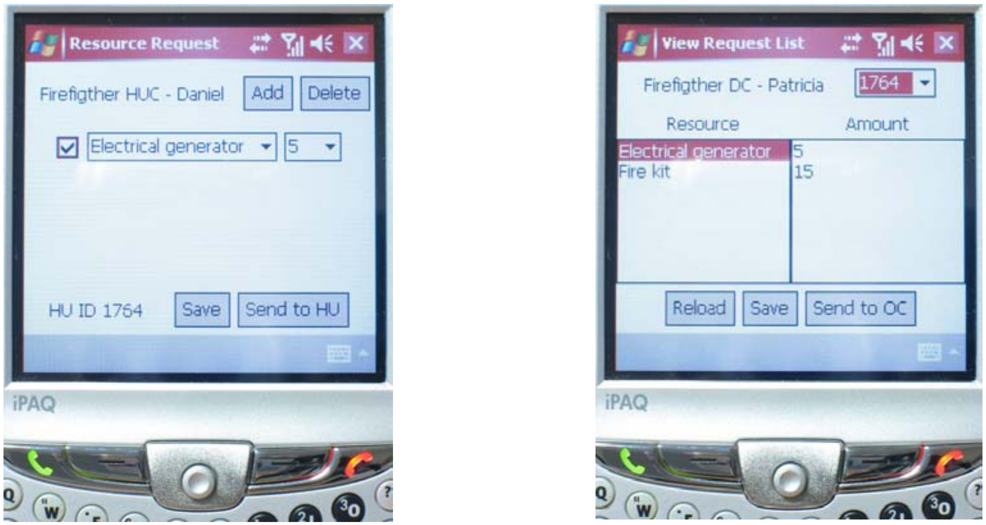
4. CMs prepare and send the help resources. In this case all resources are HUs so they locate nearby the security perimeter and their HUC wait for instructions from the corresponding DC.

5. During emergency mitigation, DCs communicate with 1) other DCs, in order to know about the situation and anticipate the needs, 2) their HUC, to receive new resource requests or provide instructions. For example, police units may coordinate to disseminate through building floors, 3) the CM, to send more resource requests according to the needs reported by HUC.

6. Eventually, a DC may free resources when not required. This decision may be taken upon previous conversation between HUC and DC.

Coordinators Interfaces

In order to illustrate how the integration framework helps to support logical and physical communication between VDT members, we have developed a sample application using mobile offices that implements resource management tasks. Using a laptop on the server side and a PDA as the client, an emergency coordinator (HUC or DC role) can manage resource requests. Figure 4 graphically shows the HUC (left side) and DC (right side) interfaces to ask for resources and to view the received requests for all HUs respectively. Daniel is a firefighter HUC that requires more electrical generators for his HU, which ID is 1764. Using the resource request interface (fig. 4.a) selects the appropriate resource and indicates the amount. When the request is completed, the "Send to HU" button generates an information flow to the corresponding Deployment Coordinator. It should be noted that Daniel is not aware about where the DC is nor who the DC is at that moment. Moreover, Daniel visualizes only the information required to do his work, due to access control mechanisms allows Daniel to visit the *resource request* interface but not the *view request list* page, so information overload is minimized in a transparent way. Patricia is the firefighter DC, who receives the requests of all the firefighter HU under her responsibility. She selects to view the requests made by HU #1764 (fig. 4.b), which includes electrical generators and fire kits, and she can reload (request the latest resource list to the HUCs), save the request to local file or send the request to the Operation Center. Through other interface, she can modify the request according to information received from other HUs before sending it to the Operation Center.



Firefigther HUC - Daniel

☑ Electrical generator ▾ 5 ▾

HU ID 1764

Firefigther DC - Patricia 1764 ▾

Resource	Amount
Electrical generator	5
Fire kit	15

a) Help Unit Coordinator Resource Request b) Deployment Coordinator Resource List

Figure 4. Emergency firefighter coordinator interfaces

CONCLUSIONS AND FUTURE WORK

We have presented a framework that addresses physical and logical communication problems supporting horizontal and vertical communication. Horizontal flows keep VDTs updated about the emergency situation. Vertical flows help to clarify affected people needs and to determine which resources have to be requested and where to deliver them. Finally, unnecessary resource usage and information overload are minimized: only pertinent data is visualized by the right person.

Emergency management distributed information systems can benefit from the proposed framework. For instance, the results of an intervention in an emergency can be recorded in the operation centers by the Communication Manager. This information may include which decisions were taken during the emergency mitigation, how different VDTs were coordinated, what operation results were, which resources were used, etc. In turn, this traced information can be exploited as the basis for support decision systems, or guidelines elaboration and procedures refinement, as well as preparing teaching material targeted to different social groups. Finally, strategic planning can gain experience by taking into account previous results.

ACKNOWLEDGMENTS

This work is supported by the ARCE++ project (TSI2004-03394) funded by the Spanish Ministry of Science and Education (MEC) and a cooperation agreement between "Universidad Carlos III de Madrid" and "Dirección General de Protección Civil y Emergencias" (Ministry of the Interior). The authors would like to thank Serena Fritsch and Jenny Munnelly for helping with the incorporation of the UILE Framework.

REFERENCES

1. Aedo, I., Diaz, P. and Sanz, D. (2006). An RBAC Model-Based Approach to Specify the Access Policies of Web-Based Emergency Information Systems. *International Journal of Intelligent Control and Systems (in press)*
2. AIIMS: Australasian Fire Authority Council. (2004). The Australian Inter-service Incident Management System, Australasian Fire Authority Council, Third Edition, Version 1, 3.
3. ANSI INCITS 359-2004. American National Standard for Information Technology. Role-Based Access Control.
4. Bui, T. and Sankaran, S. (2006). Foundations for Designing Global Emergency Response Systems (ERS). *Proceedings of the third International Conference on Information System for Crisis Response and Management, ISCRAM 2006,* Newark, NJ (USA), 72-81.
5. Chen, N. and Dahanayake, A. (2006). Personalized situation aware information retrieval and access for crisis response. *Proceedings of the third International Conference on Information System for Crisis Response and Management, ISCRAM 2006,* Newark, NJ (USA), 214-222.
6. Fritsch, S., Munnelly, J., and Clarke, S. (2006) Towards a Domain-Specific Aspect Language for Ubiquitous Computing, *Proceedings of Open and Dynamic Aspect Languages Workshop (ODAL) at AOSD 2006*.
7. Gómez Bello, P., Aedo, I., Sainz, F., Diaz P., Munnelly J. and Clarke, S. (2007). Improving Communication for Mobile Devices in Disaster Response, *Lecture Notes in Computer Science (LNCS) by Springer*, in press.
8. ICS: Incident Command System. (2005). *U.S Department of Labor, Occupational Safety & Health Administration,* http://www.osha.gov/SLTC/etools/ics/index.html
9. Meissner, A., Wang, Z., Putz, W. and Grimmer, J. (2006) MIKoBOS, A Mobile Information and Communication System for Emergency Response. *Proceedings of the third International Conference on Information System for Crisis Response and Management, ISCRAM 2006,* Newark, NJ (USA), 92-101.
10. NIMS: National Incident Management System. (2005). *The Secretary of Homeland Security, Federal Emergency Management Agency*, FEMA, http://www.fema.gov/emergency/nims/index.shtm
11. Steinfield, C., Jang, C., and Pfaff, B. (1999). Supporting virtual team collaboration: the TeamSCOPE system, *Proceedings of the international ACM SIGGROUP conference on Supporting group work*, Conference on Supporting Group, Phoenix, Arizona (USA), 81-90.
12. Zhu, H. and Zhou, M. (2006). The role transferability in Emergency Management Systems. *Proceedings of the third International Conference on Information System for Crisis Response and Management, ISCRAM 2006,* Newark, NJ (USA), 487-496.