Modelling emergency response communities using RBAC principles

Ignacio Aedo, Daniel Sanz and Paloma Díaz
Laboratorio DEI
Universidad Carlos III de Madrid
aedo@ia.uc3m.es, dsanz@inf.uc3m.es, pdp@inf.uc3m.es
Jorge de Castro
Dirección General de Protección Civil
Ministerio del Interior (Spain)
jcastro@procivil.mir.es

ABSTRACT

One of the main design challenges of any Emergency Management System (EMS) is the diversity of users and responsibilities that must be considered. Modelling the access capabilities of different communities of users is a relevant concern for which the RBAC (Role-Based Access Control) paradigm provides flexible and powerful constructs. In this paper we describe how we used an RBAC meta-model to specify at different levels of abstraction the access policy of a specific EMS called ARCE ("*Aplicación en Red para Casos de Emergencia*"). This approach has made it possible to face access modelling at earlier development stages, so that stakeholders got involved in analytical and empirical evaluations to test the correctness and effectiveness of the access policy. Moreover, since the RBAC meta-model is embedded into a web engineering method, we put into practice a holistic process which addresses different design perspectives (structure, navigation, presentation, interaction and access) in an integrated way.

Keywords

Emergency management system; role based access control; web engineering; user-centred design.

1 INTRODUCTION

One of the main design challenges in an Emergency Management System (EMS henceforth) is the great variety of users and responsibilities that have to be considered. One the one hand, there are different kinds of virtual communities involved in the emergency situation with different needs and natures: from the teams set up at the governmental agencies -where technical specialists, experts in different related areas and strategic and political representatives cooperate following well defined protocols and rules-, to less structured communities of users like invited organizations, ngo's, journalists, volunteers, anonymous users, etc. On the other hand, it is commonly recognized that each user can exercise one or more responsibilities during the emergency situation (Dykstra, 2003, Turoff et al, 2004) so that the system has to support flexibility whilst guaranteeing security and auditing. In such a scenario, modelling the access capabilities of different communities of users in a proper way becomes a decisive design concern. Another important issue to keep in mind is that access modelling has to be integrated within the rest of the modelling activities to produce a well-documented and safe system. In this way, access requirements are unified with other kinds of requirements (such as functional and non-functional requirements) so that dependencies among requirements can be taken into account (e.g. implementing fine-grained access policies influence response time and, consequently, designers should analyse tradeoffs). Furthermore, well defined requirements are easy to test, maintain and re-use (Díaz et al, 2006). When such a *holistic* engineering approach is not adopted, access requirements are often added to the system once it has been implemented, a process that is costly and error-prone, since access policies have to be shoehorned into existing code (Brose et al, 2001).

In this paper we describe how we specified access rules for different virtual communities of a specific EMS called ARCE ("*Aplicación en Red para Casos de Emergencia*") at different levels of abstraction and by following a *holistic* approach. For this purpose we applied the Ariadne Development Method (ADM), a web engineering method that assumes an RBAC (Role-Based Access Control) meta-model to specify access rules (Aedo et al, 2003; Díaz et al, 2005; Díaz et al, 2006). The RBAC paradigm (ANSI, 2004) is a most convenient option to establish access policies in a flexible, easy to maintain way (Barkley 1995, Ferraiolo et al, 1999). The key RBAC hypothesis is that

roles (i.e. responsibilities) are much more persistent than users. Once the responsibilities of an organization are defined they rarely change; what does usually change is the user or users that exercise a specific responsibility in a specific situation. Consequently, an access policy based on assigning permissions to the roles and then allocating users into the appropriate roles is much more stable and easier to maintain than user or group-based approaches.

The rest of the paper is organized as follows. First, a short introduction to the concept of RBAC and a briefly discussion of its main benefits is given in section 2. In section 3 we look at the ARCE system in section 3. Section 4 focuses on the model-based paradigm that has been used to specify and assess the different access requirements of this system. We finish by drawing some conclusions about the benefits of using RBAC to specify access policies in the context of EMS.

2 RBAC IN A NUTSHELL

RBAC regulates the access to resources based on organizational entities called roles (ANSI, 2004). The key idea is that, instead of granting privileges directly to individual users, privileges are assigned to roles, and user are made members of adequate roles. A role represents a job function or a set of responsibilities for a set of users holding that role, together with the privileges granted to them. In RBAC literature the privileges are called permissions, and they can be specified at two levels of abstraction. High-level permissions are composed by a function (e.g. *read a new*) and a role (e.g, *L9*) as in (Ferraiolo et al, 1999) so that access rules are close to the stakeholders' view of the system (e.g. <*L9, read a new*>). Low level rules are defined in a more general way (ANSI 2004) as a system object (e.g. a *file*), an operation defined for that object (e.g. *read*) and a role (e.g. <*L9, read, file=new07.xml*>. In this case, objects are the resources to be accessed by users, and operations represent all actions that can be performed on the system. In any case, privileges are granted to roles by adding permissions for that role using the permission-assignment relationship (*Has* relationship in figure 1), while users are made members of roles by means of the user-assignment relationship (*Assumes* relationship in figure 1).

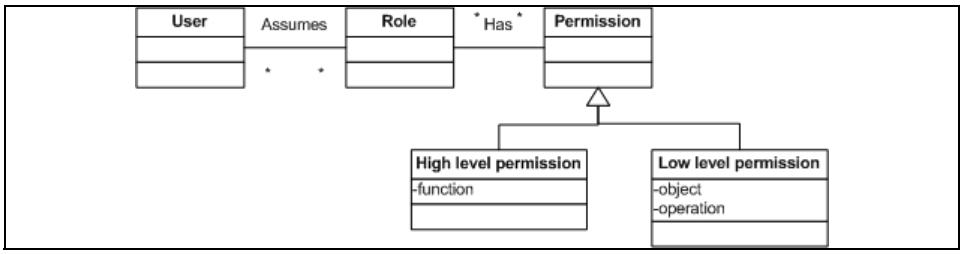

Figure 1: RBAC access rules

Other basic elements and relationships of RBAC include:

- **Role hierarchies**: are an effective means of structuring roles which reflects the organization's lines of authority. Hierarchies allow senior roles (more powerful in terms of permissions) to inherit permissions defined for junior roles (less powerful). Adding hierarchies, the roles structure becomes a tree or a graph used to gather authority, competence and responsibility in a natural way (Barkley et al, 1995).
- **Constraints**: represent limitations imposed to some RBAC elements, normally the user-assignment relationship. The most common is the separation of duty (SoD), that refers to the partition of some critical tasks, splitting the permissions needed to perform them into several roles that are mutually exclusive, so that a single user cannot be assigned simultaneously to these roles. Thus, in order to accomplish a critical task, more than one user is required, ensuring that fraud can not occur without deliberate collusion of several users. Constraints can be static or dynamic.

In the web arena, where the number of users becomes unmanageable, RBAC mechanisms are a most convenient approach to deal with security rules in an efficient and easy to maintain way (Ferraiolo et al, 1999). Firstly, permissions are expressed using roles and operations that belong to the domain of application so that they are close to the organizational perspective and, therefore, it will be easier to test with stakeholders their correctness and effectiveness. Secondly, access rules are more stable since in any organization roles rarely ever change. Which changes more regularly is the user or users that hold such role. Since RBAC rules depend on roles they tend to be quite persistent and the fewer changes are required to maintain our policy the more robust and less prone to error it

will be. Indeed, some empirical studies demonstrate that RBAC policies make possible to reduce considerably the management efforts (Kropp y Gallaher, 2001; Gallaher et al, 2002).

In the particular case of EMS, where roles have to be clearly defined in terms of the access privileges they have and users have to be trained to assume different roles during the crisis (Turoff et al, 2004), the RBAC paradigm seems to be quite adequate. Permissions defined as <role, operation> will be specified at design time, ensuring that the operation protocol is established clearly and tested with the stakeholders. Afterwards users will be allowed to assume the different roles they would be able to play. RBAC policies do not impose any kind of constraint in the number or kind of roles a user can be assigned to, and they can even be assigned at runtime since this operation does not interfere with the core of access policy that depends on the roles. Thus, users could assume any role during the emergency situation as long as they are trained to perform the responsibilities of such role using the EMS.

3 THE ARCE WEB SYSTEM

ARCE is a web-based EMS oriented towards enhancing the management of multinational disaster response within the scope of the Latin-American Association of Governmental Organisms of Civil Defence and Protection (AIGO), a multinational organism made up of representatives from 21 Latin-American countries. It is a platform to share up-to-date and reliable information among the AIGO associates and other agents in order to orchestrate an integrated and efficient response, respecting each member's autonomy. ARCE isn't expected to be used in emergency situations exclusively. It has two operation modes, routine and emergency, since if the EMS is not used on a daily basis it won't be used when an emergency occurs.

3.1 Routine mode of ARCE

In this operation mode ARCE offers a communication service and a news board. Communication is supported among the associates and other related institutions or external organizations (e.g. NGOs) as well as among the member of specific communities through messages and a chat. The **messages module** uses an information flow policy to distribute messages among the different agents. Information flow policies are aimed at ensuring that users only access the information for which they are authorized. For this purpose, both users and information have to be classified. In ARCE, users are classified using the roles in table 1 and information is categorized as strategic, operational, technical, general and public. Information flows from one role to another according to the rules in Figure 2, When a user is about to send a message, first she has to decide the kind of information to be sent and then she will be able to select who is going to receive it from a list of potential targets. For instance, an L2 role will not be able to send strategic information although she could receive it from the upper level, and she can send operational information to users holding an L2, L3 or L4 role. Communication also includes a **chat module** used to set up forums on different issues concerning civil defence. Finally, there is a **news board** where several roles, including external organizations, can post news. For instance the National Geographic Institute of Spain and the CIIFEN (International Center for Research about "El Niño") provide news to keep both the community and the society informed. For trustworthiness purposes, only authorized users can post news.

Roles		Description
Associated Organism (One per each country of AIGO)	L1	Strategic level: General Director
	L2a	Operational level General Vice-Director
	L2b	Operational level: Chief of the Regional Organism
	L3a	Technical level: expert or technical
	L3b	Technical level: Expert in natural risks
	L3c	Technical level: Expert in technological risks
	L4a	Operational level: Operations Chief at the 24H Coordination Centre, Operations chief at the organism
	L4b	Operational level: Operator at the 24H Coordination Centre
National invited organism (Each	L5	Informative level: National agencies and organisms, which can invite users with same role.

associated organism can invite as many as wanted)	L6	Informative level: National agencies and organisms, which can't invite users.
	L7	Informative level: Non governmental organizations which can't invite users.
International invited organism (AIGO can invite as many as wanted)	L8	Supranational organizations (e.g. NATO or EU)
Information provider (it will be invited by an associated organisms or AIGO)	L9	News provider
System administration	Technical administrator	Responsible for maintenance operations concerning the whole system
	Local administrator	Responsible for maintenance operations concerning a specific organism (of users and organism's information)
Public	Anonymous	Any non authenticated user

Table 1. Roles in ARCE

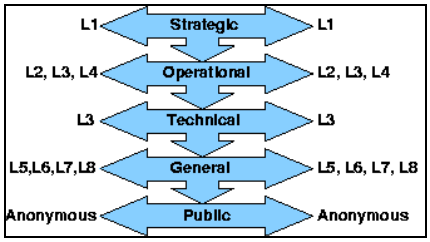

Figure 2: Information flow policy in ARCE

3.2 Emergency mode of ARCE

In this operation mode, countries affected by a disaster can manage the emergency by informing the other associates, preparing a preliminary request for urgent resources, elaborating a more detailed request and coordinating the assistance offered by other countries. Since all the entities involved in an emergency, whether the owners or the assistance suppliers, have access to updated and reliable information about the real needs and how they are being solved, there are no problems of overlapping aid. Indeed, before a supplier initiates the protocol to physically send any help its assistance has to be approved by the emergency owner. If assistance is required, the emergency owner can ask for resources (see Figure 3) which are classified using a multilingual catalogue of means and resources, that has been accepted by all AIGO associates and that also includes the SUMA[1] catalogue of humanitarian supplies. Whenever a request for assistance is received, the rest of the associates are notified by e-mail, and eventually by Fax or SMS, so that they can access the system to see what the emergency owner is asking for and how they can help (see Figure 4). For each emergency, there is updated information on which resources are requested, what quantity was originally needed and how many items have been already supplied. Thus each associate can decide what to contribute taking into account what the others are doing. The assistance is always subdued to a negotiation process between the emergency owner and the assistance suppliers, so that suppliers cannot send anything until the emergency owner has officially accepted the offer. All the actions performed in the system can be audited using the historic mechanism which records information on what was done in past emergency situations managed by ARCE.

[1] http://www.disaster-info.net/catalogo/English/dd/Ped/sumacat.htm

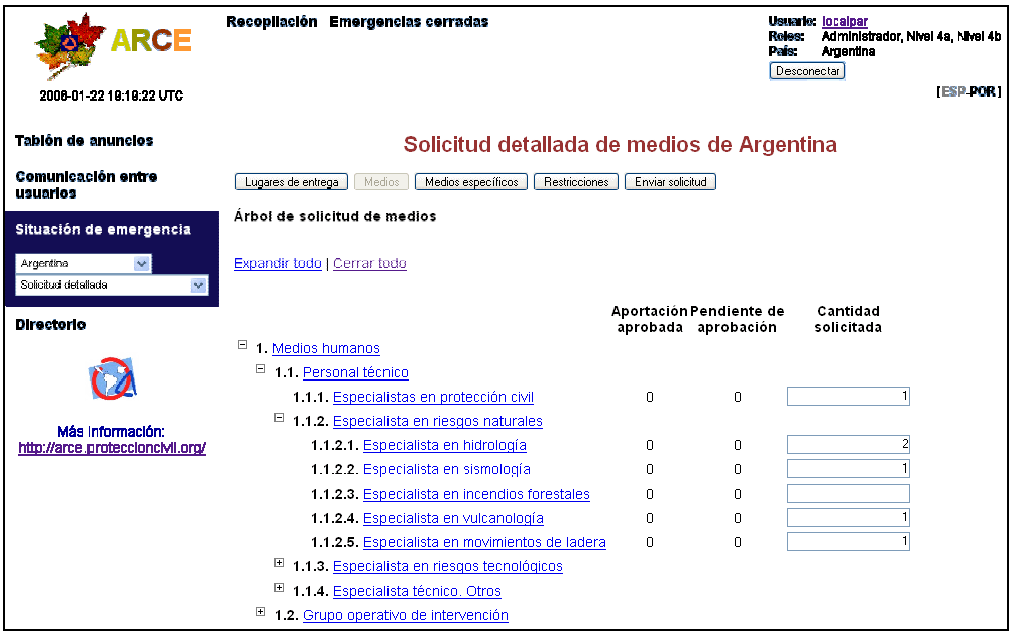

Figure 3: A request from the point of view of an emergency owner

Figure 4: An assistance from the point of view of an assistance supplier

4 MODELLING THE ARCE COMMUNITIES USING RBAC

One of the main features, and at the same time one of the main design challenges, is the diversity of responsibilities and kinds of users that make up the spectrum of potential ARCE stakeholders. On the one hand, we have a number of governmental agencies which have complex and diverse organizational structures, so that our design has to meet the needs of all of them providing a common workplace but respecting their divergences. On the other hand, there are a number of users (like invited organizations, ngos, journalists, anonymous users...) who can also access the system in order to keep themselves informed or even to contribute to mitigate a specific disaster. In order to deal with different access rights the basic principles of RBAC have been adopted and, therefore, the rules governing the system access are specified using a hierarchy of roles. In particular as we said before, we have used the ADM web engineering method and its underlying security meta-model, MARAH.

The expressiveness and flexibility of RBAC were the main reasons in applying this paradigm in order to cope with the access requirements of the different user communities of ARCE. In particular, we used the MARAH meta-model that provides designers with mechanisms to specify the rules that ensure a proper operation of any kind of web system. One of MARAH basic assumption is the use of abstractions and concepts that belong to the hypermedia/web domain in a broad sense, so that the model can be integrated into a hypermedia design method such as the ADM to provide a holistic approach dealing with different kinds of requirements. Thus while MARAH provides the formal components to specify an access policy (including roles, teams, objects, composition mechanisms, users, authorizations and so on) ADM offers a number of design models based on such components (e.g. users diagrams, structural diagrams, authorization rules, user allocation and so on) that make it possible to specify the policy, as well as other design perspectives (structure, navigation, presentation, interaction), at different levels of abstraction by means of a number of easy to understand diagrams. A complete description of MARAH can be found in (Aedo et al 2003, Díaz et al 2006) and ADM is fully presented in (Díaz et al, 2005).ADM establishes a complete, systematic, iterative, flexible and user-centred development process that consists of three phases: Conceptual and Detailed Design phases, which address design requirements from different abstraction levels; and the Evaluation phase, which is based on the assessment of prototypes and design models. Each phase is decomposed into some activities, each of which generates various models (Díaz et al, 2005). In ARCE we applied the method in several cycles, each of which has taken a different approach. The assumption of this iterative process has been considered quite useful both for developers, who were able to test their ideas and solutions in a realistic situation, and by stakeholders, who have adopted a quite positive attitude due to their active involvement in the development process.

4.1 First cycle: analysis through rapid prototyping

At the beginning of the project, the basic goal was to establish a set of feasible requirements as well as to engage stakeholders in the development process. In this case, the ADM evaluation phase, with prototyping and evaluation as main activities, played a central role. This first cycle consisted of an iterative process of analysis and evaluation. Analysis was done using a typical working group technique, where some web engineers and people with technical knowledge in civil defence issues discussed the system services. Rapid throw-it-away prototypes were used to support requirements elicitation and validation through evaluation processes. Evaluations were mainly oriented towards collecting and refining requirements and the method was an empirical evaluation of interface mock-ups. Particular emphasis was done on the study of different user roles and permissions.

4.2 Second cycle: producing a common design

The next step was to focus on technical solutions involving the stakeholders in this process. The idea was to deepen on the basic features and services of the system producing a common conceptual design that could be adapted later to the needs of each associate. In this second cycle, the basic activities are Conceptual Design and Evaluation of prototypes and design models. At the Conceptual Design phase design solutions are expressed in terms of expected types of elements that will be later translated into concrete entities in the Detailed Design Phase. In the ARCE project, the Conceptual Design offered an effective solution in establishing a coherent structure and function, providing a number of clear models which can be discussed with stakeholders with only a brief explanation on the notation. Moreover, compared to the use of prototypes, Conceptual Design models hide details that can deviate the users attention to issues, such as colours, backgrounds and so on, which are not relevant when trying to define generic and abstract features of the system. This second cycle was again an iterative process devoted to refining both design models and requirements. Design was focused on the system structure (*Structural Diagram* model), the services offered to the users (*Functional Specifications* model) and the access policy (*Users Diagram* and *Authorization Rules* models). These latter models are shown in figures 5 and 6 respectively and gather the roles structure (graphical representation of the elements in Table 1) and the high-level access rules (see figure 1).

In order to have more expressive and powerful user's structures, MARAH introduces to the roles hierarchy the concept of team. A role is an organizational position or job function that appears in the application domain (e.g. the technical administrator of the system), whereas a team is an aggregation of roles defined to represent groups of interest (e.g. the participants of a chat on prevention of natural risks), collaborative teams (e.g. the International team in ARCE that aggregates international associations and other international communities that can be invited to provide assistance in a specific emergency situation) or just to alleviate administrative tasks (e.g. ARCE users). Roles and teams support composition mechanisms in order to deal with complex user structures and can be defined at different levels of abstraction so that they can be validated in the earlier phases of the development process. Access rules are assigned to roles and teams and they are propagated through the users structure following a number

of well-defined rules. Each user will be associated with one or more roles and not only will the role assumed by a specific user determine her capabilities to modify or browse the information, but also the country she belongs to, since ARCE is implemented using context dependent roles. Finally, roles are also the basis to establish an information flow policy that is used to push valuable information to each ARCE user (see Figure 2).

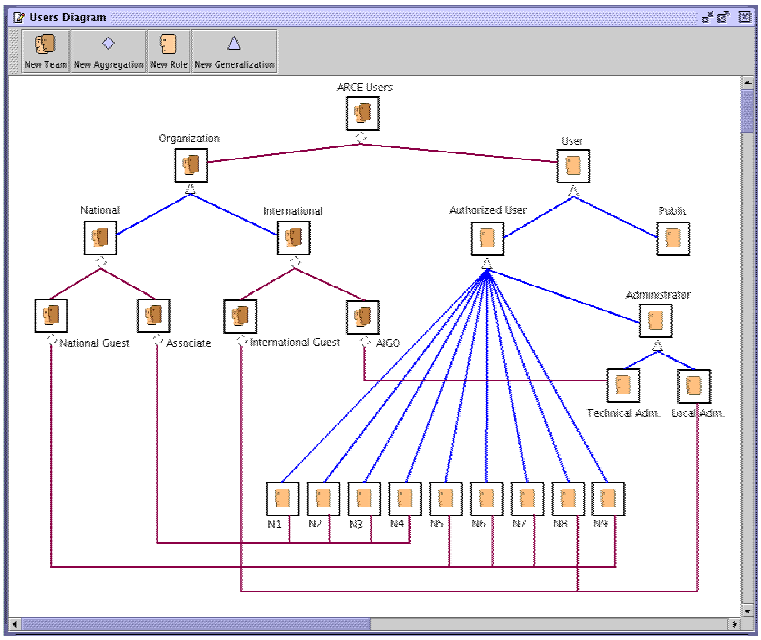

Figure 5: ARCE Users Diagram

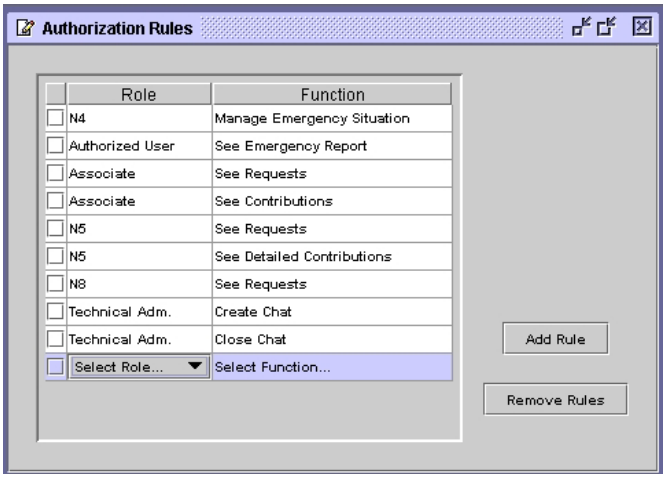

Figure 6: Example of high-level authorization rules

All these design models were assessed with the stakeholders to refine them. Sometimes such analytical evaluation gave place to changes in the prototypes and even in the requirements. Empirical evaluations of the prototypes were also performed in a number of simulation exercises with a view to assessing the system utility. These exercises, where real users took part, made it possible to improve the system.

4.3 Third cycle: adapting designs to each organization

The next step was to keep on refining the design and testing to ensure it suited the specific organizational features of each associate. In this third cycle, Analysis activities were practically anecdotal and the ADM Detailed Design came onto the scene to define concrete instances of some conceptual models. All the models of the

Conceptual Design were developed and refined and Evaluation continued as a basic activity to assess both design models and prototypes.

In particular, conceptual models representing the navigation structure and the presentation features were built. During the Detailed Design phase entities and services are fully specified. Such specific elements can be identified in a declarative way (e.g. using an identifier, url or uri) or in a procedural one (e.g. by means of scripts or database queries). Indeed, most instances of nodes and contents in ARCE were defined in a procedural way by accessing a PostgreSQL database. The access policy is also specified in a more detailed way in terms of concrete subjects and objects, that is, using low-level permissions (see Figure 1) by means of two models: the *Access Table* and the *Users Assignment*. The Access Table gathers the access rights each subject instance can exercise with each object instance (each page and item in the web system). Its values are computed automatically from the high-level design products (see figures 5 and 6) by granting each role or team the minimum clearances needed to execute each atomic operation making up the high-level function. For example, if role N4 can execute the function "Create emergency report", she has to be able to create a new Report, as well as to modify all the fields included in such page (Emergency Location, Type, Damages…). Specific users are associated roles through the *Users Allocation* model. Thus, users will be able to exercise the abilities specified for the roles they belong to according to the principles of RBAC models. A user can be associated to more than one role in order to increase flexibility.

5 CONCLUSIONS: ON THE BENEFITS OF RBAC TO MODEL EMS COMMUNITIES

Emergency and crisis management involve many different stakeholders who make up virtual communities with different characteristics, needs and responsibilities. A useful EMS should cope with this diversity by providing each user with the right information and services in the right way and in the right moment. In this work we have exclusively focused this problem from the perspective of the access policy that will enable the specification of access rules in a flexible and efficient way. The multiple HCI principles to be considered in order to properly deliver the information and services go beyond the aims of the work presented here. In particular, we advocated for the use of the RBAC paradigm and its widely known advantages in specifying organizational policies (Barkley, 1995; Ferraiolo 1999). Our approach consists on applying a RBAC meta-model within the context of a development methodology for web systems, so that access requirements can be specified at different, integrated levels of abstraction, relating them to other requirements (functional or non-functional). From this experience we can draw a number of benefits, both from the use of RBAC models and for their application within an engineering method that are summarised in the following paragraphs.

RBAC is flexible and expressive enough to capture the access needs of different kinds of EMS communities. Since the EMS is accessed by different agents, the access policy has to be carefully designed to support enough roles as to provide a certain degree of autonomy and control while maintaining reliability and efficiency. In order to avoid improper access and modification of data, ARCE relies upon the use of RBAC policies and authentication mechanisms, so that only authorized users can modify the information provided by the system. Moreover, the information flow policy ensures that messages received from the system are trustworthy, since only authorized users can send messages to those requiring or needing that information. Though in an emergency situation it cannot be predicted who will undertake a specific role (Turoff et al, 2004), it is also obvious that a user cannot assume a role she has not been previously trained for, as no organization will allow any kind of anarchical procedure where a user decides on her own to assume a role for which she is not prepared nor authorized. In such a scenario, the use of roles, hierarchies of roles, teams and the possibility of assigning each user's different roles provides a powerful and flexible specification mechanism to gather the needs of many different kinds of communities in terms of access rules. For this purpose, the use of constraints for user allocation (where the assignment of a user to a role depends on a certain condition) is also quite useful. For example, the number of times a specific user has played a role in simulation exercises might be used to dynamically determine whether she is allowed or not to assume such a role in an emergency. Furthermore, in a multinational environment the access policy has to be flexible enough to support different organizational policies while maintaining a global coherence and consistence. In our case, this requirement was fulfilled thanks to the application of a web engineering method. During the Conceptual Design stage we established a common structure and access policy adapted to each organization during the Detailed Design.

RBAC can improve the communication among designers and stakeholders. RBAC abstractions (basically the concepts of role, hierarchies of roles, operation, authorization and user allocation) make the specification of the access policy possible using a language that is familiar to the stakeholders, since it is based on organizational entities. Using the ADM, access modelling is addressed at the earliest development stages by producing a number of easy to understand models, so that stakeholders can be involved in analytical and empirical evaluations to assess the access policy before the system is already implemented. The discussions between the ARCE stakeholders and

designers to define the Users Diagram (the model where roles and teams are identified) and the Authorization Rules (where roles and teams are allocated the functions they can perform) were particularly useful to clarify the different responsibilities that should be considered by the EMS. Indeed, the design models became intellectual tools to ponder over how organizations were doing things and even to detect problems in the organizational structure (such as duplication of efforts, erroneous assignment of responsibilities, etc.) Translating this policy into a prototype enabled us to validate and improve these products in a number of simulation exercises where several associates took part in an emergency practice.

Moreover the integration of access modelling with other design views addressed by the ADM, such as information structure, presentation features, navigation capabilities or interaction mechanisms, gave place to a holistic design where requirements of different nature (structure, navigation, presentation, interaction and access were expressed using the same elements).

ACKNOWLEDGMENTS

This work has been funded by ARCE ++ project from "Ministerio de Educación y Ciencia" (TSI2004-03394). ARCE is being developed in collaboration between "Universidad Carlos III" and "Dirección General de Protección Civil y Emergencias" (Spain).

REFERENCES

1. Dykstra, E. H. Towards an International System Model in Emergency Management: information communication and coordination in emergency management- public and private sector approaches in different countries and systems. Communication. Public Entity Risk Institute (PERI), September 22-26, 2003.
2. Turoff, M. Chumer, B. Van de Walle and X. Yao, "The design of a dynamic emergency response management information system", Journal of Information Technology Theory and Applications (2004) 5:4, 1-36.
3. Díaz, P., Sanz, D., Montero, S. and Aedo, I. Integrating Access Policies into the Development Process of Hypermedia Web Systems. In Web and Information Systems Security. Eds. Ferrari, E. and. Thuraisingham, B. Idea Group Inc. pp. 149-172. 2006.
4. Brose, G., Koch, M. And Löhr, K.P. Integrating Security Policy Design into the Software Development Process. Technical Report B–01–06. Freie Universität Berlin, Nov. 13. 2001.
5. Aedo, I., Díaz, P. and Montero, S. A methodological approach for hypermedia security modelling. *Information and Software Technology*, 45(5), 2003, pp. 229–239.
6. Díaz, P., Montero, S. and Aedo, I. Modelling Hypermedia and Web applications: the Ariadne Development Method. Information Systems 30(8): 649-673. Dec. 2005.
7. ANSI INCITS 359-2004, American National Standard for Information Technology; Role Based Access Control. 2004.
8. Barkley, J., Ferraiolo, D. and Radack, S. An Introduction to Role-Based Access Control. NIST CSL Bulletin, December 1995.
9. Ferraiolo, D.F., Barkley, J.F. and Kuhn, D.R.: A Role-Based Access Control Model and Reference Implementation within a Corporate Intranet. ACM Trans. on Information and Systems Security, 2(1), February (1999), 34-64.
10. Kropp, B. and Gallaher, M. P. Access to cost savings: Role-based access control systems can save organizations time and money. Information Security Maganize (April). 2001.
11. Gallaher, M.P., O'Connor, A.C. and Kropp, B. The economic impact of Role-based Access Control. Planning Report 02-1. National Institute of Standards & Technology. March, 2002.