Computer Science and Information Systems 15(2):257–272 https://doi.org/10.2298/CSIS170227001Z

Interoperability in the Emergency Management. A Solution based on Distributed Databases and P2P Networks

Marcelo Zambrano, Francisco Pérez, Manuel Esteve, and Carlos Palau
Distributed Real-Time Systems Lab, Universitat Politècnica de València
Building 4D, 2nd floor, POB 52
Camino de Vera s/n, 46022 Valencia, Spain
oszamvi@doctor.upv.es, frapecar@upvnet.upv.es,
{mesteve, cpalau}@dcom.upv.es

Abstract. To successfully confront a disaster, it is necessary the coordinated and collaborative participation of multiple agencies related to public safety, which provide a response consistent with the requirements of emergency environment and all those affected. For this, is necessary the permanent information exchange between the involved agencies that allows to joint its efforts and to face the emergency of the best possible way. This article describes the interoperability platform architecture, which enables agencies involved in management of an emergency, exchange information using their own information systems and computer tools. The architecture core is inside its Shared Information Space, which manages it as a single storage entity, all information coming from the information systems integrated to the platform. It is founded on a non-relational distributed database and a P2P communications network, to share out the workload between all the platform nodes in order to award availability and scalability to the architecture.

Keywords: Distributed database, emergency management, information exchange, information system, interoperability, peer-to-peer networks.

1. Introduction

Emergencies can be defined as unforeseen situations, caused by a damaging incident or disaster, which endanger the environment, property and people's life. To effectively manage an emergency is necessary the participation of multiple agencies related to security and public safety, which allow actions according to the particularities of the incident and the requirements of all those concerned [6] [2] [10]. This diversity of skills, abilities and knowledge, which is essential for integral and comprehensive emergency management (EM), is also the main drawback for the agencies involved to work together and focus their efforts in the same direction, considering that each have their own resources, technology, method, etc. To solve this problem, is necessary the permanent exchange of information between all these agencies engaged, which allows

them to coordinate their operations and collaborate to manage the emergency in the best possible way [1].

Interoperability can be defined as the capability of two or more systems to exchange information and use it to achieve their objectives [14]. In diverse and complex environments, as in the case of EM, interoperability is the key to the coordinated and collaborative operation of all the resources involved [24]. Organizations such as the Federal Emergency Management Agency of the United States (FEMA) [9], the International Organization for Standardization with its Technical Committee for the Protection and Security of Society (ISO 223) [16], the United Nations Office for Risk Reduction (UNISDR) [21], among others, have published standards and recommendations emphasizing the importance of interoperability in EM. This article presents an alternative for the materialization of these recommendations, based on an interoperability platform, that allows the Information Systems (ISs) of the agencies involved, to integrate within a communications infrastructure to share and exchange information. The main contribution of this work is inside its Shared Information Space (SIS), which allows managing as a single logical storage entity, all information coming from the different IS integrated to the platform. The SIS is based on a distributed database (DDB) and a peer-to-peer (P2P) communications network, to provide platform availability and scalability.

The architecture validation was performed through functional tests to a prototype implemented based on the architecture that is described in this article. The tests were realized within a simulated scene for an emergency, in which each IS integrated into the platform, shared information regarding the identification and positioning of response units were supervised by them. This information allowed create a common situational awareness of all the resources deployed in the tests field, which served as starting point for planning and coordination of response and recovery operations.

The paper is divided into five sections. First, an introduction to the proposal and methodology used; the second one, describes the motivation and works that served as the basis for this research; thirdly, it details the architecture and the functionalities of each one of its components; the fourth one, describes the tests of functionality and the results obtained; and finally, the conclusions and final notes for this work are explained.

2. Motivation and Related Work

Among the most important issues to be considered regarding to interoperability in the EM, can be highlight the agencies autonomy, the data heterogeneity and how users access to them. Usually, users are reluctant to use external computer tools, either by affinity with their usual applications or by mistrust and lack of expertise in computer applications that they ignore. Many of Emergency Management Systems enable the information exchange between agencies, through proprietary computer tools set that use a common language and data model (e.g. Coordcom [4], GEMMA [7], DESTRIERO [11]). However, this standardized solution is limited by the usability and scope of these tools (designed by the manufacturer), and do not necessarily meet the particular requirements of all the agencies.

This article presents an architecture for the interoperability platform implementation that permits the ISs of the agencies involved in EM be integrated into a communications infrastructure to provide and / or acquire information using their own systems and computer tools. It has taken as main references for its development, to the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) and to non-relational DDBs (NoSQL DDBs).

The JC3IEDM was created by the NATO Multilateral Interoperability Program to support multinational operations and furnish the exchange of command & control information in tactical environments. It proposes the development of a middleware and the implementation of a single standardized data model to allow the involved ISs to exchange information independently to their proprietary data model and applications (Fig. 1) [18].

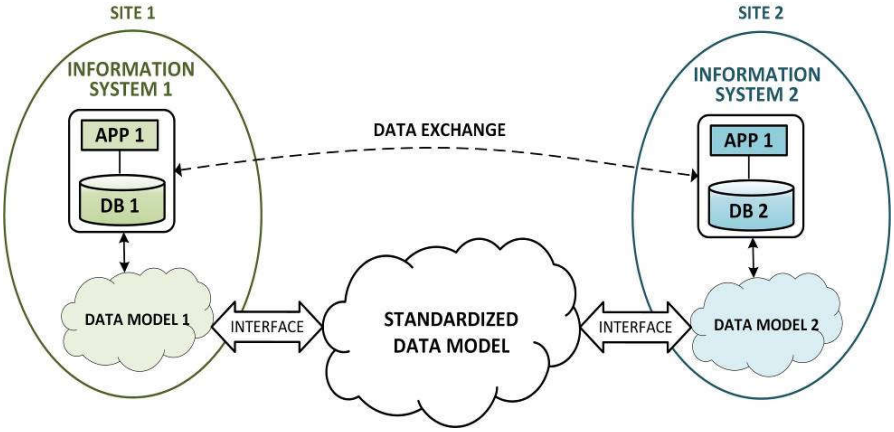

Fig. 1. JC3IEDM

The DDBs allow to take advantage of the multi-agency nature of the EM, to distribute the workload (data processing and storage) and improve performance into cluster nodes. Non-relational databases, also called No only SQL (NoSQL), allow representing and storing each object to be shared, with an independent data schema, facilitating the information exchange and solving the deficiencies of relational databases in terms of heterogeneous data management and scalability.

Figure 2 shows a diagram that summarizes the proposal for data management with NoSQL DDB for this work [5] [17]. The information shared by the ISs is distributed among all the nodes that make up the cluster of the NoSQL BDD and is stored in a standardized data schema, within the Local Storage Spaces (LSSs) of nodes.

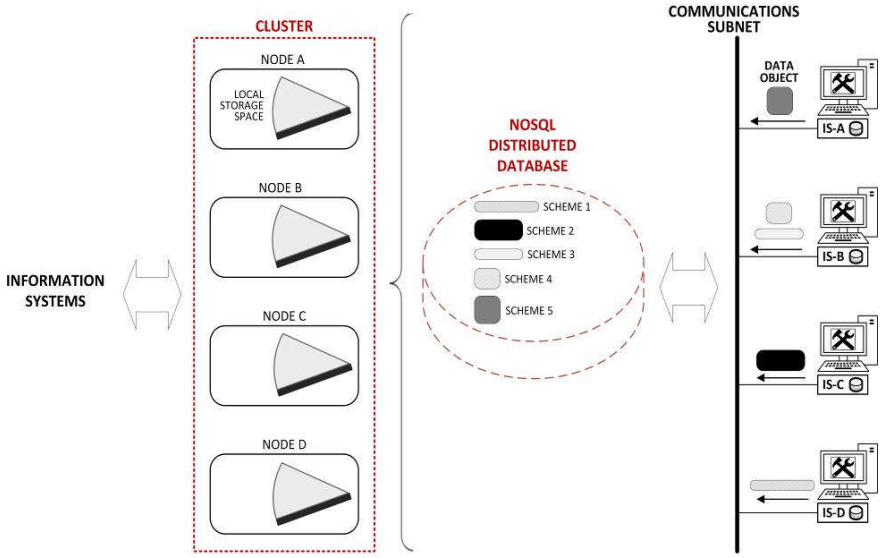

Fig. 2. Non-relational Distributed Database scheme

3. Architecture

The architecture has been designed to support the availability and scalability requirements presented in the EM. It is based on a distributed network infrastructure and a middleware layer, which allows the interchange of information in an independent way to the IS without following the data model used by each of them. The involved agencies use their own systems and computer tools for the information interchange, and the middleware layer adapts the information that comes and goes to them, to the model defined in the platform. The communication between IS and the platform follows a data model based on the standard Efficient XML Interchange (EXI) [22] [13], and the information that is considered as relevant to share, is stored in the no relational DDB conforming the SIS.

It has been split in three main elements to make possible the analysis and understanding of the architecture, as can be seen in the Fig. 3.

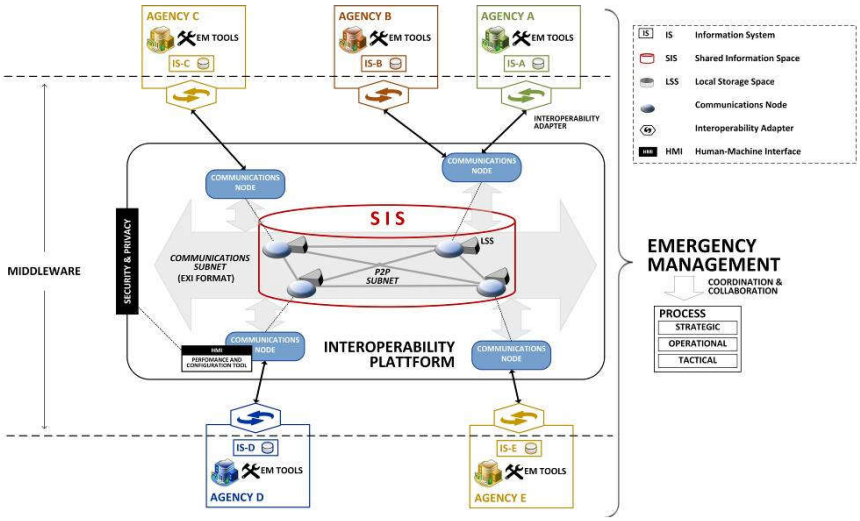

Fig. 3. Architecture

Information System, is a device, equipment or system, registered into the platform and able to feed and/or to get information from the platform thanks to its interoperability adapter.

Communications subnet is the responsible for providing connectivity between the nodes that make up the platform. Its topology and communication links technology, are transparent to the top layer (middleware layer), which expedites its implementation and scalability.

The Middleware layer meets the functions of transceiver between the communications network and the IS.

The architecture has been fully developed under free software, removing dependencies from third party makers (maintenance, updates, etc.) and leaving the door open for personalization and development of new functionalities. Thus, the selected operating system for the communication nodes is Linux, Apache Cassandra as Data Base Manager, Java as the programming language used in all the developed modules for the platform and AngularJS as framework JavaScript for the frontend development in the HMI (Human-Machine Interface).

The middleware layer is the core of this architecture and responsible of allowing the effective interchange of information among the integrated ISs and the platform. It is split in four components: interoperability adapters, communication nodes, SIS and HMI.

3.1. Interoperability Adapters

They are the responsible to adapt the information from the integrated ISs to the platform, following the defined format (EXI) in the communications subnet and vice

versa. Each adapter has an interface to the IS and other to the node, this allows the information that flows between them using web services (WS). The requests and responses from and to the ISs are performed using any typed of WS that have been defined for them (e.g. SOAP, REST, HTTP); while the requests and the response from and to the communication nodes, are performed only using SOAP, in accordance with the platform design and the standardization principles proposed.

Among the communication interfaces, there are two sublayers (transformation and communications) that allow the data format conversion in a bidirectional way. Due to the different data formats and protocols that each IS has, each IS needs its own adapter, and there are as many adapters as ISs are connected to the platform. The Fig. 4 shows a general block diagram for an interoperability adapter.

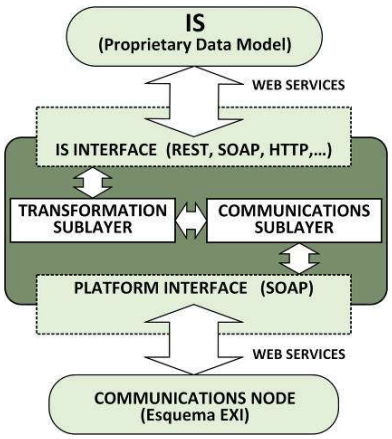

Fig. 4. Interoperability Adapter

3.2. Communication Nodes

They are the entrance gate to the platform. Their main functions are allow the integration of the ISs, store the assigned fraction of DDB, and notify to the registered ISs and the other nodes about any update realized in the SIS information.

The Fig. ***5*** shows a block diagram that summarizes the internal architecture of a communication node. In the diagram is possible identify four primary elements: an user layer, in charge of put within reach of the ISs, the services for the operational parameters configuration of the platform (e.g. ISs registration, notifications subscription, addressing) and the interaction with the SIS (read, write, delete and data updates); an operational layer, in charge of management process and internal node functions, as for example security and privacy, communication among nodes, data management, etc.; two groups of transversal services, in charge of the supervision and security of internal process and node access; and a LSS, which stores the assigned SIS fraction as well as a copy of the registered users and systems in the platform.

The communications with the nodes connected in the cluster and with the ISs integrated through it, are performed by datagrams in EXI format, that inform and alert about any change or update in the available information and/or the platform state. These datagrams should be validated and transformed before to be stored following the format defined in the SIS using the "validation and transformation" module.

It is possible to deploy as much nodes as be required, and each node can serve to more than one IS, depending on the scope of the platform, the node process capability and the requirements that each IS needs about resources, security, availability and scalability.

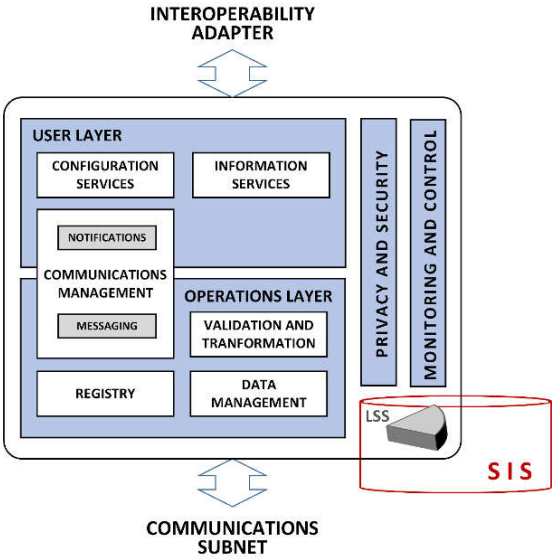

Fig. 5. Communication Node

3.3. Shared Information Space

The SIS is the core of the architecture. It uses a NoSQL DDB and a P2P network to manage the information coming from the ISs, as a unique logic storage space. It has an independent data model different than the one used by the ISs integrated to the platform, and each stored object is defined with a unique key, based on a key-value model following its own data schema. The SIS takes advantage on the distributed behavior in the architecture, to allow the fragmentation and dynamic assignment of the data storage procedure. One of its main advantages is the independence of the objects, which makes transparent the physical location and the data schema to the ISs.

Regarding to the implementation, Apache Cassandra has been used as data base manager, due to its distributed capability and the P2P algorithm used for the information

management [8]. Among its most important features, there are the decentralization, scalability and adaptability about the supported data schemas. Both the workload and the redundancy are customizable, and should be configured according to the reliability, availability and scalability required by the platform. Its internal P2P network has a logic topology not hierarchical in ring, and allows the simultaneous response of multiple nodes to multiple requests (horizontal scalability). The requests, updates, deletes and inserts of information, are managed using the proprietary language Cassandra Query Language (CQL), and the Kundera library provides support to the Java Persistency API (JPA) [3].

The Fig. 6 shows a block diagram that summarizes the internal architecture of the SIS.

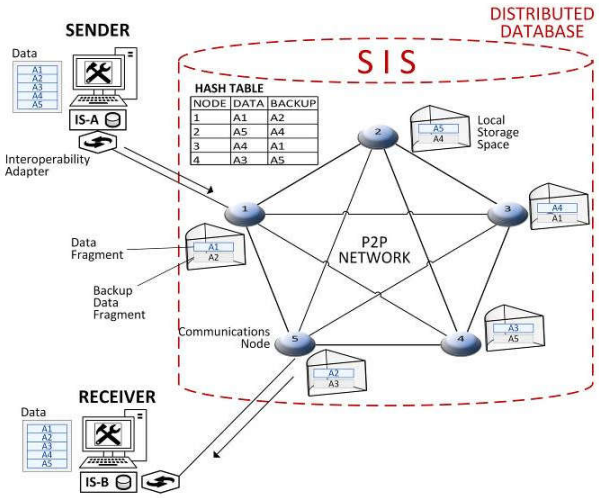

Fig. 6. Shared Information Space

3.4. Communication and Data Management

The communications between nodes, as well as the communications among node and the ISs registered in it, are performed using the standard Efficient XML Interchange (EXI), developed by the World Wide Web Consortium (W3C). The EXI is devised to optimize the performance and the use of resources in networks operating in environments with limited capabilities, as in emergencies (low process capacity and storage in the HOST, limited bandwidth, packet loss, etc.) [22] [13]. It manages the information using a XML schema exploiting the structured nature of the format to optimize the transmission and the data process. The defined EXI schema for the platform is distributed through the communication network, in such way that each node can compress and decompress the objects received or sent, following the diagram shown in the Fig. 7.

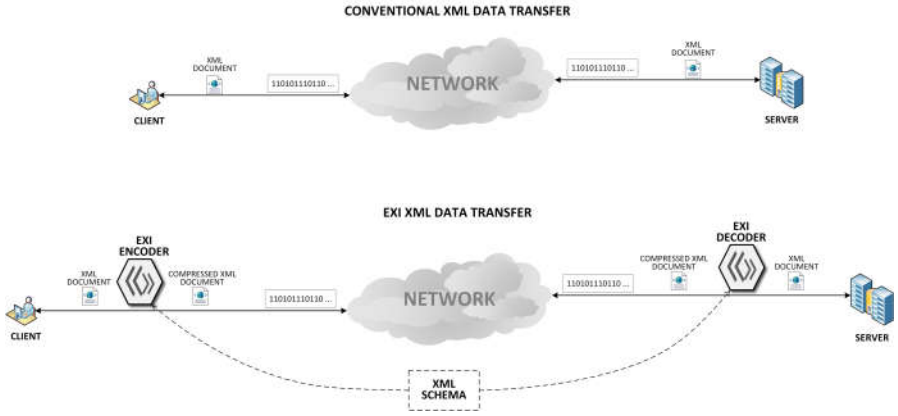

Fig. 7. Comparison between conventional data transfer and another based on EXI schema

Both the sharing and the requirements of information follow the EXI mechanism implemented based on a PUBLICATION/SUBSCRIPTION model, which allows the data and metadata distribution through the communications subnet. Whenever an IS shares information, this is validated, transformed and stored in the SIS to be accessible across each of the nodes inside the cluster.

The ISs should specify the topics related with the information provided, and also with the topics which are interesting to consume. Every time that a new information is shared in the SIS, the local node notifies it to all the registered IS as long as if it was subscribed to the information's topic, about the updated information by the notification service. If an IS considers the information interesting and is subscribed to the topic, can be able to get it from the SIS, transform it to its proprietary data schema and make it available to its computer tools. In the same way, the local node shares the update with the other nodes in the cluster using the messaging service, and the nodes notify to the registered ISs about the new information available. This process is reflected in the diagram of the Fig. 8.

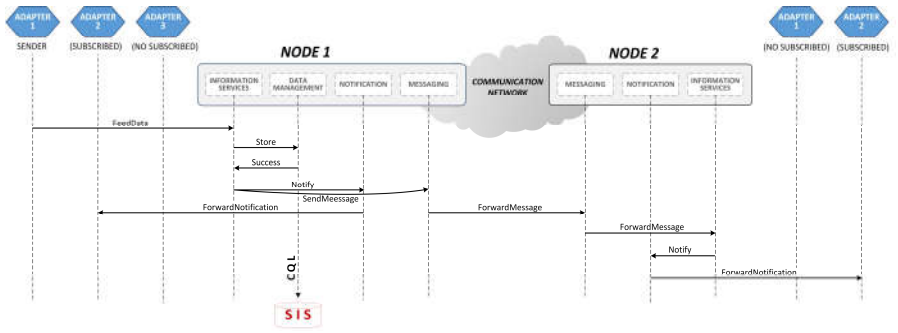

Fig. 8. Notification Process

The first step to integrate a new node into the platform is register and validate it. Once the node is authorized, the node starts to be a part of the Cassandra cluster that shapes the SIS and the other nodes start the communication with the registered node using the subnet. Each node has its own LSS, where stores the portion of the correspond data, according a HASH table created by the Cassandras' P2P algorithm [8] [3].

The Data availability is guaranteed based on multiples copies realized in different nodes (redundancy), which depends on a replication factor (number of copies of the information in different nodes) configured according the required resilience in the platform.

3.5. Human-machine Interface

The accessibility and the privacy of the platform is managed via the HMI, which allows creating users and assigning permissions and profiles, through the "privacy and security" module. It also allows the management and audits of the platform thanks to the "monitoring and control" module.

Each node has a copy of the registry with the users and systems, to be always assure and in every circumstance, the accessibility and the security of the platform

Regarding the communications security, it is managed based on the security protocols HTTPS and TLS.

4. Interoperability Tests and Results

The architecture has been validated by functionality tests to a prototype implemented based on the architecture described in this article. The tests were carried out within a simulated scenario for an emergency, which began with the collapse of the Bolarque hydroelectric plant (Cuenca, Spain), causing a flood that affected the José Cabrera nuclear power station (Guadalajara, Spain), with a possible radiological drain. Three communications nodes were implemented in three different locations (Madrid, Cuenca and Valencia), and through them, three geographic information systems (GISs) were integrated into the platform, responsible for supervising the response units on the field of operations (Fig. 9).

Thanks to the load balancing allowed by the architecture, both of the communication nodes and the GISs with their respective interoperability adapters were implemented on HOSTs with standard hardware and software characteristics, as seen in Table 1.

Each GIS shared through the platform information regarding to the identification and positioning of response units under its supervision. This information allowed creating a common situational awareness of all the resources deployed on the testing field and was used by the tactical and strategic staff of the agencies affected to plan and coordinate emergency response and recovery operations.

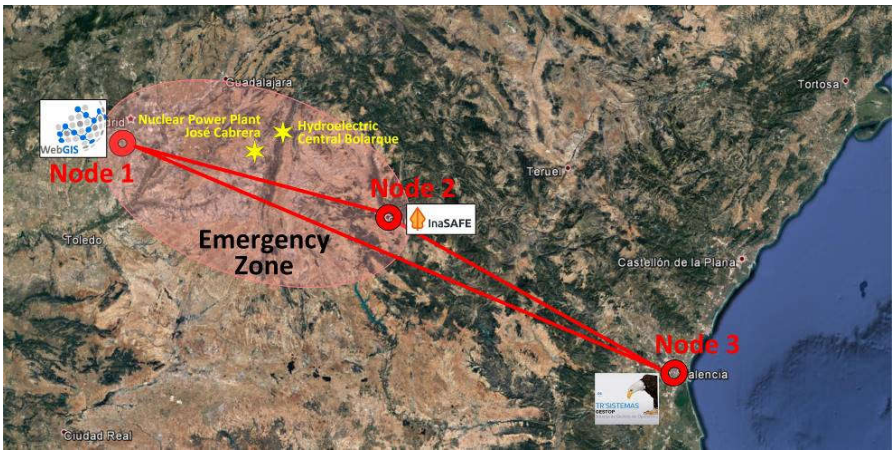

Fig. 9. Testing Scenario

Table 1. Testing Infrastructure

NODE	HARDWARE	SOFTWARE NODE	SOFTWARE IS	CONECTIVITY	SECURITY
1 Madrid	Processor Intel Core i7 2.8GHz RAM 16GB Disk 2TB Net	CentOS 7.0 Open VPN Apache Cassandra 3.2	Ubuntu 15.10 WebGIS [11] (DESTRIERO) Interop. Adapter 1	Internet (VPN)	SSL Certificate VPN1
2 Cuenca	Processor Intel Core i7 2.9GHz RAM 8GB Disk 1TB Net	CentOS 7.0 Open VPN Apache Cassandra 3.2	Ubuntu 15.10 InaSAFE [15] (OpenSource) Interop. Adapter 2	Internet (VPN)	SSL Certificate VPN2
3 Valencia	Processor Intel Core i7 3.3GHZ RAM 16GB Disk 1TB Net	CentOS 7.0 Open VPN Apache Cassandra 3.2	Windows 8.1 GESTOP [20] (UPV) Interop. Adapter 3	Internet (VPN)	SSL Certificate VPN3

Figure 10 shows in the background the GUI of each of the GIS used in the tests and, as the main plane, the WebGIS GUI node 1, shows a consolidation of all the response units on the operations environment.

Likewise, reports with information on the areas affected by the flood and the possible radiological drain were stored and published in the SIS, as shown in Figures 11.a. and 11.b.

During the tests, it was counted on the collaboration of staff of Firemen and Civil Defense of the Madrid Community, who had access to the information and reports generated by the ISs integrated to the platform. After this, a survey was carried out to the tactical and strategic personnel who collaborated in the drill, in order to tabulate their

perception regarding to the supports and helps that the platform could give them. The results obtained are shown in Table 2.

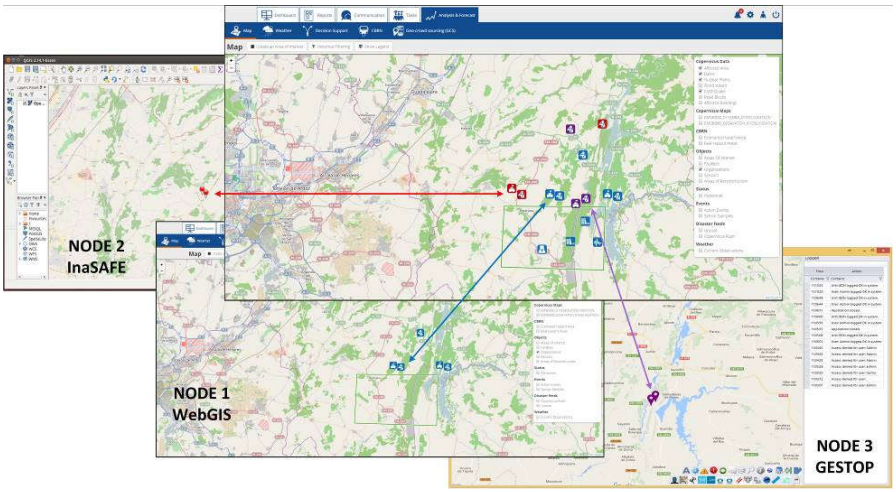

Fig. 10. Response units deployed on the testing environment

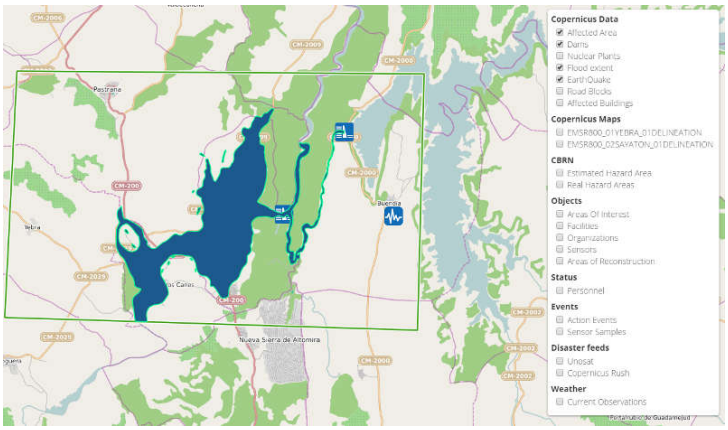

Fig. 11.a. Flood report

100% of the respondents agreed, to a greater or lesser extent, on the usability of the platform. 93% would use the platform either for training or in a real environment, and believe that their agency would benefit from the functionalities provided by it. Equally,

87% of respondents would recommend the use of this platform and agrees with the proposed approach for interoperability between agencies involved in EM.

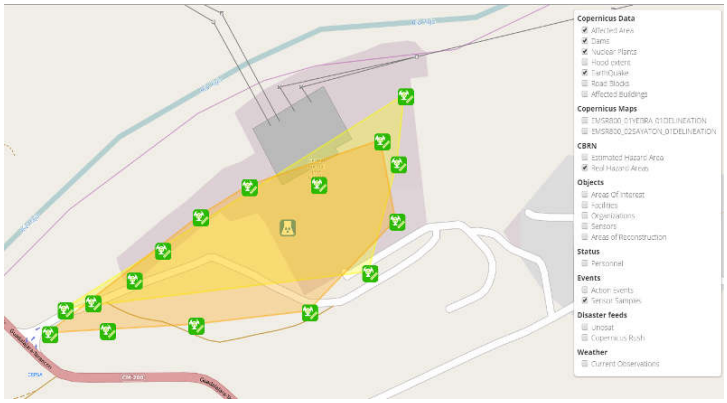

Fig. 11.b. Radiological drain report

Table 2. Survey of the simulacrum staff

QUESTIONS	(1)	(2)	(3)	(4)	(5)
I like the concept proposed for interoperability between agencies involved in emergency management	9	4			1
The key features of the platform are suitable for dealing with a disaster and emergency management	2	11	1		1
The platform offers support for obtain a common situation awareness	2	9	4		
Using the interoperability platform can help improve coordination and collaboration between agencies	4	10	1		
I think, with the interoperability platform, e.g. unnecessary communication can be reduced, thus reducing overall cost	2	8	4		1
The platform supports greater interoperability among organizations and tools involved in emergency management	4	11			
I would recommend the developing adapters for other IS	2	11		1	1
I think this platform is usable	3	9	3		
I consider a priority the interchange of data and functions among agencies	10	4	1		
I would use the platform in “real life”	3	7	3	1	1
I would use the platform for field exercises	4	10			1
I would also use the interoperability platform during the response and recovery phases of an emergency	5	8	1		1
I consider my organization's efforts in the field could benefit from the coordination facilitated by the interoperability platform	3	7	3	1	1
Notwithstanding budget constraints, my organization would see value in funding its own IS adapter and becoming a funding partner in a multi-agency interoperability platform.	1	5	5	2	2
Equivalence: (1) Completely complies - (5) Does not comply with anything					

5. Final Notes

Interoperability between the agencies involved in emergency management, is the key to an integral and comprehensive response that permit to confront any type of disaster that may arise. For this, it is necessary a permanent exchange of information, which allows all the agencies involved, coordinate their operations and collaborate to manage the emergency in the best possible way.

This article describes the architecture for an interoperability platform that allows agencies involved in emergency management to integrate into a communications infrastructure to exchange information through their own systems and computer tools. The core of the proposed architecture is in its Shared Information Space, which allows managing as a single storage entity, all the information coming from the information systems integrated to the platform. The Shared Information Space is based on a Distributed Non-Relational Database and a P2P communications network, to split the workload among all the nodes of the platform, providing availability and scalability to architecture.

The platform was validated by means of a prototype developed based on the proposal described in this article and tested within a simulated scenario for an emergency. The capabilities of the platform were verified to simplify the exchange of information between the agencies, and the personnel involved used the shared information to plan and coordinate the response and recovery operations.

The proposed architecture has been used as support for the development of the interoperability platform of the European project SECTOR [12], of which the UPV is an active part. SECTOR is currently under development and is part of the Seventh Framework Program of the European Union for Research and Technological Development (FP7), which aims to improve the interconnection, coordination and collaboration between emergency and crisis management systems.

Regarding to the future work, a new alternative is being explored for the Shared Information Space implementation, founded on a NoSQL distributed database but document-oriented. This approach uses MongoDB as database manager and allows an asymmetric distribution of the workload (according to the processing and storage capacities of the cluster nodes) and greater freedom in the data schemes of shared documents [19] [23]. On the other hand, the human-machine interface allows the administrators to access the tools of configuration and supervision of the platform; however, its implementation leaves the door open for the development of other proprietary tools, which allow to customize and improve the aids available to users. Currently, work is underway on the development of a tool for the real-time audio and video information exchange, which supports the coordination and collaboration processes between agencies integrated into the platform.

References

1. A. P. Williams, Agility and Interoperability for 21st Century Command and Control, vol. 4, CCRP (2010)

2. Alto Comisionado de las Naciones Unidas para los Refugiados, «Manual para situaciones de emergencia» ACNUR (2012)
3. Apache Software Foundation, «Apache Cassandra» (2017). [Online]. Available: http://cassandra.apache.org/doc/latest/architecture/index.html
4. ATOS, Safeguarding your citizens and assets with Emergency Management, ATOS (2014)
5. B. G. Tudorica y C. Bucur, A comparison between several NoSQL databases with comments and notes, IEEE, pp. 1-5. (2011)
6. B. Wayne, Guide to Emergency Management and related terms, definitions, concepts, acronyms, organizations, programs, guidance, executive orders & legislation, FEMA (2008)
7. Coordcom, «Carmenta» (2017). [Online]. Available: http://www.carmenta.com/en/products/carmenta-coordcom/
8. DataStax, Apache Cassandra Documentation, DataStax (2012)
9. Department of Homeland Security US, «Federal Emergency Management Agency» (2016) [Online]. Available: http://www.fema.gov/
10. Federal Emergency Management Agency, Course IS-0230.d: Fundamentals of Emergency Management (2015)
11. FP7 European Union, «DESTRIERO» (2017) [Online]. Available: http://www.destriero-fp7.eu/
12. FP7 European Union, «SECTOR» (2016) [Online]. Available: http://www.fp7-sector.eu/.
13. G. Jaiswal y M. Mishra, Why Use Efficient XML Interchange Instead of Fast Infoset, IEEE, pp. 925-930. (2013)
14. IEEE, IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, New York: Institute of Electrical and Electronics Engineers, (1990)
15. Indonesian and Australian Goverments, «InaSAFE» (2016) [Online]. Available: http://inasafe.org/
16. International Organization for Standardization, «ISO/TC 223 Societal security» (2016) [Online]. Available: http://www.isotc223.org/
17. J. Han, E. Haihong, L. Guan y J. Du, Survey on NoSQL Database, IEEE International Conference, pp. 363-366. (2011)
18. NATO, Overview of the Joint C3 Information Exchange Data Model, North Atlantic Treaty Organization - MIP (2012)
19. R. P. Padhy, M. R. Patra y S. C. Satapathy, RDBMS to NoSQL: reviewing some next non-relational databases, vol. 11, pp. 15-30. (2011)
20. TR'Sistemas, [Online]. (2016) Available: http://www.trsistemas.com/productos.php
21. United Nations, «The United Nations Office for Disaster Risk Reduction» (2017) [Online]. Available: http://www.unisdr.org/
22. Y. Doi, Y. Sato, M. Ishiyama, Y. Ohba y K. Teramoto, XML-Less EXI with Code Generation for Integration of Embedded Devices in Web Based Systems, IEEE (2012)
23. Y. Li y S. Manoharan, A perfomance comparison of SQL and NoSQL databases, Department of Computer Science, University of Auckland, pp. 15-19. (2013)
24. Zdravković, M., Noran, O., Panetto, H., Trajanović, M.: Enabling Interoperability as a Property of Ubiquitous Systems for Disaster Management. Computer Science and Information Systems, Vol. 12, No. 3, 1009–1031. (2015)

Oscar Marcelo Zambrano Received the Engineering degree in Electronics and Networks Engineering from Escuela Politécnica Nacional, Quito - Ecuador, in 2001 and Magister in Business Administration in 2009; and got a scholarship from Ecuador to study a PhD in Telecommunications at Universitat Politècnica de València Spain. He has over 15 years' experience in the computer and telecommunications areas in Ecuador,

and his current research interests are real time applications for disaster and emergency management systems.

Francisco José Pérez Received his B.Sc. and Ph.D (Dr Ing) degrees, both in telecommunication engineering, from the Universitat Politècnica de València in 2011 and 2017, respectively and right now he is geting his M.Sc. in Big Data Analytics. He currently works in the Distributed Real-Time System Lab as researcher and technical manager. He is involved in technical definitions and development task in several R&D European and national projects.

Manuel Esteve Domingo received both his M.Sc. in computer engineering and his Ph.D. in telecommunication engineering (Dr.Ing.) from the Universitat Politècnica de València in 1989 and 1994, respectively. He is Full Professor in the Escuela Técnica Superior de Ingenieros de Telecomunicación at the Universitat Politècnica de València (UPVLC), and he leads the Distributed Real-Time Systems research group. Prof. Manuel Esteve has more than 20 years of experience in the ICT research area in the area of Networking. Nowadays, he is managing several R&D projects at regional, national and international level. He has collaborated extensively in the R&D of projects for the government agencies, defence and EU-FP7 acting as chairman of the agreement between Spanish MoD and UPVLC. He is author and co-author of more than 100 research papers.

Carlos Enrique Palau received his M.Sc. and Ph.D. (Dr.Ing.) degrees, both in telecommunication engineering, from the Universitat Politècnica de València in 1993 and 1997, respectively. He is Full Professor in the Escuela Técnica Superior de Ingenieros de Telecomunicación at the Universitat Politècnica de València. He has more than 18 years of experience in the ICT research area in the area of Networking. He has collaborated extensively in the R&D of multimedia streaming, security, networking and wireless communications for government agencies, defence and European Commission. He has been the main UPVLC researcher in the FASYS project, which has funded this work. He is author and co-author of more than 120 research papers and member of the TPC of several IEEE, ACM and IFIP conferences.

Received: February 27, 2017; Accepted: February 16, 2018.