INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 12(4), 550-561, August 2017.

A Solution for Interoperability in Crisis Management

F.J. Pérez, M. Zambrano, M. Esteve, C. Palau

Francisco J. Pérez*, Marcelo Zambrano, Manuel Esteve, Carlos Palau
Communications department
Distributed Real Time Systems and Applications Lab
Universitat Politècnica de València
46022 Valencia, Camino de Vera s/n, Spain,
*Corresponding author: frapecar@upvnet.upv.es

Abstract: To effectively manage a crisis, is necessary the participation of multiple agencies related to protection and public safety, which allow actions in accordance with the demands of environment and requirements of all those affected. Interoperability is the key to comprehensive and comprehensive Crisis Management (CM), that allow to face any type of disaster, at any time or place. For this, it is necessary the permanent exchange of information that enables all the agencies involved, coordinate its operations and collaborate to manage the situation in the best way possible. This article describes the approach to interoperability in CM carried out by Secure European Common Information Space for the Interoperability of First Responders and Police (SECTOR) European Project, which has one of its main objectives, the development of an interoperability platform that allows the agencies involved in the management of a crisis, to achieve a joint, coordinated and collaborative response. The platform has a core, a Common Information Space (CIS), which manage as a single storage entity, all information of the Information Systems (ISs) connected to the platform, regardless of the model of data and computer applications used by each one of them.

Keywords: interoperability, distributed architectures, command and control, crisis management, data models.

1 Introduction

A crisis can be defined as an unforeseen situation that endangers the environment, property and / or life of people. The CM refers to those resources and processes required to deal with a crisis in the best possible way. One of its most important characteristics is its multi-agency nature, which allows meet the demands of a critical environment and the requirements of all those affected, through the resources, skills and knowledge coming from different protection and public safety agencies involved [3] [14] [15]. It presents four domains of operation: physical, information, cognitive and social.

- The physical domain is related to the environment where the crisis develops (extension and geographical location, environmental conditions, available resources, affected, etc.).
- The domain of information refers to all those aspects related to the information needed to describe the operations environment (sensor, measurement, storage, publication, etc.).
- The cognitive domain makes use of this information, to create situation awareness from which can be made decisions in line with reality.
- The social domain deals with inter-agency interaction, promoting collaboration between them and covering the three domains described above. It allows the effective exchange of information (information domain); the creation of a common situational awareness and

consensual decision making (cognitive domain); and the coordinated execution of these decisions, which bring about the desired effects on the environment (physical domain) [16] [2].

The capability of a system to exchange and understand information from other systems is defined as Interoperability [9]. In heterogeneous and complex environments such as CM, interoperability is the key to achieve the orchestration of the resources involved, and to allow a coordinated and collaborative response [20] [22] [24].

This article details the solution proposed by the European project SECTOR for interoperability in CM. SECTOR is a part of the Seventh Framework Program of the European Union for Research and Technological Development (FP7), and the Universitat Politècnica de València (UPV) has actively collaborated in its development [21]. One of its objectives is the design and implementation of an interoperability platform that allows the agencies involved integrating within a communications infrastructure to exchange and share information related to the management of a crisis. The platform has as core, a middleware layer that adapts the information coming from different ISs, to the model and format data defined in a CIS, which manages as a single storage entity, all the information coming from those ISs.

The feasibility and operability of the platform has been validated by means of functional tests on a prototype implemented based on the architecture described in this article, and within a simulated scenario for a crisis. Each of the ISs integrated to the platform, shared in the CIS, information related to the state of operations environment and the resources deployed both inside and outside himself. This information made it possible to create accurate and real situational awareness, which in turn enabled an effective planning and coordination of response and recovery operations.

The paper is divided into five sections: firstly, an introduction to the proposal and methodology used; Second, it describes the motivation and the oeuvres that have been taken as main references for the development of SECTOR project; Third, it details the propose architecture and the functionalities of each of its components: fourth, it describes the tests of functionality and the obtained results; And finally, presents the conclusions and final notes for this work.

2 Motivation and related work

One of the most important factors to be considered regarding interoperability in the CM is the heterogeneity of data and the way users access them. Many Crisis Management Systems enable inter-agency interoperability through the use of a proprietary set of IT tools and a standardized data model, that enabling the transparent exchange of information between applications and agencies (e.g. Coordcom [18], Atos [1] or DESTRIERO [19]. However, this scheme is limited by the usability and scope of those tools designed by the manufacturer, which do not necessarily achieve the particular scope and requirements of all agencies. In general, users are reluctant to use external computer tools, either by affinity with the applications they use regularly or by mistrust and expertise lack with computer applications that they do not know.

This work focuses on the CM social domain, and its main contribution lies in the capabilities of the platform, to allow the exchange of information between the agencies involved, regardless of data model, systems and applications computer used in each of them. Agencies use their own tools and ISs to exchange and share information between them.

The architecture detailed in this article has taken as main references for its development to the National Information Exchange Model (NIEM) and the non-relational Data Base (DB) (No Structured Query Language (NoSQL) DB). NIEM was created by the United States Department of Defense (DoD) and the Department of Homeland Security (DHS) in order to interconnect communities with the need to exchange information to fulfill a common goal. It proposes the development of a middleware layer and the adoption of a normalized data model to allow the ISs involved to exchange information independently of their data model and proprietary applications (Figure 1) [7].

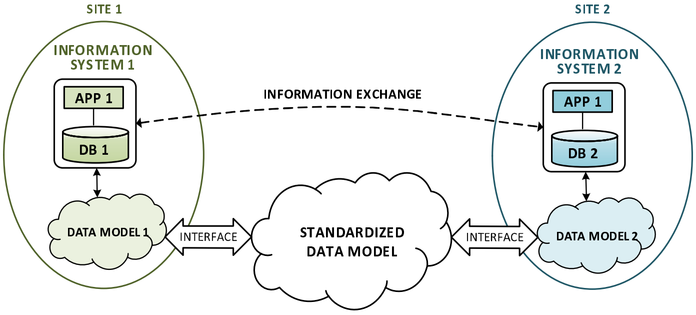

Figure 1: NIEM Schema

On the other hand, the NoSQL DBs allows to store each object with an independent data schema, solving the deficiencies of relational DBs in how many to the management of heterogeneous data [6] [13]. Figure 2 shows a diagram that summarizes the proposal made by SECTOR in terms of data management with NoSQL DBs.

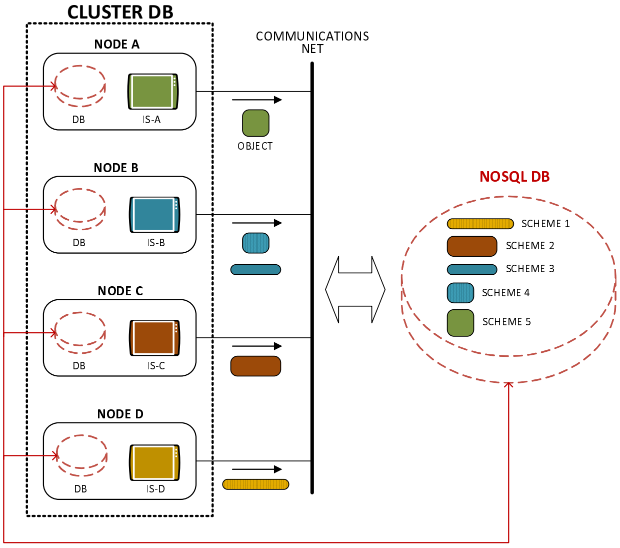

Figure 2: No Relational Distributed Data Base Schema

3 Architecture

The architecture has been designed to support the requirements of availability, scalability and information heterogeneity present in the CM. It is based on a Communications Distributed Infrastructure (CDI) and middleware layer, which enable ISs to exchange and share information regardless of their data model, systems and computer applications. The middleware layer adapts the information coming from the ISs to the data model defined in the CDI. The information that needs to be shared is stored locally on a NoSQL DB, in order to later distribute it said information on the other nodes DBs that make up the CDI. The sharing and exchange of information are done through a messaging and notification mechanism (detailed below), under the eXtensible Markup Language (XML) data schema defined in NIEM and a Data Distribution Service (DDS) protocol.

The architecture has been developed entirely under free software, eliminating dependence with manufacturers (maintenance, upgrades, etc.) and leaving an oppen-door for customization and development of new functionalities. Linux has been chosen as the Operating System for the communication nodes, MongoDB as NoSQL DB Manager [23], Java as a programming language for the development of the various modules of the platform, and AngularJS [13] as framework JavaScript for the development of the Human Machine Interface (HMI). To facilitate its design, implementation and scalability, the architecture has been divided into three main elements(Figure 3):

- Information Systems: devices, tools or computer systems, registered on the platform to contribute and / or obtain information from it.
- CDI: responsible for providing connectivity between the nodes that make up the platform. Its topology, as well as the technology used in the communication links, are transparent to the middleware layer, which facilitates the implementation and scalability of the platform.
- Middleware layer fulfills the functions of transceiver between the CDI and the ISs. It is responsible for allowing the exchange of information between ISs integrated to the platform. It is subdivided into four components: Interoperability Boxes (IBXs), communications nodes, CIS and HMI.

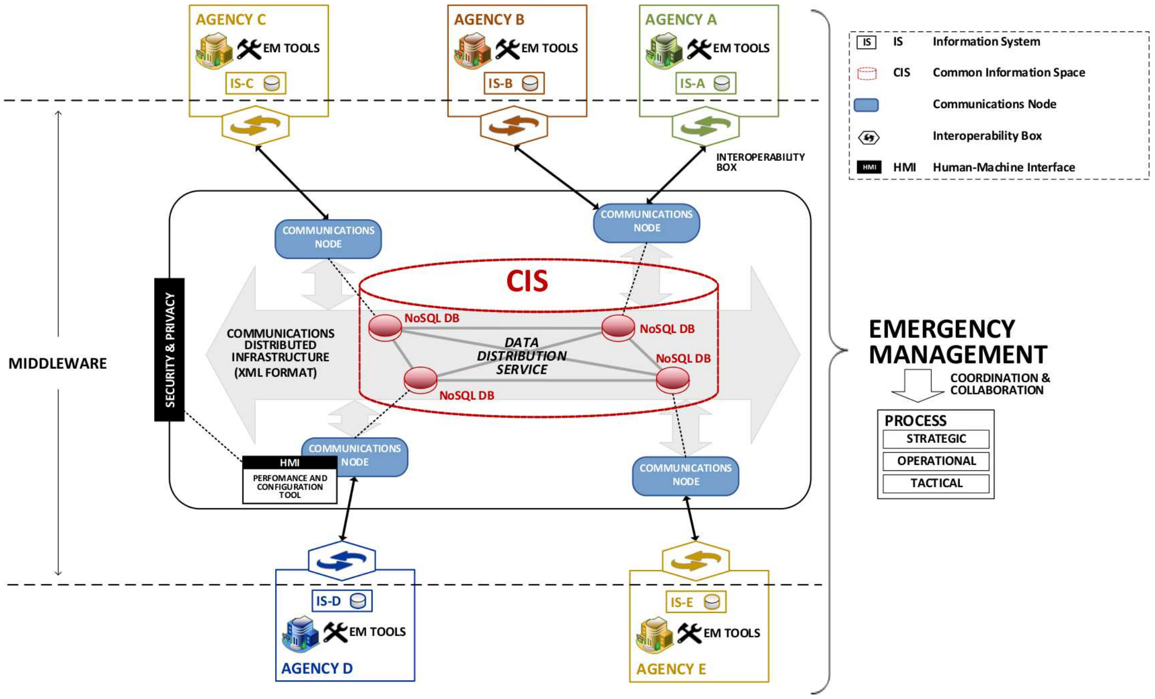

Figure 3: Architecture

3.1 Interoperability boxes

They are responsible for adapting the information coming from the ISs to the XML format defined in the CDI, and vice versa. Each IBX has an interface to the IS and another to the comunications node, allowing the flow of information between them through Web Services (WS) [12]. The requests / responses from and to the ISs are made through the WSs that have been defined in the IS in question (Simple Object Access Protocol (SOAP), Representational State Transfer (REST), Hypertext Transfer Protocol (HTTP), etc.), while the requests / responses from and to the communications nodes, according to platform design and following the principles of standardization proposed, are made only by SOAP.

Among the communication interfaces, there are two sublayers (transformation and communications), which allow the conversion of the data format in a bidirectional way. Due to the heterogeneity in the formats and protocols used by ISs, each of them needs their own IBX, and there will be as many IBXs as ISs will be integrated into the platform. Figure 4 (left panel) shows a general block diagram for an IBX.

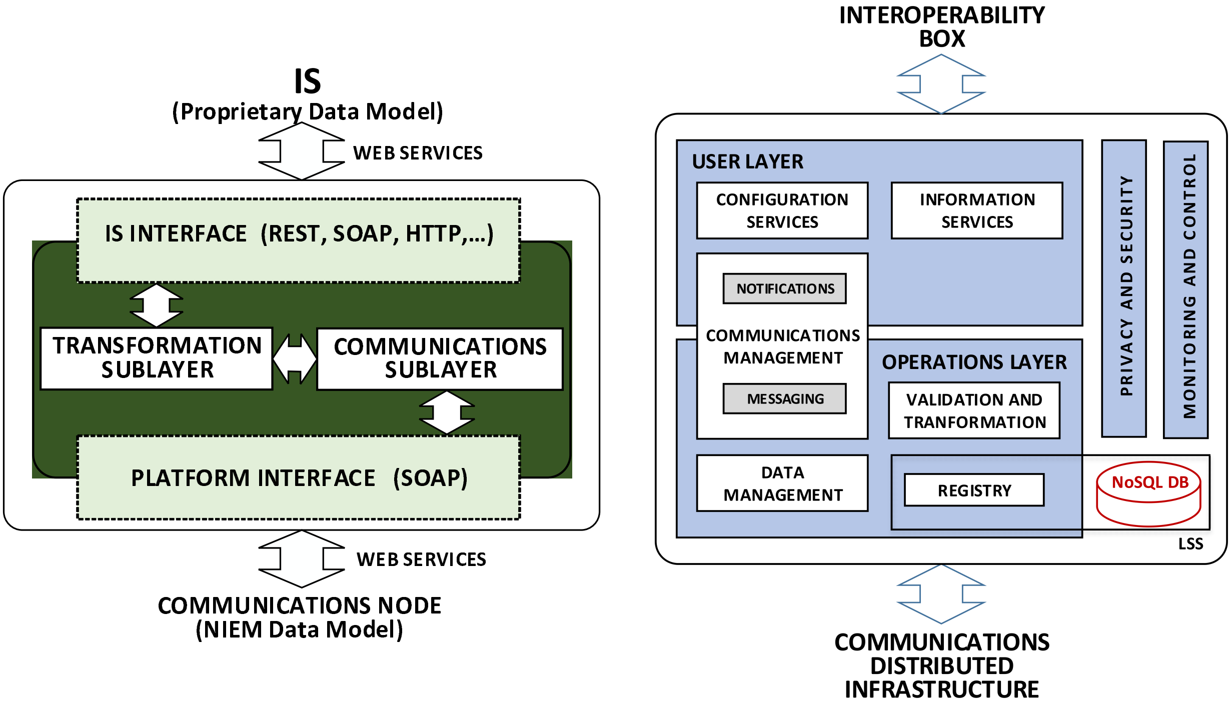

Figure 4: Interoperabilty Box (left panel) and Communications Node (right panel)

3.2 Communications nodes

They are the gateway to the platform and among its main responsibilities are the registration of users and systems, as well as the notification of any information changes or relevant event on the platform, to the local ISs (integrated to the platform through it) and other communications nodes.

Figure 4 (right panel) shows a block diagram summarizing the internal architecture of a communications node. Four main elements can be observed: a user layer responsible for making available to ISs, the platform configuration services (e.g. ISs registration, notifications subscription, addressing, etc.) and interaction with the CIS (Reading, writing, deleting and updating data); A layer of operations responsible for the management and functional processes inside node (e.g. data validation, node-to-node communication, data management, etc.); Two groups of transversal services responsible for the security, processes supervision and node access; And a Local Storage Space (LSS), in which is it stored a replica of the CIS and the users and systems register.

When a new node needs to be integrated into the platform, the first step is to register on the same. Once authorized its access, the node becomes part of the Cluster that shapes the CIS, and initiate communications with the other nodes through the CDI. The information received (data and metadata) is stored in the LSS, which is accessible by all ISs registered in that node, and will be forwarded to the other nodes that so require it.

The platform can be configured with the number of nodes required, and each node can serve more than one ISs, depending on the scope of the platform, the processing capacity of the node, and the specific requirements of each IS in terms of resources, security, availability and / or reliability.

3.3 Common information space

The CIS is the core of the architecture. It allows the management of all the information coming from the ISs registered in the platform, as a unique storage entity, and it is based on a NoSQL DB cluster, to enable the storage of each data object under an independent schema. The CIS presents a data model based on NIEM, with a binary documental structure type JSON (BSON), this promotes the exchange of information and the transparency of the physical objects location. Moreover it takes advantage of the architecture distributed character to replicate the information in each of the cluster nodes, balancing the data processing, and providing availability, reliability and scalability to the platform. Among its most important features, it is important highlight the decentralization, scalability and adaptability about the data heterogeneity. Both the workload as the diffusion level are parameterizable, and they should be configured following the crisis environment needs.

SECTOR uses MongoDB as DB engine, due to its multiplatform character open source and the document-orientation storage [23]. Regarding the information management, it has been selected OpenSplice (open source distribution of DDS protocol) for the implementation of Publish/Subscribe mechanism on data distribution [4]. Figure 5 summarizes a block diagram with CIS internal architecture.

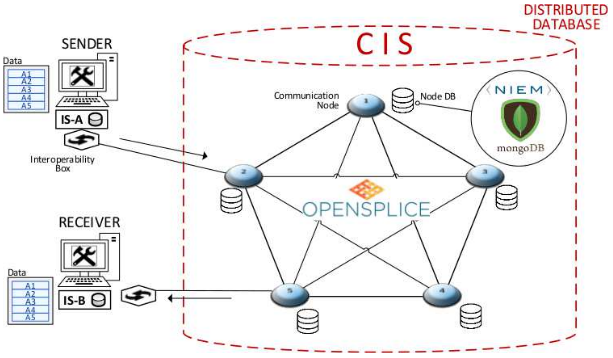

Figure 5: Common Information Space.

3.4 Communications and data management

The information exchange among nodes, and among a node and the local ISs, it is performed using a Publish/Subscribe mechanism, with a XML data schema based on NIEM. The XML datagrams, contain the data and metadata required to notify, to the ISs and the communication nodes, about any change performed in the availability of information and/or the platform status. Before the data storage, the datagrams should be validated and transformed to the binary format BSON defined in the CIS, through Validation and Transform modules available in each node.

The Publish/Subscribe mechanism has been developed taking in to account the performance optimization and the use of network resources operating in low capability environments. This is the case for CM situations with low process capacity and storage, limited bandwidth, packet loss etc. [23] [5].

The information publication and the information requests, use the DDS protocol to distribute the data and metadata through the CDI. The ISs should specify the Topics of which they will be providers, and the Topics of which they want subscribe as consumers. Every time that new information is shared through the CIS, the local node notifies to the local ISs subscribed to the Topic, about the information update via "Notification" service. If the information is relevant for a IS, the registered IBX can retrieve the information from the CIS, transform it into its proprietary data model and make the adapted information accessible to their informatics tools and/or systems. Similarly, the local node shares the update with the other nodes in the platform using the "Messaging" service, and these notify to their ISs if applicable about the new information available. This process is shown in Figure 6.

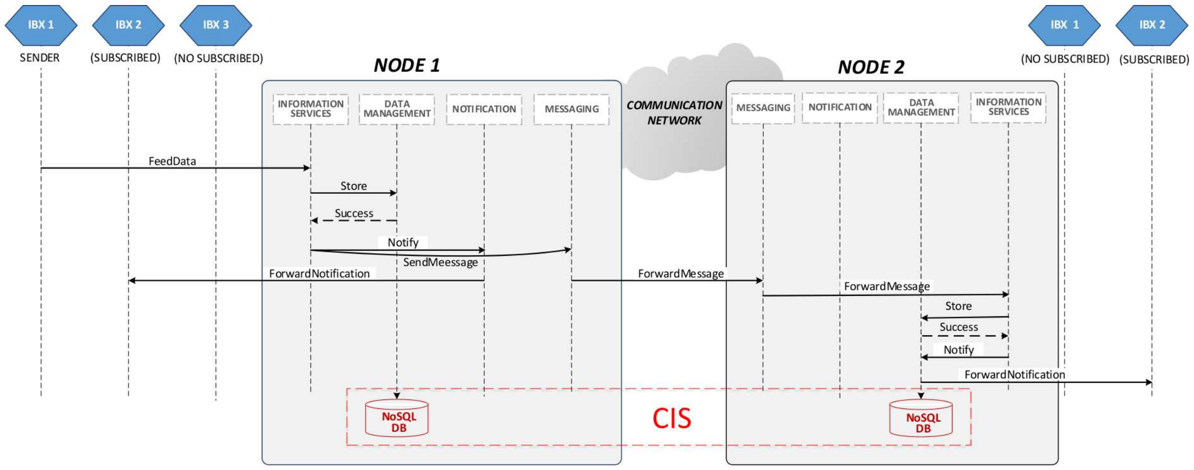

Figure 6: Notification Process.

3.5 Security and human machine interface

The platform access and privacy is managed through the HMI. It is able to create users, manage profiles and assign permissions using the "Privacy and Security" module. It also allows the maintenance and the audits of the platform via "Monitoring and Control" module.

Each node, stores a copy of information related with the users and systems registry, guaranteeing always the accessibility and the security in the platform.

Regarding to the communications security, it is managed using security protocols as Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS), and using security certificates to enable the CIS access.

4 Validation and results

The platform feasibility and functionality, was validated using a prototype developed following the architecture described in this paper and executing a simulation in a flood scenario in Roermond city (Netherland). Two communication nodes were deployed, and used by the involved agencies in the simulation, for sharing and interchanging information related with the flood and the environment status. Figure 7, shows the final deployment configuration for the scenario validation.

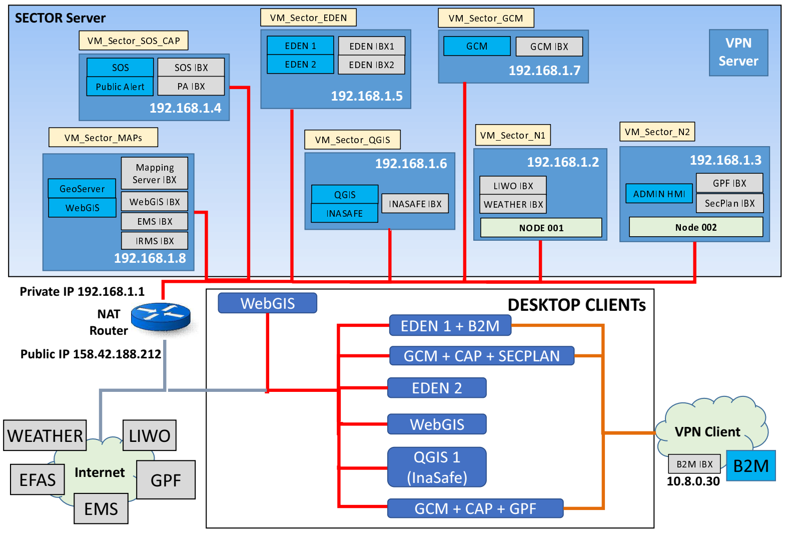

Figure 7: Platform deployment schema

The distributed architecture of SECTOR platform, divides the data processing load among all the CDI nodes and decreases the hardware and software requirements in the communication nodes. A unique HOST with standard features regarding to the hardware and the software (I7 octa core processor, 32GB of RAM, 2TB of disk and VMware vSphere 6.5) was used during the tests for virtualizating the 2 communication nodes and the ISs with their respective IBXs.

Each participating agencies, added and/or got information from the CIS, using their own tools and informatics systems. Table 1, shows a summary with the participation of the agencies, and the ISs used by them during the tests.

Table 1: Scenario actors and information systems

Coordination type	Organization	Actor	System
Local	Fire Brigades	SGSP	EDEN
	Police	PSNI	InaSafe
	Red Cross	IAEMO	EDEN
	Roermond Mayor	SSV	GCM
	Directorate for National Safety and Security	External End-User1	WebGIS
International	Bavarian Police	PAS	InaSafe
	UK Red Cross	IAEMO	GPA
	AMI	External End-User2	GPF+GPA

The simulacrum starts with the information sharing related with the environment conditions and the status of the rivers Maas and Mesue, by the local CM agencies. After the information analysis, and following the obtained forecasts, the protocol of an imminent flooding is started. After the corresponding preventive actions, including reports publication and generation of alerts through the CIS (e.g. affectation perimeter, climatic and ambient conditions of the operational environment, hot spots, location and planning of first responders units, etc.). The flooding overflows the local response capacity, so the emergency state was declared and the help of national and international neighbouring agencies was requested by the local authorities. During the response phase and the situation stabilization, the information related with the actual situation of the environment, the permanent status reports, and location of first responder units, victims and affected people were shared through the CIS. Following the information shared in the CIS, the response and recovery actions were planned, deploying five multi-agency response groups, covering all the affected zone by the flooding. Figure 8, summarizes the participation of the different actors in the exercise, and some of the tools used.

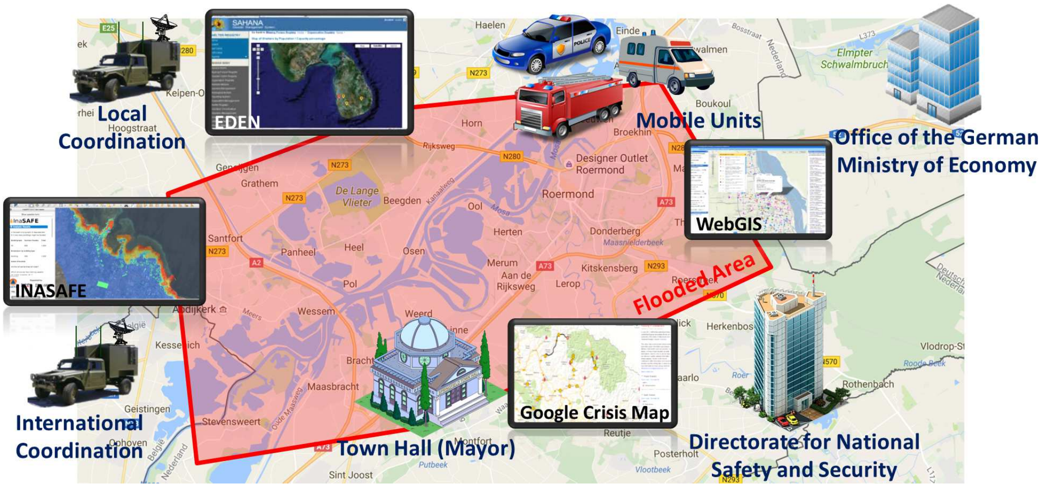
Local Coordination
EDEN
Mobile Units
Office of the German Ministry of Economy
WebGIS
INASAFE
Flooded Area
International Coordination
Town Hall (Mayor)
Google Crisis Map
Directorate for National Safety and Security
Roermond

Figure 8: Test scenario

During the simulacrum, and with the final purpose of validate the platform, it was attended by collaborative personnel, both tactical and strategic, from the participant agencies, as well as representatives of several agencies related with the CM in European Union. After the simulacrum, a questionnaire was carried out to the attendant personnel, to have a general impression about the platform functionalities. The obtained results are summarized in Appendix A, Table 2.

The 100% of the respondents were agree, to a greater or less extent, with the platform usability. An 81% would use the platform, either for training or a real environment, and believes that its agency would benefit with the platform functionalities. A 3% would not use the platform, and a 16% would be undecided about its use. In addition, an 87% of the respondents would recommend the use of the platform and agrees with the proposed approach for the inter-agency interoperability.

The proposed solution has been validated for this use case, but it is possible to generalize it in any scope for CM (fires, earthquakes, etc.). The only requirement for the integration of new tools into the platform is the IBXs development, which allow the data exchange and the communication with the nodes following the NIEM format defined in the CDI.

5 Final notes and conclusions

In complex and diverse environments such as CM, the interoperability is the key for an integrated and comprehensive management, allowing a flexible and effective response to any type of disaster that may arise. For this, it is necessary a continuous exchange of information, allowing all involved agencies, to coordinate their operations and collaborate to manage the situation in the best possible way. This paper describes the approach of the European project SECTOR, for the interoperability between the agencies involved in the CM. It describes the architecture of an interoperability platform, able to integrate into a communication infrastructure the information from the different systems, used by the involved agencies, sharing and interchanging information.

The main contribution of the platform, is found in its capability to manage heterogeneous data, and allow users from different agencies, to obtain and share information, using their own systems and informatics tools.

The core of the architecture, is in its CIS, which allows manage as unique storage entity, all the information coming from different information systems registered in the platform. It is based on a No Relational Distributed DB, and NIEM data model, allowing the heterogeneous data management and divide the work process among all the nodes in the platform.

The platform was validated using a developed prototype following the architecture described in this paper, and tested in a simulated scenario for a crisis. The platform capabilities were verified to facilitate the exchange of information among agencies, and the shared information was used by the personnel involved to plan and coordinate the response and recovery operations.

Moreover, the stored information in the CIS, may be used as support for the management of future crisis, assisting decision support and command & control systems, with relevant information regarding problems and solutions raised in previous events.

Regarding to the future work, alternatives for the implementation of the CIS are being explored, based on distributed database schemas, that allow the requirement optimization in hardware and software for the storage and the data processing [11] [10]. On the other hand, the human machine interface, currently allows administrators access to the platform configuration and monitoring tools. However, its implementation leaves an open-door for the development of other type of tools for customization or requirements compliance.

Currently a proprietary tool is being developed, and it is able to exchange audio and video information in real time, regardless of the communication technology used in the data link between the nodes.

Acknowledgment

This work is funded by European Commision as part of FP7 (No. 607821). Project Supported by LEONARDO company, Universitat Politècnica de València, ASELSAN Elektronik Sanayi ve Ticaret A.S, Totalforsvarets Forskningsinstitut, ITTI SP ZOO, Consorzio Interuniversitario Nazionale Per L'Informatica, SAADIAN Technologies Limited, E-GEOS SPA, Universitaet Stuttgart, Thales SA, Police Service of Nothern Ireland, Wyzsza Szkola Policji W Szczytnie, Health Service Executive HSE, Szkola Glowna Sluzby Pozarniczej, Stichting Studio Veiligheid, and Eberhard Karls Universitaet Tuebingen.

Bibliography

[1] Atos (2014); *Safeguarding your citizens and assets with emergency management*, ATOS, 2014.

[2] Defense Department, O.F.T. (2005); *The Implementation of Network-Centric Warfare*, Government Printing Office, 2005.

[3] Federal Emergency Management Agency; *Course IS-0230.d: Fundamentals of Emergency Management*, FEMA, 2015.

[4] Foster A. (2016); *DDS at the Tactical Edge - Next Generation Military Fog Computing and Cloudlets Live Webcast*, PRISMTECH, 2016.

[5] Garg P., Sharma M. (2016); "BIG DATA" Analysis Using Hadoop & MongoDB, *International Journal of Modern Computer Science*, 4(3), 153–156, 2016.

[6] Han J., Haihong E., Guan L., Du J. (2011); Survey on NoSQL Database, *2011 6th International Conference on Pervasive Computing and Applications*, 363–366, 2011.

[7] Hay D. C. (2014); *National Information Exchange Model. Core Evaluation*, Essential Strategies International, Houston, 2014.

[8] Huang C.Y., Yang T.T., Chen W.L, Nof S. Y. (2010); Reference Architecture for Collaborative Design, *International Journal of Computers Communications & Control*, 5(1), 71–90, 2010.

[9] IEEE; *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*, IEEE, 1990.

[10] Li Y., Manoharan S. (2011); A performance comparison of SQL and NoSQL databases, *2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, Victoria, BC, 15-19, 2013. doi: 10.1109/PACRIM.2013.6625441

[11] Padhy R. P., Patra M. R., Satapathy S. C. (2011); RDBMS to NoSQL: Reviewing some next Non-relational Database's, *International Journal of Advanced Engineering Sciences and Technologies*, 11(1), 15–30, 2011.

[12] Pirnau M. (2010); Implementing Web Services Using Java Technology, *International Journal of Computers Communications & Control*, 5(2), 251–260, 2010.

[13] Tudorica B. G., Bucur C. (2011); A comparison between several NoSQL databases with comments and notes, *2011 RoEduNet International Conference 10th Edition: Networking in Education and Research*, IEEE, 1–5, 2011.

[14] UNCHR (2012); *Manual for Emergency Situations, United Nations High Commisioner for Refugees*, 2012.

[15] Wayne B. (2008); *Guide to Emergency Management and related terms, definitions, concepts, acronyms,organizations, programs, guidance, executive orders & legislation*, FEMA, 2008.

[16] Williams A. P. (2010); *Agility and Interoperability for 21st Century Command and Control*, vol. 4, CCRP, 2010.

[17] [Online]. Available: https://angularjs.org/, Accesed on 31 March 2017.

[18] [Online]. Available: http://www.carmenta.com/en/products/carmenta-coordcom/, Accesed on 2 May 2017.

[19] [Online]. Available: http://www.destriero-fp7.eu/, Accesed on 2 May 2017.

[20] [Online]. Available: http://www.fema.gov/, Accesed on 14 April 2017.

[21] [Online]. Available: http://www.fp7-sector.eu/, Accesed on 14 April 2017.

[22] [Online]. Available: http://www.isotc223.org/, Accesed on 12 April 2017.

[23] [Online]. Available: https://www.mongodb.com/json-and-bson, Accesed on 31 March 2017.

[24] [Online]. Available: http://www.unisdr.org/, Accesed on 11 April 2017.

Appendix A: Questionair

Table 2: Questionair for tactical and strategic personnel

Question	(5)	(4)	(3)	(2)	(1)
The key features of the platform are suitable for dealing with crisis response.	8	18	5		
The SECTOR platform offers added value to support faster decision making in response activities.	10	20	1		
The SECTOR platform offers added value to support improved decision making regarding resource and activity planning in crisis response.	11	16	4		
SECTOR enhances the COP for the current Crisis Management Tools.	8	23			
Using the SECTOR platform can be effective to speed up response time.	9	20	2		
The SECTOR platform combines useful Neutral 3rd party applications and information sources for crisis response.	8	18	5		
SECTOR boosts interoperability and information exchange among different organizations.	16	14	1		
Access to the data from the integrated IT Systems and tools is available quickly and efficiently.	6	20	5		
SECTOR provides new capabilities, which enhance the use of the Crises Management Tools.	6	21	4		
I would recommend a fully developed SECTOR platform to a colleague.	8	14	9		
I would use the SECTOR platform in "real life".	5	16	8	2	
I would use the SECTOR platform for field exercises.	9	20	2		
I would also use the SECTOR platform during the recovery phase of a crisis.	7	13	10	1	
I consider my organization's efforts in the field could benefit from the coordination facilitated by the SECTOR platform.	6	15	9	1	
A tool based on SECTOR would be a valuable asset in crises and emergency management.	6	23	2		
Notwithstanding budget constraints, my organization would see value in funding its own SECTOR service or becoming a funding partner in a multi-agency SECTOR service.	2	11	17	1	
A pay-per-use model is a good way for organizations to fund a SECTOR service.	1	10	15	2	3
A fixed, flat annual fee is a good way for organizations to fund a SECTOR service.	3	15	13		