Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 64 (2015) 750 – 757

Procedia Computer Science

Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2015 October 7-9, 2015

SECTOR: Secure Common Information Space for the Interoperability of First Responders

Marcello Cinque[a], Christian Esposito[a], Mario Fiorentino[a]*, Jana Mauthner[b], Łukasz Szklarski[c], Frank Wilson[d], Yann Semet[e], Jean-Paul Pignon[f]

[a]*Consorzio Interuniversitario Nazionale per l'Informatica (CINI), Via Cinthia, Complesso Universitario di M.S. Angelo, 80126 Napoli, Italy*
[b] *Universität Stuttgart, Institut für Arbeitswissenschaft und Technologiemanagement, Nobelstraße 12, 70569 Stuttgart, Germany*
[c]*ITTI Sp. z o.o., ul. Rubież 46, 61-612 Poznań, Poland*
[d]*Stichting Studio Veiligheid (SSV), Saturnusstraat 60, 2516 AH Den Haag, Netherlands*
[e]*Thales Research & Technology, Campus Polytechnique, avenue Augustin Fresnel 1, 91767 Palaiseau Cedex France*
[f]*Thales Communications & Security SAS, 4 Avenue des Louvresses, 92622 Gennevilliers Cedex, France*

Abstract

The ever-growing human, economic and environmental losses due to natural and/or man-made disasters demand a systematic, holistic, inter-governmental and multi-disciplinary approach to the management of large-scale crisis. However, crisis management is usually coordinated by local authorities, supported by a variety of different national and international crisis management organizations, all acting relatively autonomously. Coordination actions usually adopt non-interoperable information management tools, due to the heterogeneity of the involved organizations, limiting or even hindering the coordination efforts. This paper introduces the efforts conducted in the context of the EU-funded project called SECTOR, which aims at establishing the foundations of future Collaborative Crisis Management (CCM) Information Spaces by expanding the European scientific knowledge base on (cross-border) multi-agency processes and their complications when setting-up and designing the enabling information systems.

Peer-review under responsibility of SciKA - Association for Promotion and Dissemination of Scientific Knowledge

Keywords: Collaborative Crisis Management; Common Information Space; Interoperable Systems

* Corresponding author. Tel.:+39081676770; fax: +39676770.
E-mail address: mario.fiorentino@consorzio-cini.it

Peer-review under responsibility of SciKA - Association for Promotion and Dissemination of Scientific Knowledge
doi:10.1016/j.procs.2015.08.622

1. Introduction

The accelerating rates at which disasters have unfolded in recent years, and the unprecedented levels of economic losses associated with them indicate we have entered a new era of catastrophes (NatCatSERVICE, 2012). In fact, we have witnessed a series of large-scale disasters, such as the Chernobyl nuclear accident, the Kobe and Marmara earthquakes, the March 11 earthquake and tsunami in Japan, including the nuclear crisis due to the Fukushima nuclear plant damages, and the September 11 terrorist attacks in New York and Washington, which have in common massive effects on large concentrations of people, activities and wealth. As a concrete example, in October 2014, the head of the Scottish Government Critical Infrastructure Protection Unit (CIRU) was awoken in the night to discover that a ship carrying nuclear material was adrift without engine power in the North Sea, and was close to active Oil Rigs containing crews pumping oil. In a brief time, air crews (planes and helicopters) were scrambled in Scotland and Norway and high speed protection vessels were also dispatched. The exchange of information relied on the good working relationship between Norway and Scotland around North Sea Oil. Disaster was averted. Many disasters are not averted (e.g. UK Kings Cross Station Disaster) (Desmond, 1998), and all of them have proved limitations of governments to properly react and recover from them and of containing their devastating effects, which may lead to other consequent disasters. In fact, it is shown that the failure to ensure "common information" sharing is a cause of failure in the response phase (Desmond, 1998). This kind of events has negative consequences for the involved populations, but also a short-term destabilizing effect on the economy (OECD, 2004).

The traditional approach of a single organization involved in the crisis management and recover is not feasible in the case of large-scale disasters, due to their scale, impact and severity. Therefore, several different first responder organizations at national and international level act together, and are coordinated by a given organization such as OCHA (Office for the Coordination of Humanitarian Affairs), paving the way for a Collaborative Crisis Management (CCM). Since decision-making must be flexible and responsive (OECD, 2004), there is a great demand for CCM intensive information sharing among the organizations involved in the crisis management. However, this is hindered by the high level of heterogeneity of the involved organizations, which can be classified as (i) technological heterogeneity (i.e., organizations use different computer-based tools), (ii) data heterogeneity (i.e., each organization may assume a given information model), (iii) informatisation heterogeneity (i.e., some organization may adopt GIS (Cai, 2005) or Collaborative Tools (Erl, 2005), while others only deals with paper-based documents or rather simple computer-based tools). Such heterogeneity is a great obstacle to information sharing in a timely and efficient manner, making impossible to exchange data with other organizations or to comprehend data from others. There are a few initiatives currently in place to improve interoperability among crisis management stakeholders (e.g., MIC, GDACS V-OSOCC, PDNA, etc.), but no common approach, technique or tool is available to support the whole crisis management cycle (from prevention to recovery) across agencies and across borders. Flexible concepts and tools are lacking, that enable cross-border networks of crisis management organizations to set-up flexible support systems for a joint operation in which information is continuously updated and shared between organizations, leveraging on existing Information Systems from the involved organizations, and in which progress is monitored and resource sharing facilitated.

SECTOR is an EU-funded project that aims at providing an answer to the increasing demand for data sharing and interoperability in large-scale disaster management by offering a systematic, holistic, inter-governmental and multi-disciplinary approach to the collaboration of heterogeneous first responder organizations when managing large-scale disasters. We intend to show how a Common Information System (CIS) can help avert disasters, and this, driven by guidance from leading experts in interviews and on-going direction via our expert group, provides a unique approach and contribution to solve the "non-collaboration" problem by enabling interoperability through multi-agency cooperation and collaboration (House et al., 2014). Starting from the analysis of past events and the state of the art on information sharing platforms and procedures, in Section 2 we define the main requirements that future CCMs shall fulfil. In Section 3 we propose the SECTOR solution to address the identified needs, whereas in Section 4 we describe the typical large-scale disaster scenario for which the SECTOR solution is needed to coordinate a wide range of heterogeneous first responder organizations. We conclude the paper with the current state of the project and future work.

2. Information sharing and collaboration needs and requirements

One of the first objectives of SECTOR has been the definition of the key requirements to be satisfied in order to realize a successful crisis management in case of large-scale disasters. The work has progressed along two parallel lines: the analysis of past crisis events to understand the elements that cause their successful or unsuccessful management; and the study the available IT tools and practices, considering specifically the communication issues. The main driving idea of our work has been the assumption that a better availability of knowledge after crisis situations could help to reduce damage and losses as well as shorten the recovery (Greene, 2002). Our study of past events mainly involves cross-border or/and cross-agency events by gathering a description of them, the involved actors, the consequences (e.g., economic or social impacts), and the context (e.g., weather, special events, etc.).

This analysis on end-users needs and requirements has been conducted by means of a series of interviews to domain experts of the end-users involved in the SECTOR project and also external end-users that have shown interest in the project. Firstly, the data collection methodology was defined and described in order to investigate information sharing procedures, processes and tools within first responders' and police authorities' organizations. Secondly, a draft interview guideline for gathering information on data sets, procedures and tools was developed and in order to get an overview of the usability of the interview guideline, the SECTOR end-user partners accomplished in the next step an interview pre-test using the developed guidelines. The final versions of the interview guidelines were achieved after incorporating the feedback of the SECTOR partners and reflecting the results of the interview pre-test. Finally, we have conducted a number of 48 interviews in different countries: Poland (35%), Germany (19%), Northern Ireland (13%), Netherlands (10%), Ireland (8%), France (6%), Scotland (4%), Portugal (2%), Italy (2%). The data gathering process of data sets, procedures and tools was led by means of (i) personal and telephone interviews, as well as (ii) personal meetings with crisis management actors both performed using interview guidelines, (iii) reviews of literature and crisis communication plans, and (iv) lessons learned analysis. The SECTOR research team interviewed critical infrastructure security experts in 9 countries covering roles such as: Government Ministerial Advisor, Critical Infrastructure Protection Team Leader, Emergency Response Planner, Senior Police CI / Anti Terrorist Team Leader and "Gold" and "Silver" level commanders in first responder organisations. Such authorities are really hard to contact and we have been able to engage them through personal interviews with the scope to investigate in depth their world and their concerns. During one-to-one interviews with these leading experts, we have explored issues such as supporting resilience implementation strategies (The Scottish Government, 2011), development of public-private partnerships for resilience (Grangemouth Petroleum, 2014), and implementing partnership strategies where cross-institutional sharing of information is critical to success of security and safety objectives (SCORDS, 2014). Collected data was categorized, analysed and iteratively refined. Consequently, boundaries and relations between different crisis management activities and systems in general as well as operational procedures were identified. We have collected a total number of 40 past events, as shown in Figure 1, and classified them in two distinct groups: Natural disasters, and Technological disasters, by also considering their cross border nature.

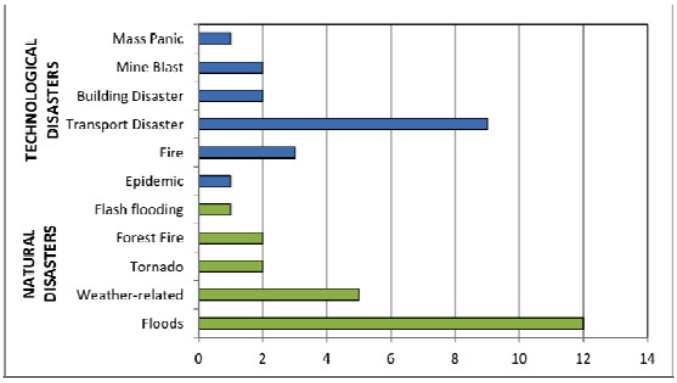

Figure 1 - Classification of collected past events.

Apart from the complete description of each past events, i.e., injured/killed people, damaged buildings and size of the overall affected area, kinds of consequences of the disaster occurrence and number and type of the involved organizations, we tried to understand which factors allowed a successful management of the collected past events. Main requirements for successful crisis management discovered in the analysis are accurate assessment of threat, harm and risk, timely and accurate passage of information, communication as well as coordination of limited resources. Furthermore, the conducted interviews have shown that efficient and effective collaboration and coordination mainly rely on information sharing. Poor crisis management is accordingly amongst other a consequence of a lack of options to share information among organisations involved in crisis management; a lack of awareness of information about activities of other organisations involved in crisis management; and a lack of collaboration in view of the consolidation and interpretation of information available. But effective and efficient crisis management depends not only on sharing information. It requires a mutual understanding for goals procedures and requirements. This is especially true, because some aspects of coping with crisis situations and recovery work are written down in negotiated procedures and processes (e.g. laws, regulations etc.). Summarising, crisis management can be characterized by (i) time pressure causing a merge of planning and execution phases (in fact, they usually take place at the same time); (ii) a need to manage cooperation among multiple decision makers and responding actors in case of large-scale events, especially: governmental, military, civil defence, non-governmental organization (NGO), fire service, police, ambulance, paramedics, coast guard, involved chemical, railway, road services, gas, security companies and voluntary social organizations; (iii) uncertainty and unpredictability of crisis events. Our analysis on past events gave us hints on the needed prerequisites for successful crisis management: assessment of threat, harm and risk, timely and accurate passage of information, communication and coordination of limited resources.

After having determined the ideal prerequisites to satisfy in order to have a successful crisis management, we have focused our work on the analysis of (IT) management tools, (information sharing) processes and procedures as well as standards currently in use. Furthermore, characteristics (differences and similarities) of existing national and organizational crisis management systems and structures were analysed. Such an analysis led us to specify the following prerequisites that the adopted IT tools have to verify: (i) Collaborative assessment of threats, harms as well as risks and coordination of limited resources, (ii) data aggregation and visualization, (iii) timely, secure and accurate transmission of information, (iv) interoperable communication paths, provided through national and international information management networks, (v) interoperable (IT) systems that enable actors to gain an accurate situational awareness of the event, and (vi) necessary expertise of actors to successfully operate in multi-agency and cross-border environments. Accordingly, an interoperable crisis management has to consider the following aspects:

- Semantic, planning, resilience and (inter-) organizational interoperability issues;
- Pragmatic technical and syntax aspects, taking into account first responders' needs and mass notification to the population as conditions for rapid operational improvements, and
- Communication interoperability between command and control centres to improve coordination and cooperation efficiency.

Our analysis highlighted that organizations involved in crisis management are currently using a multiple set of IT systems for decision support. For this reason, the information sharing with other organizations in crisis situations that is most often not interoperable. However, due to the dynamic and complex work in crisis management, most of the crisis management organizations IT systems need to be flexible and able to ensure that required information reaches the right organizations and responsible actors timely and in valid formats that facilitate effective response actions. Nonetheless, the design of crisis management information systems and technologies that can support successful coordination in multi-agency events is challenging due to information system incompatibility, unfamiliarity with systems and possible information overload.

We have summarized our findings in a list of system and technical requirements, reported in the Table 1.

Table 1 - Requirements for successful IT-based crisis management of large-scale disasters

Requirement Id	Name	Description
SYS_01	Multi-organization Collaboration	Cooperation must be established among multiple decision makers and responding actors by properly exchanging data and by defining a crisis management meta-model and processes to define joint cross-agency and cross-border orchestration of these processes.
SYS_02	Timeliness	Data must be shared in a timely manner; otherwise the delivery of data too late may be dangerous or unusual.
SYS_03	Security	Data exchanged among the actors for crisis management are critical and must be protected.
SYS_04	Interoperability	Several IT tools can be jointly used and must be integrated in an interoperable manner. Information sources should be queried to provide added values for the Common Information Space.
SYS_05	Data Visualization	Effective data visualization techniques are needed to efficiently present the exchanged data, typically by giving a geographical context.
SYS_06	Common Taxonomy	Common information taxonomy should be defined in order to facilitate information sharing among partners.
SYS_07	Decision Support	Decision support functionalities are needed in terms of data mining, for the analysis of a huge set of information, and artificial intelligence, for the optimization of available information and computational capacities.

3. The SECTOR Solution

The solution to the information sharing and collaborations needs provided by the SECTOR project consists in a flexible Common Information Space (CIS) concept, as depicted in Figure 2. The CIS provides users with "peer-to-peer" type functionalities to dynamically set-up cross-agency collaborative platforms and information spaces for information and resource sharing across agencies and across borders. Such functionalities can be set-up on the fly for an ad-hoc crisis management need, or as a permanent Common Information Space, depending on the needs, with the capabilities to facilitate the coordination of cross-organizational services.

The SECTOR CIS concept takes into consideration elements of Computer Supported Collaborative Work (between Agencies) and Process Aware Information Systems (collaborative crisis management), integrating international information services, and existing systems, to facilitate multiple collaborative agencies to build "their CIS", combining different characteristics:

- Provide an information space in which the needs are modelled according to the CCM process;
- Provide available "peer-to-peer" information sharing concepts, using system interfaces to automate information sharing between agencies, about situation awareness and available resources for joint crisis resolution and management;
- Provide public domain information sharing concepts, in which internationally available public domain environmental information (e.g., SEIS, UN-SPIDER, Virtual-OSOCC, etc.), crisis information (e.g., Google Crisis Response, OCHA 3W, etc.) information will become available to crisis managers and operators in combination with relevant "peer-to-peer" information on the crisis situation, its dynamic, available resources and services, in combination with a multi-layer GIS type interface.

The concept will expand on the recent IsyProc (Bidoux et al., 2014) and OMAR (Aligne and Savéant, 2011) tools, in which a cross-agency collaboration process and system architecture have been modelled, as a basis for a Common Information Space. The IsyProc bundle comprises a modelling methodology, a general collaborative crisis management meta-model and an associated software module with collaborative workflow generation and analysis capabilities. It takes its foundations on preliminary work performed within the IsyCri project from 2007 to 2010, called "Interoperability of Systems in Crisis Situation" and funded by the French National Agency for Resarch (ANR).

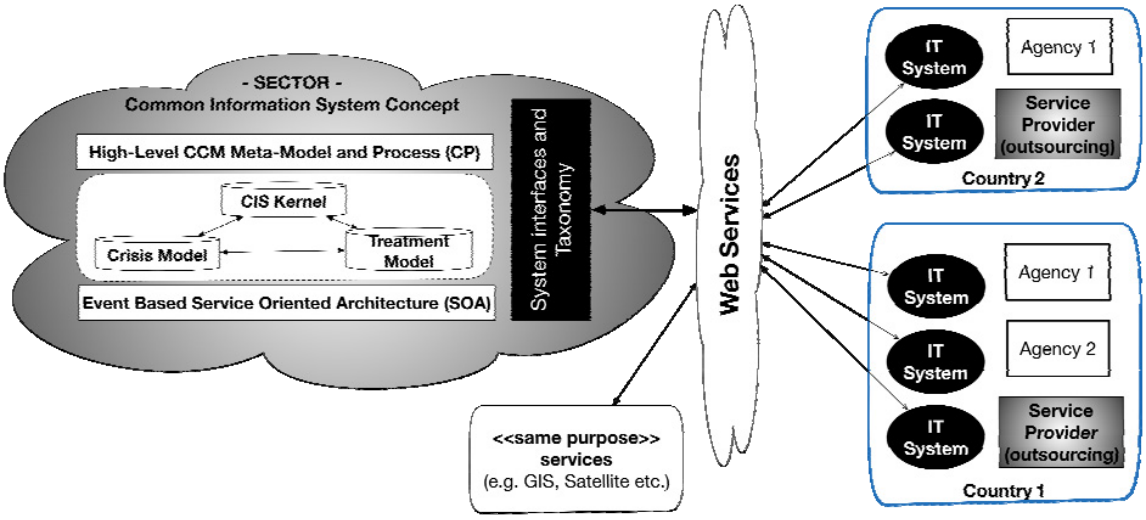

Figure 2 - Overview of the SECTOR CIS elements

IsyProc proposes – in a semi-automatic way – a plan / process implementing an efficient way to conduct cooperation of agencies involved in the crisis response. Based on models of context knowledge (including the ongoing crisis) and of responders' capabilities, ISyProc designs a collaborative process that orchestrates and coordinates different actors activities for the crisis resolution. From an operational point of view, there is a strong focus in the provided decision support on available resources within the crisis management organizations and agencies that collaborate in the CIS in order to optimize (shared) resource allocation simultaneously with inter-agency activities orchestration. Feasibility of collaborative processes proposed by IsyProc is achieved as it selects and schedules services that the actors are able to run. The overall approach is model driven through a crisis meta-model, and the design is based on inference of logical rules on ontology.

OMAR was developed within the Descartes project (2008-2011). It is a CCM example application of Artificial Intelligence (AI) planning techniques. AI Planning refers to the computer science area devoted to designing algorithms to solve the general "planning" problem of finding a sequence of actions, with matching required pre-requisites and post effect predicates, to go from a specified initial state to a final state satisfying a number of specified goal conditions. Planning problems are usually described with the PDDL language, which provides a formal, systematic structure to the problem definition. This allows for the use of generic solvers taken from the state of the art in AI. OMAR includes the design of a CCM ontology and PDDL description of part of the crisis resolution process, namely victim extraction, care, and evacuation as specified in the national and locally declined crisis handling protocols. Planning tools for crisis response usually do not anticipate for predictable situation evolutions that might hamper parts of the decided plan, such as traffic jams, getting in the way of ambulances at peak hours. To overcome this bottleneck, THALES has additionally endowed the OMAR tool with a dynamic, forecast-based planning capability that allows for smart temporal decisions for optimal dispatch. By providing optimal, quantified and anticipative workflows based on either actually available or putative resources, SECTOR, by exploiting the OMAR tool, will provide strategic decision makers with a multi-faceted tool that can help them (i) to optimize response speed efficiency, (ii) to make available and accessible most of the resources within the involved organizations, (iii) to assess whether available resources are indeed sufficient for the purpose, and (iv) to conduct "what-if" analysis to help decision making and how more resources should be called for.

The architecture depicted in Figure 2 shares a lot of similarities with the available solutions for enterprise integration in order to deal with the technological and syntactical heterogeneity characterising off-the-shelf systems that need to be integrated within a seamless infrastructure for information sharing (Truptil et al., 2010). However, the SECTOR CIS solution has been thought tailored on the needs of the disaster management domain by equipping it with a proper ontological solution in order to resolve the semantic heterogeneity affecting trans-national disaster

management involving heterogeneous first responders' organizations (House et al., 2014). One of the contributions to this work to the progress beyond the current state of the art in interoperable crisis information systems is to have an ontology that does not limit to model concepts in a single area (e.g., resources, processes, damage or disasters), as most of the current ontological approaches in the literature (Liu et al., 2013), but handle concepts in multiple areas tailored for the emergency and disaster domain.

4. Application Scenario

The application scenario selected for SECTOR is derived from historical flood incidents concerning "loss of transport in European waterways" that affected social and commercial interests in several ways. The combination of mass flooding in European rivers, along with effects on river transportation (freight and passenger) due to a sunken ship blocking a key river transport channel (named Lorelei), has highlighted a range of cross-border and inter-institutional challenges requiring interoperability of responders. The general focus that was derived from analysis reported in Section 2 emphasises European rivers as a geographical basis for economic activity. High water levels threaten the physical infrastructure (bridges, banks, harbours, container stores, etc.), with consequent threats to business and communities around the river area. The scenario develops over a period - not a big bang, and so management requires early knowledge exchange to support collaborative decision-making and preparation for action. The ensuing resilience discussion, focusing freight transport, has to take account of

- Monitoring and exchanging information on infrastructure status;
- Monitoring river and river traffic status;
- Planning for re-routing: (i) Critical incoming freight (food, medical supplies, oil, etc.), and (ii) Critical outgoing freight (commercial production);
- Identifying risks / cascade effects (e.g. hospital power loss);
- Planning joint response to imminent danger.

Authorities, commerce and responders face several knowledge sharing challenges around map-based environment data, availability of safe routes, alternative freight handling, and the rapid preparation of a joint response plan for public and private partners. These issues have national and international dimensions that emphasise the need for a common operational picture (COP), exchange of status information (ships, water courses, roads and rail alternatives, resilience activities underway), and collective discussion of joint operations.

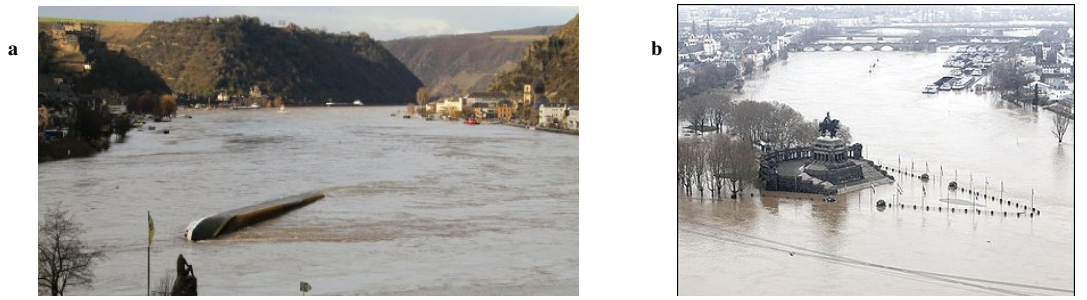

Figure 3 - (a) Sinking at Lorelei passage (Rhine); (b) Rhine and Mosel flood at Koblenz

The actors involved in the target scenario potentially include freight transport operators, harbours, container storage, emergency services, river authorities and other public agencies. Such a partnership requires secure information exchange at the early phase, while weather and water levels indicate imminent danger, and while they can monitor and prepare as the situation develops. This may involve resource sharing such as images captured by air/satellite, marine traffic position data, alternative transport databases, maps and river routes, river police situation assessments, river agency status information, etc.

Our intentions for testing in this scenario is to demonstrate how several agencies can learn and use the CIS, and can be reactive to an impending flood disaster where the features of its development are declared from outside (realism) and they can utilise the CIS to explore its support for collaborative decision making and response planning.

5. Conclusions

This short paper has introduced the information sharing and collaboration needs that recent large-scale disasters have imposed. The EU-funded project named SECTOR aims at providing a solution to these needs by means of a collaboration platform to make interoperable heterogeneous crisis information systems. The current state of the project is to collect all the requirements for the management of large-scale disasters, investigating the pros and cons of the available information sharing platform for crisis management and highlighting a tentative architecture for the envisioned collaboration platform. An opportunity has been identified to support collaboration, not through a single unique system or platform, as has failed in the past, but through a "Common Information Space" (CIS) where the joint ownership of precious information will empower those on whom we rely for civil and critical infrastructure protection. This has benefitted from intensive collaborations with a range of very scarce experts. With their continued guidance we will implement and fully test the CIS and report its usage in a realistic flooding scenario now jointly addressed by seven major EU Funded safety and security projects (DOMINO, 2015)

Acknowledgements

This work has been partially supported by European Commission in the framework of the Collaborative Project “Secure European Common Information Space For The Interoperability Of First Responders And Police Authorities” (SECTOR, http://www.fp7-sector.eu/ - Grant agreement no: 607821).

References

1. OECD (2004), "Large-scale Disasters, LESSONS LEARNED", available on line at http://www.oecd.org/futures/globalprospects/40867519.pdf.
2. Desmond F. (1998), “Investigation into the King’s Cross Underground Fire”, available online at http://www.railwaysarchive.co.uk/documents/DoT_KX1987.pdf
3. *NatCatSERVICE (2012), "Münchener Rückversicherungs-Gesellschaft", Geo Risks Research.*
4. *Cai, G. (2005), "Extending Distributed GIS to Support Geo-Collaborative Crisis Management", Geographic Inf. Science 11(1), 4–14.*
5. *Erl, T. (2005), "Service-Oriented Architecture: Concepts, Technology and Design", Prentice-Hall.*
6. *Greene, R.W. (2002), “Confronting catastrophe. A GIS handbook”, Esri Press.*
7. *The Scottish Government (2011), “Secure and Resilient – A strategic framework for Critical National Infrastructure in Scotland”, Scottish Government pubs.*
8. *Grangemouth Petroleum and Chemical Complex (2014), “Major Incident Control Committee (MICC) Emergency Response Manual”, Petro-INEOS.*
9. *Scottish Resilience Development Services (SCORDS) (2014), “Prospectus Supporting the Commonwealth Games 2014”, Scottish Government pubs.*
10. *L. Bidoux et al. (2014), “ A model driven system to support optimal collaborative processes design in crisis management”, Proceedings of the 11th Conference on Information Systems for Crisis Response and Management (ISCRAM), pp. 245-249*
11. *F. Aligne, and P. Savéant (2011), “Automated planning in evolving context: An Emergency Planning Model with Traffic Prediction and Control”, Future Security 2011.*
12. *DOMINO conference and workshops (2015), “First in a series supported by EU projects Predict, Fortress, Casceff, Sector, Miracle, Driver, and CIPRne”, Zwindrecht, Netherlands.*
13. *A. House, N. Power, and L. Alison (2014), “A systematic review of the potential hurdles of interoperability to the emergency services in major incidents: recommendations for solutions and alternatives”, Cognition, Technology & Work, vol. 16, no. 3, pp 319-335.*
14. *S. Truptil, F. Bénaben, N. Salatge, C. Hanachi, V. Chapurlat, J.-P. Pignon, H. Pingaud (2010), “Mediation Information System Engineering for Interoperability Support in Crisis Management”, Enterprise Interoperability IV, pp 187-197.*
15. *S. Liu, C. Brewster, D. Shaw (2013), “Ontologies for Crisis Management: A Review of State of the Art in Ontology Design and Usability”, Proceedings of the 10th International ISCRAM Conference.*