A System for Collaboration and Information Sharing in Disaster Management

Benjamin Barth, Govinda Chaithanya Kabbinahithilu, Tomaso de Cola, Alexandros Bartzas, and Spyros Pantazis

Abstract Natural and man-made hazards are complex situations involving multiple organizations that need to collaborate. Communication and information exchange are critical for responding to these situations, while at the same time organizations can locally and internationally benefit from expertise, knowledge, and information exchange also outside of an ongoing response for preparation. In order to improve the capabilities of these involved organizations, a communication system is designed based on a content-oriented federated architecture tailored to disaster management. It includes a catalogue that is offering web services for publishing, subscribing, and discovery of disaster information and further services for collaboration of agencies and first responders. The main requirement is access control as responders deal with sensitive data. The system has been designed and successfully evaluated together with end users from several disciplines involved in disaster management.

Keywords Information sharing · Preparedness · Response · Disaster management · Content-oriented architectures

Introduction

Natural and man-made hazards are highly complex situations involving a lot of actors and organizations such as command and control centers, civil protection and medical services, and police and fire fighting units. Communication means are critical for a successful response; a coordinated response is not possible without sharing information, knowledge, actions, and plans. The scale of the hazard thereby

B. Barth (✉) · G. C. Kabbinahithilu · T. de Cola
German Aerospace Center (DLR), Cologne, Germany
e-mail: Benjamin.Barth@dlr.de; Govinda.Kabbinahithilu@dlr.de; Tomaso.deCola@dlr.de

A. Bartzas · S. Pantazis
Space Hellas S.A., Athina, Greece
e-mail: abartzas@space.gr; span@space.gr

H. J. Scholl et al. (eds.), *Disaster Management and Information Technology*,
Public Administration and Information Technology 40,
https://doi.org/10.1007/978-3-031-20939-0_4

influences the complexity, the bigger the event, the more actors are involved. In cross-border case, it becomes an international event requiring bilateral agreements and interoperability which is a major gap as identified by the International Forum to Advance First Responder Innovation (IFAFRI). Ten common capability gaps have been defined out of which Gap 5 is the lag of maintaining interoperable communications with first responders (The International Forum to Advance First Responders Innovation, 2018).

On the other hand, the climate change leads to more extreme weather situations in regions that were known to be moderate. This leads, for instance, to heat waves, droughts in all over Europe, or to forest fires like in Sweden in 2018, where the authorities and first responders are not so used to respond to these hazards as, for example, in the South of Europe where during the fire season forest fires are frequent events. The experience of Southern European countries can help the first responders in the north in this case. Similar conditions and requirements for knowledge exchange can be found in other regions in the world as well.

Our goal is to foster data and information sharing among multidisciplinary stakeholders of multiple organizations also in an international context in order to improve the cooperation capabilities. The work presented in this chapter has been supported by end users from European firefighters, civil protection, medical services, police, and command-and-control organizations and is tailored for the needs of those. We consider the preparedness and response phase of the disaster management cycle in which there are three potential use cases for collaboration and data sharing:

1. During the response of an ongoing incident. Multiple organizations are usually involved either in national or international context. Information exchange and communication among the involved organizations is critical, for example, firefighters are in charge to respond to forest fire situations, but also the police might be involved to for blocking roads and other tasks. Information exchange is the basis for building and maintaining a common operational picture (COP) in this use case. It includes also the communication to the political level and the decision-makers. A good picture about the situation, plans, conditions, and possibilities has to be communicated to them in order to find or justify a good decision and decide for a way forward. Also, the public needs to be considered.
2. Preparedness and training for such an incident. Responsible organizations can prepare by building appropriate scenarios that are used as basis for drills and trainings. Partner organizations, for example, of neighboring countries, could share their information about past incidents and prepare in cooperation scenarios and common response plans.
3. To build a network of end users to exchange expert knowledge, experiences and general information for instance about hazards, scenarios and response plans. Organizations are not necessarily affected by the same incident in this case but are benefitting from the knowledge that other organization have about hazards with similar conditions, for example, by exchanging scenarios and lessons learnt.

In order to improve the interoperability of disaster management organizations, a cloud-based approach is investigated by (Flachberger & Gringinger, 2016; Pottebaum et al., 2016). However, not all organizations have the legal framework for this, or they even have legal constraints that can block end users from uploading data into a cloud drive and share data this way. Response plans and scenarios can include sensitive data such as critical infrastructure which must be handled with care, especially in an international context. The end users need at any point in time information and control about who can access the data.

To address these issues, we propose a content-oriented federated architecture consisting of multiple local units (LU) and a catalogue that provides multiple services for communication and collaboration via RESTful web services, for example, for publications and subscriptions. Thereby, the catalogue is a web server where the LUs connect to for information discovery and other services. As LU, in general, the system for disaster management of an organization can be seen where we take LU as an instance of a HEIMDALL system (Barth et al., 2019). The HEIMDALL project developed a system for scenario building, response planning, and collaboration including the catalogue which was integrated into the system to connect several instances. In principle, the idea is that an LU is owned and managed by an organization having access to its own data sources and other external systems (e.g., weather services). The LU generates and collects data belonging to this organization which can include, for instance, information about the current situation that could also be beneficial for other involved stakeholders.

The content-oriented architecture increases the efficiency of data sharing and allows for access control. The catalogue organizes the communication and data sharing but has no access to the data itself. Data is transmitted from LU to LU in a peer-to-peer-like mode using direct links but with the overall organization of the catalogue, that is, the catalogue stores a description of the data and the LU where it is located and forwards only this information. In this way, the first responders have full control about who can access the data which might be necessary given the sensitivity of some data they deal with or legal constraints they have.

Content-oriented approaches describe a new paradigm of networking that has drawn quite big attention in the research community. The goal is to overcome problems of the host-centric approach of today's internet with high request for digital content of the modern society by using a content-centric approach. Users looking for content request it directly from the network and not from a specific host. Multiple copies of the content can be available in the network which is identified by its name or content descriptor (CD). The nearest copy to the requester is usually delivered which increases the efficiency of the network. In principle, the new paradigm needs a dedicated network consisting of nodes that are able to perform content-oriented routing and provide caching, but it is also possible to run such a network on top of TCP/IP.

Seedorf et al. (2020) presented the use of information-centric networks (ICN) during disaster situations with the focus on damaged communication infrastructures. ICN is a dedicated implementation of a content-oriented architecture. Open research topics are pointed out, and benefits are highlighted. The scenario considered in the study deals with data sharing to users in the field and among the users in the field, while we are considering the data is shared among different organizations at command and control (C&C) level that are usually placed outside the disaster area. Nevertheless, some of the benefits are still interesting for this scenario. By using a content-based approach, we see the following advantages for the communication system:

1. Authentication of named data objects
2. Decentralized content-based access control
3. Publish/subscribe mechanism
4. Sessionless
5. Discovery by name

The approach provides flexibility since it can be adapted to other systems and can provide additional services via the catalogue in future implementations and at the same time due to access control and direct exchange of the data among users ensure security of the data. The remainder of the chapter is organized as follows: the design of the system architecture is detailed including the content-oriented approach, the services and implementation details of the catalogue are presented, and finally, we conclude the chapter.

System Architecture

The content-oriented sharing and collaboration system are integrated in the HEIMDALL system for scenario building and response planning, but its design can be generalized also to use cases outside of disaster management and independently from the integrated system. The integrated system architecture can be seen in Fig. 1. The system has been codesigned with end users during the EU-H2020 HEIMDALL project. It is a modular design based on RESTful web services which allows for an open and flexible access to data products, scalability, and facilitated updates (Barth et al., 2019). It includes various data sources and modules in a single platform offering the services via a web-based graphical user interface (GUI) to the user. The primary users considered are the command and control centers, but the web-based approach allows remote access if connectivity is available, for example, at incident command posts. A service platform connects the modules and provides general integration services such as a geographic information system (GIS) database. User and role management provide security by authentication and access control on a local basis.

The system makes use of different inputs that are shown directly to the user or used as basis to provide further services. During the project, a terrain movement monitoring system and satellite-based earth observation systems have been integrated; other external services can be any web-based services or sensor network and include, for example, weather services which are also used as basis for simulation tools, or the European Forest Fire Information System (EFFIS).

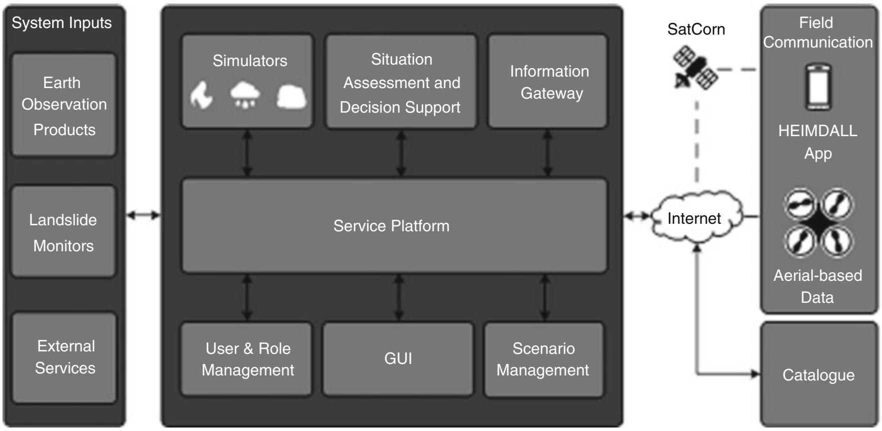

Fig. 1 HEIMDALL system architecture

The system inputs together with the core functionality form the LU, a system instance that is meant to be managed by an organization. The scenario management module is the heart of the system fusing all information flows and feeding a scenario data structure. The scenario data structure has been designed during the project with the end users and allows to store information in a standardized way. It includes, among others, hazard characteristics, decisions and plans, collected data from sensors, and lessons learnt. It is used during the response to record data or to create hypothetical or historical scenarios for preparedness. For interoperability, the scenario data structure can fully be mapped to the EDXL-SitRep format (OASIS, 2016) allowing to share the data with standard compliant receivers.

Furthermore, the HEIMDALL system includes simulation tools to determine the evolution of the hazards; weather conditions for this can be loaded from web services or set manually. The system integration focused on forest fires, floods, and landslides. Therefore, a simulator module for each hazard is provided, but due to the modular design, it can be extended to other types of hazards. Situation/impact assessment and decision support services are provided based on the simulation results.

The HEIMDALL system considers two use cases for information sharing. The first is field communication and information sharing within an organization and the second is communication and collaboration with other organizations. For the first, the HEIMDALL system, including all available information, can be accessed by web browser from anywhere after authentication, for example, from the field. However, for specific situations, it is not helpful to have all information available, especially first responders in the field can be overloaded by the amount of information. For them, an app has been designed that connects via the information gateway to the HEIMDALL platform. Using EDXL-SitRep, a light version of the scenario data is transmitted via the information gateway to the app which includes only the necessary data for first responders in the field. The other way around, the

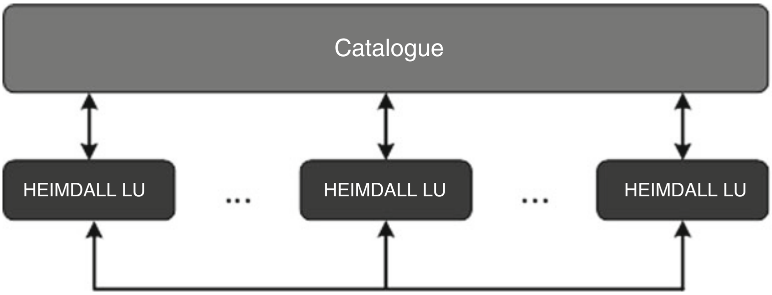

Fig. 2 Federated architecture

app can be used to transmit messages, pictures, locations, and waypoints to get information from the field. Furthermore, the information gateway provides alerting features based on the common alerting protocol (CAP) that can be used for field communication, activation of responders, or warning of the general public.

For field connectivity, a satellite channel or general internet access by mobile networks is considered. The satellite is the backup if terrestrial infrastructure is damaged. A satellite terminal provides a Wi-Fi access point to be able to connect commercial smartphones and equipment.

For the second case, the collaboration with other organizations, the catalogue module connects multiple LUs. The selected approach is based on the Content Oriented Pub/Sub System (COPSS) (Chen et al., 2011). The network structure can be seen in Fig. 2. A global catalogue serves as a so-called rendezvous point that deals in our case with data related to hazards and disaster management, but in principle, it is not limited to this. For scalability, a setup with multiple catalogue modules which exchange information among each other is also possible. In contrast to COPSS, data is not transmitted over the rendezvous point because of data security issues. The data is transmitted using a direct link among LUs. The catalogue helps with the information discovery and the connection to other authorities and offers additional services, which is also a diversion from the underlying COPSS approach. The catalogue is a webserver offering RESTful web services by an application programmable interface (API) that connects to the LUs' components. The basic function is the provision of publish and subscribe features (pub/sub). The LUs are connected to the catalogue on the one hand, and on the other, they can use dedicated interfaces to establish data exchange among themselves via a direct link.

The LUs are the source of the data shared and are owned by the according first responder organization; in content-oriented view, they are also called content owner. They might have access to their own data source, like sensors, etc., or access other external systems like weather providers. The basic idea is that if a content owner wants to share data, it publishes the data using the catalogue by sending a content descriptor (CD). The CD can, for instance, be the name of the data or a meta-data file describing the content. Important is that the CD is unique for each content in the network so that it can be explicitly identified. Subscribers also use a CD to subscribe to topics; here no limitations are given, the more detailed a subscriber defines its CD for subscription, the narrower will be the results. For instance, if there is an interest in lessons learnt for forest fires with wind speeds above 200 km/h, users can subscribe to this or only to forest fires. In the latter case, the results are still fitting, but it might lead to an overhead with data the user is not interested in. Consequently, a defined format for the CDs tailored to the specific needs of first responders supports the approach and improves the user experience.

Our setup is built on top of a TCP/IP network: the catalogue maps between the content-oriented world of the first responder data and the IP world by maintaining tables with CDs and the corresponding LU addresses or identifiers (IDs). If a user wants to subscribe to content, it sends a subscription message (containing a CD to which the user wants to subscribe) to the catalogue which initiates the next steps. In contrast to COPSS, as mentioned, the data is not transmitted via the RP, and the LUs directly exchange the data which on the other hand means that the publisher and subscriber are not decoupled. As communication system, the catalogue is agnostic to the CD format and values, but as mentioned, a well-defined format of the CD is beneficial and more efficient. Our design is based on a JSON meta-data file which can simply be mapped to a URL-based naming scheme as it is common for content-oriented approaches. We defined for each data type in the system a dedicated JSON structure that is completed by the data source and identifies the data uniquely. The meta-data consists of a root element, common for all data types available in the system, and a dedicated part which is specific for each type. Since our approach is JSON based, the format of the CD follows a key value principle; an example in URL form would be:

```
Response Plan/Discipline/Fire Fighters/Hazard/Forest Fire/Area/
Spain/Catalonia/La Jonquera/Key/Value ...
```

Some of the included fields are mandatory from development side; others are tailored directly for the need of first responders. The following fields are specified in the root element:

1. An ID of the organization (LU ID)
2. Role of the user publishing the data, for example, incident commander
3. The discipline of the content owner, for example, emergency medical service, police
4. The area the data applies, subdivided into country, state, and municipality
5. The country the content owner is based
6. The language

This root element structure can be in general be used to describe data for first responders as it holds the main parameters for sharing; it could also be applied to other architecture concepts and can be extended with further fields in the future.

Access Control

As mentioned, security and access control are major requirements, and it is emphasized to be based on role, discipline, and area. With this, data can, for example, be shared only with firefighters, firefighters of a dedicated country, incident commanders of a dedicated country, or any combination. Also, it shall be possible to set it to public so that all participants in the network will be able to access it. As technical solution for the access control, three options have been identified.

In the first option, access control rights are included in the root element of the CD when data is published. In this case, access rights are a mandatory field. The catalogue checks at subscription requests for the necessary access rights before informing the publishers. If access rights are updated at the LU, the updated rights must be forwarded to the catalogue.

The second considers the design presented in (Fotiou et al., 2012) where access control provider (ACP) is a dedicated user and role management module of the LU, that is, a distributed ACP approach. The catalogue does not receive any information about access rights. Received subscriptions are forwarded to the publishers which check on their side if they grant access to this request or not. The check is consequently moved to the LU and allows for a maximum of control.

Last option for access control is attribute-based encryption (Ion et al., 2013). In this approach, the data is authenticated and encrypted at the same time. A key authority (which could be the catalogue) distributes keys based on the access roles set by the data owner. The access roles depend on so-called attributes. Only subscribers fulfilling the attributes can decrypt the data. Attributes, for example, can be the role, discipline, area, or any logical combination.

Catalogue Design

The catalogue itself is based on RESTful web services and offers an API as access point. The architecture of the catalogue is presented in Fig. 3. It includes database tables, for publications and for subscriptions, to offer the basic pub/sub services. Additionally, other services for collaboration and information sharing are provided that have been designed with end users and are presented in the following. Inherently, the web-based architecture offers sustainability by being flexible for possible future services and enhancements.

- Publish (Pub): This is used if a data owner wants to share data with other entities or stop sharing data. For publication, the CD including the root element is sent to the catalogue. The catalogue updates the table of publications and matches it with the subscription table. Subscribers are informed about the update. The CD needs to be completed in order to have a unique name and enabling discovery by name. Given the three options for access control, eventually the first one was implemented: access rights included in the CD. This was an implementation

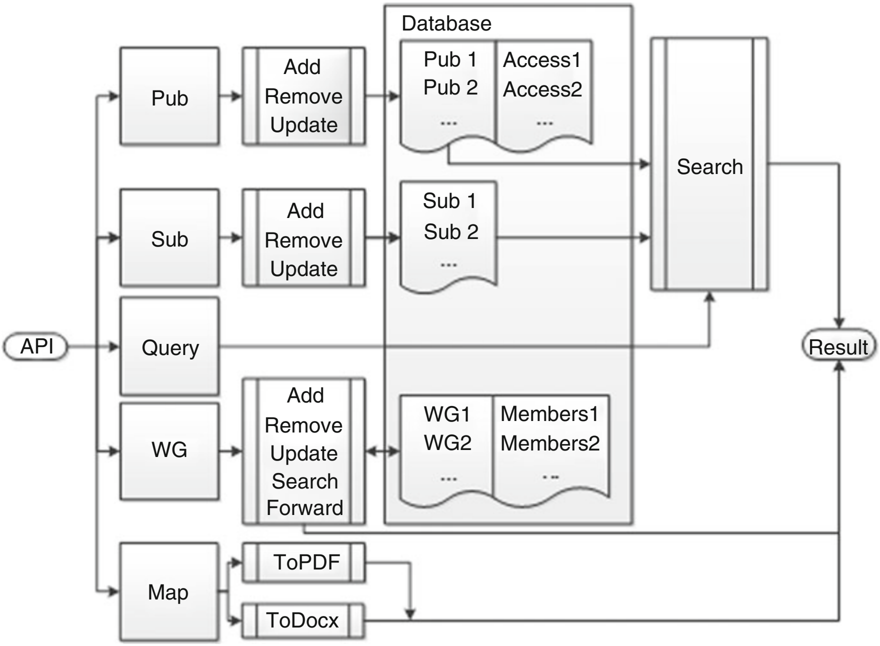

Fig. 3 Catalogue architecture

choice; the other options are valid, have their benefits as discussed, and could replace the selected choice without negative effects. The current implementation foresees that the access rights are transmitted included in the root CD structure. Access rights can be set by combination of LU ID, roles, discipline, and area where area is further divided into country, state, and region as introduced in the section system architecture. It follows the logical equation:

$$(\text{LU ID} \wedge \text{role}) \vee (\text{role} \wedge \text{discipline} \wedge \text{area})$$

This allows sharing it with a specific organization and specific roles of this organization or with certain types of organizations, roles, and areas. It is possible, for instance, to share data with all firefighters of one country, or all incident commanders of a dedicated region. The catalogue applies the access control while matching subscriptions and queries with publications. Access rules are optional; if no rules are set, data is accessible by any entity, and user connected to the catalogue, that is, it is within the network publicly accessible. This enables a network of users and knowledge exchange.

- Subscription (Sub): This is called if a user wants to un-/subscribe to a dedicated topic. A CD including the root element needs to be sent to the catalogue which stores the request in the table of subscriptions and informs publishers that provided suitable content. If subscribed and access rights match, the user will receive a notification for new content once available in the system and can access the data via direct link. In difference to publications, a subscribe request does not include access rights. Subscribing CDs can include only parts of a full descriptor. The more detailed a subscriber defines its CD for subscription, the narrower the results will be. A fully defined CD for subscription will lead to only one result as it defines a unique CD. If the CD contains less fields, for example, only data type and hazard type, more results will be delivered. This very much depends on the user's needs and grants all freedom to define search parameters.

- Query: In contrast to subscription with stored request and automatic notifications, a query is a single request of matching data available in the network. It can be basically understood as a search for data. Queries are performed by CD where search parameters are attached to corresponding part of the CD. The catalogue does not store the data. Consequently, it cannot perform a complete match itself, but it uses the publications table to determine a list of possible matches. If the content fits and access control allows, data is transmitted using the direct user link.
- Map: The map method allows for mapping the EDXL-SitRep files of the scenario data structure to predefined user-friendly reports in PDF or docx format. This enables sharing event information to involved actors that do not have access to EDXL standard receivers or the HEIMDALL system such as, for example, politicians. It creates a formatted printout of the scenario data providing a report of the situation. The data is transmitted to the catalogue with the selected format, and the catalogue returns the converted data. Optionally, a list of addresses can be added. In this case, the catalogue automatically shares the converted data with the addresses.
- Working group (WG): WG enables live collaboration on a scenario structure synchronized among all members. A responsible agency invites other partners to the work group where any scenario can be used as a starting point. During response, members are able to update the scenario structure based on certain access rules to stay compliant with legal formalities; however, after consultation with the end user, all partners of the group shall able to read the information. This means, a fast way of sharing all information among the involved actors as they all get the same information fosters the cooperation capabilities and improves the COP of all involved organizations. Nevertheless, read and write rights are a matter of configuration and could be adapted case by case. After closing the WG, a local copy of the scenario can be distributed for documentation, and it can be used as recorded historical event for training, analyses, and lessons learnt process. Any entity can create a new group and add or remove members by sending a scenario ID, a group name, and the LU IDs of the members. Confirmation requests are sent out in this case. The creator owns the scenario and can decide to close the group. The idea is that it will be the legally responsible organization triggering the group. Creating a new work group returns a unique work group ID (WID). Access to the scenario is locally granted to the members of the group, that is, the data is not shared with the catalogue. An update of data structure triggers a notification to every member of the group informing them

about new entries. Using the WID, any member of a group is allowed to push a message to all others in the group.

Conclusion and Future Work

The design of the catalogue module for data sharing and collaboration of actors in disaster management was presented. The catalogue is the connecting unit and enabler of a decentralized federated content-oriented architecture of multiple local units (LUs) offering services for data publication, subscription, discovery, and other services for collaboration and networking. Data security and access control are major requirements considered. Data is neither forwarded nor stored at the catalogue. Content descriptors (CDs) are tailored for first responders for improved user experience. Furthermore, it offers options to map data to standardized formats generating reports in a predefined structure.

With the federated architecture based on content-oriented design, a flexible solution is provided that at the same time ensures security and holds extension opportunities for future implementations. This includes services available at the local units and at the catalogue. An example could be a translation service: especially, in cross-border scenarios, language can be a big problem if several organizations are involved. The predefined fields of scenario data structure could be translated into several languages. Interoperability and a standardized model are required for this.

The presented concept is integrated as part of the HEIMDALL system and has been evaluated and demonstrated throughout the project in operational environment with end users from firefighters, medical service, civil protection, command and control, and police. During a set of four demonstrations, feedback was collected and integrated into the development presented. An interesting topic to be further investigated is the access control; other options for future additional mechanisms for providing access to shared content can be investigated. Such mechanism that can achieve strong consent between the disciplines wishing to share/exchange content is the use of smart contracts and block-chain encryption.

Acknowledgments The HEIMDALL project received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 740689.

References

Barth, B., et al. Design of a multi-hazard collaborative system for scenario-based response planning. In *Lecture notes in informatics, proceedings, Informatik 2019*, 23–26 Sept 2019.

Chen, J., Arumaithurai, M., Jiao, L., Fu, X., & Ramakrishnan, K. (2011). COPSS: An efficient content oriented publish/subscribe system. In *Seventh ACM/IEEE symposium on architectures for networking and communications systems*.

Flachberger, C., & Gringinger, E. (2016). Decision support for networked crisis & disaster management – A comparison with the air traffic management domain. In *ISCRAM 2016 conference proceedings – 13th international conference on information systems for crisis response and management*, Rio de Janeiro.

Fotiou, N., Marias, G. F., & Polyzos, G. C. (2012). Access control enforcement delegation for information-centric networking architectures. In *ICN'12*, August 17th, 2012, Helsinki, Finland.

Ion, M., Zhang, J., Schuchard, M., & Schooler, E. M. (2013). Toward content centric privacy in ICN: Attribute-based encryption and routing. In *SIGCOMM'13*, August 12–16, 2013, Hong, Kong, China.

OASIS. *Emergency data exchange language situation reporting (EDXL-SitRep) version 1.0*, 6 Oct 2016, available at http://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/edxl-sitrep-v1.0.html. Last accessed 9 Mar 2022.

Pottebaum, J., Schäfer, C., Kuhnert, M., Behnke, D., Wietfeld, C., Büscher, M., & Petersen, K. Common information space for collaborative emergency management. In *Proceedings of the IEEE international symposium on technologies for homeland security 2016*. Waltham, MA, USA.

Seedorf, J., Arumaithurai, M., Tagami, A., Ramakrishnan, K., & Blefari-Melazzi, N. *IETF RFC 8884, "Research directions for using information-centric networking (ICN) in disaster scenarios"*, Oct 2020. https://doi.org/10.17487/RFC8884.

The International Forum to Advance First Responders Innovation (IFAFRI), Statement of Objectives (SOO) for Technologies Related to: The ability to maintain interoperable communications with responders in any environmental conditions, Dec 2018.