A Content Oriented Information Sharing System for Disaster Management

Benjamin Barth
German Aerospace Center (DLR)
Benjamin.Barth@dlr.de

Govinda Chaithanya Kabbinahithilu
German Aerospace Center (DLR)
Govinda.Kabbinahithilu@dlr.de

Alexandros Bartzas
Space Hellas S.A.
abartzas@space.gr

Spyros Pantazis
Space Hellas S.A.
span@space.gr

Tomaso deCola
German Aerospace Center (DLR)
Tomaso.deCola@dlr.de

ABSTRACT

In response to natural and man-made hazards multiple organisations usually are involved in a very complex situation. On the other hand, extreme weather situations due to the climate change create hazards in areas which were considered safe before. In order to improve the capabilities of involved organisations in responding and preparing for disaster events, the availability of an efficient information sharing approach is a key enabler. To this end, we propose a communication system based on a content oriented architecture tailored to disaster management. It includes a catalogue that is offering web services for publishing and subscribing of disaster information and for further collaboration amongst agencies and first responders. Moreover, the considered approach also allows for full content access control and enables a flexible system. The paper shows the current status of the system design. Next steps will include the implementation and evaluation of the approach.

Keywords

Information Sharing, Preparation, Response, Content Oriented.

INTRODUCTION

Natural and man-made hazards are highly complex situations involving a lot of actors and organisations such as command and control centres assessing the risk for the population and infrastructure and preparing and coordinating the response, civil protection units and medical services save lives, police and fire fighting units regulating and responding to the hazard. The situation can become even more complex at international level if for instance bilateral agreements are missing or unstandardized protocols are used. The IFAFRI forum identified the lag of maintaining interoperable communications with first responders as Gap5 out of ten of their common capability caps (IFRAFRI, 2018) which shows a key requirement for effective cooperation of all involved stakeholders and first responders is communication. At any point in time it is crucial for end users to have information about the situation and evenly important to know who else has already access to this information.

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 head 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.

Our goal is to foster data and information sharing among multi-disciplinary stakeholders of multiple organisations also in an international context in order to improve the cooperation capabilities. Our work is tailored for the needs of first responder organisations and disaster management but the approach can also be applied to other use cases. Accordingly, for collaboration and data sharing there are three potential use cases:

- First, an actual ongoing incident in which multiple organisations are usually involved. This also applies to an international context where cross border scenarios could engage multiple organisations from more than one country. Information exchange and communication among the involved organisations is critical, e.g. in a forest fire situation usually dealt by firefighters, the fire can approach the road network and the police will be involved to block the road. Information exchange is the key in building and maintaining a common operational picture.
- Second, preparedness and training for such an incident. Responsible organisation could prepare for such incidents by building appropriate scenarios together that are used as basis for drills and training. Fire fighters of neighbouring countries could for instance share information about past incidents and prepare in cooperation scenarios and common response plans.
- Third case, is more globally to build a network of end users to exchange expert knowledge, experiences and general information for instance about hazards, scenarios and response plans. Organisations are not necessarily affected by the same incident in this case but are benefitting from the knowledge that other organisation have of hazards with similar conditions and the response to it in order to strengthen their own capability to respond e.g. by exchanging scenarios and lessons learnt.

Recent projects aiming to improve the interoperability of disaster management organizations follow a cloud based approach (Flachberger, 2016, Pottebaum, 2016). However, during the requirements collection we found that some organizations have legal constraints that can block end-users from uploading data into a cloud drive and sharing it in this way with other actors: some data can be quite critical and sensitive especially in an international context. The end-users need at any point in time information and control about who can access the data.

For these three use cases, we propose in this work in progress paper a content oriented federated architecture for data sharing and information exchange consisting of multiple local units (LU) and a catalogue that provides collaboration services. As LU basically the system for disaster management of an organisation can be seen. We assume as LU in this paper an instance of a HEIMDALL system (Barth et al., 2019) owned by an organisation and having access to its own data sources and other external systems (e.g. weather services). The design of the solution, however, can also be adapted to other disaster management systems and with this be used as communication system in general. The LU generates and collects data belonging to this organisation which are important for the first responders. Data can include for instance information about the current situation that could also be beneficial for other involved stakeholders.

The architecture is organised in a content-oriented way which increases the efficiency of data sharing. A global catalogue to which all LUs can connect organises the communication and data sharing. The catalogue has no access to the data itself, the data is transmitted from LU to LU in a peer to peer likemode but with the overall organisation of the catalogue. 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. Multiple services for communication and collaboration are offered by the catalogue via RESTful web services e.g. for the discovery of data offered by other authorities.

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. The content is identified by its name or a content descriptor (CD) and it can be multiple copies of it in the network. The closest one 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 (Seedorf et al., 2018) presented how information centric networks (ICN) can be used during disaster situations with the focus being 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 organisations 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:

- Authentication of named data objects
- De-centralized content-based access control
- Publish/subscribe mechanism
- Sessionless
- Discovery by name

Our 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 sections of the paper are organised as follows: (I) the design of the system architecture is detailed including the content oriented approach, (II) the current emphasized services of the catalogue are presented, and (III) concludes the work in progress paper.

SYSTEM ARCHITECTURE

The selected approach is based on the Content Oriented Pub/Sub System (COPSS) (Chen, 2011). The network structure can be seen in Figure 1. 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. 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 can offer other 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.

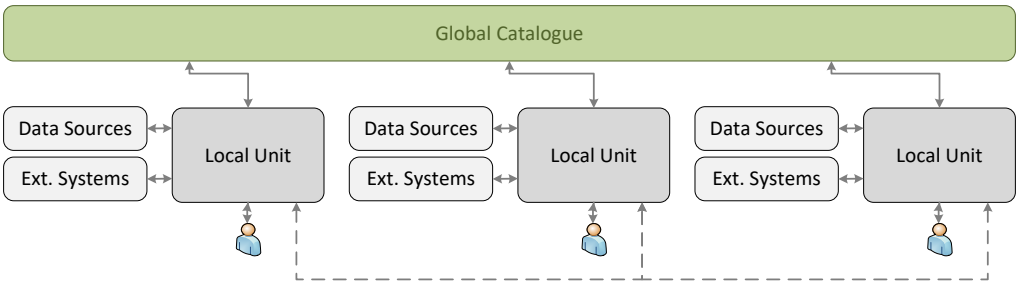

Figure 1. Data Sharing

The LUs are the source of the data that is shared and are owned by the according first responder organisation, 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 the results be. 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 a table with all 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 for this subscription. In contrast to COPSS (Chen, 2011), as described the data is not transmitted via the RP, the LUs directly exchange the data which on the other hand means that the publisher and subscriber are not decoupled.

Our approach provides opportunities for future implementations: on one hand, different services can be available in each local unit and made accessible to users accessing other local units by means of publishing them

in the catalogue. On the other hand, additional external services can be easily added to the overall architecture by publishing the corresponding services or information in the catalogue and establishing the corresponding connection, without additional integration efforts at the LU.

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, hence, during our design we agreed on a JSON based 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 our system a dedicated JSON structure that is completed by the data source and identifies the data uniquely. 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/Fire fighters/Hazard/Forest Fire/Area/Spain/Catalonia/La Jonquera/Key/Value …

We define a root element that is common to all data types available in our system. Some are mandatory from development side; others are tailored directly for the need of first responders. The meta-data shall include this root part and the dedicated part is attached to it. It includes the following fields:

- role of the user publishing the data, e.g. incident commander;
- an ID of the organisation;
- the discipline of the content owner, e.g. emergency medical service, fire fighters;
- the area the data applies to as string, including if possible, country, state, municipality;
- the country the content owner is based

The definitions of the CD can in principle be applied with some adaptions to other data meaningful for first responders which would increase the availability of data in the system but it could also be used for other systems as the description of the data is generic. Our definitions can be used as basis for this, for example our CD for a fire simulation could be extended and used for other simulation types. The root element can be in general be used to describe data interesting for first responders as it hold the main parameters for sharing it. This could also be applied to other architecture concepts and can be extended with further fields in future.

ACCESS CONTROL

As mentioned security and access control is a main requirement and it is emphasized to be based on role, discipline and area. With this data can for example be shared only with fire fighters, fire fighters 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 approach, the access control rights are included in the root element of the CD when data is published. In this case it is 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 approach considers the design presented in (Fotiou et al., 2017) where access control provider (ACP) is a dedicated user and role management module of the LU, i.e. 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 approach for access control is attribute-based encryption (Ion et al., 2013), (Goyal, 2006). In this approach the data is authenticated and encrypted at the same time. A key authority distributes keys for decryption based on the access roles set by the data owner. The access roles depend on so called attributes. Only subscribers which fulfil the attributes can decrypt the data. Attributes for example can be the role, discipline, area or any logical combination.

MODULE DESIGN

The catalogue itself is based on RESTful web services and offers an API for this. It includes two database tables, one for publications and one for subscriptions, to offer the basic pub/sub services. Other services can be included in the API and offered via web. The functionality presented in this paper reflects the work in progress where we are considering the services presented in the following and illustrated in Figure 2. Further services can be considered for future implementation.

Publish (Pub): this can be 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 forwards the information to suitable subscribers. The CD should always be as complete as possible in order to have a unique name and enabling a good discovery of the name.

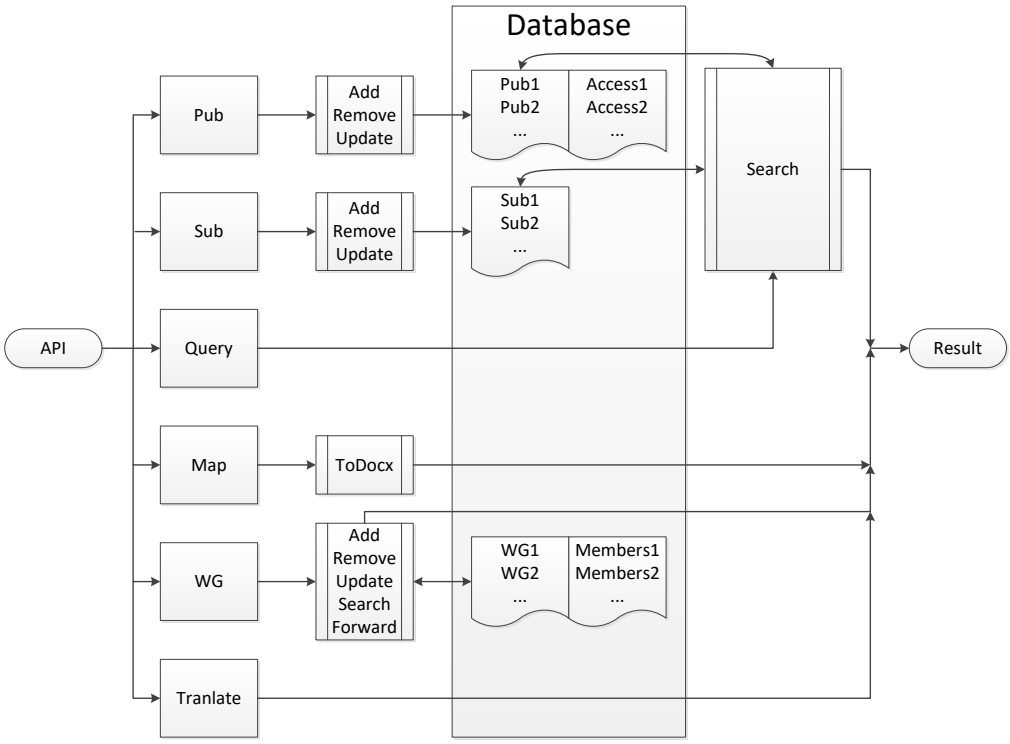

Figure 2. Module Design

Subscription (Sub): this can be called if a user wants to un-/subscribe to a dedicated topic. A CD including the root element needs to be send to the catalogue which stores the request in the table of subscriptions and informs publishers that provided suitable content. If subscribed, the user will receive available data once available in the system, i.e. someone published matching content.

Query: in contrast to subscription where there are continuous updates, a query is a single request of matching data available in the network. 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: this method can be used to map some data formats to another and shall increase interoperability. For instance, the HEIMDALL system offers a structure for storing scenario information, for interoperability this can be mapped to common standards. Specifically it is foreseen to map some parts of the scenario data to EDXL-SitRep (OASIS, 2016) as situation report and this on the other hand to PDF or MS-Word in order to share it with other organisations or politicians. The data is transmitted to the catalogue with the supported and desired 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.

Temporal Working Group (WG): this offers all functionality needed for forming a WG. The idea is that in response mode (during a disaster situation) all or some involved organisations can form a WG that lasts for this incident. The WG works on a synchronized scenario object which means that they automatically have access to the same information. If e.g. fire fighters update the perimeter of the hazard, other involved actors receive the update automatically. This improves the common operational picture of all involved organisations and fosters the cooperation capabilities. If the incident is over the group is resolved and included organisations keep their local copy of the scenario object. To start this process an organisation sends a reference to a scenario object to the catalogue and invites other organisations to join. Also references to an empty scenario object can be transmitted. All organisations can now perform updates on their scenario object which are automatically updated via the direct user links. The catalogue supports with the synchronisation and services for group management.

Translation: especially, in cross border scenarios language can be a big problem if several organisations are involved. For this, standard compliant values can be mapped to different languages and help with the

understanding.

CONCLUSION AND FUTURE WORK

In this paper we presented our design of the catalogue module for data sharing and collaboration of actors in disaster management. The catalogue is the connecting unit and enabler of a federated architecture of multiple local units (LUs). The catalogue is based on a content orient approach and does offer services for data publication, subscription and query. Content descriptors are tailored for first responders. Furthermore, it offers options to map data to standardized formats and a working group feature for cooperative management of scenario files. It is based on a defined content descriptor for certain data types which improves the user experience.

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. The presented concept is in design phase and will be implemented in a next step and integrated as part of the HEIMDALL system. It will be tested in practice and evaluated in a demonstration event with end users from different disciplines involved in disaster situations. We expect feedback on the design and improvements as well as additional services to be considered.

We will investigate more on the access control and decide which out of the options can be considered. The access control is also not limited to these options present. Furthermore, other options for future additional mechanisms for providing access to shared content will 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 is receiving funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740689.

REFERENCES

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", December 2018

C. Flachberger, and E. Gringinger, "Decision Support for Networked Crisis & Disaster Management – A Comparison with the Air Traffic Management Domain", ISCRAM 2016 Conference Proceedings – 13th International Conference on Information Systems for Crisis Response and Management. Rio de Janeiro, 2016

J. Pottebaum, C. Schäfer, M. Kuhnert, D. Behnke, C. Wietfeld, M. Büscher, K. Petersen, "Common information space for collaborative emergency management", Proceedings of the IEEE International Symposium on Technologies for Homeland Security 2016. Waltham, MA, USA.

Benjamin Barth et al., "Design of a multi-hazard collaborative system for scenario-based response planning", Lecture Notes in Informatics, Proceedings, Informatik 2019, 23rd-26th 2019

irtf-icnrg-disaster-09, Jan Seedorf et al., "Research Directions for Using ICN in Disaster Scenarios", Work in Progress, Internet Research Task Force, Nov. 2019

J. Chen, M. Arumaithurai, L. Jiao, X. Fu, K Ramakrishnan, "COPSS: An Efficient Content Oriented Publish/Subscribe System", Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems, 2011

Nikos Fotiou, Giannis F. Marias, George C. Polyzos, "Access Control Enforcement Delegation for Information-Centric Networking Architectures", Aug. 2017

M. Ion, J. Zhang, M. Schuchard, E. M. Schooler, "Toward content centric privacy in ICN: Attribute-based encryption and routing," Aug. 2013

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", The 13th ACM Conf. CCS, Oct 2006.

OASIS, "Emergency Data Exchange Language Situation Reporting (EDXL-SitRep) Version 1.0", 06th October 2016, available at http://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/edxl-sitrep-v1.0.html , last accessed 23.01.2020