

Modelling emergency management capabilities and information flows of interdependent systems

Mariachiara Piraina and Paolo Trucco

Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milano, Italy, E-mail: mariachiara.piraina@polimi.it; paolo.trucco@polimi.it.

Effective emergency response requires to share information and to coordinate actors' activities, since there is not a single organization able to provide all the information, resources and competences to manage an emergency. This is an even more challenging issue that it comes with interdependent and interconnected systems (e.g. critical networked infrastructure systems). On one side, there is a clear need to assess responders' capabilities with the aim of improving the effectiveness of a collective response; on the other, information flows needed to orchestrate available resources and coordinate activities should be clearly detailed in terms of contents and means of communication. This study aims at developing a new integrated methodology to standardize the modeling of organizational and operational emergency capabilities of different actors and the related information flows. It entails the adoption of a set of coherent modeling and analysis tools that are usable by and shared among different actors. To this end, the scientific and technical state-of-the-art was critically reviewed. The extant body of knowledge resulted to be scanty and highly fragmented, particularly when it comes to methodologies applicable under an all-hazard approach and to heterogeneous multi-actor environments. Departing from this background, the paper proposes a novel methodology which grounds on a selected subset of tools, part of the NATO Architecture Framework (NAF), and generalizes its use in a public emergency management context.

Keywords: Emergency Management, Interdependent infrastructure systems, Response capabilities, Resource orchestration, Information sharing, Modeling, NATO architecture framework.

1. Introduction

Effective emergency response requires to share information and coordinate actors' activities (Nunavath et al. 2015), since there is not a single organization able to provide all the information, resources and competences to manage an emergency (Petrenj et al. 2013). Actors with different roles and competences are involved in emergency situations, thus communication and coordination become fundamental (Cedergren et al. 2018).

This is an even more challenging issue when it comes with interdependent and interconnected systems (e.g. critical networked infrastructure systems). In the specific case of critical infrastructure, the focus is on assets or systems that are essential for the maintenance of vital societal functions and whose disruption impacts the society (European Commission 2008). The imperative of protecting them against well-known and unknown threats, requires the collaboration of different actors, such as governmental agencies and the private sector (Department of Homeland Security (DHS) 2009).

Moreover, when transboundary interdependent infrastructure systems are at stake the complexity of the overall socio-technical system increases, as well as the implementation of information sharing and, cooperation processes between different

organizations (Kapucu 2009). To favor an effective interaction, when organizations from different countries are present, it is fundamental to have understandable and interoperable information, that means sharing data that are compatible with different organizations' systems (Vollmer et al. 2019).

The presence of tools and technologies to share the information and communicate simplifies the response process (Goubran et al. 2016) but is not enough. Indeed, responders are located in different areas, operate on different portion of the system with different responsibilities and priorities, and their data are not homogeneous. It becomes fundamental to ensure "that the right people get the right information at the right time" (Singh et al. 2009). Indeed, according to Patriarca et al. (2017), the complexity of unforeseen scenarios can be managed thanks to human flexibility and in particular through the interaction among individuals.

Furthermore, the transmission of correct and timely information is strongly dependent on the level of trust between actors (Norris et al. 2008). According to Seppänen et al. (2013), "a certain amount of trust exists between actors. However, if trust could be increased the availability, reliability, and temporal accuracy of information could be improved". In many cases, communication problems are the result of

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference.

Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio

Copyright © 2020 by ESREL2020 PSAM 15 Organizers. *Published by* Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2020psam15-paper

organizational differences like languages, cultures, rules, norms, but also personal differences and inter-personal relationships that may lead to a lack of trust (Fischer et al. 2016).

As a contribution to overcome the abovementioned open issues, this research aims to investigate emergency management capabilities and information flows of interdependent systems. On one side, there is a clear need to assess responders' capabilities with the aim of improving the effectiveness of a collective response; on the other, the information flows needed to orchestrate available resources and coordinate activities should be clearly detailed in terms of contents and means of communication.

Coherently, this study aims at answering the following research question:

RQ: How to develop a comprehensive methodology which integrates information flows analysis into the mapping and analysis of intra- and inter-organizational emergency management capabilities?

The research process is divided into two phases. Firstly, a thorough review of extant scientific and technical literature on the subject will be carried out, to capitalize on existing knowledge, select the most relevant tools and methods, and possibly envisage opportunities for technology/practice transfer (e.g. from Military&Defence to Civil Protection and CIP). The results of the first phase will be used to design a novel framework for inter- and intra-organizational capability mapping where information flows and communication channels are properly detected and analyzed. Finally, recommendations will be drawn on the use of the framework for different purposes and on other relevant implementation issues (methodology).

The rest of the paper is structured as follows. Section 2 presents the literature review on methodologies, methods or techniques for system mapping and analysis, focusing more on the NATO Architecture Framework. Stemming from what is missing in the literature, a framework has been developed in Section 3 for modelling emergency management capabilities and information flows of interdependent systems. In Section 4 the way of implementing the framework is presented. Finally, Section 5 draws the conclusions and the next steps of the research.

2. State-of-the-art review

A systematic search of the scientific and technical literature was conducted on Scopus and Google respectively by adopting multiple combinations (AND sequences) of keywords: "information flow*", "information sharing", "capabilit*", "map*", "tool*", "framework*", "critical infrastructure", emergency. At first, the search

started on Scopus limiting the results on English sources and only 35 documents were found, after the exclusion of contributions focused on the technical aspects of information sharing (e.g. communication protocols). Then a snowballing sampling was adopted starting from the references of the first sample of papers, and 3 more papers were included. In addition, the search was enlarged looking at the technical literature on Google (e.g. research projects) using the same keywords. Finally, the selected scientific and technical literature was critically reviewed, focusing on the modelling of information flows and of emergency management capabilities, thus proposing frameworks, methods or tools. At the end of this selection process 9 useful sources were mainly identified that are the ones included in the state-of-the-art review: three of them come from the scientific literature, while six belong to the technical literature.

The existing body of knowledge resulted to be scanty and highly fragmented, in particular when it comes to methodologies, methods or techniques for system mapping, analysis and assessment, which are applicable from an all-hazard perspective and to highly heterogeneous multi-actor environments.

The importance of information sharing and the related challenges in the emergency management context, clearly emerged in the majority of collected literature. According to Norri-Sederholm et al. (2017) the absence of a shared terminology can generate misinterpretation of the messages with consequent communication problems and possible poor decisions. The importance of having integrated platforms to coordinate the emergency response tasks assigned to people working in different sectors it is highlighted by Choi et al. (2019). According to Usuda et al. (2017), the absence of a nationwide information sharing system causes issues like much time spent by organizations on collecting information, and difficulties in coordination. For instance, this is the case of the European project IN-PREP, that is aimed at creating "a platform to enable crisis managers across Europe to collaborate, train together, and cooperate on planning processes" (Vollmer et al. 2019).

However, the large majority of contributions in literature focus on technical aspects of the information sharing process, whereas the organizational issues, in the preparedness and response phases, are not well addressed. For instance, from the literature, there is evidence of some communication protocols, like the Common Alerting Protocol (CAP), used to standardize the way emergency messages are disseminated among the communications systems of different actors (FEMA 2019). What is missed is a methodology that allows to model coordinated

emergency management operations and the features of information flows among interdependent actors.

Despite scholars largely agree on the need of cooperation among all the stakeholders involved to implement a timely and adequate response (Müller and Reinert 2014), the literature on how to design and implement a cooperative operations model is still scanty. For instance, this is one of the main issues addressed by the SALUS project (SALUS 2019) that wanted to provide “a framework and approach to coordinate the perspectives of different types of stakeholders within a PS&S [Public Safety and Security] organization” (Müller and Reinert 2014). It was based on the adoption of an Enterprise Architecture aimed at both describing the different parts of the organization and defining the interactions between them. The framework proposed is the Open Safety & Security Architecture Framework (OSSAF) that incorporates concepts from the Zachman Architecture Framework (ZAF), the TOGAF framework and the NATO Architecture Framework (NAF) (Brouet et al. 2014). In particular, in the SALUS project, some views from NAF Version 3 were used to provide a vocabulary and an approach to describe the architectures.

2.1 NATO Architecture Framework

Considering the literature reviewed and the objectives of this research, a subset of tools which are part of the NATO Architecture Framework (NAF) were selected to be part of the methodology developed in this study. “The aim of the NATO Architecture Framework Version 4 (NAFv4) is to provide a standard for developing and describing architectures for both military and business use” (NATO Architecture Framework 2018, p.11). This methodology is based on the use of some of the Viewpoints of NAFv4 which represents a mean to describe and analyze particular aspects of the actors involved in the analysis.

In particular, NAF relies on the use of Architecture Frameworks to show how to organize and represent a system (e.g. a system could be a company, a product or a service) through the description of the architectures (NATO Architecture Framework 2018) that are “the fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution” (ISO/IEC/IEEE 40210, 2011).

This framework was chosen since it allows to standardize the way of mapping the information flows between different actors and offers a way of

representing an enterprise in terms of its processes, resources and capabilities.

NAF gives the possibility to adopt a varied set of Viewpoints (NATO Architecture Framework 2018) that belong to the following categories:

- *Concept Viewpoints*: are used to organize and analyze the high-level capabilities of a given system;
- *Service Specification Viewpoints*: are used to sustain the description of services (not adopted in this study);
- *Logical Specification Viewpoints*: are used to map and analyze the interactions between nodes (i.e. organizations involved in emergency management);
- *Physical Resource Specification Viewpoints*: are used to represent human and material resources;
- *Architecture Meta-Data Viewpoints*: are used to sustain the architecture’s administrative aspects (not adopted in this study).

However, according to the analysis conducted and to the specific objectives of the study, a sub-set of Viewpoints, which are the most suitable, can be selected and new ones can be added when needed. Starting from the entire list of Viewpoints in NAFv4, they have been analyzed and a specific short list of tools have been selected, as shown in Table 1.

Table 1. NAFv4 tools selected and their use within the proposed methodology.

Tools	Use
C1 – Capability Taxonomy	To represent and organize emergency management capabilities of organizations.
C3 – Capability Dependencies	To highlight the dependencies among the capabilities.
C4 – Standard Processes	To show in which emergency management phase the capabilities are required.
C7 – Performance Parameters	To represent the resources that emergency responders have (e.g. materials, people, physical infrastructure systems, competences).
L2 – Logical Scenario	To represent the interactions between different organizations (e.g. exchanged information, communication channels used), highlighting the presence of unidirectional or bidirectional communication.
L3 – Node Interactions	To represent the sender and recipient of the information, the typology of exchanged

	information, or the communication channels used.
L6 – Logical Sequence	To show the chronological sequence of activities, highlighting the emergency management phase when the information is exchanged.
P2 – Resource Structure	To show the interactions between different organizations and the resources they have. It is like a summary of the main information collected through the other tools.
P4 – Resource Functions	To represent the key roles inside each single organization and thus to understand the responsibilities of different actors.

3. A methodology for analyzing interdependent systems

The idea behind the development of a framework for modelling emergency management capabilities and information flows of interdependent systems is to provide a methodology to analyze these systems according to three main levels of analysis. In particular, the most suitable NAFv4 tools are selected and grouped on the basis of the goals for which they can be used.

The framework is organized to support three levels of analysis, according to different stages or purposes of the study:

- A) General mapping of emergency management operations and information flows;
- B) Emergency scenario-based mapping of operations and information flows;
- C) Inventory of inter- and intra-organizational capabilities.

The unit of analysis adopted for this study is the organization, thus, the term *actor* doesn't represent a single person but an entire organization. Having this idea in mind, a capability of an organization "is a demonstrable ability to respond to, and recover from, a particular threat or hazard" (Cabinet Office 2012), thus it can be considered as the tasks an organization is able to provide when a disruptive event occurs. In a simpler way, a similar definition is recalled in NAF: "a capability is a description of an ability to do something" (NATO Architecture Framework 2018, p.73).

However, before applying the developed framework, there are some decisions to make regarding the scope of the analysis. At first, it is necessary to identify the geographical boundaries, by selecting the systems and organizations that we

want to analyze in the defined geographic area. Moreover, with respect to interdependent systems, it is required to define which type of interdependence to consider (geographic, physical, cyber, logical) and thus the systems and actors to include in the study.

The following paragraphs present the combination of tools selected to support each level of analysis, according to their specific goals.

3.1 General mapping of emergency management operations and information flows

At first, it is suggested to focus the attention on the NAF tools that could be adopted for the general mapping of emergency management operations and information flows. It includes all the tools used to have a general overview of the organizational structure of the actor under analysis. In particular, this level of analysis is used to represent the roles of emergency responders, the exchanged information with other actors, the communication channels used, the resources owned and the capabilities each organization is able to provide. Thanks to this general mapping, the "as is" situation is analyzed so that the main criticalities and points of possible improvement are identified.

At this level, it is suggested to make an analysis independently from the specific emergency management phases in which the actors are involved. However, it is possible to customize the way some tools are used, thus making a distinction between different emergency management phases (i.e. prevention, mitigation, preparedness, response, recovery).

The tools adopted for this first level of analysis are depicted in Fig. 1, the specific subset of tools is placed on the left and the goals to be achieved on the right. Some tools are connected by a logical sequence (i.e. L3 and L2, C7 and C1, C7 and P2). For instance, it is suggested to implement the tool C7 before C1 because the identification of the resources owned by organizations (i.e. C7) will help in identifying what the relative capabilities are (i.e. C1). On the other side, there are tools that can be developed in parallel since they are used to represent different aspects (e.g. P4 and L3).

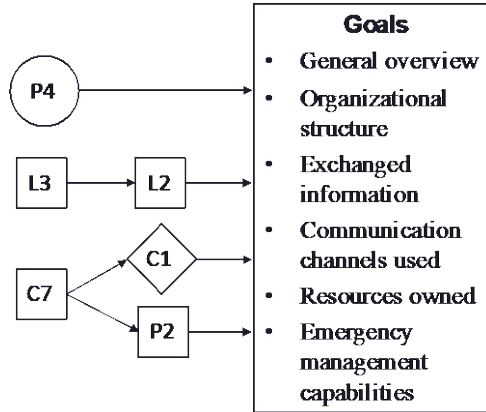


Fig. 1. Level A of the framework: general mapping of emergency management operations and information flows.

3.2 Emergency scenario-based mapping of operations and information flows

When a higher level of detail is required, thus introducing the need to focus on specific events or scenarios, another type of analysis is suggested. In this case, the goal of the analysis is to investigate the information flows, the emergency management capabilities and the resources available for specific emergency scenarios, highlighting the interactions among actors.

Even if Level B is independent from Level A, in cases where both the levels are required, it is suggested to implement them in sequence (A→B).

The tools selected for emergency scenario-based mapping are reported in Fig. 2. Most of the tools identified are the same used for the general mapping, but they are implemented with a different level of detail. For instance, in this case, there is a higher focus on the analysis of the information flows in different emergency management phases. At Level A the information collected are more general and are not related to specific events.

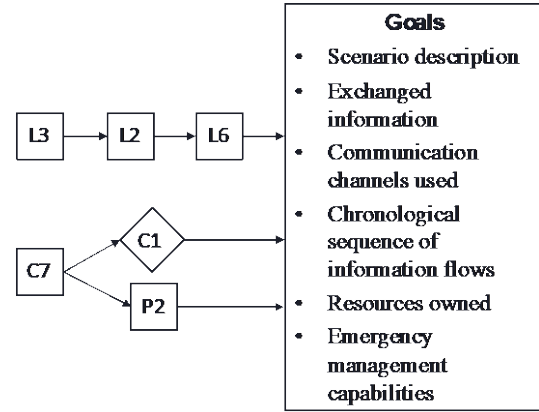


Fig. 2. Level B of the framework: emergency scenario-based mapping of operations and information flows.

3.3 Inventory of inter and intra organizational capabilities

The last level of analysis (Level C) is aimed at defining the inventory of inter- and intra-organizational capabilities, where the unit of analysis is the organization. As shown in Fig. 3, it is suggested to start from the analysis of the resources owned by each organization, and thus from the viewpoint C7, in order to define and measure the capabilities. This type of analysis provides information readable by all the actors involved in the management of an emergency. This because it guarantees a minimum level of visibility on the capabilities that other actors can provide, thus reducing the time needed to orchestrate the interactions among them.

In summary, the goal of Level C is to create an inventory of the resources owned by each one of the organizations involved, their emergency management capabilities and the relationships between inter- and intra-organizational capabilities.

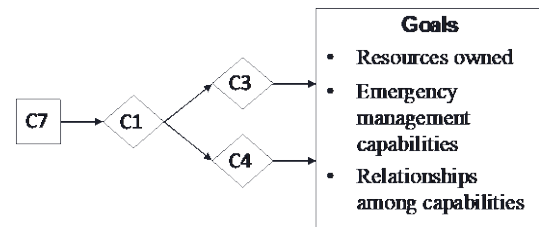


Fig. 3. Level C of the framework: inventory of inter- and intra-organizational capabilities.

Table 2. Goals and levels of analysis covered by the framework.

GOALS	A) General mapping of emergency management operations and information flows	B) Emergency scenario based mapping of operations and information flows	C) Inventory of inter and intra organizational capabilities
Overview of the organizational structure: key roles and responsibilities inside each single organization.	X		
Interactions among different organizations: exchanged information and communication channels used.	X	X	
Identification of information flows for each emergency management phase.		X	
Identification of the resources that emergency responders have (e.g. materials, people, competences).	X	X	X
Identification of organizational capabilities.	X	X	X
Identification of the relationships among the capabilities.			X




4. Implementation

The adoption of the proposed framework and the way of implementing it depend on the goals to achieve. The three levels of analysis (A, B, C) that can be performed in parallel or in sequence, or just one of them, can suffice the needs of the study. In the cases where it is needed to investigate emergency management operations and information flows, both for a general mapping and for the investigation of specific emergency scenarios, it is suggested to start from Level A. In this way, a general overview of how different organizations are structured and operate during emergencies, including their main interactions, is obtained first. Afterwards, some specific events (incidents and/or disruptions) that affect the infrastructure system can be analyzed more in detail; the interactions between actors are then mapped with a specific reference to the selected scenario through the tools related to Level B (Fig. 2).

The classification shown in Table 2, will help in identifying the required level of analysis (on the columns) on the basis of the objectives to be achieved (on the rows). There are cases where the same goal is achieved through different levels of analysis. For instance, the tool C7, used to identify the resources owned by emergency responders, is present in all three levels. However, the information shown in each level may be different. Indeed, Level A will represent all the

resources owned by an organization, independently from the events where they are used. Instead, in Level B only the resources adopted for specific events will be depicted. Finally, considering the way the tool C7 is used in Level C, the information shown could be the same present in Level A.

Table 3. Collection of information.

Symbol	Meaning
	The information needed to complete the tool can be collected through <i>formal documents</i> provided by the organization being examined (e.g. organizational charts, emergency plans, reports of past events).
	It could happen that the <i>documents</i> provided are not enough to collect all the information, thus <i>interviews</i> are needed.
	Some information are very detailed and difficult to be collected. In these cases, it is suggested to run <i>interviews</i> with key informants. For instance, identify, document and assess organizational capabilities.

However, there is high flexibility in the way the tools are used and in the sequence of the activities. Indeed, it is possible to implement just some of the tools present in a given level of analysis.

Another important aspect regards the collection of the information needed to map the framework. Considering the tools used in the framework, they are represented through three main symbols according to the rule explained in Table 3. As shown in the table, there are information collected through formal documents and others through interviews. The idea is to analyze the documents provided by the organization, as well external documents. For instance, in the last case, we refer to legislations specific for the country where the study is applied. This because, considering the actors under analysis, there could be territorial competences defined by the specific legislation of the country where the actors operate.

However, there are cases where documents are not enough to collect the information. In these situations, it is suggested to run individual interviews with key informants (e.g. risk and security manager). Indeed, given the sensitivity of the topic, individual interviews are preferred to focal groups since they allow to avoid misalignment and communication issues between different interviewees (especially if they belong to different organizations).

5. Conclusions

The present study starts from the need of improving information sharing between actors involved in emergency management operations of interdependent systems, as a prerequisite for achieving higher collaboration and coordination in coping with incidents. In particular, the proposed framework aims at providing a set of coherent modelling and analysis tools that are usable by and shared among different actors.

From the state-of-the-art review, the importance of the information sharing process, the related challenges and the technical aspects clearly emerged. What is missed is a methodology to model coordinated emergency management operations and information flows. However, what resulted useful is a selected subset of tools which are part of the NATO Architecture Framework (NAF).

As a contribution to fill in the literature gaps, a novel framework has been developed for the modelling of emergency management capabilities and information flows among the key actors. The framework is particularly devoted to develop collaborative and coordinated response to emergencies involving interdependent infrastructure systems. The peculiarities and the main advantages of the framework, if compared to the state-of-the-art are briefly summarized in the following:

- The framework is sufficiently general to be applied to analyze different emergency

management contexts and to model highly *heterogeneous multi-actor environments* (e.g. cross-border emergency operations).

- It enables the adoption of a *common terminology* and a standardized way of representing actors' information. In this way, the sharing of information and the communication processes between organizations are facilitated.
- The framework can be implemented in a *flexible* way. It is possible to adapt and personalize the selected tools according to specific needs and to easily update them over time.

A structured approach to EM capability and information flow modelling is the first and preliminary level of information sharing between EM actors; thus, considering the mutual relationship between information sharing and trust (Hunt and Eburn, 2018; Soni et al. 2014), it may play a pivotal role in nurturing inter-organizational trust in a virtuous cycle that leads to even more structured and integrated data sharing processes.

The standardized way of mapping the information is on one side a good way to facilitate the information sharing process, but on the other it could represent a shortcoming of the framework developed. Indeed, there could be organizations for which the tools selected are not enough to represent their operational and organizational complexity. To overcome this limitation, a pilot application of the framework and of the methodology in a real complex context is envisaged; it will give the opportunity to collect feedbacks and refine the framework, where needed.

Finally, this study represents the first step of a more articulated research endeavor to develop a complete methodology. The next steps will be devoted to:

- Test and refine the proposed framework based on a pilot application in the context of a realistic case where cross-border emergency operations are envisaged. To this end, the SICt project (Resilience of Cross-Border Critical Infrastructure) will be used. It aims to strengthen the joint risk management capacities linked to events that may partially or totally disrupt the continuity of critical transport infrastructures service between Italy and Switzerland.
- Develop and test a novel method to assess intra- and inter-organizational emergency management capabilities to be integrated as a further level of analysis in the framework.

Though, the current level of development already contributes to practice by providing public

officers, first responders and CI managers with general guidance and a set of suggested tools to model emergency management capabilities and information flows. The tools are easy to use and were picked-up to be well-coordinated in a unique and coherent framework.

References

- Brouet, J., H. Marques, J. Rodriguez, J. Neves, A. Nyanyo, S. H. de Groot, B. Bouwers, P. Force, and F. Reinert. (2014). System Requirements, Enterprise Architecture and Methodology. *Deliverable 3.1, SALUS: Security And Interoperability in Next Generation PPDR Communication Infrastructures*.
- Cabinet Office. (2012). Glossary - Revision to Emergency Preparedness. <http://www.cabinetoffice.gov.uk/sites/default/files/resources/chapter2-cooperation.pdf>.
- Cedergren, A., J. Johansson, and H. Hassel. (2018). Challenges to Critical Infrastructure Resilience in an Institutionally Fragmented Setting. *Safety Science* 110, 51–58.
- Choi, J., A. Deshmukh, and M. Hastak. (2019). Seven-Layer Classification of Infrastructure to Improve Community Resilience to Disasters. *Journal of Infrastructure Systems* 25 (2).
- Department of Homeland Security (DHS). (2009). National Infrastructure Protection Plan - DHS. Washington, DC.
- European Commission. (2008). Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. *Official J. of the EU*.
- FEMA: Federal Emergency Management Agency (2019). <https://www.fema.gov/common-alerting-protocol>
- Fischer, D., O. Posegga, and K. Fischbach. (2016, June). Communication Barriers in Crisis Management: A Literature Review. *24th European Conference on Information Systems, ECIS 2016*.
- Goubran, L., A. Parush, and A. Whitehead (2016). Modelling Information Flow and Situational Awareness in Wild Fire Response Operations. *International Conference on Human Interface and the Management of Information*, pp. 11-19. Springer, Cham.
- ISO/IEC/IEEE 40210. (2011). Systems and Software Engineering — Architecture Description. <https://doi.org/10.1007/BF01077867>.
- Kapucu, N. (2009). Interorganizational Coordination in Complex Environments of Disasters: The Evolution of Intergovernmental Disaster Response Systems. *Journal of Homeland Security and Emergency Management* 6 (1).
- Müller, W. and F. Reinert. (2014). A Methodology for Development of Enterprise Architecture of PPDR Organisations. *International Conference on Software Engineering Research and Practice (SERP)*.
- NATO Architecture Framework. (2018). NATO Architecture Framework Version 4.
- Norri-Sederholm, T., M. Joensuu, and A. M. Huhtinen. (2017). Ensuring Information Flow and the Situation Picture in Public Safety Organisations' Situation Centres. *European Conference on Information Warfare and Security, ECCWS*, 267–73.
- Norris, F. H., S. P. Stevens, B. Pfefferbaum, K. F. Wyche, and R. L. Pfefferbaum. (2008). Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness. *American Journal of Community Psychology* 41 (1–2), 127–50.
- Nunavath, V., J. Radianti, M. Comes, and A. Prinz. (2015). Visualization of Information Flows and Exchanged Information: Evidence from an Indoor Fire Game. *ISCRAM 2015 Conference Proceedings - 12th International Conference on Information Systems for Crisis Response and Management*.
- Patriarca, R., G. Di Gravio, and F. Costantino. (2017). MyFRAM: An Open Tool Support for the Functional Resonance Analysis Method. *2017 2nd International Conference on System Reliability and Safety, ICSRS 2017 IEEE*, 439-43.
- Petrenj, B., E. Lettieri, and P. Trucco. (2013). Information Sharing and Collaboration for Critical Infrastructure Resilience - A Comprehensive Review on Barriers and Emerging Capabilities. *International Journal of Critical Infrastructures* 9 (4), 304-29.
- SALUS: Security and interoperability in next generation PPDR communication infrastructures (2019). <https://cordis.europa.eu/project/rcn/109811/factsheet/en>
- Seppänen, H., J. Mäkelä, P. Luokkala, and K. Virrantaus. (2013). Developing Shared Situational Awareness for Emergency Management. *Safety Science* 55, 1-9.
- Singh, P., P. Singh, I. Park, J. K. Lee, and H. R. Rao. (2009). Information Sharing: A Study of Information Attributes and Their Relative Significance during Catastrophic Events. *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*, 283-305.
- Usuda, Y., M. Hanashima, R. Sato, and H. Sano. (2017). Effects and Issues of Information Sharing System for Disaster Response. *Journal of Disaster Research* 12 (5), 1002-14.
- Vollmer, M., P. Sendrowski, and L. Müller. (2019). IN-PREP, D2.4 Recommendations on Relevant Organisational, Policy, Social and Human Factors Relevant for System Developments.