

## Exploration of Network Theory to Evaluate Organizational Resilience

**Cristina Ruiz-Martin**

Department of Systems and Computer Engineering,  
Carleton University, Ottawa, Canada.

*Corresponding author:* cristinaruizmartin@sce.carleton.ca

**Gabriel Wainer**

Department of Systems and Computer Engineering,  
Carleton University, Ottawa, Canada.  
E-mail: gwainer@sce.carleton.ca

**Adolfo Lopez-Paredes**

Department of Business Management,  
University of Valladolid, Valladolid, Spain.  
E-mail: aparedes@eii.uva.es

(Received on May 12, 2021; Accepted on December 2, 2021)

### Abstract

Recent disasters and rapid changes in the environment have shown various open issues in organizational resilience, in particular the use of communications. We explore the use of Network Theory to study the robustness of communications in organizations regardless their structure and the communication mechanisms used. We focus on how a collapse in the communication mechanisms affects the communication structure in an organization. We use a case study based on an emergency management plan from a Nuclear Power Plant in Spain. We show that Network Theory along with the number of connected components in a network provides a cost-effective way to analyze the communication infrastructure and organizational relations. Network Theory also allows us to build awareness about the communication and information structure inside an organization, and to design a more robust communication network.

**Keywords-** Emergency plans, Robustness, Crisis management, Organizational structure, Communication mechanisms.

### 1. Introduction

When a disaster happens, experts usually identify lessons learned from the incident. They principally analyze the events that aggravated the crisis or did not help in its resolution. They also set the directions for improving the organization and the emergency management. Because of the various studies conducted, we know the importance of a well-managed and robust communication infrastructure while managing the emergencies (Chewning et al., 2013; Langlois, 2013; Omoto, 2013). The communications mechanisms are a key element in the resilience of systems (Longstaff and Yang, 2008). As organizations can be considered systems (Kast and Rosenzweig, 1972), the communications mechanism is also a key element for organizational resilience. Moreover, building situation awareness about the organization and its environment contributes to improving the organizational resilience (Vogus and Sutcliffe, 2007; McManus et al., 2008; Gibson and Tarrant, 2010).

We discuss the use of Network Theory (Newman, 2003) to study the robustness of the communications in organizations regardless of their structure and the communication mechanisms used. We focus on how a collapse in the communication mechanisms affects the communication

structure in an organization, on building situation awareness, and on improving the robustness of the communication infrastructure and the structural relations in the organization. Our main contribution is to show how to use of Network Theory to analyze and improve the communication structure of organizations and how this contributes to organizational resilience.

Network Theory is an extended used method to model and study the relations between entities. The main advantage of Network Theory to study communications in an organization is the perfect match between the elements defined in the method (i.e., nodes and links) and the entities in the system. We can model the organization as a network where the nodes represent the organization's employees, and the links represent the relations between them. The graphical representation of the network allows to easily communicate the organizational structure and build awareness about the current state of the organization. This representation also allows us to answer the question: "Which nodes or links in the network are the most crucial for the network's connectivity if they were removed?" (Newman, 2003). The answer to this question, which is well-studied in the context of Network Theory, provides a metric to evaluate the robustness of the network. If the number of crucial nodes or links is high, the network has a low robustness level. Otherwise, the robustness would be high. As the network is a model of the communication structure in the organization, the answer to this question is also a metric of the robustness of the organization communication system.

The answer to the above-mentioned question is not straightforward using other methods such as Agent Based Model or Discrete Event System Analysis. Network Theory is a formal method in which the model can be univocally represented using a mathematical notation. Available tools hide the mathematical complexities to the modeller, making it more accessible for all decision makers. Additionally, to carry preliminary analysis we do not need to include the dynamic of the communications such as the frequency, the content of the information transmitted or the path the communications follow among the employees.

To show the applicability of the proposed method, we will discuss a study about the robustness of an emergency plan from a critical infrastructure: a nuclear power plant in Spain. We discuss the effects of a downfall in the different communications mechanisms used by the Nuclear Emergency Plan (NEP). This study provides awareness about the key issues in the emergency plan communication system. After identifying the issues, we provide mechanisms to improve the robustness of the communication systems. This study contributes to improving the resilience of the organization building situation awareness about the key issues in the emergency plan communications and proving ways to improve the robustness of the communication mechanisms. The method followed in the case study is applicable to do similar analysis in other organizations.

The paper is organized as follows. In section 2, we review the concept of resilience, organizational resilience, and its relation to emergency management. In section 3, we explain Network Theory as a method to study the robustness of the communication infrastructure in an organization. In section 4, we present the case study. In section 5, we analyze how failures in the communication mechanism affect the NEP management. In section 6, we discuss the results of the analysis. Finally, in section 7 we remark the conclusions and state the lines for future work.

## 2. Resilience, Organizational Resilience, and Emergency Management

In this section, we review the concept of resilience and how is resilience understood inside organizations. We highlight the importance of communications in the context of organizational resilience.

Despite the spread use of the concept resilience, there is neither an accepted definition nor an agreement about in which field it was first introduced (Manyena, 2006). Some authors agree that the concept resilience was popularized after Holling's work "Resilience and Stability of Ecological Systems" in 1973 (Bhamra et al., 2011; Annarelli and Nonino, 2016).

Holling introduces the concept resilience to differentiate between the stability of a system and its resilience in the context of ecological systems to deal with resource management (Holling, 1973). He defines resilience as "a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist" and stability as "the ability of a system to return to an equilibrium state after a temporary disturbance". Following these definitions, resilience and stability are properties of the system. Resilience is the probability of extinction or persistence of the system. Stability is the degree of fluctuation around the states in the system. Therefore, a system can be very resilient having low stability (Holling, 1973).

Different definitions of resilience have been proposed for research in ecology, psychology, disaster management, organization management, sociology, or engineering. Even in the same area, different definitions coexist (Folke, 2006; Manyena, 2006; Bergström et al., 2015; Annarelli and Nonino, 2016).

This variety of definitions reveals an important question to understand the concept: Is resilience a measure, a feature, a philosophy, or a capability? (Bhamra et al., 2011). We agree with the authors (Bhamra et al., 2011) in the thought that how to understand the concept may depend on the field. However, following the original definition of Holling (1973), we can conclude that it is more a feature or a capability of the system than a measure or a philosophy. Although Holling defines it as a measure, he also states that it is an ability and a property of the system.

As we mentioned, the study of resilience covers different areas that is isolated and independent. One may think that building resilience in disaster management field is not related to other areas such as building resilient individuals, systems, or organizations. However, this is not the case. Rose (2004) proposed a perspective under which we can combine all fields. He states that resilience occurs at three levels: microeconomic (firms, households, and organizations), mesoeconomic (individual market or cooperative group) and macroeconomic (combined individual units and markets). The interrelation among these levels provides the relation among the different areas of resilience. In this work, we focus on the study of resilience at the level of organizations in the field of disaster management.

In the field of Organizational Theory, there is neither an agreement of what organizational resilience is (Banahene et al., 2014). One of the first definitions of organizational resilience we find in the literature is provided by (Horne III, 1997; Horne III and Orr, 1997). He defines resilience as "a fundamental quality of individuals, groups, organizations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behavior". And organizational resilience as "the ability of a system to withstand the stresses of environmental loading based on combination/composition of the system pieces, their structural linkages, and the way the environmental change is transmitted and spread throughout the entire system". Since then, several definitions have been proposed (Hamel and Valikangas, 2003; Lengnick-Hall and Beck, 2005; Bhamidipaty et al., 2007; Grøtan and Asbjørnslett, 2007). This issue has been partially solved by the recent Organizational Resilience ISO standard that defines organizational resilience as the "ability of an organization to absorb and

adapt in a changing environment" (ISO, 2017).

The lack of consensus over years defining resilience and organizational resilience brings a lack of agreement about what elements or factors contributes to building a resilient organization. Different approaches have been proposed to identify the elements that contribute to organizational resilience.

A review of the characteristics and factors that contribute to resilience (Ruiz-Martin et al., 2018) shows that these approaches sometimes overlap, sometimes show complementary points of view to improve resilience. However, there is not an agreement about the factors that contribute to resilience and the indicators to evaluate and measure it. Despite the lack of agreement, there are common and repeated characteristics or factors to consider enhancing resilience. These characteristics include *situation awareness, having resources, managing organization's vulnerabilities, redundancy, robustness, improvisation capacity, ability to anticipate events, agility, resilient individuals, learning capacity, collaboration, and flexibility*.

The Organizational Resilience ISO standard (ISO, 2017) has also provided clarity on the factors that contributes to organizational resilience. It highlights "effective communications to improve understanding and decision making" as one of the key coordinated approaches to achieve organizational resilience. The importance of communications to achieve resilience is also supported by the analysis of recent disasters in history.

For example, during the accident at TEPCO's Fukushima Nuclear Power Plant, the off-site emergency management center lost its functionality and made the communication systems unavailable (Omoto, 2013). The International Atomic Energy Agency (IAEA) suggested, among other improvements, strengthening management systems, response arrangements, transparency, and effectiveness of communications mechanisms (Langlois, 2013).

Following the Darfield earthquake in September 2010, in Whitman et al. (2014), the authors carried out a survey among New Zealand's organizations. They used this survey to find the most helpful factors in mitigating the disruption in the operations after the earthquake. These factors are well-designed and well-built buildings, the relationship with staff and the capability to restore critical services quickly or not to get them interrupted.

After Hurricane Katrina in New Orleans in 2005, the most important industries in the area were destroyed. In Chewning et al. (2013), the authors studied how Information and Communication Technology (ICT) were used by organizations to aid in their recovery after the Hurricane. Through their empirical study, they showed that the organizations that can use ICT in these situations are more resilient. These organizations used ICTS to improve their connection, coordination and share the evolution of the emergency with both external and internal stakeholders.

Following these examples, the ISO standard and the literature about disasters, we conclude that a robust communication system contributes to improving the emergency management and the resilience of organizations.

This research focusses on exploring the use of Network Theory, to improve the robustness of communications in an organization to achieve organizational resilience. It also studies how to build situational awareness. The research fills a gap in the study of organization resilience, where most approaches are prescriptive (i.e., they mention what characteristics an organization should improve

but they do not specify how). One example is the Organizational Resilience ISO standard (ISO, 2017), which highlights the importance of *shared information and knowledge*. The standard states that knowledge and information should be shared in a timely manner with all relevant interested parties. However, it does not state how. Our work is complementary to prescriptive approaches that highlight the important of communications to achieve resilience.

### **3. Network Theory as a Method to Improve Organizational Resilience**

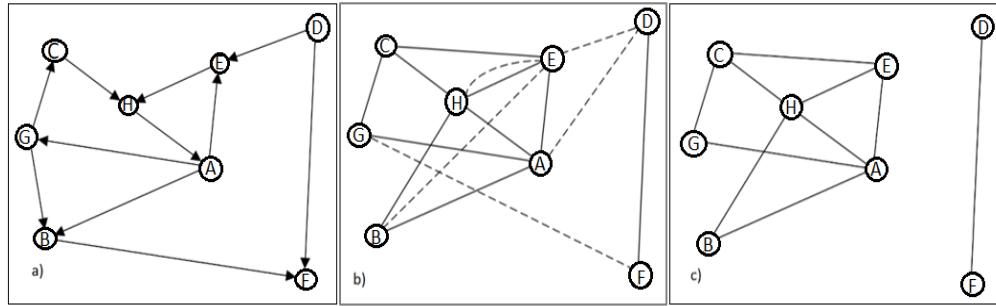
As stated in the introduction and Section 2, a robust communication system is a key element for any organization. It has even more importance while facing a crisis and it is considered a key element for building organizational resilience. It has special importance in those organizations that rely on the communication to coordinate their resources. However, the relations between people defined in the organization also have a key role in the robustness of the communications. To study the robustness of this organizational and communication infrastructure, we need a method that allows us to model and study the relations between entities.

Network theory has shown to be a useful method to model and study the relations between entities (Newman, 2003; Newman et al., 2006). Network Theory provides a set of techniques to study the networks that represent relations between discrete objects. It has been widely applied in different fields where one needs to model systems that have strong interdependence within entities (Strogatz, 2001). Some examples in Biology include the modeling of food chains (Dunn and Wilkinson, 2015), metabolic networks (Gallos et al., 2007) or brain structure and functions (Bullmore and Sporns, 2009). In Medicine, it has been used, for instance, to model the spreading of disease (Chami et al., 2013), drug and vaccine administration (Ibrahim et al., 2013; Poland et al., 2013). It has been used in different technological systems, including power grids (Negeri et al., 2015), transport networks (Deng et al., 2015; Zhu and Luo, 2016), communication infrastructure (Peng et al., 2012), and social networks (Liu et al., 2016). Finally, it has been used for Project Management (Fang et al., 2012; Ruiz-Martin and Poza, 2015), Supply Chain Networks (Hearnshaw and Wilson, 2013), Socio-ecological Systems (Janssen et al., 2006) and Social Economy (Poza et al., 2011; Santos et al., 2012).

In the area of resilience, Network Theory has been applied to study the structure, redundancy, and robustness of a water distribution network to improve its resilience (Yazdani et al., 2011). It has also been used to find the most critical element in industrial symbiotic networks (Chopra and Khanna, 2014), to identify which communities are more vulnerable in network systems and be able to prioritize resources to protect the critical elements (Rocco S. and Ramirez-Marquez, 2011) and to study critical infrastructure connection and topology (Eusgeld et al., 2009; Ouyang, 2014). Likewise, it has been applied in analyzing vulnerabilities in process plants in particular cascading effects (Khakzad and Reniers, 2015), to improve resilience in communication networks infrastructure (Brinkmeier et al., 2009), and to improve resilience in air traffic management (Cook et al., 2015; Dunn and Wilkinson, 2015).

These works show the applicability of Network Theory to analyze and improve the robustness of the communication system in an organization. We represent an organization and its communication mechanisms as a network. The nodes represent the organization's employees and the links, the relations between them. We distinguish the different communications mechanism (such as phone, fax, internet, or radio) in different layers.

In Network Theory, a system is modeled as a set of nodes connected by links. The nodes and the links can have different meanings. For example, nodes can be cities and the links roads between them. The nodes can also be people and the links the social relation between them, etc. In Figure 1, we show several types of networks.



**Figure 1.** Examples of networks. a) Simplex directed network with eight nodes. b) Multiplex bidirectional network with one component. The distinct types of lines represent the different layers. c) This network represents the resultant network when the dot-line layer in figure b) fails or disappears. After the failure, we get a simplex bidirectional network with two components.

Networks can be classified following different criteria, as follows (these classifications are non-exclusive).

Based on the meaning of the links, networks can be simplex (Figure 1a, 1c) or multiplex (Figure 1b). In simplex networks, all the links have the same meaning. In multiplex networks, the links have different meanings. Each type of link is a different layer of the network. Although multiplex networks can include specific properties in each layer, how to define the interconnections between layers and how to define global network metrics is not yet developed (Gómez et al., 2013). However, there have been advances in this area. For example, centrality measures to study multiplex networks have been proposed (Sole-Ribalta et al., 2014). In addition, there is software to visualize multiplex networks (De Domenico et al., 2014).

Based on the type of the links, they can be Directed (Figure 1a), Bidirectional (Figure 1b, 1c) or Mixed. In directed networks, all the links are directed (i.e., all nodes have a source node and a target node). The opposite connection represents a different relation (i.e., the connections are not reciprocal). As shown in (Figure 1a), an arrow represents the direction of the link. In bidirectional networks the source and target node are interchangeable. There is not a specific direction for the link (i.e., the relations are reciprocal). A Mixed network combines direct and bidirectional links.

If we consider the weight of the links, networks can be weighted or non-weighted. The links in non-weighted networks represent the existence or absence of the relation. Instead, in weighted networks, the links have a weight associated. This weight is a measure of how strong the relation between the entities is.

There are various metrics to characterize and extract properties from a network based on the analysis we are interested in. These metrics include the network density, its diameter, the degree distribution, its clustering, modularity, or number of connected components among other. We want to obtain a measure to analyze the robustness of the organization communication system. We focus

on how a collapse in the different communication channels or mechanisms affects the communication structure in an organization. We want to evaluate if these downfalls isolate groups or individuals, and therefore they cannot receive communications. We want to see whether the communication network is robust against these types of failures or not. Analyzing the different metrics offered by Network Theory, we found that the number of connected components in the network is the most appropriate for this study because it easily allows us to identify if there are isolated individuals that cannot receive the information.

A network component consists of all the connected nodes of the network. A network can have a single component (Figure 1b) or multiple ones (Figure 1c). The number of connected components allows us to identify whether these downfalls isolate individuals/groups or not. If the resultant network has more than one component, it will mean that the collapse in that communication channel isolates individuals or groups. Therefore, the network will not be robust against a collapse in the communications channel we are studying. In Figure 1c, we simulate a downfall in the dot-line layer in the network represented in Figure 1b. Network represented in Figure 1b is not robust against a downfall in the dot-line layer. After the downfall, we have two components in the network (Figure 1c).

We use the tool Gephi as supporting tool for the analysis process and to elaborate the figures of the network. Gephi is an open-source tool to visualize and calculate different properties of the network (Bastian et al., 2009).

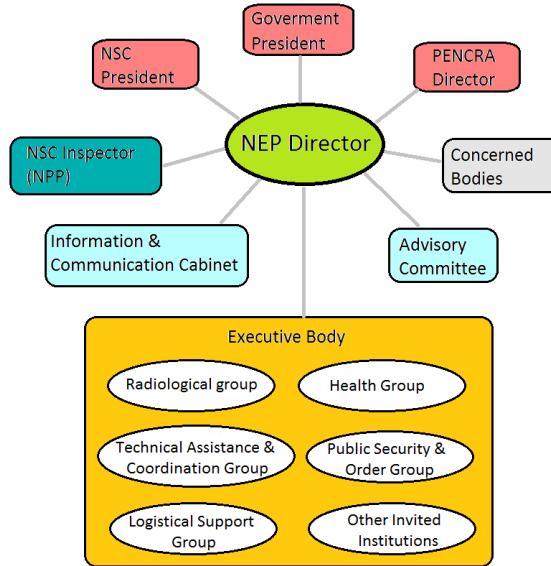
#### **4. Case Study Definition**

To analyze the robustness of the communication infrastructure in an organization against a collapse in different communication mechanisms, we choose as case study an emergency plan from a critical infrastructure in Spain: an external Nuclear Emergency Plan (NEP). We make this choice because a NEP is one of the most complex communication systems we may find in an organization.

A full description of the case study has been presented in Ruiz-Martin et al. (2015). The authors identified all the people working on the plan, the organization structure, and the relations among the people. In this section, we summarize the nuclear elements to understand our approach to the problem.

##### **4.1 Organizational Structure**

In Figure 2, we present a sketch of the structure of the NEP. The chair is delegated to the NEP Director. Government President can relegate the NEP Director based on the evolution of the emergency. The NEP Director is supported by Nuclear Safety Commission (NSC) President and the Central Response and Support Nuclear Emergency Plan (PENCRA) Director. The NSC Inspector at the nuclear power plant must inform the NEP Director about any issue inside the plant during the emergency. The Advisory Committee helps the NEP Director in decision-making analyzing the data and providing reports. The Information and Communication Cabinet oversees the relations with the media. The Executive Body oversees doing the actions commanded by the NEP Director to solve the emergency. It is constituted by Health, Radiological, Public Security and Order (PS&O), Logistical Support and Technical Assistance and Coordination (TA&C) groups. These groups have their own structure, and they use different communication mechanisms. In each group, there are heads at different levels, people working in the emergency (field teams) and replacement teams. The NEP Director may ask other institutions to join the Executive Body based on the evolution of the emergency.



**Figure 2.** Sketch of the structure of the NEP.

## 4.2 Communication Channels

The communication channels defined in the NEP include fax, mobile and wired phone, special mixed radio-phone networks, Internet, satellite phone, two different radio channels and communication among people in the same location. The NEP also includes the possibility to use military communication channels upon request of the NEP Director when the other communication channels fail. Since military communications are not available until the infrastructure is deployed, we do not consider them as an available communication mechanism since the beginning of the emergency.

### 4.2.1 Phone Communications

This is the most extended communication mechanism in the NEP. There are two types of phone communications: landline and mobile. They are used by all groups based on the structure shown in Figure 2 and the structure of the teams of each member of the executive body. The NEP does not state who has access to the landline phones and who can only use cell phones.

### 4.2.2 Fax and Internet Communications

Fax and Internet communications can be used at different levels in the NEP:

- Inside the TA&C group following the internal structure.
- Between the NEP Director and the head of the PS&O group.
- Among the Heads of the PS&O group.

The NEP establishes that a confirmation of reception is need when using these communication mechanisms.

### 4.2.3 Special Mixed Radio-Phone Communications

This type of communication systems can be used in the following groups: the Radiological group and PS&O group. There are three different types.

The special mixed radio-phone communication system used by the Radiological group only allows communications within the members of this group. When the communications include members of other groups, they must be by phone or in person (if they are in the same area). The communications inside the group must follow the hierarchy defined in the NEP.

The PS&O group uses two types of special mixed radio-phone communication systems. The PS&O group is divided into three bodies: the Civil Guard, the Autonomous Police, and the Local Police. The Civil Guard use one type of system and the Autonomous Police a different one. It means that members of the Civil Guard group cannot use this special system to communicate with the members of the Autonomous Police. Communications between these groups are by land or cell phone and person to person. If the heads are involved, fax is also used. These two mixed radio-phone communication systems also support satellite communications in case the other ones fail. However, it takes a while until the satellite communication is enabled. All the communications must follow the hierarchy defined in the NEP.

#### **4.2.4 Radio Communications**

Two radio channels (Reman & Remer) are available to be used while managing an emergency. The radio channel called Reman allows communications among the following individuals:

- The heads of the TA&C group.
- The town emergency plan heads of Zone I (i.e., those towns at most 10 km away from the Nuclear Power Plant).
- One of the communication centers of the PS&O group.
- The three communication centers of TA&C group.

All members connected to this network hear the communications managed by Reman radio channel. The radio channel called Remer is a broader communication network than Reman. It includes the individuals in the Reman communication network and the following ones:

- The town emergency plan heads of Zone II (i.e., those towns between 10 and 30 km away from the NPP).
- The emergency plan teams in the town.

All members connected to this network and the population can hear the communications. Therefore, this specific channel cannot be used to transmit confidential commands and/or information.

As already we already mentioned, all the individuals that have access to these networks can hear all the information transmitted. However, the communications must follow the structure defined in the NEP. For example, a member of the emergency plan team of Zone I cannot directly tell information to a town plan head of Zone II. She must refer to the town plan head of her municipality.

#### **4.2.5 Satellite Communications**

The Satellite communication system is a limited communication mechanism. It only allows communication between the following individuals:

- Nuclear Emergency Plan Director
- PENCRA Director
- NSC President
- Government President

- The town hall of a municipality in Zone I.
- The Satellite communications must also follow the hierarchy defined in the NEP.

## 5. Analysis of the Communication Network Robustness

To construct the network representing the NEP, we identify all the people involved in the emergency and all their communication mechanisms. The nodes represent the agents, or the people involved in the nuclear emergency. The links represent the communication relations between the agents, or the people involved. The resulting network is a multiplex network composed of 832 nodes and 10 layers. The layers represent specific communication mechanisms: fax, Internet, landline, and cell phone, Reman radio channel, Remer radio channels, satellite, Autonomous Police radio-phone network, Radiological Group mixed radio-phone network, Civil Guard mixed radio-phone network, and communications in-situ.

The costliest part of the study is collecting all the information and storing it in a standard format such as a two csv files, one for the nodes and another one for the links with a label for the layers. Once the process is done, replicating the graphs and the results using Gephi is simple. The data is not provided due to a confidentiality agreement.

In this section, we study the effects of a downfall in the communication infrastructure, and it affects the structure of the organizational network. We analyze the following communication channels downfalls: (1) phone, (2) fax, (3) Internet, (4) radio, (5) satellite, and (6) phone, fax, and internet at the same time

The following assumptions are done during the analysis:

- (i) Although we distinguish different communication layers, we assume that the communication links are equivalent. This is justified because all the links allow communications between agents. Therefore, we analyze the multiplex network as a simplex one.
- (ii) We group Reman and Remer radio channels under the radio communication channel. This assumption is done because they are different frequencies on the radio network. Moreover, if the individuals only have a radio device, they can only tune a single channel.
- (iii) We accept that communications in-situ do not fail (i.e., talking face to face is a robust communication mean).
- (iv) We assume that the Civil Guard mixed radio-phone network, the Radiological Group mixed radio-phone network and the Autonomous Police mixed radio-phone network are robust and they do not fail since they are held by two networks (phone and radio). A failure in this communication mechanism implies a simultaneous interruption of both radio and phone networks.
- (v) We assume that the mobile and landline phones use the same communication channel. This assumption is justified because in most cases, the communication involves both mobile and line phones. If one of them fails, the communication is not going to be established.
- (vi) The NEP communication network is dynamic. The potential communications between people change as their location do. We assume a static network and we analyze it using different scenarios to lighten this assumption.

We use two scenarios for the analysis of a downfall in the different communication channels. In Scenario 1, we represent the NEP communication network after declaring the nuclear emergency and the members of Executive Body are together, but no further action has been taken (i.e., the field teams have not been positioned). In Scenario 2, we represent a following situation in when all

teams have been situated.

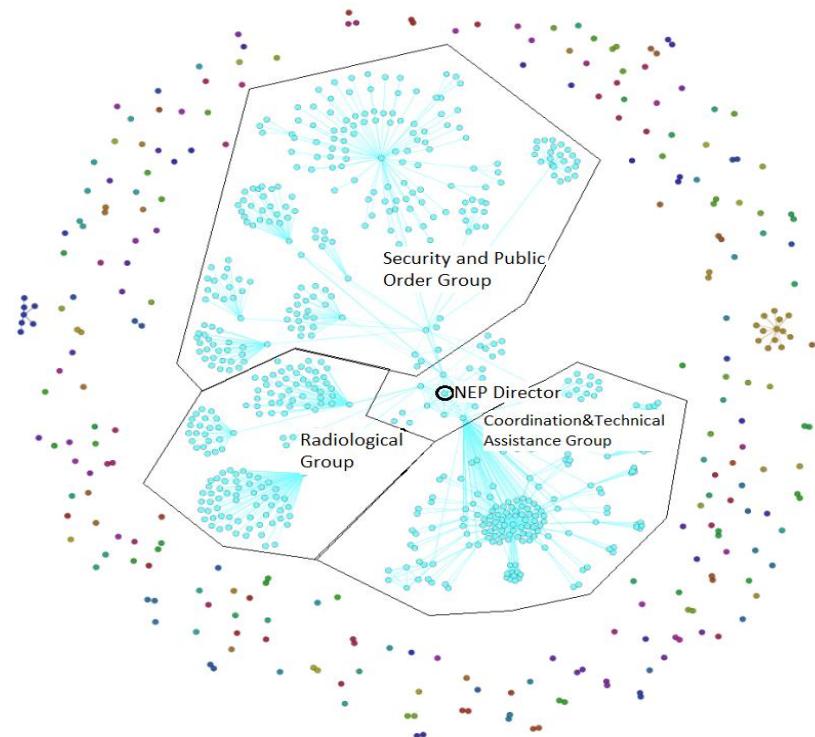
Within each scenario, two cases are analyzed. Case 1 includes the whole network (i.e., all the people involved in the NEP), composed of 832 agents containing the replacement teams. Case 2 represents the network excluding the replacement teams (i.e., only the individuals working at a certain moment are included). This reduces the size of the network to 522 agents.

### 5.1 Downfall in Phone Communication Channel

To simulate the effects of a downfall in the phone communications, we remove from the network model of the NEP the links that only manage landline and cell phone communications and we calculate the number of connected components using Gephi. As we will see below, the number of connected components is greater than one in both analysis scenarios and both cases (i.e., this downfall isolates individuals while managing the emergency).

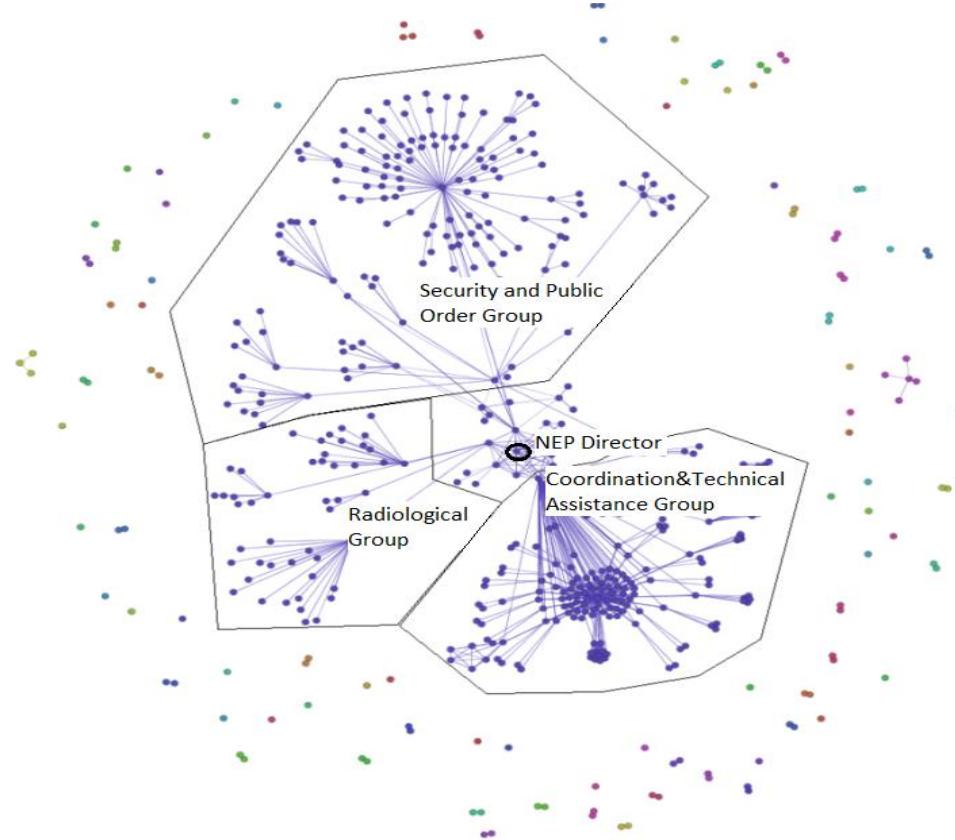
#### 5.1.1 Scenario 1

In Figure 3, we show the NEP network in Case 1 if the phone communication channel does not work. In this case, the number of connected components in the network is 207. The figure is made with Gephi, and it depicts one view of the network. We choose this view because it provides a good visualization of the number of components in the network. In the middle of the figure is the bigger component, which includes 68.63% of the nodes (571 nodes). The NEP Director and the heads of the Executive Body belong to this component. Members from the Radiological Group, PS&O group, and TA&C group also belong to it. The other 261 nodes, depicted in the figure surrounding the bigger component, represent isolated individuals or teams.



**Figure 3.** Collapse in the phone communication channel. Scenario 1. Case 1.

From this analysis, we conclude that the phone communication channel is not robust in Case 1 in Scenario 1. To better identify the isolated individuals, we made the same analysis in Case 2 (i.e., not including the replacement teams).



**Figure 4.** Collapse in the phone communication channel. Scenario 1. Case 2.

In Figure 4, we show the NEP network in Case 2 if the phone communication channel does not work. In this case, the network has 87 connected components. The figure is made with Gephi, and it depicts one view of the network. We choose this view because it provides a good visualization of the number of components in the network. In the middle of the figure is the bigger component, which includes 74.71% of the nodes (390 nodes). The NEP Director and the heads of the Executive Body belong to this component. Members from the Radiological group, PS&O group and TA&C group also belong to it. The other 132 nodes represent the isolated teams or individuals. They are depicted in the figure around the major component. From this analysis, we conclude that the phone communication channel is not robust in Case 2 in Scenario 1.

Since the number of nodes in the bigger component is different between both cases, we can conclude that some replacement teams were connected to the major component despite the downfall. All the replacement teams connected to the bigger component belong to the PS&O group (specifically to the Civil Guard) and the Radiological group. This affirmation is done comparing the nodes that belong to the bigger component in Case 1 and 2.

The isolated individuals or teams in Case 2 are:

- The Autonomous Police
- The Local Police
- The directors and teachers in the schools in Zone I and II
- The Government Education Supervisor
- The different ministries involved in the emergency
- The NSC Inspector at the NPP
- The whole Health group

In Case 1, they are the same as in Case 2 but including all the replacement teams, except for the one from the Radiological Group and the Civil Guard.

### **5.1.2 Scenario 2**

When the phone communication channel does not work, in Case 1, the NEP network has 139 components. The bigger component includes the 83.41% of the nodes (694 nodes). The other 138 nodes are the isolated individuals or teams. If we analyze the number of components, it is significantly reduced to 19 components due to in-situ communications. In this case, the bigger component includes 96.55% of the nodes (504 nodes). From this analysis, we conclude that the phone communication channel is not robust in Scenario 2.

As in Scenario 1, the number of nodes in the bigger component differs from Case 1 and 2. This difference shows that replacement teams remained connected to the bigger component despite the downfall. All these teams belong to the PS&O group (specifically to the Civil Guard) and the Radiological Group. This affirmation is done comparing the nodes that belong to the bigger component in Case 1 and 2.

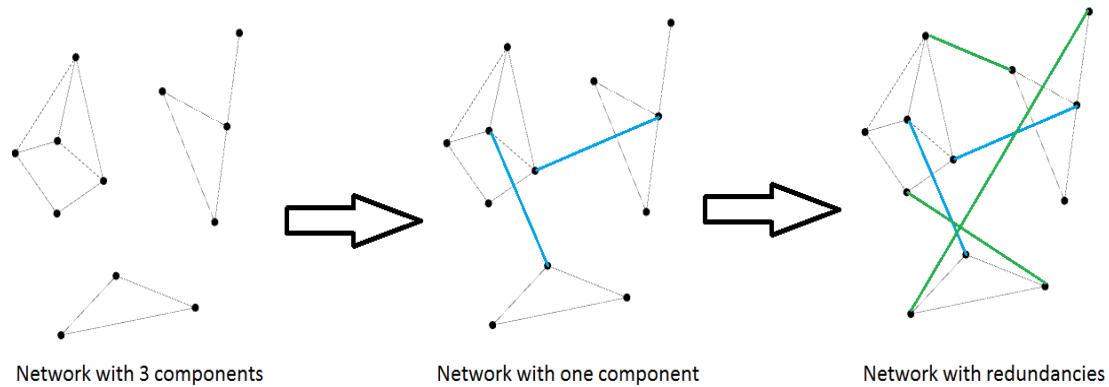
Comparing Case 1 and 2, we can see that when the network is positioned, the number of isolated individuals decrease but the isolation problem does not disappear. Apart from the replacement teams, other 18 agents or individuals are isolated. These agents are:

- The 5 Ministries
- The NSC Inspector at the NPP
- The 5 heads in the health group
- The first response and emergency medical health teams in the province capital of the NPP location
- The welfare team
- The Government Education Supervisor
- The Local Police heads

After the analysis of a downfall in the phone communication channel in different scenarios and cases, we conclude that the phone communication is not robust. If this communication mechanism fails, the transmission of information will be cut down for individuals. This will produce a loss of efficiency in the overall performance of the NEP.

To solve the isolation problem in the network is not necessary to duplication all links; we just need to consider the isolated individuals or groups and connect them to the network. The minimum number of communication links to be added will be the number of connected components minus one. This solution is only possible after the analysis if the downfall in the communication channel

and the identification of the isolated individuals or communities. In Figure 5, we show an example of how we can connect a network with three components adding just two communication links. We also show how we can create redundancies adding just three more links



**Figure 5.** Connection of the three components of a network with two links. Building redundancies adding more links.

## 5.2 Downfall in the Fax Communication Channel

To simulate the effects of a downfall in the fax communications while managing the emergency, we remove from the network model of the NEP the links that only manage fax communications and we calculate the number of connected components using Gephi. The number of connected components is one in both analysis scenarios and both cases (i.e., this downfall does not isolate some people while managing the emergency). Therefore, we conclude that the fax communications are redundant and therefore robust.

However, the use of this communication channel has limitations. For example, it cannot be used to send information or commands to field teams. The communication with these teams is important because they are who implement the actions to solve the emergency. Moreover, to be sure that the person has received your information or command we need to wait for confirmation. Therefore, fax redundancies are not enough to build a robust network.

## 5.3 Downfall in the Internet Communication Channel

In the NEP, the Internet is used to send information via e-mail. To simulate the effects of a downfall in the Internet communications while managing the emergency, we remove from the network model of the NEP the links that only handle e-mail communications and we calculate the number of connected components using Gephi. The number of connected components is one in both analysis scenarios and both cases (i.e., this downfall does not isolate some people while managing the emergency). Therefore, we conclude that this type of communication is redundant and therefore robust. However, despite e-mails can be read in cell phones, the use of this communication channel has the same limitations as fax. The NEP does not define e-mail communications to field teams and a confirmation of reception is needed. A way to improve the robustness of the communication system in the emergency plan would be allowing e-mail communications to field teams.

## 5.4 Downfall in Radio Communication Channel

To simulate the effects of a downfall in the radio communications while managing the emergency,

we remove from the network model of the NEP the links that only handle communications through the Reman and Remer radio communication channels, and we calculate the number of connected components using Gephi. The number of connected components is one in both analysis scenarios and both cases (i.e., this downfall does not isolate some people while managing the emergency). Therefore, we conclude that this type of communication is redundant and therefore robust.

However, this communication mechanism has some limitations related to both Reman and Remer channels. The radio coverage in Zone I and II is limited due to the landform. Moreover, the Raman radio channel does not cover all municipalities. It is only deployed within the municipalities that are closer to the NPP. Related to Remer channel, it is important to remember that the population can also hear the communications along this channel. This issue makes the Remer radio channel not suitable for confidential information. As consequence, this channel cannot be used to transmit some information. Therefore, radio communication redundancies are not enough to build a robust network.

### **5.5 Downfall in Satellite Communication Channel**

To simulate the effects of a downfall in the satellite communications while managing the emergency, we remove from the network model of the NEP the links that only handle this type of communications and we calculate the number of connected components using Gephi. The number of connected components is one in both analysis scenarios and both cases (i.e., this downfall does not isolate people while managing the emergency). Therefore, we conclude that this type of communication is redundant and therefore robust.

However, this communication mechanism has limitations. The main drawback of this redundancy is that it is not an extended communication mechanism along the NEP. It only supports the communications between five nodes: NEP Director, NSC President, PENCRA Director, Government Presidency, and the town hall of a municipality in Zone I. Moreover, four out of the five individuals connected by this communication channel are high government ranks that do not take direct action to solve the emergency. They only must be informed about the situation. We can see that this network does not support important communications between field teams (who are people that take direct actions to recover from the emergency) and their supervisors. Adding more satellite communication links between first responders would improve the robustness of the network.

### **5.6 Downfall in Phone, Fax, and Internet Communication Channels**

The justification to simulate a downfall in the phone, fax, and internet communication channels at the same time is based on the following two points. The landline phone and fax are managed by the same infrastructure. Related to internet, the communications that this network supports in the NEP are e-mails. These e-mails are sent to institutional e-mail accounts. These accounts are read from the computers in people's job places. It is likely that if the landline phone fails, then the Internet also stops working. This affirmation is based on the type of infrastructure that supports Internet communications in an NPP area. Following the internet map coverage and infrastructure deployed in Spain (Spanish Goverment, 2015), the most probable Internet connection in job places in the area is ADSL (Asymmetric Digital Subscriber Line). ADSL is a transmission technique applied over the traditional phone landline networks.

To simulate the effects of this downfall while managing the emergency, we remove from the network model of the NEP the links that only oversee this type of communications and we calculate

the number of connected components using Gephi.

The results of this analysis are like the phone communication downfall. It causes the isolation of the same individuals. This means that the communications that can be handled by phone, e-mail, and fax at the same time, they are also handled by other communication mechanisms. For example, in the PS&O group, they are also handled by the special mix radio-phone communication network. In the TA&C group are also handled by the Reman and Remer communication channels. However, the redundancies implemented in the communication network are not enough to create a robust communication network against this failure.

## 6. Discussion about the Results in the Case Study

With this study, we show that the NEP communication network in our case study is robust against a collapse in the satellite, internet, fax, and radio communications. However, it is not robust against a downfall in the phone communication channel. The redundancies implemented in the network are not enough to provide robustness against a collapse in the phone communication channel. This downfall would result in important consequences as stated below.

We could see that only the replacement teams in the PS&O group (specifically the Civil Guard) and in the Radiological Group remain connected to the bigger component (i.e., to the component that most people that work in the emergency are connected to, including the NEP Director) when a downfall in the phone communication channel occurs. This means that it will only be possible to establish communication with the replacement teams within these two groups. The other replacements teams, as they are isolated, will not be able to receive the orders and information to act.

As we saw in the previous section, when a downfall in the phone communication channel occurs, the NSC Inspector at the NPP is isolated. This means the lack of in-situ information about the incident evolution at the NPP, and the actions taken inside the plant to solve the situation. These cause that the actions taken outside to control the effects of the emergency will be defined without up-to-date data. It is important to remark that the phone, which connects the NEP director with the NSC at the NPP, is a special cable line phone between these two people. The communication is not held by the regular phone network. A lesson learned is the need to establish communication redundancies between the organization and the outside management centers.

The isolation of the individuals increases the complexity of communications. Therefore, it also probably increases the time required to transmit the information to a specific person. For example, the isolation of the Local Police implies that the only way to receive information and orders is through the Civil Guard. This means that the Civil Guard must reach the Local Police location. In Scenario 1, this problem is more important than in Scenario 2. In Scenario 1, the network is not deployed, and the Civil Guard teams and the isolated individuals are not located in the same area. However, in Scenario 2, the teams are deployed and the chances to be in nearby positions are bigger. This means that the time to reach the location of the isolated individuals is higher in Scenario 1 than in Scenario 2.

The isolation of the individual in the health group in scenario 1 implies that these people will not receive instructions and information about the evolution of the emergency. This issue may cause different problems such as that the teams do not know what they must do. In this uncertainty situation, we do not know the decisions each team will take, and if they will be accurate or

erroneous. This problem is partially mitigated when we move from Scenario 1 to Scenario 2. In both scenarios, the health group teams cannot communicate with their supervisors directly. In Scenario 2, this problem is partially solved due to in-situ communication. The teams can receive instructions and information from the PS&O group teams. However, the time and the complexity of the communications increase: the information transmission process will take at least five steps instead of three.

Another issue is related to receiving feedback. When a downfall in the phone communication occurs, the feedback provided by the Local Police and the Heath Group teams will not often occur since it can only be transmitted through the Civil Guard. This group also needs to conduct their own tasks. In Scenario 1, the Civil Guard teams must reach the location of the other teams to make these communications. In Scenario 2, this problem is less critical as the teams are positioned and there would be a Civil Guard team in a nearby location.

The isolation of schools' directors and teachers in Scenario 1, and the Government Education Supervisor in both scenarios is relevant if the schools must be evacuated. This issue is solved in Scenario 2, since the Civil Guard and/or Local Emergency Teams from the TA&C group will communicate the order. However, in Scenario 1, the evacuation will be delayed as the Civil Guard and the Local Teams are not positioned yet. In both Scenarios, the Government Education Supervisor will lack information about emergency and the evacuated schools.

If the five ministries are isolated, the NEP Director will not be able to ask for their support or for additional information. Moreover, they are not going to be directly informed about the evolution of the emergency.

In scenario 1, the isolation of the Autonomous Police is such that they will not receive the commands of the NEP Director until the satellite communication is deployed, the Civil Guard is positioned, or communications in-situ appear. The Autonomous Police and the Civil Guard Group, in case their communications systems fail, or they found it is the needed, they can activate satellite communications. However, since they request the activation until it is operative, it takes an elapsed time.

## 7. Conclusions and Future Work

We have introduced the use of Network Theory as a method to study the robustness of the communications in organizations and building organizational awareness, which are two key factors that contribute to organizational resilience. We presented a case study showing how to use the method.

The process to apply the method to any organization has two steps. First, we define the network, identifying the individuals in the organization, their relations, and the communication mechanisms they use. We represent people as the nodes in the network and their communication relations as the links. Each link has a label associated indicating the communication mechanisms that the two people connected can use. Building and visualizing the network provided awareness about the organization structure and the relationships, a key factor to achieve organizational resilience.

Then, we study the collapse in different communication mechanisms. To perform this analysis, we can select single or multiple communications channels at the same time. We identify links for each channel, and we remove them from the network. For example, if we want to study the robustness

against a failure on email communications, we remove the links representing the email channel. Then, we calculate the number of connected components. If the number of connected components remains one, it means that the information will flow among the whole organization and therefore the communication network is robust against that failure. If there is more than one component, it means that individuals are isolated, and they were not going to get the information. Having a robust communication network in an organization contributes to organizational resilience.

Our research also provides guidelines on how address the isolation problems (i.e., resulting networks with more than one component). As detailed in section 5.1, to solve the isolation problem in the network is not necessary to duplication all links; we just need to consider the isolated individuals or groups and connect them to the network. The minimum number of communication links to be added will be the number of connected components minus one.

Using this same approach, we can also study what happens in the communication structure of the organization if a person disappears (we delete the node), or if only communications are broken (we delete the links that represent these communications).

This method provides a cost-effective way to analyze the communication infrastructure and organizational relations. It also allows building awareness about the communication and information structure inside the organization. It also provides ways to improve the robustness of the network. As stated in section 2, improving the robustness, and building situation awareness are among the factors that enhance organizational resilience. Therefore, this work contributes to building organizational resilience providing a mechanism to build situation awareness and to improve the robustness of the communications inside an organization.

In future work, we will analyze how other network metrics can complement these studies. We will also investigate how to include the dynamics of the network and we simulate the message transmission to study how long it takes to receive a message since it is sent or how long it takes to get the confirmation of the accomplishment of an action. The rationale behind the proposed analysis is that having information in a timely manner is another key factor for organizational resilience.

#### **Conflict of Interest**

The authors declare that there is no conflict of interest for this publication.

#### **Acknowledgement**

The authors express their gratitude to the reviewers for their valuable suggestions towards the improvement in the quality of the paper.

## **References**

- Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: current state of research and future directions. *Omega*, 62, 1-18.
- Banahene, K.O., Anvuur, A., & Dainty, A. (2014). Conceptualising organisational resilience: An investigation into project organising. In ARCOM Conference Proceedings. 2014 ARCOM 30th Annual Association of Researchers in Construction Management Conference (Vol. 2, pp. 795-804). ARCOM. Portsmouth, UK.

- Bastian, M., Heymann, S., & Jacomy, M. (2009). Gephi: an open-source software for exploring and manipulating networks. In *2009 International AAAI Conference on Weblogs and Social Media* (Vol. 8, pp. 361-362). PKP Publishing Service. San Jose, California USA.
- Bergström, J., Van Wissen, R., & Henriquez, E. (2015). On the rationale of resilience in the domain of safety: a literature review. *Reliability Engineering & System Safety*, 141, 131-141.
- Bhamidipaty, A., Lotlikar, R., & Banavar, G. (2007). RMI: a framework for modeling and evaluating the resiliency maturity of IT service organizations. In *2007 IEEE International Conference on Services Computing* (pp. 300-307). IEEE. Salt Lake City, UT, USA.
- Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review, and future directions. *International Journal of Production Research*, 49(18), 5375-5393.
- Brinkmeier, M., Fischer, M., Grau, S., Schäfer, G., & Strufe, T. (2009). Methods for improving resilience in communication networks and p2p overlays. *PIK-Praxis Der Informationsverarbeitung Und Kommunikation*, 32(1), 64-78. <https://doi.org/10.1515/piko.2009.0013>
- Bullmore, E., & Sporns, O. (2009). Complex brain networks: graph theoretical analysis of structural and functional systems. *Nature Reviews Neuroscience*, 10(3), 186-198.
- Chami, G.F., Molyneux, D.H., Kontoleon, A.A., & Dunne, D.W. (2013). Exploring network theory for mass drug administration. *Trends in Parasitology*, 29(8), 370-379.
- Chewning, L.V., Lai, C.H., & Doerfel, M.L. (2013). Organizational resilience and using information and communication technologies to rebuild communication structures. *Management Communication Quarterly*, 27(2), 237-263.
- Chopra, S.S., & Khanna, V. (2014). Understanding resilience in industrial symbiosis networks: Insights from network analysis. *Journal of Environmental Management*, 141, 86-94.
- Cook, A., Blom, H.A.P., Lillo, F., Mantegna, R.N., Micciche, S., Rivas, D., Vazquez, R., & Zanin, M. (2015). Applying complexity science to air traffic management. *Journal of Air Transport Management*, 42, 149-158.
- De Domenico, M., Porter, M.A., & Arenas, A. (2014). MuxViz: a tool for multilayer analysis and visualization of networks. *Journal of Complex Networks*, 3(2), 159-176.
- Deng, Y., Li, Q., & Lu, Y. (2015). A research on subway physical vulnerability based on network theory and FMEA. *Safety Science*, 80, 127-134.
- Dunn, S., & Wilkinson, S.M. (2015). Increasing the resilience of air traffic networks using a network graph theory approach. *Transportation Research Part E: Logistics and Transportation Review*, 90, (39-50).
- Eusgeld, I., Kroger, W., Sansavini, G., Schlapfer, M., & Zio, E. (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering and System Safety*, 94(5), 954-963.
- Fang, C., Marle, F., Zio, E., & Bocquet, J.C. (2012). Network theory-based analysis of risk interactions in large engineering projects. *Reliability Engineering and System Safety*, 106, 1-10.
- Folke, C. (2006). Resilience: The emergence of a perspective for social-ecological systems analyses. *Global Environmental Change*, 16(3), 253-267.
- Gallos, L.K., Song, C., Havlin, S., & Makse, H.A. (2007). Scaling theory of transport in complex biological networks. *Proceedings of the National Academy of Sciences*, 104(19), 7746-7751.
- Gibson, C.A., & Tarrant, M. (2010). A “Conceptual Models” approach to organisational resilience. *The Australian Journal of Emergency Management*, 25(2), 8-14.

- Gómez, S., Díaz-Guilera, A., Gómez-Gardeñes, J., Pérez-Vicente, C.J., Moreno, Y., & Arenas, A. (2013). Diffusion dynamics on multiplex networks. *Physical Review Letters*, 110(2), 1-5.
- Grøtan, T.O., & Asbjørnslett, B.E. (2007). Information and communication technology in resilient global logistics (RGL). *Proceedings of ESREL 2007* (2349-2356). Taylor & Francis. Stavanger, Norway.
- Hamel, G., & Valikangas, L. (2003). The quest for resilience. *Harvard Business Review*, 81(9), 52-65.
- Hearnshaw, E.J.S., & Wilson, M.M.J. (2013). A complex network approach to supply chain network theory Edward. *International Journal of Operations & Production Management*, 33(4), 442-469.
- Holling, C.S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4(1), 1-23.
- Horne III, J.F. (1997). The coming age of organizational resilience. *Business Forum*, 22(2/3), 24-28.
- Horne III, J.F., & Orr, J.E. (1997). Assessing behaviors that create resilient organizations. *Employment Relations Today*, 24(4), 29-39.
- Ibrahim, G.M., Rutka, J.T., & Snead III, O.C. (2013). Network analysis reveals patterns of antiepileptic drug use in children with medically intractable epilepsy. *Epilepsy & Behavior*, 28(1), 22-25.
- ISO. (2017). *ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes*.
- Janssen, M.A., Bodin, O., Andries, J.M., Elmquist, T., Ernstson, H., McAllister, R.R.J., Olson, P., & Ryan, P. (2006). Toward a network perspective of the study of resilience in social-ecological systems. *Ecology and Society*, 11(1), 15.
- Kast, F.E., & Rosenzweig, J.E. (1972). General systems theory: Applications for organization and management. *Academy of Management Journal*, 15(4), 447-465.
- Khakzad, N., & Reniers, G. (2015). Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. *Reliability Engineering and System Safety*, 143, 63-73.
- Langlois, L. (2013). IAEA action plan on nuclear safety. *Energy Strategy Reviews*, 1(4), 302-306.
- Lengnick-Hall, C.A., & Beck, T.E. (2005). Adaptive fit versus robust transformation: How organizations respond to environmental change. *Journal of Management*, 31(5), 738-757.
- Liu, N., An, H., Gao, X., Li, H., & Hao, X. (2016). Breaking news dissemination in the media via propagation behavior based on complex network theory. *Physica A: Statistical Mechanics and Its Applications*, 453, 44-54.
- Longstaff, P.H., & Yang, S. (2008). Communication management and trust: their role in building resilience to "surprises" such as natural disasters, pandemic flu, and terrorism. *Ecology and Society*, 13(1), 3.
- Manyena, S.B. (2006). The concept of resilience revisited. *Disasters*, 30(4), 433-450.
- McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). Facilitated process for improving organizational resilience. *Natural Hazards Review*, 9(2), 81-90.
- Negeri, E., Kuipers, F., & Baken, N. (2015). Designing reliable and resilient smart low-voltage grids. *International Journal of Critical Infrastructure Protection*, 9, 24-37.
- Newman, M.E.J. (2003). The structure and function of complex networks. *Society for Industrial and Applied Mathematics Review*, 45(2), 167-256.
- Newman, M., Barabasi, A.L., & Watts, D.J. (2006). *The structure and dynamics of networks*. Princeton University Press, Washington.
- Omoto, A. (2013). The accident at TEPCO's fukushima-daiichi nuclear power station: What went wrong and what lessons are universal? *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 731, 3-7.

- Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering and System Safety*, 121, 43-60.
- Peng, H., Lu, S., Zhao, D., Zhang, A., & Li, J. (2012). An anti-attack model based on complex network theory in P2P networks. *Physica A: Statistical Mechanics and Its Applications*, 391(8), 2788-2793.
- Poland, G.A., Kennedy, R.B., McKinney, B.A., Ovsyannikova, I.G., Lambert, N.D., Jacobson, R.M., & Oberg, A.L. (2013). Vaccinomics, adversomics, and the immune response network theory: Individualized vaccinology in the 21st century. *Seminars in Immunology*, 25(2), 89-103.
- Poza, D.J., Santos, J.I., Galan, J.M., & Lopez-Paredes, A. (2011). Mesoscopic effects in an agent-based bargaining model in regular lattices. *PLoS ONE*, 6(3), (1-11).
- Rocco S, C.M., & Ramirez-Marquez, J.E. (2011). Vulnerability metrics and analysis for communities in complex networks. *Reliability Engineering and System Safety*, 96(10), 1360-1366.
- Rose, A. (2004). Defining and measuring economic resilience to disasters. *Disaster Prevention and Management: An International Journal*, 13(4), 307-314.
- Ruiz-Martin, C., Lopez-Paredes, A., & Wainer, G. (2018). What we know and do not know about organizational resilience. *International Journal of Production and Management Engineering*, 6(1), 11-28.
- Ruiz-Martin, C., & Poza, D.J. (2015). Project configuration by means of network theory. *International Journal of Project Management*, 33(8), 1755-1767.
- Ruiz-Martin, C., Ramírez Ferrero, M., Gonzalez-Alvarez, J.L., & Lopez-Paredes, A. (2015). Modelling of a nuclear emergency plan: communication management. *Human and Ecological Risk Assessment: An International Journal*, 21(5), 1152-1168.
- Santos, J.I., Poza, D.J., Galán, J.M., & López-Paredes, A. (2012). Evolution of equity norms in small-world networks. *Discrete Dynamics in Nature and Society*, 2012, 1-18.
- Sole-Ribalta, A., Domenico, M.De., Gómez, S., & Arenas, A. (2014). Centrality rankings in multiplex networks. In *ACM Conference Proceedings. 2014 ACM Conference on Web Science* (pp. 149-155). ACM. Bloomington Indiana, USA.
- Spanish Goverment. (2015). *Cobertura de Banda Ancha en España en el Primer Trimestre de 2015*. <https://avancedigital.mineco.gob.es/banda-ancha/cobertura/Documents/cobertura-BA-1trimestre2015.pdf>.
- Strogatz, S.H. (2001). Exploring complex networks. *Nature*, 410(6825), 268-276.
- Vogus, T.J., & Sutcliffe, K.M. (2007). Organizational resilience: towards a theory and research agenda. In *IEEE Conference Proceedings. 2007 IEEE International Conference on Systems, Man and Cybernetics* (pp. 3418-3422). IEEE. Montreal, QC, Canada.
- Whitman, Z., Stevenson, J., Kachali, H., Seville, E., Vargo, J., & Wilson, T. (2014). Organisational resilience following the Darfield earthquake of 2010. *Disasters*, 38(1), 148-177.
- Yazdani, A., Otoo, R.A., & Jeffrey, P. (2011). Resilience enhancing expansion strategies for water distribution systems: A network theory approach. *Environmental Modelling and Software*, 26(12), 1574-1582.
- Zhu, L., & Luo, J. (2016). The evolution analysis of Guangzhou subway network by complex network theory. *Procedia Engineering*, 137, 186-195.



Original content of this work is copyright © International Journal of Mathematical, Engineering and Management Sciences. Uses under the Creative Commons Attribution 4.0 International (CC BY 4.0) license at <https://creativecommons.org/licenses/by/4.0/>