UNIVERSIDAD DE NAVARRA

ESCUELA SUPERIOR DE INGENIEROS INDUSTRIALES

Resilience Framework for Critical Infrastructures

DISSERTATION

submitted for the Degree of Doctor of Philosophy by

Leire Labaka Zubieta

under the supervision of

Dr. Jose María Sarriegi and

Dr. Josune Hernantes

Donostia-San Sebastián, July 2013

To all my teachers in life,
formal and informal, especially those who taught me what love is.

Eskertzak

Zalantza askoren ostean hartutako erabakia izan zen doktoretza egiten hastearena, baina, lan honek eta bide honetan zehar lortutako beste hainbat helburuk, ezbairik gabe, erabaki zuzena hartu nuela baieztatzen dute.

Lehenik eta behin TECNUN, Nafarroako Unibertsitatea, eta bereziki, Antolakuntza Industrialeko departamentua eskertu nahiko nituzke, tesia egiteko aukera paregabe hau eskaini eta taldekide bat gehiago bezala onartzeagatik. Nire eskerrik beroenak, baita ere "UN-Escuela" bekari nire ikerketa finantzatzeagatik.

Urte guzti hauetan eskaini didaten laguntzagatik, nire eskerrik beroenak merezi dituzten bi pertsona nabarmendu nahiko nituzke. Batetik, eskerrik asko Sarriri nire tesiko zuzendari izateagatik. Berak erakutsi dit ikerketa on baten oinarriak ezartzen eta zehaztasun akademikoaren garrantziaz jabetzen. Bera izan da, batez ere, erronka eta ideia berrien iturri. Bestetik, nire eskerrik beroenak Josuneri, nire zuzendari ordea izateagatik eta bereziki, oso une zailetan eskaini didan laguntzagatik. Eskerrak berari unibertsitatean nirekin

igaro dituen hainbat eta hainbat orduengatik, lanak gainbegiratzeagatik, nire ideia berritzaileak entzuteagatik eta tesirako hainbatetan proposatu dizkidan hobekuntza baliagarriengatik.

Eskerrak eman nahi nizkieke, nola ez, departamentuko lankideei nire tesirako eskaini didaten laguntzagatik eta baita erlazio pertsonalak indartzeko hain beharrezkoak diren kanpoko ekintza interesgarri eta laneko giro atseginagatik. Bereziki, nire TECNUNeko lagunak azpimarratu nahiko nituzke, beraiekin bizi izan baititut inoizko une berezi eta ahaztezinenak.

Agder-eko Unibertsitatearei ere nire eskerrik beroenak, atzerriko egonaldia egiteko aukera eskaintzeagatik. Batez ere Jose eskertu nahi dut, Norvegiako egonaldian eman didan adeitasun eta laguntzagatik.

Azkenik, baina ziurrenik garrantzitsuenak, eskerrik beroenak nire senar Xabi eta gurasoei. Atzerriko egonaldiak eta nire tesian zeharo murgildurik ordenagailu atzean igarotako orduek gure eguneroko bizitzan eragin handia izanik, beraien pazientzia eta eskuzabaltasunak ahalbidetu baitute nire helburua lortzea.

Besterik gabe, espero dut tesi hau irakurtzen, nik idazten adina gozatzea.

Leire Labaka

Acknowledgements

Starting doing the thesis was a very difficult decision but this work and several achievements reached during this time confirm, undoubtedly, the correctness of that decision.

First of all I want to thank TECNUN, University of Navarra, and especially the Management Department for taking me on board and for granting me the opportunity to carry out my doctoral thesis. I would also like to express my gratitude to the "UN-Escuela" scholarship for funding this thesis work.

Secondly, there are two people who really deserve all my profound thanks for all the support they have provided me during these years. First, I want to thank Sarri for being my thesis supervisor. He showed me how to set up a good research and taught me the true meaning of academic rigor. Above all, he was a source of continuous inspiration and challenge. Second, I am especially grateful to Josune for being my co-supervisor for the way she helped me during my research especially in emotionally difficult times. I thank her for the infinite hours she spent with me at the university reviewing my work, listening to my ideas, and suggesting me useful improvements for my dissertation.

I would also like to thank my colleagues at the department for their help and support on my work and for creating such good atmosphere and interesting outdoor activities to develop personnel relationships. In particular, thank you to my friends at TECNUN with whom I have shared some of the most unforgettable and special moments.

I am also especially grateful to the University of Agder for granting me the opportunity to make an international stay. Especially, I would like to thank Jose for his kindness and support during my stay in Norway.

Last, but in fact first and foremost, my immense gratitude goes to my husband, Xabi, and my parents. The hours I spent behind my computer absorbed by my research and the stay abroad have deprived us of our personnel lives. Their generosity and patience have allowed me to reach this objective.

I hope you will enjoy reading it as much as I have enjoyed writing it.

Leire Labaka

Outline

Figures

Tables

Abstract

The welfare of society has increased significantly in the last few decades throughout the world due to advances in many sectors such as technology, health, communication, etc. But at the same time, this has also increased our dependency towards the correct functioning of these Critical Infrastructures (CIs). Therefore, a proper functioning and a high service reliability level of CIs are vital for the society's welfare.

In light of this situation, it is paramount to improve the resilience level of the CIs in order to prevent crises occurrence and absorb the impact when they occur. Resilience is defined as a capacity of a system to prevent a crisis occurrence, and in case it occurs, the capacity to absorb the magnitude of the impact and recover efficiently to the normal situation. Literature presents several definitions and perspectives regarding the resilience concept. However, it lacks to provide a detailed prescription about how crisis managers can improve their CI's resilience level holistically.

This research presents a framework that would help crisis managers to improve the resilience level of CIs. This framework provides a list of policies and sub-policies that crisis

managers should implement in their CIs to enhance the resilience level. These policies have been defined holistically taking into account internal and external stakeholders taking part in a major industrial accident as well as covering the four dimensions of resilience already defined in the literature.

Furthermore, the influence of each resilience policy on the three resilience lifecycle stages has been determined. The main conclusion obtained from this analysis is that internal policies are the ones which most influence during the prevention stage whereas both internal and external policies assist on the absorption and recovery stages.

An implementation methodology has also been defined in order to efficiently implement this framework in practice. It is difficult to implement all the policies at the same time. Furthermore, some policies require others prior implementation to achieve higher efficiency in their implementation. Therefore, this implementation methodology provides the temporal order in which the policies and sub-policies should be implemented in order to achieve a high resilience level.

In order to carry out this research different kinds of research methods have been employed. Some methods aim to gather experts' knowledge through workshops and questionnaires such as Group Model Building, Delphi, and Survey methods. Others, on the other hand, are based on analysis of past major industrial accidents or real cases such as case studies in CIs. From this variety of methods valuable and complementary information was gathered in order to develop and validate the resilience framework for CIs.

1 Introduction

This chapter presents the general overview of the problem where this research aims to contribute. Nowadays, the welfare of society is totally dependent on the proper functioning of Critical Infrastructures (CIs). However, these CIs have become more interdependent and, as a result, the consequences of a disruption in one of them affect significantly the society as many recent crises have warned us.

In light of this situation, establishing a proper crisis management process within CIs is essential to ensure the welfare of society. Crisis management has evolved considerably since its origins and nowadays, it is not only focused on establishing preventive measures and developing response procedures but on improving the decision making process in order to be able to deal with unexpected and unpredictable situations. Therefore, improving CIs resilience has become the major challenge of crisis managers. This research aims to present a resilience framework for CIs which helps crisis managers to improve the resilience level of CIs from a holistic point of view and facilitates the implementation of this framework in practice.

1.1 Overview

The welfare of society has exponentially increased in recent decades in almost every country throughout the world. Technological advances in health, education, energy, communication, etc. have supposed significant benefits for our quality of life. But, at the same time, our current daily life has become absolutely dependent on the stable service of a wide range of Critical Infrastructures (CIs).

Can you imagine the consequences that a big blackout lasting for a week could have? Or how would society respond if we run out of drinking water for a month? What economic and social consequences can these kinds of accidents generate? What other CIs could be affected if air-traffic in Europe is halted for a week? How should we prepare and manage to prevent or face these situations?

All these questions make us aware of the importance of crisis management in CIs for the proper functioning of the society. CIs support the economic, safety, and social welfare of modern society and therefore, CIs reliability and safety level should be high. Thus, several governments around the world have concluded that CIs are fundamental for the basic needs of the society and therefore, ensuring their proper functioning is vital (Hämmerli and Renda, 2010).

Furthermore, current CIs are becoming increasingly more interdependent each other (see Figure 1.1). For example, if an outage occurs due to an accident in a power grid, this crisis situation rapidly spreads through other CIs such as, health and transport affecting their functioning. CIs are highly interconnected and it is often difficult to predict how a crisis would evolve or what systems would be affected. Moreover, some crises may even cross national borders affecting the CIs of other countries. Therefore, the consequences that a disruption in one CI may have on society have increased significantly due to interdependencies among CIs and the dependency of the society on the proper functioning of CIs.

Figure 1.1: Interdependences and cascading effects among CIs.

Thus, when we think of CIs, we cannot think of them as isolated entities, but as a network of interconnected and interdependent elements. Recent crises, such as Japanese Tohoku earthquake and resulting Fukushima nuclear accident (Broad, 2011; Dempsey and LaFraniere, 2011), several power cuts in Western Europe (Andersson et al., 2005; Union for the Coordination of Transmission of Electricity, 2004; US-Canada Power System Outage Task Force, 2004; Larsson and Danell, 2006) and the eruption of Iceland's Eyjafjallajökull volcano and resulting air traffic crisis (Hall, 2010; Barr, 2010) have admonished us about the importance of CIs proper functioning for the welfare of society.

These examples show that society and companies are very dependent on the reliability and safety of CIs. Due to the Fukushima nuclear accident, over 100,000 people had to leave their houses and the surrounding environment was completely contaminated (World Nuclear Association, 2013). In addition, several companies in Japan and over the world suffered disruptions in their supply chain (Zeiler, 2011). Companies such as Nissan and Toyota had to stop their production plant for several reasons: power cuts, oil shortage, lack of part and components supply due to the closure of suppliers, etc.

Similarly, the eruption of the Eyjafjallajökull volcano and the subsequent ash cloud stopped the whole air traffic of the north of Europe affecting several countries such as United Kingdom, Ireland, Belgium, Norway, Netherlands, Sweden, etc. In particular, airports in United Kingdom and Ireland were closed for more than a week affecting thousands of passengers and leading to shortages in raw material supply such as medicines, and vegetables and fruits (Hall, 2010). Furthermore, several studies confirm that if the airports have turned out to be closed for few days more the companies would have needed more than a month to recover (Lee and Preston, 2012).

These examples show that current CIs are interdependent and the lack of sufficient prevention and preparedness level in a country or in a CI could lead to detrimental effects on many other CIs and society. Therefore, improving the crisis management within CIs is a must. This research focuses on major industrial accidents which are defined as crises that starts in a CI and spread through the whole CI network, affecting other CIs and also the society.

1.2 Crisis Management evolution

Several crises in the 1970s and 1980s increased the awareness towards crisis management. Three Mile Island nuclear accident (1979), Bhopal disaster (1984), Chernobyl nuclear accident (1986) and Exxon Valdez oil spill (1989) are some examples that raised preoccupation regarding the management of crises. As a result, many researchers started analyzing in this area proposing some procedures and plans about how to deal with crises.

Crisis management has evolved significantly since its origins. Initially, crisis management activities were focused only on developing response plans but then they realized that prevention measures were also necessary to avoid a crisis occurrence.

Some authors (Fink, 1986; Mitroff and Anagnos, 2000; Coombs, 2007) believe that dealing with crises could be a well-planned process, where the outcomes of a crisis are predictable, what could be done about it could be well planned, and that anyone could be well trained to respond properly when a

crisis occurs. However, nowadays, CIs are increasingly complex and interdependent which makes their management and control significantly more difficult. The escalation of incidents can go unnoticed until the crisis occurs. Furthermore, the globalization and tight interrelationships exacerbate the consequences that a disruption in a CI could have. In light of this complex situation, it is difficult to be ready for all kind of possible crises and a different approach needs to be adopted.

Although crisis management has received much consideration and provided useful tools and insights for preparing and responding to incidents, it has also received several criticisms. Some authors claim that crisis management is too focused on developing specific preparation and response procedures for planned situation and lacks to prepare for unexpected situations (Boin et al., 2003; Boin, 2004; Lagadec, 2007). Beforehand established procedures often fail to provide enough support to adequately face the unplanned situations. Thus, different crisis management approaches are needed to also deal with these situations.

Sometimes, beforehand established mitigation efforts may not be effective or even desirable to deal with crises and their cascading effects (Sarriegi et al., 2012). Furthermore, although the same type of crisis can occur in the same area, the challenges may be completely different; the consequences can be different and the same response procedures and activities might not be appropriate to handle them.

Therefore, crisis management should focus on preventing and preparing for all kind of hazards rather than adopting a triggering event based approach. The training should be concentrated on the process of making decisions and determining who needs to be involved to deal with a specific program rather than establishing the specific decisions or procedures.

Nowadays, crisis management strategies are also focused on training workers to make flexible and creative decisions (Van de Walle & Turoff, 2008). This allows workers to be able to make sense of the unknown situation, to gather relevant observations and data, and to make decisions and take actions

in a stressful situation, without much information. When previously established procedures are not suitable to handle crises, workers should improvise actions to respond and adapt to the new situation as soon as possible. Thus, they should train these skills for being able to perform adequately in face of these scenarios.

Furthermore, the number of agents involved in crisis management has increased and as a result, the complexity and management of the problem. External stakeholders such as government, first responders and society play also an important role in managing crises. Their adequate preparation is of utmost importance in order to properly deal with crises. Therefore, coordination activities and cooperation agreements should be established among the involved stakeholders in order to adequately cope with crises. These stakeholders may have different training, expertise, and mental models. Without measures that join these differences, crisis response will suffer from poor coordination and low integration. Thus, establishing a proper crisis management strategy, creating robust and redundant systems, preparing personnel to respond adequately, and improving the communication and coordination procedures among involved stakeholders are essential.

Finally, it is worth noting that nowadays CIs are often private companies where their main objective is to be profitable. Improving crisis management may be a costly activity and its potential is often not appreciated unless a crisis occurs. Therefore, CIs tend to reduce resources allocated to crisis management when other priorities come to light. However, not being prepared to face a significant incident could lead to detrimental effects and the closure of the company.

1.3 Critical Infrastructures Resilience

In this situation, the aim of CIs and involved stakeholders is to create resilience based organizations where workers at the company are committed with resilience building process (De Bruijne, 2006; Boin and McConnell, 2007; De Bruijne and Van Eeten, 2007; Hämmerli and Renda, 2010). Resilience is the

capacity of a system to prevent a crisis occurrence, absorb the impact and reduce the recovery period. Having resilient systems allows reducing the likelihood of having crises and also responding efficiently when one does occur. Resilience provides a wider scope, from prevention to recovery, and it makes us aware that crisis management should not focus on developing specific measures and procedures for each type of crisis but it should adopt a more holistic approach. Workers not only should focus on learning response procedures but it is also necessary to develop interpretation and adaptability skills in order to be able to respond properly in face of unplanned situation.

In light of this situation, CIs have moved their efforts towards improving the resilience level of their companies. The aim is to create resilient organizations in order to enhance the management of crises.

Literature provides several definitions regarding the resilience concept. As Moteff (2012, p. 2) states "There are almost as many definitions of resilience as there are people defining it". In addition to the definitions, some authors also characterize the principles that companies need to have in order to be resilient. However, these principles are often very theoretical and managers encounter difficulties implementing them in practice. Boin and Van Eeten (2013) corroborate our conclusion claiming that few empirical studies have been carried out on the implementation of the resilience principles.

Furthermore, these principles are often focused on organizational aspects of CIs without taking into account other aspects such as technical or social aspects. As we already explained, external entities also have an important role during the crisis response and recovery activities; therefore, their resilience level should also be improved to properly deal with crises.

What actions should be carried out to improve resilience, how resilience principles can be integrated in the general management of companies and how the implementation of these actions should be ordered to efficiently implement them are some of the main questions that crisis managers want to know.

1.4 Research objectives

The main objective of this research is to develop a resilience framework for CIs, taking into account internal and external stakeholders, in order to improve CIs resilience level and consequently reduce the crisis probability and increase their capacity to cope with crises in the most efficient and rapid way.

Below, the sub-objectives to reach the overall goal of this research are defined:

1. Develop the resilience definition that this research will take as a basis. Define the resilience types, dimensions, and lifecycle stages within the overall resilience.
2. Identify resilience policies and sub-policies that CIs and external stakeholders need to develop in order to enhance resilience. These policies and sub-policies will be defined holistically and closely related to the general management of CIs in order to facilitate their implementation in practice.
3. Assess the influence of each resilience policy on different stages of resilience.
4. Define the implementation methodology to efficiently apply this set of policies and sub-policies in a CI. The implementation methodology provides the order in which the resilience policies and sub-policies should be implemented in order to achieve high efficiency in their implementation.

1.5 The structure of the thesis

The following chapters of this thesis are structured as follows:

- *Chapter 2:* presents the literature review regarding the safety and reliability of CIs as well as the resilience concept and different existing frameworks to improve CIs' resilience. Based on the literature review the contribution of this thesis is stated.
- *Chapter 3:* explains the research methodology carried out to develop this research and how the research methods have been applied.

- *Chapter 4:* presents the resilience framework for CIs which is composed of the following three main parts: the list of resilience policies and sub-policies, the influence of the resilience policies on different resilience stages and the implementation methodology of this resilience framework.
- *Chapter 5:* explains the validation process of this research through different case studies in CIs.
- *Chapter 6:* highlights the main conclusions and the limitations of this research, and proposes future areas of research.

2 State of the Art

This section reviews the literature regarding crisis management, normal accident theory, high reliability theory, and finally, it explains the resilience concept. This research posits that resilience covers the whole crisis management process and presents a more holistic approach than other theories. Therefore, the aim of the CIs is to improve their resilience level in order to manage crisis efficiently and diminish their occurrence.

Although the literature provides several definitions regarding the resilience concept, little information can be found concerning how to improve the resilience level of the CIs. There are some frameworks and principles but they are still limited to the activities performed within the boundaries of the organization without bearing in mind external agents and their role in crisis management. Furthermore, these principles are theoretical concepts which present great difficulties to put them in practice. Therefore, this research provides a framework that aims to overcome these limitations and to help crisis managers to improve the resilience level of CIs.

2.1 Introduction

This research is focused on the crisis management of CIs, in particular, on improving the resilience level of the CIs. CIs are essential for the welfare of society; therefore, a disruption in these systems can lead to serious effects on society. Resilience provides a suitable approach to ensure the safety and reliability of these CIs. Literature presents several frameworks to improve the resilience of the systems but they still have several gaps and limitations as they will be explained in this chapter.

2.2 Terminology: from Emergencies to Crises, from Incidents to Catastrophes.

There are many concepts and definitions in the literature regarding this terminology. Although there are still no unanimously accepted definitions regarding these concepts, we adopt the following ones for this research.

An incident is defined as an unexpected or unwanted change from normal system behavior which has the potential to cause a crisis (Cooke and Rohleder, 2006). Perrow (1984), on the other hand, distinguishes between incident and accident based on the extension of the damaged part and if the system gets disrupted or not. He argues that if the damage is limited to a component or a set of components, whether the system temporarily disrupts or not, we should call it an incident. In this case, if the system gets disrupted temporarily, it comes to the normal functioning without the need to be fixed. However, if the damage extends to a subsystem or to an entire system, and disrupts the operation of the system requiring a fix to start functioning again, then the proper term will be accident.

In a higher level, a disaster is defined as a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources (United Nations International Strategy for Disaster Reduction, 2009). Quarantelli (2006)

distinguishes between disaster and catastrophe providing the following six characteristics for catastrophes compared to disasters: (1) most of the community built structure is heavily impacted, (2) local workers are not able to undertake their usual work role, (3) nearby communities cannot provide help, (4) most of the everyday community functions are interrupted, (5) higher attraction of the mass media, and (6) the political arena becomes even more important.

In addition to these concepts, there are another two which are often conflated: crisis and emergencies. Wybo and Lonka (2002) provide a useful distinction between these concepts: They state that emergencies become crises if the system's resilience and emergency preparedness is insufficient to manage the event response and recovery. In the Katrina crisis, for example, plan procedures were incompatible with the emergent reality and therefore, responders had to improvise activities in order to face the situation (U.S. House of Representatives, 2006). Large-scale events do not become crises if resources and remedies are adequate to face the situation.

Taking into account all these definitions we consider that incidents and accidents are classified within emergencies whereas disasters and catastrophes are within crises (see Figure 2.1).

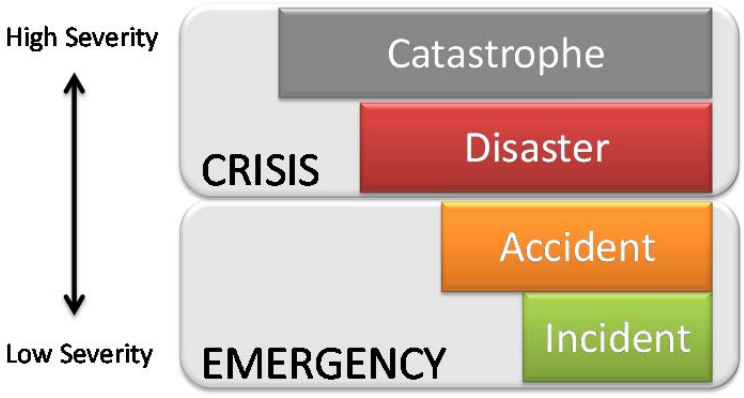


Figure 2.1: Terminology.

A crisis is caused by a low probability, high-impact event that threatens the viability of the affected system (Pearson and Clair, 1998). In the same vein, other authors define a crisis as a consequence of an unexpected and unpredictable triggering event that suddenly strikes all the system (Mitroff and Anagnos, 2000; Pearson and Clair, 1998; Coleman, 2004). However, sometimes, a crisis may be a result of the incubation of small events that slowly evolve and finally lead to an occurrence of a big crisis (Turner, 1976; Coombs, 2007; Roux-Dufort, 2007; Roux-Dufort, 2009). Perrow (1984) argues that most industrial crises are not only due to system errors but also due to a combination of serious failures occurring at the level of components, operators, procedures, equipment, the environment and the system. Pauchant and Mitroff (1992) extend this view by exploring other aspects of the organization that could anticipate a crisis: the organizational strategy, the organizational structure, the organizational culture and assumptions, and the psychology of managers and leaders.

Hwang and Lichtenthal (2000) define two types of crisis (abrupt crises and cumulative crises) based on how and why CIs fail and the probability of this happening. Abrupt crises are prompted by a sudden external or internal triggering event creating tension throughout the system. Their occurrence probability is constant and independent of the age of the CI. Cumulative crises, on the other hand, grow over time until a certain threshold-limit is reached. Instead, in this situation, the probability of failure is an increasing function of time.

In spite of these formal definitions, in reality researchers and practitioners use these terms (incident, accident, disaster, catastrophe, emergency and crisis) interchangeably (Dugdale et al., 2009).

Crisis situations create acute feelings of stress, anxiety and uncertainty. Many authors (e.g., Pearson and Clair, 1998; Shrivastava et al., 1988; Pearson and Mitroff, 1993) believe that coping with a crisis can be a very well-planned process, where the outcomes of a crisis are very predictable, what can be done about it can be very well planned, and anyone can be very well prepared to respond properly when a crisis occurs. Others (e.g., Boin et al., 2003; Lagadec and Rosenthal, 2003; Boin, 2004; Lagadec, 2007) state that many times crises

strike unpredictably and unexpectedly and therefore it is not possible to prepare a response plan in advance since nobody knows when, how and what would be affected by the crises.

Mitroff and Anagnos (2000) believe that current crises are inevitable because they have become an integral feature of the new information/system age. They define five important characteristics to describe the current world:

- *Complexity:* current organizations have more parts and do more things than ever before.
- *Coupling:* everything anywhere is simultaneously connected with and may be affected by everything else in the world.
- *Scope & Size:* the current systems are bigger in their scope and size and they are distributed over large portions of the earth's surface.
- *Speed:* all the effects (good and bad) spread more rapidly than ever before.
- *Visibility:* it is difficult to hide the effects of a crisis or large-scale system breakdowns.

Although it is difficult to prevent crises, their impact can be diminished and the recovery period can be reduced significantly if they are managed efficiently. This is possible by establishing an appropriate and advanced crisis management strategy in place before the crisis occurrence (Mitroff and Anagnos, 2000).

2.3 Crisis Management

The nature of crisis management and the research in this field has evolved since its origins. During the 1980s the field was concerned mainly with a tactical approach, developing specific plans and checklists. The researchers were focused on writing down the crisis management plan to know how to respond when a crisis occurred. This approach established rigid tasks with little chance to modify them (Fink, 1986; Fearn-Banks, 2007; Murray and Shohen, 1992).

During the 1990s, researchers in this field began to give more importance to strategic issues. They moved toward a continuous, cyclical perspective on crises. The authors realized that the crisis plan was insufficient to assure the safety and they changed their focus toward preventive action (Mitroff et al., 1996; Coombs, 2007). Crisis prevention, detection and response became an integral part of the company's way of managing crises (Mitroff and Anagnos, 2000).

However, it is often difficult to foresee the low frequency events that cause crises. It cannot be known when the triggering event will occur, which part of the system will be damaged and how it will spread through other sectors (Perrow, 1984). Weick and Sutcliffe (2007) state that reliable organizations do not confine themselves to anticipating all possible triggering events, because this is impossible and can lead to gaps in prevention and preparedness. Instead, they pursue the ability to make sense of emerging signals and a culture that favors organizational learning from errors as opposed to only the prevention of errors.

Therefore, more recently, crisis researchers have focused on organizational culture and transformation. Interactions between the CI and external stakeholders and developing a crisis culture within the organizations have become the most promising alternative for current crisis managers. Not only preventing and developing specific plans but also adopting an adaptive behavior plan is essential to face crisis situations (Gilpin and Murphy, 2008; Weick and Sutcliffe, 2007; Elwood, 2009; Boin and McConnell, 2007).

The literature on crisis management basically identifies three to six phases within the crisis management process (see Table 2.1). Some authors (Smith, 1990; Richardson, 1994; Coombs, 2007) define three stages within the crisis management process based on the three main phases of the crisis lifecycle: pre-crisis, peak of the crisis, and post-crisis. Other authors focus more on the aim of the activities carried out during the crisis management process. Drennan and McConnell (2007) and Alexander (2002) define mitigation, preparedness, response, and recovery phases within the crisis management process where the first two are carried out before the crisis occurrence.

Table 2.1: Crisis management phases in the literature.

PHASES	Smith (1990)	Richardson (1994)	Coombs (2007)	Drennan and McConnell (2007)	Fink (1986)	Myers (1993)	Pearson and Mitroff (1993)	Van de Walle & Turoff (2008)
Pre-crisis	Crisis of management	Pre-crisis / disaster phase	Pre-crisis	Mitigation	Prodromal crisis stage	Normal operations	Signal detection	Preparedness
								Training
				Preparedness			Preparation/ Prevention	Mitigation
								Detection
Peak of the crisis	Operational crisis	Crisis impact / rescue phase	Crisis event	Response	Acute crisis stage	Emergency response	Containment/ Damage limitation	Response
					Chronic crisis stage	Interim Processing		
Post-crisis	Crisis of Legitimation	Recovery / demise phase	Post-crisis	Recovery	Crisis resolution stage	Restoration	Recovery	Recovery/ Normalization
							Learning	

Fink (1986) and Myers (1993) also define four stages but in this case they divide the peak of the crisis stage into two different stages. Several authors disaggregate some of these four basic stages in several stages. Pearson and Mitroff (1993) define a five stage crisis management process: signal detection, preparation/prevention, containment/damage limitation, recovery, and learning. Disaggregating even more, Van de Walle and Turoff (2008) define a six step process within the crisis management: preparedness, training, mitigation, detection, response, and recovery/normalization.

However, majority of authors take as a basis the classification which includes the following four basic phases (Drennan and McConnell, 2007; Alexander, 2002): mitigation (prevention), preparedness, response and recovery (see Figure 2.2).

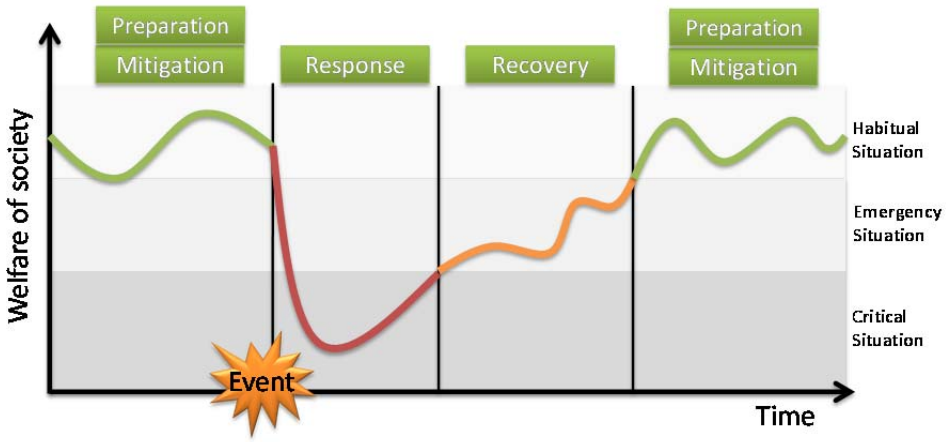


Figure 2.2: Crisis Management Phases.

Mitigation is also known as prevention and it refers to the actions taken to identify risks, avoid their occurrence and reduce possible negative effects on human life and personal property. Crisis managers often detect warning signals and then take actions designed to prevent their unfolding.

Given that crises cannot be prevented, it is also essential to be prepared for their response. Preparation has to do with the activities taken prior to the

triggering event that enables crisis managers and public to be able to respond rapidly and efficiently when a crisis does occur.

Following the triggering event, the response phase starts when all the preparation activities that were designed and trained before the triggering event should be applied. During this period, response actions are performed to minimize the potential impact of the triggering event and to reduce the human and property losses as much as possible.

Finally, the recovery stage covers all the activities carried out to return to the normal social and economic situation. It is important to return quickly to reduce as much as possible the impact. In this phase it is also important to learn from the crisis and identify lessons learned and improvements that need to be made.

Having well established crisis management procedures and protocols helps in the sustainability and continuity of the organizations. However, in most of the cases, the potential of these procedures and protocols does not flourish because crises are low probability events. Furthermore, when crisis management is well implemented, the benefits of these best practices are not appreciated since successful management events often pass unnoticed (Repenning and Sternman, 2001). Therefore, normally crisis management resources have to compete against profit-driven activities which can provide immediate benefits (Stephenson et al., 2010).

Nonetheless, recent crises such as the 9/11 terrorist attack or power cuts in Europe, such as Italian power cut (2003) and Sweden power cut (2003), have raised the crisis awareness level. These crises have shown that having well defined and integrated crisis management procedures and protocols within the overall management of the company is paramount to reduce the likelihood of crises and provide a reliable service.

2.4 Normal Accident Theory (NAT) vs High Reliability Theory (HRT)

The significant socio-technical crises which occurred during the 1970s and 1980s, such as the Bhopal disaster (1984), the Three Mile Island nuclear accident (1979), and the Chernobyl nuclear accident (1986), raised awareness and elicited grave concern regarding the safety and reliability level of complex, high-risk technological companies. This preoccupation led to two prominent schools of thought: Normal Accident Theory (NAT) and High Reliability Theory (HRT). Both analyze the reliability, safety, and crisis management in complex and high-risk technological organizations.

2.4.1 Normal Accident Theory (NAT)

Normal Accident Theory (NAT) was developed by Charles Perrow (1984). He posits that accidents are inevitable or "normal" in complex organizations that operate high-risk technologies. In particular, Perrow (1984) states that complex and high-risk technologies have certain features which make the occurrence of crises unavoidable. These characteristics are interactive complexity and tight coupling. Interactive complexity refers to the extent of unfamiliar and unexpected interactions among the system's components whereas tight coupling refers to the minimal time lag between the processes the system executes.

Perrow (1984) argues that when circumstances are just "right", a failure can trigger other failures and they can cascade very rapidly through tightly coupled systems due to complex interactions. Thus, under such circumstances, prevention of crises is almost impossible. He explains that large-scale system accidents are the result of simultaneous and interactive failure among various system components, procedures, operators, supplies and materials, environment and design (Perrow, 1984). The challenge then, from an organizational perspective, is to develop the capacity to cope with complex interactions and tight coupling.

This theory is of great interest and has to be considered especially in the field of CIs, as technological advances have allowed these organizations to significantly expand their operational capacity catering the society's demands. However, this expansion, in turn, has increased the complexity level of CIs which makes accident anticipation and prevention difficult and as a result, jeopardizes CIs' service reliability level.

2.4.2 High Reliability Theory (HRT)

However, in response to NAT approach, some researchers argue that instead of just waiting for these normal accidents to occur organizations can take proactive measures that can help to avoid a crisis occurrence (Roberts and Rousseau, 1989; Roberts and Bea, 2001).

Researchers from the University of California in Berkeley studied how some organizations that operate complex and high-risk technologies manage to remain accident-free for long periods of time while simultaneously achieving highly variable and demanding production goals. They called these organizations High Reliability Organizations (HROs). In order to identify this type of organization, Roberts (1990, p. 160) proposes the following question: "How often could this organization have failed with dramatic consequences? If the answer to the question is many thousands of times the organization is highly reliable".

The development of this theory was based on direct observation of error-free systems. Initially, these scholars studied three "error-free" organizations (Roberts, 1993): the Federal Aviation Administration's air traffic control (Rochlin et al., 1987), Pacific Gas and Electric Company's operation of its nuclear power plant, and the US Navy's nuclear powered aircraft carriers.

All the organizations studied had something in common. All of them were complex technological systems where reliability was vital since they operated in a very high-risk environment without a second chance. They argue that organizations can become more reliable by creating a positive safety culture and reinforcing safety-related behaviors and attitudes (Weick and Roberts,

1993). These characteristics enable them to both achieve and maintain an excellent safety performance record. However, the main characteristic of HROs is not that they are error-free, but they avoid unfolding failures (Rochlin, 1993). For this reason, HROs analyze in depth and learn from every small error that occurs in the organization.

Through these studies they identified several characteristics and processes that help these organizations to reach and maintain their excellent safety records (Roberts and Rousseau, 1989; Roberts, 1990; Roberts and Bea, 2001):

- *Deference to expertise during emergencies:* In normal situations the decision making is hierarchical where the responsibilities of each worker are clearly defined. However, during crisis situations, decision-making migrates to individuals with more expertise in the field regardless of their position within the organization.
- *Management by exception:* Managers are only involved in strategic and tactical decisions and they only get involved in operational decisions when required.
- *Climate of continuous training:* Continuous training is provided to operators in order to enhance and maintain their knowledge of complex operations within the organization, and improve their technical competence to recognize hazards and respond to "unexpected" problems appropriately.
- Several channels are used to communicate safety critical information and to ensure that crisis managers can access it in a timely manner, especially in crisis situations.
- *Redundancy:* Having back-up systems in case of a failure, internal cross-checks of safety-critical decisions and continuous monitoring of safety critical activities ensures the proper management of crises.

HROs are known for the capability to absorb and recover from errors as well as for their capability to foresee possible errors they might happen. Scholars from the University of Michigan state that HROs are able to avoid crises because they have a certain state of mindfulness (Weick and Sutcliffe, 2007). They define mindfulness as the capability for rich awareness of

discriminatory detail that facilitates the discovery and correction of potential crises (Weick and Sutcliffe, 2007). Mindfulness is less about decision making and more about clear and detailed comprehension of potential threats.

Weick and Sutcliffe (2007) define five principles that lead HROs to reach their state of mindfulness:

- *Preoccupation with failure:* HROs are very preoccupied with failures and any little incident is analyzed in depth because they know that something could have severe consequences if several separate small errors happened to coincide.
- *Reluctance to simplify:* they know that the world they face is complex, unstable and unpredictable and simplification could lead to the non-detection of failures and consequently a crisis might occur. Therefore, they are reluctant to simplify processes.
- *Sensitivity to operations:* they make continuous adjustments that prevent errors from accumulating and enlarging.
- *Commitment to resilience:* HROs develop capabilities to detect, contain and bounce back from the inevitable errors by training and preparing personnel with deep and varied experience.
- *Deference to expertise:* HROs push decision making down to the people with the most expertise to make better decisions because they are the ones who know more about the problem.

The first three principles are focused on anticipating possible failures whereas the last two are containment principles (Weick and Sutcliffe, 2001; Van de Walle and Turoff, 2008).

Recently, Lekka (2011) performed an extensive literature review regarding HROs and developed a mind map summarizing the most important processes and characteristics of high reliability organizations (see Figure 2.3). The defined features are aggregated into the following six main groups: containment of unexpected events, problem anticipation, learning orientation, mindful leadership, definition, and just culture. Within each of them three to six characteristics are defined.

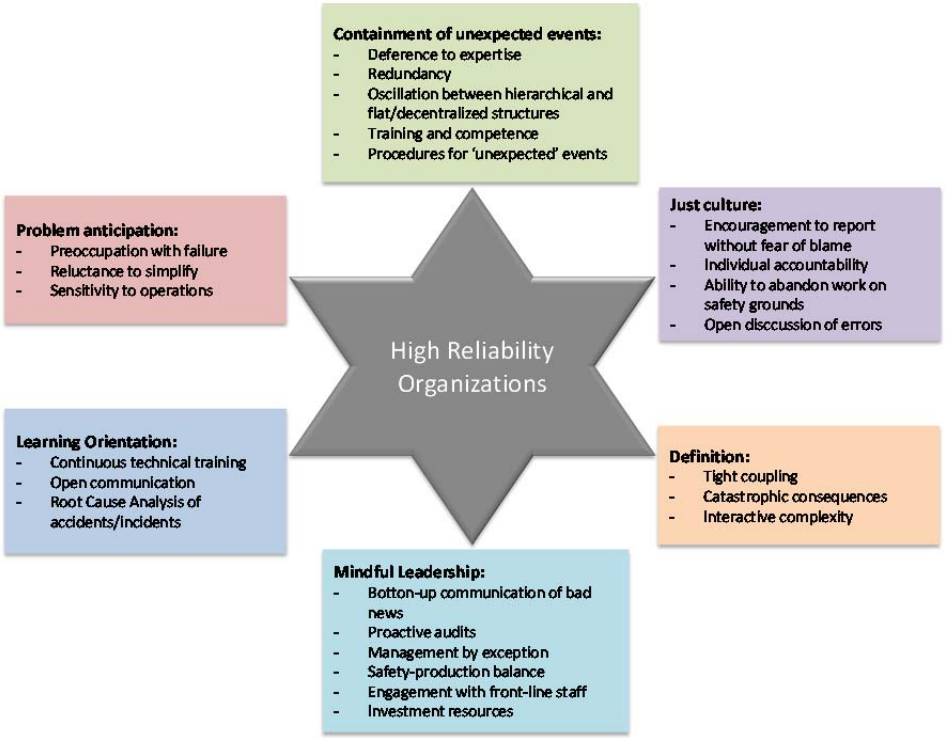


Figure 2.3: Mind map with the main characteristics of HROs. Adapted from (Lekka, 2011).

2.4.3 Limitations of both theories

Since the emergence of both theories, a great debate has evolved between the two views regarding management of accidents. Both theories address the issue of reliability in high-risk technological organizations but they come to different conclusions. However, both present some limitations, as they will be explained below.

NAT recognizes the difficulty of dealing with uncertainty but underestimates and oversimplifies the potential ways to cope with uncertainty, whereas HRT underestimates the problems of uncertainty (Marais et al., 2004). Perrow's NAT presents some limitations when defining the two main features of high-risk technological organizations and leads to more pessimism with respect to designing and operating complex high-risk systems (Marais et al., 2004). HRT, on the other hand, provides more suggestions but some of them

are inapplicable to complex systems or oversimplify the problems involved, for instance, focusing only on simple redundancy or studying systems which are relatively simple and loosely coupled.

Leveson et al. (2009) argue that Perrow (1984) provides vague definitions regarding the two main features of these systems (interactive complexity and tight coupling). This problem, in turn, leads to another two: inappropriate comparisons between incomparable properties and misclassification of industries. Regarding the first one, Leveson el al. (2009) criticize that when evaluating the level of risk of the systems Perrow (1984) only considers the probability of a crisis occurring and ignores the magnitude of it. Concerning the second one, Leveson et al. (2009) state that it is necessary to distinguish among many different types of complexity and coupling.

Further, Hopkings (1999) highlights five limitations of NAT:

- Only applies to a small number of crises.
- The main characteristics of NAT are poorly explained
- There are some crucial aspects that seem to be wrong.
- Recent efforts to improve the theory by expanding it fail to do so.
- Lacks provision of policies that help avoiding crises.

Regarding HRT, some authors argue the lack of precision when defining concepts such as safety and reliability (Hopkins, 2007; Leveson et al., 2009). HRT uses these two concepts interchangeably. However, Leveson et al. (2009) make a distinction between these concepts. They define reliability as "a probability that a component satisfies its specific behavioral requirements over time and under given conditions" (Leveson et al., 2009, p. 234). On the other hand, they believe that safety is a system property and they define it as "freedom from unacceptable losses" (Leveson et al., 2009, p. 234). They argue that there can be safe systems with unreliable components and also state that increasing system reliability may reduce the system safety (Hopkins, 2007; Leveson et al., 2009). Connected with the system thinking approach, Leveson et al. (2009) also argue about the deference to expertise principle defined by HROs. They state that decentralized decision making is required in some

critical situations but they emphasize that decisions must be taken from a system level rather than from a component or worker level.

Although some authors view both approaches as contradictory, others state that they analyze different stages and they can be perfectly complementary. Shrivastava et al. (2009) explain why both theories still remain in the literature and why there is not one which prevails over the other one. They state that both theories focus on entirely different stages within the process towards a system crisis. During the initial stages of an accident, when component failures occur, Perrow (1994) argues that it is very difficult for all failures to combine in a manner that defeats all safety measures, triggering a crisis. However, he argues that the higher the level of complexity of interactions and coupling within a system, the higher will be the probability to end up in a crisis. Thus, HRT focuses on the early stages of a crisis where little incidents may incubate and lead to a crisis. However, NAT concentrates on later stages when failures are already combined in a risky manner and the triggering event has already occurred.

Despite the two theories (NAT and HRT) and their importance in the literature, we consider that there are still some limitations in their definitions and descriptions. NAT explains the problems of the current organizations, but it does not provide any detailed policy to deal with them. HRT, on the other hand, presents some theoretical principles to cope with crises and to create reliable companies. However, most of the principles are still theoretical and therefore, crisis managers have significant difficulties to implement them in practice. As Waller and Roberts (Waller and Roberts, 2003) claim these theoretical principles should be transformed to more suitable processes and actions for companies in order to facilitate their implementation. Although there has been much research in defining and explaining the characteristics of HROs, there have been few efforts to define how these principles can be transferred to the general management of CIs (Boin and Van Eeten, 2013; Lekka and Sugden, 2011). Furthermore, as HRT principles are general, the transferability of the principles might be context-specific (Lekka and Sugden, 2011). Empirical research has been more prominent in the health sector where

reliability enhancing principles have been applied in different disciplines to improve their reliability and safety level (Madsen et al., 2006; Van Stralen et al., 2005; Agency for Healthcare Research and Quality, 2008). However, it is harder to find empirical studies about how to implement these principles in the context of other type of CIs because it is sometimes difficult to balance safety with profit driven activities (Boin and Schulman, 2008; Hopkins, 2000).Therefore, further research is required to illustrate the way of how reliability principles should be applied in practice.

2.5 Critical Infrastructures (CIs)

Having reliable and safe organizations is even more important in the field of CIs since current society is highly dependent on their proper functioning.

CIs are systems, services and assets, whether physical or virtual, so vital for the welfare of society that a disruption or destruction of such systems and assets has severe impact on the health, security, safety or economic well-being of citizens and on the effective functioning of the government (Rinaldi, 2004; Commission of the European Communities, 2005). Although there is not a unique list of CIs (Farrell et al., 2002), the European Commission (2005) proposes the following sectors: energy, information and communication technologies (ICT), water, food, health, financial, public & legal order and safety, civil administration, transport, chemical and nuclear industry and space and research.

According to La Porte (1996) there are some specific characteristics of these particular systems that make critical infrastructures:

- Tightly coupled technically and complex operating requirements and management aspects.
- Non-substitutable, with few competing organizations delivering the same service.
- Driven to achieve the maximum performance.
- Source of public anxiety when interruptions in the service or serious operating failures occur.

- Critical for the effective functioning of the society.

Modern CIs are becoming increasingly more interdependent locally, regionally and globally, constituting a system of systems (Eusgeld et al., 2011; Sarriegi et al., 2008). A crisis that starts in a CI spreads through the whole CI network very rapidly. According to Rinaldi (2004) there are four types of CI interdependences:

- *Physical:* If the state of each CI depends upon the material output(s) of other CI.
- *Cyber:* If the state of a CI depends on information transmitted through the Information and Communication Technologies (ICT) infrastructure.
- *Geographic:* If local environmental changes affect the CIs in that region, e.g., when the flooding of a reservoir knocks out a generator, this implies close spatial proximity.
- *Logical:* If the state of each CI depends upon the state of another one via policy, legal, regulatory or some other type of governmental mechanism.

Nowadays, CIs underpin the economic, safety and social sustainability of modern society, where 24/7 reliable provision is paramount for the welfare of society (De Bruijne, 2006; Egan, 2007). Therefore, in order to provide uninterrupted service, CIs must be highly reliable in performance.

Some years ago, CIs afforded a high level of reliability in their services, raising the social expectations. Accustomed to this high level of reliability in the past, society took reliable service for granted and did not allow disruptions of CIs. In order to provide this service, CIs have grown in size and complexity, but as a result, they have also inadvertently increased their vulnerability. Furthermore, current terrorist attacks and natural disasters that threaten the proper functioning of CIs have increased the concern and the preoccupation regarding the reliability and safety level of CIs (Boin et al., 2003; De Bruijne, 2006).

2.5.1 Critical Infrastructure Protection (CIP)

Promoted by this concern, a new knowledge area known as Critical Infrastructure Protection (CIP) was created. This is a recent concept which was consolidated in the USA under the Presidential Directive in 1998 and in Europe Though the European Programme for Critical Infrastructure Protection (2006)[1]. CIP can be defined as actions and programs, undertaken jointly by Government and the operators of CIs, to identify CIs and their components, assess their vulnerabilities, and take preventive and protective measures to reduce vulnerabilities (Auerswald et al., 2005). CIP integrates a significant number of existing strategies, plans and procedures to deal with prevention, preparedness, response, and recovery issues within the CIs. Furthermore, several handbooks have been published recently regarding the security and protection aspects of CIs such as International Critical Information Infrastructure Protection (CIIP) Handbook (Brunner and Suter, 2008) and Protecting Critical Infrastructure in the EU (Hämmerli and Renda, 2010).

However, several academics have highlighted the limitations of conventional crisis management approaches for effective CIP in the literature (Boin and McConnell, 2007; De Bruijne and Van Eeten, 2007). Boin and McConnell (2007) argue that prevention and planning efforts provided by conventional crisis management approaches may not be enough to face unexpected and unpredictable situations. They state that CIs also need to develop adaptive capacities to better deal with "extraordinary" crises (De Bruijne and Van Eeten, 2007). Therefore, they posit that CIs should develop more resilience based strategies to ensure the safety and reliability in the context of this complex environment (De Bruijne, 2006; Boin and McConnell, 2007; De Bruijne and Van Eeten, 2007; Hämmerli and Renda, 2010).

[1] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

2.6 Resilience

Resilience has widely been used in different disciplines such as environmental science (Holling, 1973; Perrings, 2001), engineering (Lecoze and Capo, 2006), psychology (Zimmerman and Arunkumar, 1994), organizational studies and economics (Briguglio et al., 2009). Despite its extended use, there is no agreement on the definition and the scope of this concept (Manyena, 2006). As a generalization, the term implies both the ability to adjust to "normal" or to anticipate events, and also to adapt to sudden shocks and unexpected events.

Resilience has also become a very relevant concept in the field of crisis management. However, there are also diverse definitions and perspectives in the literature regarding this concept.

Some authors differentiate between anticipation (mitigation or resistance) and resilience. For them, resilience involves the capacity of a system to absorb disturbances, respond effectively and bounce back to the initial state as soon as possible (Longstaff, 2005; McEntire, 2005; Mileti, 1999; Vogus and Sutcliffe, 2007). However, other authors expand this definition by considering resilience to be a capacity generated from both proactive and reactive activities (Bruneau et al., 2003; Kahan et al., 2009; Brunsdon and Dalziell, 2005; Hollnagel et al., 2006; Westrum, 2006; Seville et al., 2008).

Regarding the first approach, Longstaff (2005) describes resilience as the "capacity of a system to absorb disturbance, undergo change, and still retain essentially the same function, structure, identity and feedbacks" (p. 15-16) and resistance as "the strategy that attempts to keep the danger away from the system in the first place" (p. 15). Therefore, resilience only refers to the reactive response while resistance is more focused on the proactive response. McEntire (2005) also uses the terms resistance and resilience to refer to proactive and reactive crisis responses, respectively. Mileti (1999) also considers resilience a reactive response, while referring to the preventive work as mitigation rather than resistance. In the same vein, Vogus and Sutcliffe (2007) define resilience as a process of building capabilities for recovering from unexpected events rather than eliminating or avoiding them.

On the other hand, according to the second perspective on resilience, Bruneau et al. (2003) extend the concept of resilience by defining it as the capacity of the system to reduce the probability of failure, to reduce the consequences from failure and to reduce the time needed to carry out all the response and recovery activities. Focusing on CIs, Kahan et al. (2009) posit that resilience results from activities that limit damage to infrastructure (resistance), mitigating the consequences (absorption) and reducing the recovery period to the pre-event state (restoration). Brunsdon and Dalziell (2005) provide an organizational development perspective on the development of resilience, including sensitivity to recoverable limits (risk management), increasing the boundaries which define the recoverable limits (business continuity planning), reducing the recognition time (situational awareness), and improving the capacity to recover soon (creativity and responsiveness). More generally, Seville et al. (2008, p.18) define resilience as "the ability to survive and potentially even thrive, in times of crisis".

Some authors stress that failures often come from the dynamic instability of a system and therefore, resilience is also dynamic, rather than a static concept. From this viewpoint, crisis management includes the need to understand and be able to foresee when a system may lose its stability in the future (Hollnagel et al., 2006). Instead of just focusing on aspects that go wrong, Hollnagel et al. (2006) define resilience as the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress. Hollnagel (2011) extends this perspective, defining Resilience Engineering as a process that increases the number of things that go right and thereby improves the performance of the system when it is challenged. Westrum (2006) divides the dynamics of resilience into three major components: (1) foresee and avoid referring to the ability to prevent something bad from happening, (2) cope with ongoing trouble related to the ability to keep something bad from becoming worse, and (3) repair after catastrophe focused on the ability to recover from something bad once it has happened. Table 2.2 summarizes this collection of resilience definitions within the literature.

Table 2.2: Contrasting definitions of "resilience".

Resilience Perspective	Authors	Contribution to the definition of "resilience"
Resilience (absorption and recovery)	Longstaff (2005) & McEntire (2005)	Differentiation between Resistance and Resilience
	Mileti (1999)	Differentiation between Mitigation and Resilience
	Vogus and Sutcliffe (2007)	Building capabilities for recovering from crises
Resilience (prevention, absorption, and recovery)	Bruneau et al. (2003)	Reduce the probability of failure, reduce the consequences, and reduce the recovery time.
	Kahan et al. (2009)	Outcome of resistance, absorption, and restoration
	Brudson & Dalziell (2005)	Risk management, business continuity planning, situational awareness, creativity and responsiveness
	Hollnagel et al. (2006)	Intrinsic ability to face dynamic instabilities
	Hollnagel (2011)	Resilience Engineering: focus on increasing the number of things that go right
	Westrum (2006)	Foresee and avoid, cope with ongoing trouble, repair after catastrophe.
	Seville et al. (2008)	The ability to survive and even thrive in times of crisis.

In this research, we align our belief to the latter group of scholars, as we consider resilience from both proactive and reactive perspectives, and we believe that resilience is dynamic since it changes over time. Our understanding is that resilience serves not only to reduce the magnitude of the impact after the triggering event has occurred, but also helps to avoid the occurrence of a crisis. Furthermore, we consider that the resilience level of a system can vary depending on the measures established in the system.

If resilience changes over time based on action or inaction and it has different aims, its definition should include some notion of dynamics. We

characterize a dynamic resilience lifecycle in three stages, based on the definitions already mentioned in the literature review (Bruneau et al., 2003; Kahan et al., 2009; Westrum, 2006) (see Figure 2.4):

- *Prevention:* the capacity of a system to prevent a crisis occurrence.
- *Absorption:* the capacity to reduce the magnitude of the impact.
- *Recovery:* the capacity to recover rapidly and efficiently to the normal state.

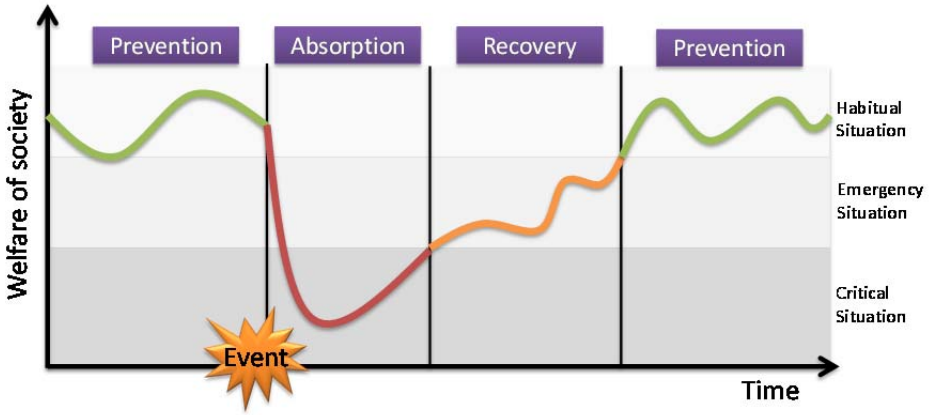


Figure 2.4: The resilience lifecycle stages during a crisis lifecycle.

Resilience affects all the lifecycle phases. During the pre-crisis phase, it assists in resisting any potential threat that could lead to a crisis. When a triggering event occurs, resilient systems are able to absorb the impact and avoid the damage to grow due to preparation activities carried out in the pre-crisis stage. Finally, resilience facilitates the recovery process in reducing the total impact and the time to recover.

2.6.1 Relationships among the crisis management phases and resilience lifecycle stages

Taking as a basis the crisis management phases defined in the literature, the relationships among these phases and the resilience lifecycle stages can be defined (see Figure 2.5). Before a crisis occurrence, the aim of CIs is to mitigate a crisis occurrence and prepare for a critical situation. In this stage, regarding

resilience, the aim of the system is to prevent the unfolding of incidents that could lead to a severe crisis. For that, CIs aim to build resistant systems that are able to withstand incidents and to prepare workers to detect early warning signals and to act as soon as possible to avoid further damage.

However, not always it is possible to avoid a crisis occurrence. When a crisis occurs, the target of CIs is to absorb the impact and reduce its magnitude. This has a relationship with the response phase within the crisis management phases. Finally, once the situation is under control, the recovery period starts. CIs need to develop their capacity to efficiently bounce back to the initial stage in order to reduce the consequences. This last stage is entirely related to the recovery phase defined within the crisis management cycle.

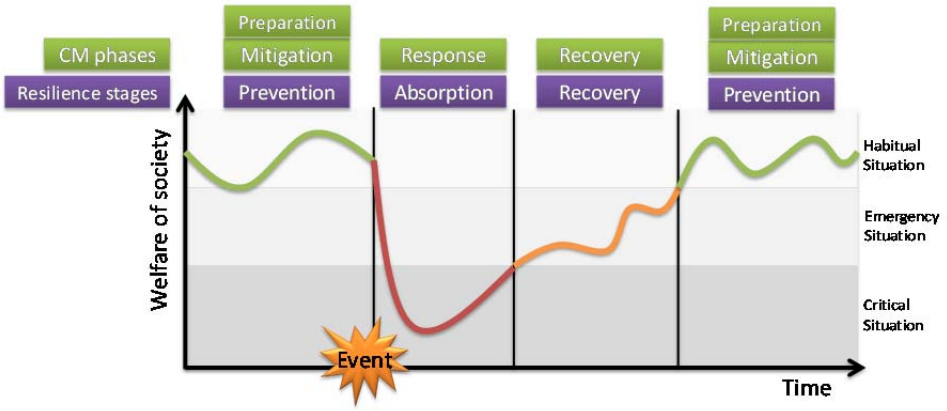


Figure 2.5: Relationship among crisis management phases and resilience lifecycle stages.

2.6.2 Resilience dimensions and principles

Some authors break resilience down into four dimensions (Bruneau et al., 2003; Multidisciplinary Center for Earthquake Engineering Research (MCEER), 2008; Zobel, 2010; Gibson and Tarrant, 2010):

- *Technical resilience:* this refers to the ability of the organization's physical system to perform properly when subject to a crisis.

- *Organizational resilience:* this refers to the capacity of crisis managers to make decisions and take actions that lead to a crisis being avoided or at least to a reduction of its impact.
- *Economic resilience:* this refers to the ability of the entity to face the extra costs that arise from a crisis.
- *Social resilience:* this refers to the ability of society to lessen the impact of a crisis by helping first responders or acting as a volunteer.

In order to describe the resilience concepts, some authors define the following characteristics as the main features of resilience (Bruneau et al., 2003; Multidisciplinary Center for Earthquake Engineering Research (MCEER), 2008; Zobel, 2010):

- *Robustness:* refers to the strength or the capacity of a system or an element to resist the impact of a triggering event, in terms of magnitude of the impact or loss of functionality.
- *Redundancy:* refers to the extent to which components of the system are substitutable, or able to be replaced when functionality has been lost or reduced.
- *Resourcefulness:* refers to the capacity to efficiently respond to a crisis, identifying problems, establishing solutions, and mobilizing the required resources.
- *Rapidity:* refers to the rate or speed at which a system is able to bounce back to the normal situation and achieve goals in order to reduce the magnitude of losses and avoid future disruptions.

In the same vein, Gibson (2010) defines six key principles to define the resilience concept:

- *Resilience is an outcome:* resilience is not a process, management system, strategy or predictive measurement but a trait that can be observed in response to a critical circumstance.
- *Resilience is not a static trait:* an organization's resilience will not be constant but dynamic, it will increase or decrease as the context changes.

- *Resilience is not a single trait:* resilience arises from a complex interaction of many factors. As circumstances may change, the presence, importance, and contribution of each of these factors to resilience may change in turn.
- *Resilience is multidimensional:* resilience can be mainly disaggregated in four dimensions: technical, organizational, economic and social.
- *Resilience exists over a range of conditions:* resilience can exist over a range of conditions from low resilience (vulnerable) to high resilience (resilient).
- *Resilience is founded upon good risk management:* resilience is built up based on assessment, treatment, and monitoring and communication of risk.

Brunsdon and Dalziell (2005) propose that resilience can be broken down into two components: vulnerability and adaptive capacity. The first one refers to the ease with which an organization is pushed into a new state and adaptive capacity as the ability to cope with that change. They provide a way of evaluating the resilience level, stating that the resilience of the organizations is a function of the area under the curve, relating to both the magnitude of the impacts experienced by the organization (function of vulnerability) and the time it takes for that organization to recover (function of adaptive capacity) (see Figure 2.6).

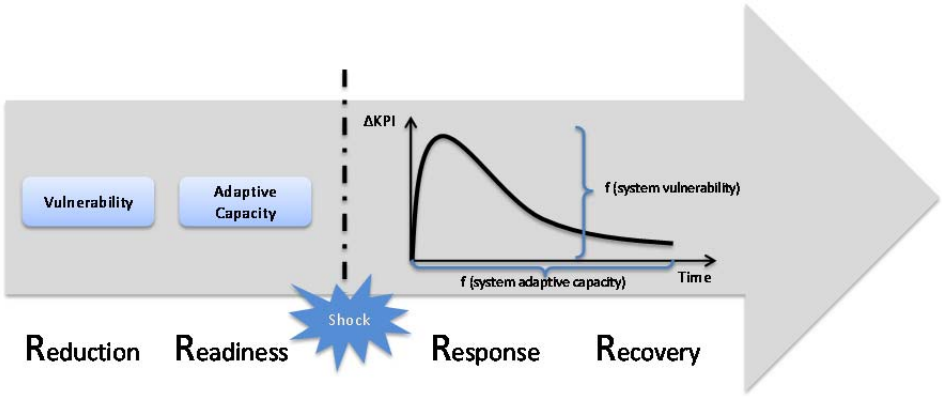


Figure 2.6: Resilience as a function of the area under the curve (Brunsdon and Dalziell, 2005).

2.7 Crisis Management and Resilience Standards

There are several standards regarding risk management and business continuity. The International Organization for Standardization has issued the ISO 31000:2009 standard that defines some generic principles and guidelines for risk management. It addresses personnel responsible for developing, evaluating, and ensuring that risk management policies are implemented within the organization. The standard provides eleven principles that organizations need to establish so that the risk management process is efficient. Alongside these principles, it presents a management framework to guide organizations in the risk management process. The required components and their interrelationships are defined within this management framework. Finally, the process of managing risk is shown highlighting that this process should be an integral part of management, integrated in the culture and day-to-day functioning, and adapted to the business processes of the organization.

The AS/NZS 5050:2010 Australian standard explains how to apply the ISO 31000:2009 standard by providing some detailed guidance and a methodology for determining how a disruption can affect the continuity of the organization. More recently, a new Disaster Management Standard: ISO 22320:2011 entitled "Societal Security - Emergency Management - Requirements for Incident Response" has been developed to help organizations to minimize the impact of disasters, terrorist attacks, and other major crises. It establishes a foundation for the coordination and cooperation amongst all involved stakeholders during a crisis, in order to minimize misunderstandings problems and ensuring a more efficient use of combined resources. The ISO 22320:2011 also provides best practices for establishing command and control organizational structures and procedures, decision support, and traceability and information management.

The American National Standards Institute defines an organizational resilience standard (ASIS SPC 1-2009) which aims to provide a management framework to enhance an organization's capacity to manage and survive the event and take appropriate actions to ensure the continuity and sustainability of organizations. It proposes guidance for an organization to develop its own organizational management system that assists in anticipating and preventing,

if possible, and preparing for and responding to disruptive incidents. Based on the plan-do-act-check model, it develops an organizational resilience management system flow diagram which describes the activities encompassed in each stage (policy, planning, implementation and operation, checking and corrective action, and management review). In addition to these standards, literature also defines some frameworks and principles to enhance the resilience level of the organizations. Below, we will explain the most important ones.

2.8 Framework for Building up the resilience of the systems

Crises can be unpredictable and unexpected what makes difficult to foresee how they will occur and evolve in order to implement measures to prevent them. However, some authors claim that despite the inherent uncertainty of crises we can substantially limit or prevent their occurrence implementing some measures and creating more resilient systems (Marais et al., 2004).

Regarding organizations, McManus et al. (2007) focus on building up the organizational resilience level. They define three dimensions and fifteen indicators to assess and enhance the organizational resilience level of companies. Taking this framework as a basis, Stephenson (2010) extends it, emphasizing the importance of resilience culture for improving the organizational resilience level adding six more indicators to better measure the resilience level of an organization. Finally, a survey together with a factor analysis was conducted to refine the framework and define the most influencing factors to improve the organizational resilience (Lee et al., 2013). The new framework is composed of thirteen resilience indicators grouped into three attributes: leadership and culture, networks, and change ready (Resilient Organisations, 2012).

The leadership and culture attribute refers to the leadership capacity of the organization to manage and make decisions in times of crises and to the level of

engagement and awareness of the staff to improve resilience based culture within the company. Within the leadership and culture attribute five resilience indicators have been defined: leadership, staff engagement, situation awareness, decision making, and innovation and creativity. The networks attribute corresponds to the external relationships the company has in order to share knowledge, experiences, and resources with other stakeholders involved in crisis management. This attribute is divided into four resilience indicators: effective partnerships, leveraging knowledge, breaking silos, and internal resources. Finally, change ready is related to how the organization develops its strategy and communicates to its members and how it trains the staff to be ready to detect early warning signals and response efficiently in face of a crisis. Four resilience indicators have been identified within this attribute: unity of purpose, proactive posture, planning strategies, and stress testing plans.

In the same vein, a workshop conducted by Trusted Information Sharing Network's Community of Interests describes eight key attributes of resilience organizations (Parsons, 2007): awareness, agility and flexibility, change readiness, interdependency knowledge, integration, culture and values, leadership, and communications. When a crisis occurs, these attributes enable the organization to effectively:

- Anticipate and understand emerging threats.
- Understand the impact of threats on the organization, supply chain, the community in which it operates, and upon the lives of staff.
- Develop and maintain supportive partnership with critical stakeholders.
- Respond, recover, and grow from disruptions as a unified organization.
- Adapt to disruption and react flexibly to restore and improve functioning and strengthen the organization.
- Ensure staff is willing and able to support the organization to achieve organizational objectives.
- Articulate clear organizational objectives and establish a strong sense of purpose in response to recovery and growth from a disruption.
- Lead with clear direction while enabling decentralized problem solving.

The framework proposed by Resilient Organisations group, as well as the attributes defined by Parsons, focus on organizational management, without providing significant information about other dimensions of the resilience (technical, economic, and social) identified earlier in section 2.6.2. Furthermore, these authors do not describe the path forward to developing resilient systems.

Johnsen (2010) takes a step forward and provides an explicit technical dimension to resilience. He describes seven principles (based on organizational and technical aspects) that organizations need to be resilient.

- *Graceful and controlled degradation:* identifying risks and implementing measures to prevent their occurrence lead to avoidance of a crisis occurrence. Furthermore, the ability of a system to recover and return to the initial situation should also be developed. Organizational competence and appropriate technical systems contribute to increase the resilience level.
- *Management of margins:* organizations need to constantly ensure that performance boundaries are not crossed. However, extensive testing also needs to be conducted to analyze the capacity of a system to manage margins.
- *Common mental models:* having common mental models among all the stakeholders is essential to ensure communication and collaboration across all of them.
- *Redundancy:* redundancy provides an alternate way to perform a function by different technical systems or by different procedures when the current one fails. However, care should be taken because redundancy also introduces new vulnerabilities in the system and increases complexity.
- *Flexibility:* flexibility includes being able to perform actions in different ways and to improvise in stressful and critical situations to cope with crises.

- *Reduction in complexity:* reducing the complexity of an organization is important to decrease the likelihood of a crisis occurrence, and to detect a failure and stop its spread easily.
- *Reduction of coupling:* reducing the coupling between processes decreases the probability of crises. This can be achieved by enabling processing delays and flexibility in many aspects such as using methods, resources, availability of substitutes, etc.

Nonetheless, as in the earlier cases, the processes and transformations required to create resilience building activities are not specified. From a more holistic point of view, Kahan et al. (2009) argue that resilience applies to three critical areas, society, economy, and government, and within each of them soft and hard aspects can be identified. They propose eight principles that resilient systems should achieve bearing in mind technical, organizational, and economic aspects within CIs:

- *Threat and hazard limitation:* this proposes that crisis managers should try to anticipate, detect, identify, interdict, neutralize, avoid, or redirect damage mechanisms before they occur.
- *Robustness:* this has to do with the capability and capacity of critical systems to withstand severe internal and/or external stresses and to maintain key functions that are critical for daily life.
- *Consequence mitigation:* this indicates the capabilities of critical systems and their key functions to control and reduce cascading adverse effects of a damage event and then, recover quickly and resume normal activity.
- *Adaptability:* a resilient system is able to maintain equilibrium in case of a damage event or return to an equilibrium state after experiencing unanticipated adversity.
- *Risk-informed planning:* to ensure that resilience principles contribute to desired resilience outcomes, they need to be implemented in relation to the threat, vulnerability, and consequence factors identified for critical systems and their key functions.

- *Risk-informed investments:* the allocation of resources to investments in meeting the resilience requirements of any critical system or key function needs to be done, including the risks faced by those assets.
- *Harmonization of purposes:* the above mentioned six principles need to be mutually reinforcing to be fully effective in serving their purpose.
- *Comprehensiveness of scope:* recognizing that resilience encompasses all the CIs' and society's safety is the central principle in order to understand resilience and develop practical ways and means to make this happen.

Externally, Cutter et al. (2010) define a set of indicators to evaluate disaster resilience levels and in turn, the efficiency of the established policies that foster the resilience level. However, these policies are focused on natural disasters and therefore, they only provide policies for external stakeholders. Furthermore, little is stated about how to improve these indicators.

2.9 Contribution of this research

In summary, there is a broad set of works discussing general characteristics and principles about how to build the CIs resilience level. However, the literature still lacks a detailed prescription for crisis managers about which activities should be carried out and how resilience principles should be transformed and applied in CIs. The definitions of the principles limit to describe their meaning and advantages but they lack to provide the activities or actions that need to be carried out to implement these principles in practice (Boin and Van Eeten, 2013; Lekka and Sugden, 2011). The language used in their descriptions is not associated with the day-to-day language used in the companies what makes even more difficult the application of the principles in CIs (Waller and Roberts, 2003). Furthermore, literature hardly provides empirical researches and case studies about the implementation of these principles in CIs.

In addition, most of the current sets of principles still focus on activities within the boundaries of the CI or even only on activities to improve the organizational resilience, underestimating the role of external agents and their

influence on improving the CIs resilience. The effects of CI failures often cross organizational boundaries, and the activities and information needed to ensure their resilience are sometimes neglected. Although there are some frameworks to evaluate the external resilience level, they are mostly focused on natural (Cutter et al., 2010).

CIs are embedded within a network of stakeholders (other CIs, first responders, government, etc.) where relationships are very tight and therefore, consequences of different policies established by other agents affect CIs resilience directly. Thus, resilience not only should be developed within the CI but closely related agents also contribute to the CI resilience level in order to efficiently respond to adverse situations.

In light of this situation this research presents a resilience framework that helps crisis managers to improve CIs resilience level. First, this framework facilitates the understanding of the resilience concept and highlights the dynamic aspect of the resilience. It provides a set of tangible policies that should be implemented in CIs and external stakeholders to increase CIs resilience level. Furthermore, some policies have been disaggregated into several sub-policies to better define the policies and how their implementation should be performed. The influence of each policy on the three resilience lifecycle stages (prevention, absorption and recovery) defined in this research has also been assessed in order to provide more information regarding the resilience policies' effects. This framework has been defined holistically covering the four dimensions defined in the literature and considering also the external agents that get involved when a crisis occurs explicitly. Furthermore, in order to validate the framework and obtain some insight about how this framework can be implemented in a CI, some empirical research was carried out.

Due to the interdependency of the policies and sub-policies and in order to efficiently implement this framework in a CI, an implementation methodology has also been developed. This methodology guides crisis managers when implementing the resilience framework, establishing the temporal order in

which the policies and sub-policies should be performed in order to achieve high efficiency in the implementation of the framework.

3 Research Methodology

This section presents the methodology carried out in order to develop this research. The methodology is composed of three main phases: (1) conceptualization, (2) development of the framework, and (3) validation of the framework.

Within each phase different research methods were applied to obtain the required information and knowledge. In the field of crisis management, most of the information remains in the experts' mind. Therefore, most of the applied research methods focus on gathering experts' knowledge to develop and validate the results. Multidisciplinary experts with different backgrounds took part in the development of this research.

Bearing in mind that resilience building process is primarily an applied discipline, empirical research was also required to add more applicability to the proposed results. Therefore, case studies were developed in different CIs to validate the framework and its usefulness to improve the resilience level of CIs.

Literature Review, Group Model Building, Multiple Case Studies, Delphi Method, Survey and Case Study methods have been applied to perform this research. .

3.1 Introduction

The research methodology should be appropriate according to the research topic, research objectives and the desired results. This research is focused on a theoretical concept such as resilience and the aim is to develop a framework to improve the resilience level of CIs. Different research methods were applied to develop and validate the framework.

During the development phase, most of the applied research methodologies were focused on gathering knowledge from experts in the field. For the validation phase, due to the low occurrence rate of crises, it was difficult to test the contribution of this framework in face of a real crisis. Therefore, the validation of this framework was carried out especially based on evidence and examples gathered through studies in CIs. This chapter explains the general characteristics of the research methods used in this research and how these methods were applied in this particular case.

3.2 Research methodology

The methodology used in this research consists of three main phases: (1) conceptualization and formulation of the research questions, (2) development of the resilience framework, and (3) validation of the resilience framework. In each phase, combinations of different research methods were applied: (1) Literature Review, (2) Group Model Building, (3) Multiple Case Study, (4) Delphi Method, (5) Survey, and (6) Case Study.

Figure 3.1 resumes the research methodology, defining the research methods, the results, and the published papers in each step. Following, the phases carried out in this research will be explained in detail.

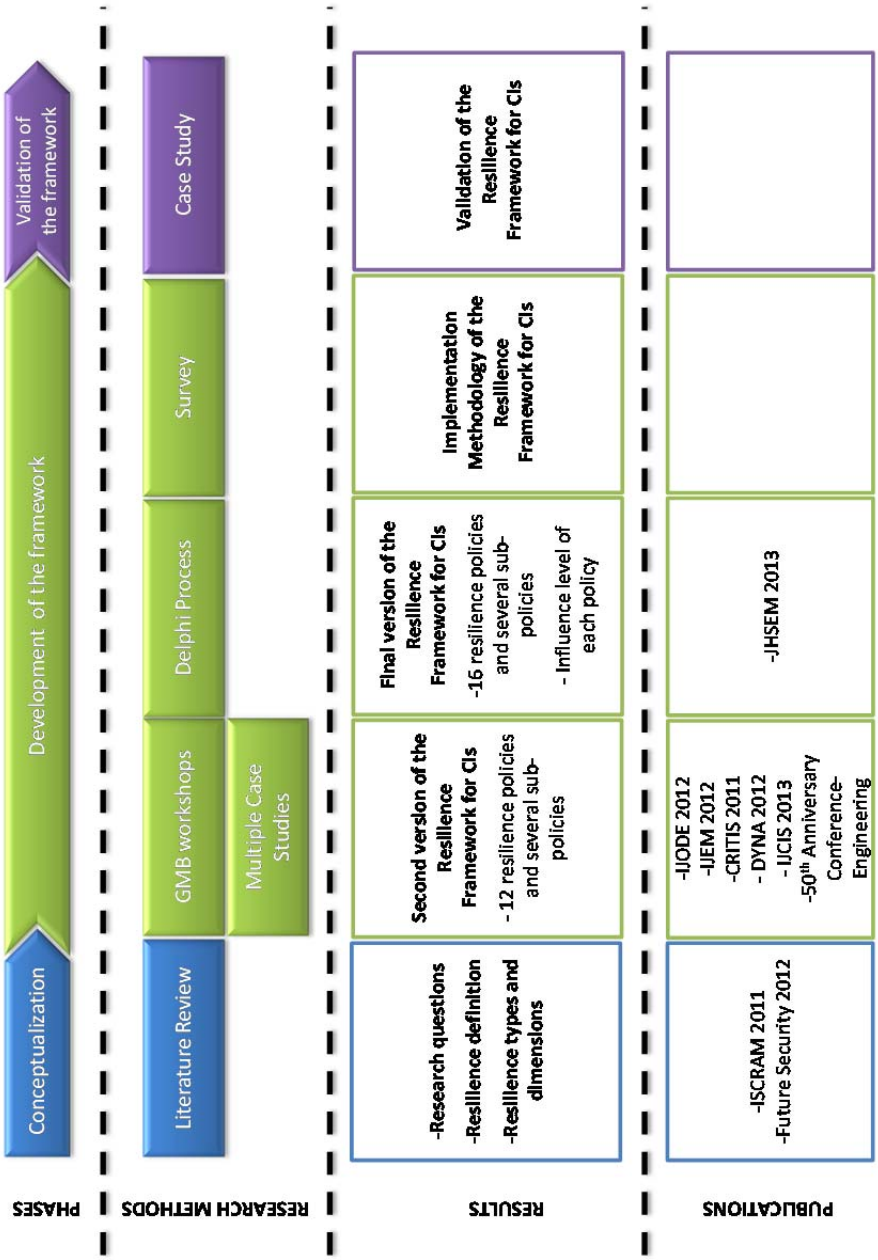


Figure 3.1: The research methodology.

3.3 Conceptualization

Before establishing the research objectives, it is necessary to have a look to what has been done and to decide where this research can contribute. Therefore, a conceptualization phase was carried out to determine the research gap and the contribution of this research. The literature review was chosen as a research method.

A fundamental part of a research is to analyze the existing literature in the field of study. It is important to determine what the literature provides and, taking this as a starting point, identify the possible contribution of the research. Furthermore, it assists on defining the context in which the study will be established and narrowing down the scope of the research into a manageable project (Croom, 2009). In addition to this, reviewing existing literature in the field provides considerable insight into the research methods that can be suitable (Croom, 2009).

Several resilience definitions were analyzed and we classified them in two main groups as it has already been explained in the state of the art section. Besides, the research questions and objectives were determined as it can be seen in chapter one.

Through the reviewed literature and taking into account that our research is mainly focused on major industrial accidents, we divided the resilience level of the overall system into two different resilience types: internal resilience and external resilience. Bearing in mind the four resilience dimensions defined in the literature, for each resilience type different resilience dimensions were determined. All these resilience types and dimensions will be further explained in chapter four.

3.4 Development of the Resilience Framework for CIs

Once the research objectives were established our aim was to start developing the resilience framework for CIs. The framework is composed of three main parts: a set of resilience policies and sub-policies, an influence table

where the influence of each resilience policy on the three resilience lifecycle stages is assessed, and an implementation methodology. Despite the fact that most of the crisis management knowledge remains in the brains of experts, the aim was to gather all this knowledge through appropriate methods.

Several iterations applying different research methods were carried out to obtain the final version of the Resilience Framework for CIs (see Figure 3.2). First, a collaborative method called Group Model Building (GMB) was used to gather knowledge about the problem from the experts. A very basic framework composed of eight resilience policies was developed with the knowledge extracted from the European project workshops' documentary reports. Afterwards, multiple case studies method was applied to improve the framework. Through this step, new resilience policies and several sub-policies were introduced to the resilience framework. Finally, the improved version of the list of resilience policies and sub-policies was obtained based on experts' knowledge through the Delphi process. Furthermore, the influence level of each policy on the three resilience lifecycle stages was assessed within the same Delphi process.

In order to define the implementation methodology, a survey was conducted where experts defined the temporal order in which the policies and sub-policies need to be implemented in order to achieve a high efficiency in the application of this framework in a CI.

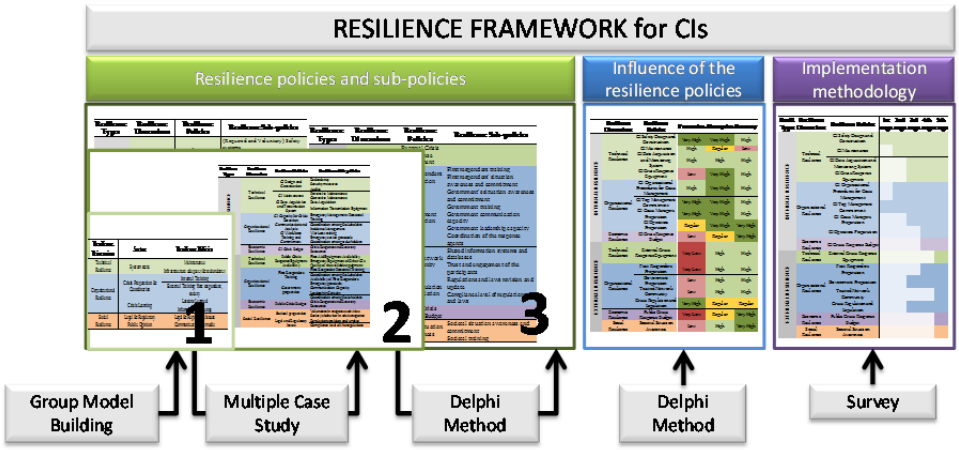


Figure 3.2: The main steps within the development phase.

3.4.1 Group Model Building (GMB)

GMB is a collaborative method which enables integrating fragmented knowledge, initially residing on the minds of different agents, into aggregated models (Richardson and Andersen, 1995). Modelers in collaboration with domain experts develop simulation models that provide insights to the problem (Andersen et al., 1997; Andersen et al., 2007; Rich et al., 2009). Through established activities (stakeholders' analysis, policies and indicators identification, behavior over time of the indicators, etc.), modelers were able to integrate experts' fragmented knowledge into aggregated models. However, it is important to involve many participants in the modeling process to gain more confidence on the model (Vennix, 1996).

Three workshops were arranged in San Sebastian (Spain) within the context of the European project SEMPOC (Simulation Exercise to Manage Power Cut Crises) in the field of Critical Infrastructure Protection (CIP) during 2010-2011. The target of this project was to assess the European power production and distribution system's ability to deliver service and mitigate damage in the face of a major power cut. SEMPOC employed the GMB method to gather knowledge about the problem from domain experts. Through scripted and facilitated activities, the experts' fragmented and tacit knowledge was integrated into a system dynamics model. Experts from different institutions

such as energy companies, first responders and organizations for civil protection, health care and CIs protection took part in the elicitation and modeling activities (see Table 3.1).

Table 3.1: Organizations of experts that took part in the SEMPOC workshops.

Organization	Country	Sector
National Operations Centre	Holland	National Civil Protection
Sjöland&Thyselius	Sweden	Safety Consultancy
Swedish Civil Contingencies Agency	Sweden	National Civil Protection
REE (Spanish Energy Company)	Spain	Energy
Gas Natural - Fenosa (Spanish Electric and Gas Company)	Spain	Energy
Faculty of Criminal Justice and Security	Slovenia	Academic
Gjovic University College	Norway	Academic
CNPIC (Critical Infrastructure Protection National Center)	Spain	National Civil Protection
Argonne National Laboratory	USA	Energy
Directorate for Civil Protection and Emergency Planning	Norway	National Civil Protection
Danish Emergency Management Agency (DEMA)	Denmark	National Civil Protection
SAMUR (Emergency and Rescue Service)	Spain	First Responders
Eles (Elektro Slovenija)	Slovenia	Energy
EPES (Public Emergency Health Organization)	Spain	First Responders

The workshops provided a wealth of information about the variety of stakeholder perspectives on crisis management, including the recognition of stakeholders taking part in the crisis management process, identification of indicators and their reference modes, and policies to build the system's resilience level. Hernantes et al. (2012a; 2012b) explain in great detail the activities carried out and the obtained results.

As a starting point of our research, the policies to build the system's resilience level that experts identified during the workshops were extracted from the SEMPOC project's documentary reports. Eight resilience policies

classified in five sectors were defined in the SEMPOC workshops (Hernantes et al., 2012a). Although the SEMPOC project was mainly concerned with crises in the power sector, the policies defined could be applicable to other CI sectors as well.

3.4.2 Multiple Case Studies

In order to provide more confidence in the initial list of policies, several previous large-scale crises were analyzed using the multiple case studies method (Yin, 1994). Yin (1994) defines four types of designs for case studies based on two magnitudes: the first one refers to the amount of cases studied and the second one to the number of units of analysis addressed.

Our aim with this study was to complete the initial list of resilience policies we obtained in the SEMPOC project, through the study of multiple cases. In order to do that, we considered analyzing several past major industrial accidents of different sectors to expand the suitability of this set of policies to other sectors as well. The units of analysis addressed during the research were causes of the triggering event, and correctly or badly established measures that lead to a proper or improper recovery, respectively.

Major nuclear accidents, blackouts, oil spills, mining accidents and air traffic accidents were studied to obtain evidence of the consequences of having a low or high degree of effective implementation of each policy and to complete the initial list of policies. The cases were selected based on the available information and magnitude of the impact (see Table 3.2).

Through this study, the list of policies was improved and the second version of the resilience framework for CIs was developed. This version was composed of a set of twelve policies that help crisis managers to improve the resilience level of CIs (Labaka et al., 2013). Furthermore, some sub-policies were identified for each policy in order to better understand the scope and the definition of each policy.

Table 3.2: Analyzed major industrial accidents during the multiple case studies.

Type of accident	Accident	Year
Air-Traffic accident	DC aircraft accident in Paris	1974
	DC aircraft accident in Chicago	1979
	Tenerife aircraft accident	1977
	Spanair aircraft accident	2008
Transport accident	Ford motor company	The 1970s
Power blackouts	Canadian Blackout	2003
	Italian Blackout	2003
Chemical accident	Bhopal Accident	1984
Oil spills	BP Oil Spill	2011
	Exxon Valdez	1989
	Prestige	2002
Nuclear accidents	Chernobyl	1986
Mining accidents	San José Mining accident in Chile	2010
	Pasta de Conchos Mining accident in México	2010

3.4.3 Delphi method

Based on the information gathered through multiple case studies, the resilience framework was improved. However, this version of the framework still required more corroboration from experts in order to affirm the suitability of the defined policies in other CI sectors. The aims of this step were to complete the list of policies and sub-policies and to improve their description. In addition, an assessment of the influence of the resilience policies on the three resilience lifecycle stages was carried out to provide information about the timing and relative importance of the activities in response to CI risks and concerns.

This research applied Delphi method to refine and extend the second version of the framework. Delphi is a systematic and iterative process for structuring a group communication process in order to obtain a consensus about a complex problem (Dalkey, 1969; Linstone and Turoff, 1975; Okoli and Pawlowski, 2004).

Delphi method was originally designed to reduce the confrontation and inhibiting effects of interacting groups, while at the same time retaining the power of combined knowledge from a group of experts (Dalkey, 1969; Linstone and Turoff, 1975). Rowe and Wright (1999) describe four key features of the classical Delphi method:

- *Anonymity of participants:* experts express their opinion freely without the pressure or fear not to agree with others.
- *Interaction:* experts can refine their answers based on the results of the group from round to round.
- *Controlled feedback:* the process informs the participants of other participant's opinion and provides the opportunity to justify or change their answers.
- *Statistical aggregation of group response:* the Delphi method allows for a quantitative analysis and aggregation of data.

The Delphi method consists of multiple rounds of questionnaires and feedback among informants. In the first round a questionnaire is sent to all the experts. After all the answers are collected a new round is distributed. The first questionnaire is supplemented with each expert's previous answers and the mean of the group's ranking (Skulmoski et al., 2007). The expectation is that each expert may reflect on their earlier answer and, over time, some convergence may be obtained. The process is anonymous and is repeated until the stopping criterion is reached: for example, a fixed number of rounds have been completed or a consensus has been achieved. Delbecq et al. (1975) propose that two or three interactions are enough for most researches.

The Delphi method provides primarily two advantages comparing with collaborative methodologies: reduction in time investments for participants since they do not have to move, and reduction in cost for the research group since there are not displacement costs (Delbecq et al., 1975). Furthermore, being iterative helps refining the answers of the participants and also matches with the cyclical nature of model-building. However, regarding the satisfaction of participants with the procedure, they argue about the lack of opportunity for

interaction and clarification of ideas with other experts (Nelms and Porter, 1985).

Concerning the number of participants that should take part in the process, Delbecq et al. (1975) propose that the sample should be between ten and fifteen people in case the sample is homogeneous. On the contrary, if disparate participants are involved then Linstone and Murray (1975) propose that four to five experts from each field are needed to perform the process.

The Delphi participants are characterized by the following four "expertise" requirements (Skulmoski et al., 2007):

- They should have knowledge and experience with the issue under investigation.
- They should be willing to participate.
- They should have sufficient time to participate in the process.
- They should have effective communication skills.

Multidisciplinary experts from different sectors (academics, transport, energy, and first responders) took part in the process. Before starting with the Delphi process, a pilot study was carried out with three experts in the field of crisis management and Delphi method to test the adequacy of the questionnaires. After ensuring that questionnaires were appropriate for the process, an invitation was sent to thirty-two experts closely related to the field of crisis management to know their willingness to participate in the Delphi process.

While we attempted to enlist the same number of experts in each field, there was an imbalance of respondents, especially in the transport category. Twenty-one experts agreed to collaborate in this validation process, and fifteen completed the entire process. Therefore, the panel of experts was composed of fifteen multidisciplinary experts from four fields (academic, transport, energy, and first responders) (see Table 3.3).

It is worth noting that most of the experts that took part in the Delphi method were different from the experts that participate in the SEMPOC workshop activities. Only three experts took part in both processes.

Table 3.3: Organizations of experts that took part in the Delphi process.

Organization	Country	Sector
Norwegian University of Science and Technology	Norway	Academic
University of Agder / Centre of Integrated Emergency Management	Norway	Academic
North Carolina State University	USA	Academic
Universita Campus Bio-Medico	Italy	Academic
University of Warwick	United Kingdom	Academic
AERTEC Solutions	Spain	Transport
Mobility and Logistics Cluster	Spain	Transport
Iberdrola (Spanish Energy Company)	Spain	Energy
REE (Spanish Energy Distribution Company)	Spain	Energy
Spanish Nuclear Energy Company	Spain	Energy
Argonne National Laboratory	USA	Energy
SGSP Main School of Fire Service	Poland	First Responders
Public Emergency Health Organization	Spain	First Responders
Emergency Response and Meteorology of the Basque Country	Spain	First Responders
SAFETEC	Norway	First Responders

Two different questionnaires with different aims and content were used (see Appendix C). In each round, the experts were given a week to answer the questionnaires (they had the option not to answer a question if they did not feel comfortable doing so), and we then spent another week analyzing the results and preparing the material for the next round.

The scope of these questionnaires was on major industrial accidents. We defined major industrial accidents as crises that affect a CI or a network of CIs and extend to the surrounding areas affecting also the society. In total, three

rounds were carried out with two iterations for each questionnaire (see Figure 3.3).

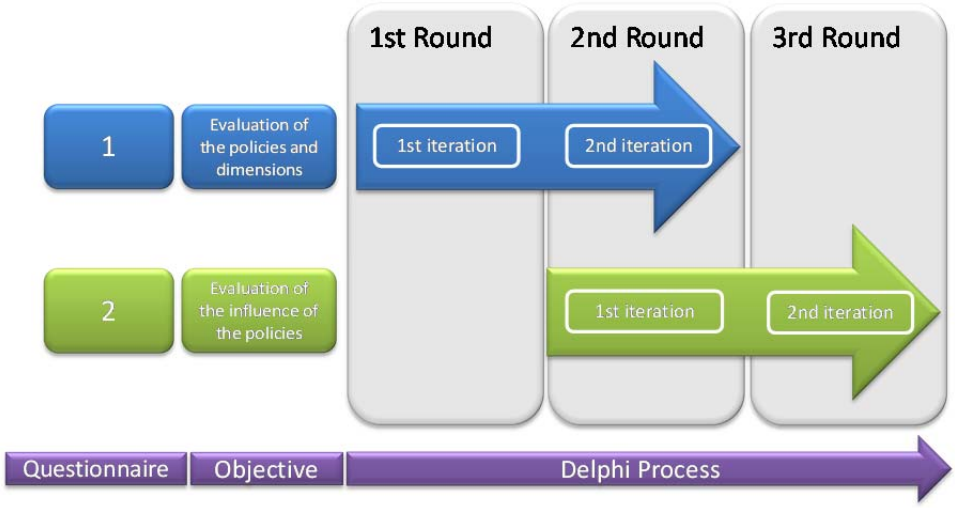


Figure 3.3: The Delphi Process.

In the first round the first questionnaire was sent to experts. The target of the first questionnaire was to validate and complete the list of policies and sub-policies of the second version of the framework with the experts' opinion. The experts were asked to evaluate from 0 to 5 (being 0 the lowest value and 5 the highest one) the completeness and clarity level of the definition of the policies and the appropriateness of the policy within the corresponding resilience dimension (technical, organizational, economic and social). Moreover, we also asked them to evaluate from 0 to 5 the completeness and clarity level of the definition of the resilience sub-policies and their appropriateness within the corresponding resilience policy. Finally, we encouraged them to propose other policies and sub-policies in order to build up each resilience dimension level.

In the second round of the process, the experts had to reevaluate their initial answers of the first questionnaire based on the other experts' answers from the first iteration. In addition, new policies and updated definitions proposed by experts were added to the initial questionnaire. Further, the first round of the second questionnaire was also sent to the experts.

The aim of the second questionnaire was to assess how each policy influences the three resilience lifecycle stages. In order to do that, experts were asked to evaluate from 0 to 5 the influence of each resilience policy in each resilience lifecycle stage, with 0 being no influence and 5 strong influence.

Finally, in the last round of the process, the second questionnaire was sent again to the experts with the answers gathered from the previous round in order to reevaluate their answers.

As a result of this process, an improved version of the list of policies and sub-policies was obtained; four new resilience policies and several sub-policies were introduced to the framework based on the experts' knowledge (see Appendix C). Furthermore, the influence level of each resilience policy in the three resilience lifecycle stages was assessed taking into account the experts' opinion (see Appendix C). All these results will be further explained in chapter four.

3.4.4 Survey

Once the set of resilience policies and sub-policies was defined and the influence of each resilience policy on the three resilience lifecycle stages was assessed, the aim was to define the implementation methodology of the resilience framework for CIs. This method aims to facilitate crisis managers in the implementation of this framework in a CI and ensure the highest efficiency in performing this task.

This implementation methodology was defined based on experts' knowledge. A survey was chosen as a research method to gather knowledge from experts. A survey consists of a systematic and standardized approach to collect information from a large group of people through questionnaires (Marsden and Wright, 2010; Forza, 2002). Four basic tasks compose the core of the survey method:

- *Sampling:* a representative sample of the population should be selected to complete the questionnaire. This sample should provide unbiased estimates of the characteristics of the chosen population.

- *Inference:* statistical inference allows the generalization of sample results to estimate the parameters of the population within calculable margin of errors.
- *Measurement:* how the questions are asked and the format of the questionnaires would elicit the experts to provide valid and reliable answers.
- *Analysis:* Data analysis techniques facilitate the analysis of the data and the definition of complex statistical relationships among the variables.

Surveys can be performed with different targets (Kerlinger, 1986; Malhotra and Grover, 1998). They can contribute during the early stages of the research gaining preliminary insight on a topic (exploratory research). Surveys can also help in later stages testing the adequacy of the concepts developed or constructing a theory (confirmatory research). Finally, when the aim is to understand the relevance of a certain phenomenon and its distribution on the population, surveys can also be a suitable method (descriptive research). In this research, the survey method has been used as a confirmatory research since the aim was to construct theory regarding the temporal order in which the policies should be implemented in order to achieve the highest efficiency in the application of the resilience framework for CIs.

The collection of the information can be performed using three different means: mail questionnaire, telephone interview or face-to-face interview (Malhotra and Grover, 1998). This research used mail-questionnaire to conduct the survey. Mail questionnaire is a cheap mean to conduct a survey and very easy to distribute since it is enough with just placing the URL of the survey in the cover letter. Furthermore, experts can easily access to it with just clicking on it. However, some authors (Solomon, 2001) argue that mail-questionnaire presents some pitfalls such as significantly lower response rates or low control regarding the people who can access to the questionnaire. This research has taken into account all these issues and has found a solution in order to avoid these problems by sending personalized cover letters to ask for their participation and filtering the gathered answers.

Forza (2002) defines a six step process to carry out a theory-building survey:

1. *Link to the theoretical level:* First, the scope of the research and the theoretical concepts required for the survey should be clearly defined. The unit of analysis should also be determined.
2. *Design:* constrains of the process, the needed information, the sample, the data collection method, and the measurement instruments are determined in this step.
3. *Pilot test:* before sending the questionnaire to the experts, it is important to make a pilot test to verify that the instructions and questions are understandable, the answers concur with the expected ones, and there is not data missing.
4. *Collect data for theory building:* once the pilot test provides positive results, the questionnaire is sent to experts to collect their answers.
5. *Analyze data:* the obtained data should be analyzed with proper analysis techniques to construct theory according to the information gathered from experts.
6. *Generate report:* all the obtained results as well as the most important conclusions obtained in the process should be documented in a final report.

The aim of the developed survey was to gather information to develop the implementation methodology. Taking as a basis the set of policies and sub-policies already defined in previous stages, the target was to define the temporal order in which these policies and sub-policies should be implemented to achieve the highest efficiency in their implementation.

A sample of forty-five experts from all over the world in the field of crisis management and critical infrastructure areas was selected from different sectors such as energy, transport, telecommunications, water, academics, first responders, and national civil protection. We selected a web-tool based questionnaire to perform the survey since this mean is very easy to use for the experts, very cheap, avoid loss of data, and provides the fastest way to answer to the questionnaire.

Before sending the questionnaire to experts, a pilot study was conducted. Once the questionnaire draft was done, we sent it to four experts in the field of crisis management and survey method to provide feedback about the clarity, completeness, and appropriateness of the survey introduction, instructions, and questions. As a result of the pilot study, changes were made to the language used in the instructions and to the formulation of some questions. The questionnaire was composed of two main parts: In the first part, for each resilience policy the experts were asked to define the temporal order in which the sub-policies should be implemented in order to achieve the highest efficiency in the implementation of the policy. In the second part, the experts were asked to determine the temporal order in which the resilience policies should be implemented in order to achieve the highest efficiency in the implementation of the resilience framework (see Appendix D).

After improving the questionnaire, the data collection step was carried out. A cover letter explaining the aim of the research, the general instructions of the survey and providing the link to access to the questionnaire was sent to the experts. They had two weeks to answer to the questionnaire.

In total twenty-five experts took part in the survey. Table 3.4 resumes the country and the sector of each expert that took part in the process. Although we tried to involve more practitioners in the survey, their engagement level was low and therefore, only seven practitioners from transport, energy, water and telecommunications fields took part.

Once all the answers were gathered, the data was analyzed and the results were obtained (see Appendix D). The implementation methodology was defined based on the obtained information from experts. The developed implementation methodology will be further explained in chapter four.

Table 3.4: Organizations of experts that took part in the Survey.

Organization	Country	Sector
Norwegian University of Science and Technology	Norway	Academic
University of Agder / Centre of Integrated Emergency Management	Norway	Academic
Universita Campus Bio-Medico	Italy	Academic
University of Utrecht	Netherlands	Academic
University of Linköping	Sweden	Academic
University of California, Berkeley	USA	Academic
Delft University of Technology	Netherlands	Academic
University of Canterbury	New Zealand	Academic
Queensland University of Technology	Australia	Academic
Massey University / University of New Zealand	New Zealand	Academic
ATAC Spa	Italy	Transport
Mobility and Logistics Cluster	Spain	Transport
REE (Spanish Energy Distribution Company)	Spain	Energy
Spanish Nuclear Energy Company	Spain	Energy
Argonne National Laboratory	USA	Energy
Sydney Water	Australia	Water
BigPond	Australia	Telecommunications & Media
SGSP Main School of Fire Service (2 experts)	Poland	First Responders
Public Emergency Health Organization	Spain	First Responders
Emergency Response and Meteorology of the Basque Country	Spain	First Responders
SAFETEC	Norway	First Responders
ANCI Umbria	Italy	Safety Consultancy
FOI	Sweden	Safety Consultancy
Risk Strategies Research and Consulting	New Zealand	Safety Consultancy

3.5 Validation of the Resilience Framework for CIs

Once the framework was developed its validation was carried out. The aim of the validation process was to confirm that the framework achieved the purpose for which it was developed. The aim of the framework was to help crisis managers to improve the resilience level of CIs bearing in mind internal and external stakeholders. In order to assert that the framework reach this objective, the following three characteristics of the framework were checked: completeness, usefulness, and relevancy.

In order to carry out the validation process, the case study was chosen as a research method. Evidence and examples about the defined resilience policies and sub-policies were obtained in order to verify the following three statements: the framework is complete, the policies and sub-policies are relevant to improve the resilience level, and the framework provides value to CIs and external stakeholders to improve resilience level of the entire system.

3.5.1 Case Study

Taking into account that crisis management and, in particular, resilience building process is primarily an applied discipline, empirical research is needed to add more relevance to the proposed framework (McLachlin, 1997). The case study method was chosen for this task. The case study is defined as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, when the boundaries between phenomenon and context are not clearly evident, and in which multiple sources of evidence are used" (Yin, 1984, p. 23). This research method is considered a robust method particularly when a holistic, in-depth investigation is required (Zainal, 2007). Although case study has mostly been used in the exploratory phase to develop research ideas and questions, it is also very suitable to theory testing or refinement (Voss et al., 2002; Meredith, 1998). Case study also helps in raising more confidence in the framework and supporting previous results (Yin, 2009).

Yin (1989) emphasizes that this method is suitable when the researchers are willing to answer how and why questions, they have no control over the

behavioral events and is based on contemporary events. In our case, all these conditions were satisfied. Our aim was to get information and examples from the CIs about how resilience policies and sub-policies were applied in the CI, and what systems and measures were already applied in the CIs to improve their resilience level. The researcher only had observer's role and he could not modify or control any aspect of the CIs. Finally, the studies were mainly based on the current situation of the CIs because the obtained data and evidences were based on current documents.

This method provides many advantages to the research:

- Examination of the data is often conducted within the situation where the activity takes place (Yin, 1984).
- Several sources of data can be gathered obtaining evidences from both quantitative and qualitative categories and ensuring the reliability of the acquired data.
- Complexities of real-life situations can be captured through detailed accounts and real-life experiences that the researcher can obtained during the stay in the real place.

However, case study has also received criticisms (Yin, 1984). Case study method is often accused of lack of rigor because the researcher can equivoque in obtaining data or even influence the direction of the findings to his interests. It is also difficult to justify the generalization of the obtained results in many cases (Tellis, 1997). Finally, case study is characterized for being too long, difficult to conduct and to process the massive amount of data obtained during the study. Regarding the generalization the aspect, Zainal (2007) proposes a way to overcome this problem by triangulating the study with other methods in order to provide more confidence to the obtained results. In our research, first we used several experts based methodologies to develop the framework and then, in order to validate the framework, we carried out two case studies, one in a nuclear plant and the other one in a water distribution company. In that way, we believe that the resilience framework for CIs could be generalized to other CI sectors.

To ensure the validity and reliability of the study Yin (1989) outlined four logical tests which help gaining more confidence in the obtained results:

- *Construct validity:* this refers that obtained data should be reliable and adequate for our research. Gathering information from multiple sources such as interviews, internal documents, and observations ensures the reliability and correctness of the data.
- *Internal validity:* this refers to the data analysis where the researcher defines some relationships and patterns and compares with the expected ones.
- *External validity:* this refers to if obtained results from the study can be generalized to other cases or not.
- *Reliability:* this refers to the reliability level of the study, that is, if the same study was conducted, following the same procedures, the same results should be obtained.

Yin (1994) defines a six step process to properly apply the case study method. First, the problems or issues that will be studied should be defined. Second, the case study design should be selected determining the number of cases that will be performed and which will be the variables that are going to be analyzed. Third, before collecting data, the case study procedure should be determined and the researcher should prepare and gain skills to perform properly. After preparation, the process to collect data starts. There are many sources from where researchers can obtain data: documentation, interviews, archival records, direct observations, participant observation and physical artifacts. All the obtained data should be analyzed in depth and finally, all the obtained results should be documented in a proper report.

The aim of these case studies was to validate the framework obtaining information about the already implemented resilience building measures, gathering some examples and evidence of resilience policies and sub-policies, and confirming the usefulness of the framework in improving resilience level of CIs. Furthermore, the gathered examples and evidence for each policy and sub-policy provided some insight about how this framework could be applied in a specific CI.

Two CIs were chosen to carry out this case study: a nuclear plant and a water distribution company. The availability and willingness of CIs to carry out this study were constrained and therefore, the choices were limited. However, we managed to carry out two different cases (the first one an extent study and the second one a more reduced study) in very different fields and with different characteristics regarding resilience aspects.

3.5.1.1 Case Study in a nuclear plant

A nuclear plant in Southern Europe was selected as the first case to carry out this research study. Due to their exposure to high risk environments, nuclear plants safety level is high and they are well prepared to face critical situations. Nuclear power sector is one of the HROs examples since it is a complex system and it operates in a context of high hazard where it is continuously facing risks and improving its resilience level.

The research was carried out on-site at the nuclear plant for six months full-time. During the first month, the aim was to become familiarized with the company, its management, the organization chart and the responsibilities of each department, and more particularly, with the organization's crisis management process and the activities carried out to improve its resilience level. Furthermore, during this first period, the departments mainly responsible to develop each policy were identified (see Table 3.5).

In order to ensure the reliability of the obtained data, the information was gathered from various information sources: interviews, internal documents, internal and external procedures, archival records, and direct observations.

Table 3.5: Responsible departments to properly carry out the resilience policies.

Resilience Policies	Responsible Departments
CI Safety Design and Construction	Nuclear Security and License
CI Maintenance	Maintenance
CI Data Acquisition and Monitoring System	Instrumentation Section within Maintenance
CI Crisis Response Equipment	Nuclear & Results
CI Organizational Procedures for Crisis Management	Nuclear & Results
CI Top Management Commitment	Internal Evaluation Service section within Quality Department
CI Crisis Manager Preparation	Training and Operational Experience
CI Operator Preparation	Training and Operational Experience
CI Crisis Response Budget	Administration and Finances
External Crisis Response Equipment	Civil Protection
First Responder Preparation	Internal Evaluation Service section within Quality
Government Preparation	Internal Evaluation Service section within Quality
Trusted Network Community	Training and Operational Experience
Crisis Regulation and Legislation	Internal Evaluation Service section within Quality
Public Crisis Response Budget	Administration and Finances
Societal Situation Awareness	Communication

First of all, we analyzed internal documents to learn how the CI performed different tasks and to gather information and evidence of the implemented measures in the CI. Then, operating and organizational procedures for emergency situation established within the CI were analyzed to get more evidence for our framework. Archival records were also obtained in order to see the evolution of some indicators during the last ten years and to get evidence about the improvement of the resilience level. Furthermore, in order to contrast the obtained data and ensure its correctness, eleven interviews were conducted with several operators and managers of different fields. Table 3.6 illustrates the responsibility and department of the interviewees classified by the resilience policy where each one contributed.

Table 3.6: Interviewed workers classified by resilience policies.

Resilience Policies	Interviewee	Department
CI Safety Design and Construction	Head of department	Nuclear Security and License
CI Maintenance	Head of department	Maintenance
CI Data Acquisition and Monitoring System	Head of section	Instrumentation Section within Maintenance
CI Crisis Response Equipment	Head of department	Nuclear & Results
CI Organizational Procedures for Crisis Management	Head of department	Nuclear & Results
CI Top Management Commitment	Members of section	Internal Evaluation Service section within Quality
CI Crisis Manager Preparation	Head of department	Training and Operational Experience
CI Operator Preparation	Head of department	Training and Operational Experience
CI Crisis Response Budget	Member of department	Administration and Finances
External Crisis Response Equipment	Head of department	Civil Protection
First Responder Preparation	Members of section	Internal Evaluation Service section within Quality
Government Preparation	Members of section	Internal Evaluation Service section within Quality
Trusted Network Community	Head of department	Training and Operational Experience
Crisis Regulation and Legislation	Members of section	Internal Evaluation Service section within Quality
Public Crisis Response Budget	Member of department	Administration and Finances
Societal Situation Awareness	Head of department	Communication

Finally, we also compared the gathered information through direct observations of physical components of the CI, operations of the workers in a normal working day, the safety culture among the workers, and commitment level of the workers towards resilience.

Once all the data and evidence were gathered, a final report was developed with all the gathered information. We gathered evidence and examples for all the resilience policies and sub-policies providing insight for the validation of the resilience framework for CIs. Chapter five explains the evidence and examples obtained for each resilience policy and sub-policy.

3.5.1.2 Case Study in a Water Distribution company

A water distribution company of a province in Southern Europe was selected as a second CI to carry out the validation process. Water is an essential resource for the society's life. Its shortage or contamination can have detrimental effects on the citizens and many CI sectors. Therefore, its safety and reliability level should be high in order to avoid disruptions or severe impacts on the society.

In this case the information was only gathered through four interviews with the general manager of the company. The company did not allow us to make a deeper study and to acquire information from other sources such as internal documents or direct observations. In each interview different aspects of the framework were analyzed. In the first one, the general functioning of the company regarding the safety and reliability aspects was analyzed. We also presented our framework in order to provide context to the interviewee about our research. In the second interview, evidence and examples about the resilience policies and sub-policies within the technical resilience level were gathered. In the third one, policies and sub-policies within the organizational resilience and economical resilience dimensions were examined. Finally, in the last interview examples about the policies and sub-policies within the external resilience level were obtained.

A final report was developed with all information and examples obtained through the interviews. Although having a limited access to the company, we were able to gather evidence for all the policies and sub-policies defined in the framework. Chapter five illustrates the obtained information for each resilience policy and sub-policy.

3.6 Conclusion

The research methodology applied in this research is composed of three main phases: conceptualization, development of the framework, and validation of the framework. Each phase has its own objectives and therefore, different methods were used to obtain results. During the development phase, most of the methods were based on gathering knowledge from experts in order to develop the framework. As most of the crisis management knowledge resides in the mind of experts, several methods were applied to extract this knowledge and develop the framework. Although some few experts were the same in some steps, most of them were different in each step. Therefore, knowledge for the development of the framework was gathered from a wide variety of experts.

Once the framework was built, the aim was to validate the framework and confirm its suitability for helping CIs to improve their resilience level. Case study was chosen as a research method to perform this validation. The aim was to confirm that the framework is complete, it is useful for improving the CIs resilience level, and it provides relevant policies and sub-policies. In order to do that, evidence and examples for each resilience policy and sub-policy were gathered and information about already implemented resilience building measures were obtained. Two case studies, one in a nuclear plant and another one in a water distribution company, were performed.

4 Resilience Framework for Critical Infrastructures

This section presents the resilience framework for CIs developed within this research. The aim of this framework is to help crisis managers to improve the resilience level of CIs.

The resilience framework for CIs is composed of two resilience types: internal resilience and external resilience. Within each resilience type, several resilience dimensions have been identified. In order to improve these resilience dimensions, a set of resilience policies and sub-policies have been defined. These policies and sub-policies have been described holistically and closely related to general management of CIs in order to facilitate their implementation in practice.

Furthermore, the influence of each resilience policy on the three resilience lifecycle stages has been defined. This study shows that internal policies are the most important ones when preventing a crisis occurrence, while during the absorption and recovery stages, internal and external policies influence bouncing back to the normal stage. Finally, the implementation methodology of the resilience framework has been defined in order to efficiently implement it.

4.1 Introduction

The aim of this research is to provide a framework to improve the resilience level of CIs. This framework is composed of three main parts: a list of resilience policies and sub-policies that need to be implemented in a CI in order to improve its resilience level, an influence table where the influence of each resilience policy on the three resilience lifecycle stages (prevention, absorption, and recovery) is assessed, and finally, an implementation methodology where the temporal order in which the resilience policies and sub-policies should be implemented in practice is determined. This chapter explains in detail the Resilience Framework for CIs.

4.2 Resilience types and dimensions

This research focuses on major industrial accidents. We define major industrial accidents as crises that start in a CI due to a disruption in a system or an element and can spread through the network of CIs rapidly affecting the society. In these cases, there are some focal assets where the triggering event occurs: a ship, a nuclear plant, a grid power plant, the chemical industry, etc. Additionally, as crises may become serious and affect a large number of people, external entities such as government or first responders need to cooperate with the damaged industry or even lead the crisis resolution in the most appropriate way.

We accept that the resilience level of the focal CI where the triggering event occurs could be different to the resilience level of the rest of external entities. Therefore, we divide the resilience level of the overall system (including the CI and involved external stakeholders) into two different resilience types: internal resilience, which refers to the resilience level of the owner of the focal element/CI, and external resilience, which corresponds to the resilience level of the rest of involved agents (the government, first responders, and society).

Moreover, as it has already been explained in chapter two, literature identifies four dimensions within the overall resilience level (Bruneau et al.,

2003; Multidisciplinary Center for Earthquake Engineering Research (MCEER), 2008; Zobel, 2010; Gibson and Tarrant, 2010): technical resilience, organizational resilience, economic resilience and social resilience. Thus, based on this classification, we identified some dimensions within each type of resilience. We divided internal resilience into three dimensions: technical resilience, organizational resilience and economic resilience. External resilience, on the other hand, has been broken down into four dimensions: technical resilience, organizational resilience, economic resilience, and social resilience (see Table 4.1).

Table 4.1: Resilience types and dimensions in case of major industrial accidents.

Internal Resilience	External Resilience
Technical Resilience	Technical Resilience
Organizational Resilience	Organizational Resilience
Economic Resilience	Economic Resilience
	Social Resilience

4.3 Resilience policies and sub-policies

Once the resilience types and dimensions were identified based on the literature, we started developing our resilience framework. First of all, we gathered information from the SEMPOC project's documentary reports. During the workshops, experts were asked to determine the policies that help power companies to increase their resilience level. Hernantes et al. (2012a) resumes the resilience policies obtained by the experts classified by sectors and resilience dimensions (see Table A.1 in Appendix A). Afterwards, multiple past major industrial accidents were studied to extract more policies that assist on enhancing the resilience level of CIs. In addition to this, studying accidents from other sectors allowed expanding the applicability of this framework to

other sectors. Labaka et al. (2013) explains the obtained evidences through this multiple case study method and the identified resilience policies during this process.

Furthermore, to better define the resilience policies and to determine and limit the scope of each resilience policy, several sub-policies were identified within some resilience policies. This set of resilience policies and sub-policies constitute the second version of the resilience framework (see Table A.2 in Appendix B).

Once a more complete list of resilience policies and sub-policies was obtained, the aim was to extent and to improve the framework through the Delphi method. From the Delphi process the complete list of resilience policies and sub-policies was obtained. Within the Delphi method there were mainly two main objectives: (1) complete the initial list of policies and sub-policies and improve their description, and (2) evaluate the influence of each resilience policy on the three resilience lifecycle stages.

The aim of the first questionnaire of the Delphi process was to complete the list of resilience policies and sub-policies of the resilience framework and improve their descriptions. In order to do that, experts were asked to evaluate the completeness and clarity level of the policy definition and its appropriateness to the corresponding resilience dimension. Furthermore, they were also asked to evaluate the completeness and clarity level of the sub-policy description and its appropriateness to the corresponding resilience policy. Finally, we encouraged them to propose new resilience policies and sub-policies to complete our resilience framework. Comments obtained from the experts are explained in detailed in Appendix C. Following, the final version of the resilience framework is explained.

4.3.1 Resilience policies within the Internal Resilience

Table 4.2 summarizes the complete list of resilience policies and sub-policies within the internal resilience. Below, the detailed description of the policies and sub-policies is provided.

Table 4.2: Resilience policies and sub-policies within the internal resilience.

Resilience Types	Resilience Dimensions	Resilience Policies	Resilience Sub-policies
INTERNAL RESILIENCE	Technical Resilience	CI Safety Design and Construction	(Required and Voluntary) Safety systems
			Redundancy
			Simplicity and loose coupling
			(External and Internal) Audits
		CI Maintenance	Preventive maintenance
			Corrective maintenance
		CI Data Acquisition and Monitoring System	Data acquisition equipment
			Information monitoring equipment
		CI Crisis Response Equipment	
	Organizational Resilience	CI Organizational Procedures for Crisis Management	Coordination procedures with external stakeholders
			Crisis management procedures
			Incidents management and evaluation
		CI Top Management Commitment	Top Manager commitment and situation awareness
			Activities to promote resilience based culture
		CI Crisis Manager Preparation	Crisis Manager training
			Crisis manager situation awareness and commitment
		CI Operator Preparation	Operator training
			Operator situation awareness and commitment
	Economic Resilience	CI Crisis Response Budget	

As it has already been explained, within the internal resilience, three resilience dimensions were defined: technical, organization, and economic. In order to improve the technical resilience, four policies were identified. Within

organizational resilience another four were defined and finally only one policy was identified to enhance the economic resilience.

4.3.1.1 Technical Resilience

4.3.1.1.1 CI Safety Design and Construction

The infrastructure of the CI should have high safety level to avoid a crisis occurrence and absorb the magnitude of the impact efficiently. Having redundant systems increases the resilience level of the CI since redundancy assists in maintaining the functioning of the infrastructure in case of a failure in a component or in a system.

The infrastructure should also be robust to resist threats (Bruneau et al., 2003) as well as flexible to be able to adapt to extreme situations when the occasion demands (Kahan et al., 2009; Johnsen, 2010). However, having a complex infrastructure with many additional redundant and safety systems makes it difficult to manage the CI and to control its functioning (Perrow, 1984; Sagan, 2004; Leveson et al., 2009). Therefore, the design of the CI should have a proper level of complexity, depending on the requirements, to guarantee a high resilience level of the system.

In turn, the design should meet the existing normative specifications and requirements. Risk-based analysis can help to identify the most critical elements or systems and important threats in order to strengthen the CI's safety. Furthermore, the CI should be built based on the design in order to fulfill all the established requirements. The inclusion of new updates and enhancements should pay attention to not introducing new vulnerabilities into the system.

Within this policy four sub-policies have been identified to better define its scope: (voluntary and required) safety systems, redundancy, simplicity and loose coupling, and (external and internal) audits.

a) (Voluntary and Required) Safety systems

The CI should establish safety systems to prevent the escalation of an incident into a crisis and, when the crisis occurs, to diminish the impact (Kahan et al., 2009). Within the CI different kinds of safety systems with different aims should be implemented. Some of them would be designed to prevent a crisis occurrence whereas others would help to absorb the impact when the crisis occurs. Some of them would be placed to prevent damaging the critical part of the infrastructure whereas others can mitigate other types of events such as fires or floods. Furthermore, it is also essential to establish safety elements within the systems to ensure their proper functioning.

These systems should be reliable and should be always available to respond in the most efficient way. Furthermore, safety systems should be adapted and updated according to the CI's requirements.

b) Redundancy

Having redundant components and systems within the infrastructure ensures the continuity of the processes and activities within the CI in light of an incident in a component or a system (Bruneau et al., 2003; Johnsen, 2010). However, having more components and systems also increases the complexity of the CIs and therefore, new vulnerabilities may appear (Perrow, 1984; Sagan, 2004; Leveson et al., 2009; Johnsen, 2010). Thus, the implementation of redundant components and systems should be assessed evaluating the improvement in safety against the unwanted side effects such as an increase in complexity and risk of failures (Johnsen, 2010). Besides, redundancy would only be effective if the systems are independent (Leveson et al., 2009).

c) Simplicity and loose coupling

CIs are usually complex systems with tight relationships among their components that facilitate the propagation of an error rapidly to the whole CI (Perrow, 1984). Therefore, having tight relationships makes it difficult to stop an initial incident. In light of this situation, infrastructures should be designed to be as simple as possible and there should be loose relationships among different systems within the infrastructure (Johnsen, 2010). This would ease

the detection of incidents and interrupt their propagation. Furthermore, having independent systems and loose relationships facilitates the adaptation of the CI to new situations.

d) (External and Internal) Audits

Periodically, a deep analysis of the proper state of the systems needs to be carried out in order to ensure the proper functioning of the CI. External audits increase the organization's awareness of the importance of reliability in reducing the likelihood of a crisis and assuring the proper performance of the organization. On the other hand, internal audits help the organization to make safety improvements within the CI with the purpose of enhancing its level of resilience. Audits contribute to ensuring the proper state of CIs not only technically but also in the management aspects.

4.3.1.1.2 CI Maintenance

Not only should the CI be well designed and built but high quality maintenance activities also need to be performed periodically in order to guarantee a high reliability level of the infrastructure. Having a good level of maintenance helps to withstand incidents and also reduces the magnitude of the impact and the time to recover. In performing these activities, we make sure that the system's physical components are in an adequate and reliable state for their proper functioning.

This policy has been disaggregated into two sub-policies: preventive maintenance and corrective maintenance.

a) Preventive maintenance

Preventive maintenance activities are carried out prior to an incident to build reliable CIs and prevent failures. Furthermore, they assist on identifying early warning signals and dealing with them before their unfolding. The components of the infrastructures need a periodical revision in order to verify their proper state, renew the old parts and update the technical features to comply with new regulations. Having well maintained components and systems increases the prevention capacity of the CI as well as the absorption

capacity to withstand any major threat. Regular adjustments that prevent failures should be carried out as highlighted by the sensitivity to operations principle of HROs defined by Weick and Sutcliffe (2007). The CI must always ensure correct performance of the infrastructure in order to be able to prevent a crisis occurrence or reduce its magnitude.

b) Corrective maintenance

Corrective maintenance, on the other hand, refers to maintenance activities carried out after an incident in order to repair damages or strengthen the infrastructure. These activities help to detect early warning signals and to act upon them. The accumulation of little incidents could lead to a crisis occurrence; therefore, it is important to manage them as soon as possible (Turner, 1976). Once the failure has occurred it is important to analyze its causes and identify corrective actions so as not to happen again. The preoccupation with failure principle, described by Weick and Sutcliffe (2007), makes the companies aware that every little failure should be analyzed in depth in order to avoid an accumulation of failures that might lead to a major crisis.

4.3.1.1.3 CI Data Acquisition and Monitoring System

Having systems to monitor the state of the CI helps to ensure the proper state of the CI. Setting up the required sensors to gather information from the CI and installing adequate software and interfaces within the control panel to monitor the CI performance are some of the main activities that should be carried out in order to achieve a high implementation level of this policy. To ensure the proper functioning of these systems, it is important to have reliable components and systems to gather and monitor the required data properly. Furthermore, having redundant data acquisition and monitoring systems would ensure the availability of the data to verify the proper state of the system. Two sub-policies have been defined within this policy: data acquisition equipment and information monitoring equipment.

a) Data acquisition equipment

In order to control the proper functioning of the CI it is essential to use data acquisition equipment, such as sensors to collect critical data. The most critical components or subsystems within the infrastructure and the kind of data needed should be determined in order to be able to detect early warning signals and respond to them as soon as possible. Having redundant sensors would ensure the availability of the data continuously.

b) Information monitoring equipment

Data should be transmitted and monitored so that the workers can interpret the information and be able to detect early warning signals or even anticipate a crisis. This information should be monitored in control panels in addition to being saved continuously. Workers[2] often dispose a significant quantity of information monitored in the control panels. Thus, establishing suitable interfaces to display the data is important to facilitate the interpretation of this information. Warning lights and alarms, alerting workers of possible problems, should be installed in the monitoring and control panels since they help to detect problems quickly when something anomalous is taking place. Moreover, when a crisis occurs, having information systems that save data is important since this data would allow analyzing the problem and learning for the future once the crisis has finished.

4.3.1.1.4 CI Crisis Response Equipment

CI Crisis Response Equipment refers to the emergency equipment that the CI should have when a crisis occurs to absorb the impact and ensure the safety of the workers at the CI. Emergency equipment should be reliable to ensure its

[2] This research defines workers as all the people who are working at the CI. Within workers two types can be defined: managers and operators. Managers are the ones who are in charge of a group and they have certain responsibility within the CI. Operators, on the other hand, are defined as the staff who are working on-site in direct contact with the infrastructure (workers = managers+operators).

proper functioning when it is required. Furthermore, the CI should make sure that this equipment is always available to be able to use it when a crisis occurs. This emergency equipment may be vital in some cases to diminish the impact and ensure the safety of the workers in times of crises. This equipment should be properly maintained and updated, taking into account the specifications and requirements of manufacturers.

4.3.1.2 Organizational Resilience

4.3.1.2.1 CI Organizational Procedures for Crisis Management

CI Organizational Procedures for Crisis Management correspond to the preparation and the capacity of the organization to deal with crises and incidents. This policy includes the proper management of incidents and crisis situations as well as the ability to coordinate with external stakeholders such as government and first responders. Therefore, it is important to develop crisis management procedures in order to have the response actions and the responsibilities of each worker well defined before a crisis occurs. This would lead to absorption and recovery in a more coordinated and efficient way. Furthermore, incidents should be properly managed in order to avoid their escalation into a crisis.

Within this policy three sub-policies have been defined: coordination procedures with external stakeholders, crisis management procedures, and incidents management and evaluation.

a) <u>Coordination procedures with external stakeholders</u>

During the resolution of a crisis, CIs need help from the government and first responders. Therefore, prior to the incident, it is important to establish coordination procedures with external stakeholders in order to identify the responsibilities of each entity during the resolution period (Parsons, 2007). These procedures should be available and known by all the stakeholders involved in the crisis management process. In addition, it is important to

continuously update the procedures based on the lessons learned from previous crises and incidents.

b) Crisis management procedures

It is important to have crisis management procedures established before a crisis occurrence in order to define the activities for which each worker at the CI is responsible. Within crisis management procedures there are basically two types of procedures: operating procedures, which refer to how the infrastructure should be operated in a crisis situation, and organizational procedures, which describe specific guidelines within the emergency planning. Furthermore, within the organizational procedures two different plans are often defined: internal emergency plan and external emergency plan. These procedures provide detailed guidelines about the actions and responsibilities of each worker in light of a crisis. Furthermore, these procedures assist in establishing common mental models and priorities within all the workers at the CI in order for them to cooperate efficiently (Resilient Organisations, 2012; Parsons, 2007). Crisis management procedures should be known and available to all the workers for the moment when a crisis occurs. Moreover, they should be updated continuously in order to be useful and efficient when an incident or a crisis occurs.

c) Incidents management and evaluation

CIs should have an incident reporting system to track all the failures and incidents that occur and ensure their proper management. When an incident occurs, it should be prioritized depending on the level of risk, addressed efficiently, and analyzed to find out the causes of the incident. Responsibility and a deadline should be established for its management and resolution. As Weick and Sutcliffe (2007) state, organizations should be constantly preoccupied with failure and all incidents should be properly handled to avoid the occurrence of a severe crisis.

Furthermore, once the incident has been managed it is important to document it and evaluate the actions taken in order to identify best practices for future incidents (Stephenson, 2010). This process will ensure that the

underlying as well as immediate causes of incidents are completely understood, taking into account also human and organizational factors (Crichton et al., 2009). In the same vein, the analysis process also helps in identifying those activities that did not provide satisfactory results. Finally, an incident learning system should be developed in order to document the lessons gathered from incidents and to be available and easily visible for all the workers at the CI (Resilient Organisations, 2012).

4.3.1.2.2 CI Top Management Commitment

Top managers should be committed to the resilience building process and they have to promote a resilience based culture, attitudes and values within the CI. They are responsible for deploying resources to promote the workers' commitment and training. In addition to this, top managers' agreement is necessary to establish the required technical measures to prevent a crisis occurrence and absorb the impact. Having an adequate level of leadership capacity is also important to provide more confidence to workers and good management during times of crisis (Resilient Organisations, 2012; Parsons, 2007).

Two sub-policies have been defined within this policy: top manager commitment and situation awareness and activities to promote resilience based culture.

a) Top manager commitment and situation awareness

It is vital that top managers are aware of the importance of having a high resilience level and are committed to the resilience building process (Shaw et al., 2009; Resilient Organisations, 2012; Parsons, 2007). Furthermore, top managers should develop their leadership skills (Resilient Organisations, 2012; Parsons, 2007); their actions, decisions, and behavior regarding the safety of the CIs have a strong influence on the commitment level of the workers to improve the safety of the CIs (Boin et al., 2005). In this context it would be also easier for the top managers to transmit situation awareness down to the workers of the CI to ensure they are also aware of possible crises. Having committed top

management helps to create a resilience based-culture within the organization and in turn, improves the resilience level of the company. Additionally, top managers should promote cooperation agreements with other CIs and external agents to help each other when a crisis occurs (Resilient Organisations, 2012; Parsons, 2007).

b) Activities to promote resilience based culture

Top managers should establish different measures to promote a resilience based culture in the CI (Weick and Sutcliffe, 2007). When a worker makes a mistake or for example breaks a component, he might hide it due to fear of being blamed. However, this behavior does not promote resilience. Top managers have to encourage people to report incidents in order to respond immediately and avoid further damage (Parsons, 2007). Another way of promoting resilience could be by establishing an incentive program that encourages workers at the CI to propose new ideas to improve the resilience level of CIs.

4.3.1.2.3 CI Crisis Manager Preparation

CI Crisis Manager Preparation corresponds to the capacity of crisis managers to detect early warning signals, communicate to the stakeholders, and analyze triggering events to propose new preventive measures for the future. In addition to this, they also have to develop their sensemaking[3] capacity (Gilpin and Murphy, 2008) in order to be able to understand an unexpected event, adapt to it, and make the correct decisions in a stressful situation and without complete information. Moreover, crisis managers need to develop their mindfulness capacity (Weick and Sutcliffe, 2007) to continuously be aware of incidents or crises that can occur not only on their CI but also in other CIs. Thus, not only would the managers learn from crises that occur within their

[3] Sensemaking refers to the process of giving meaning to the occurred experiences. This process involves first noticing unexpected events, then, interpreting these events, and finally, constructing common meanings and goals to face the situation.

own boundaries, but also they could improve their resilience level by adopting lessons learned and establishing measures gathered from other CIs' incidents and crises (Crichton et al., 2009).

Within this policy two sub-policies have been defined to better define the scope of this policy: crisis manager training and crisis manager situation awareness and commitment.

a) Crisis Manager training

Crisis managers have the main responsibility for establishing the required mechanisms and procedures to detect an incident, for communicating to the corresponding person or entity and for responding, in order to avoid its escalation (Resilient Organisations, 2012). Thus, training courses such as table-top exercises or emergency drills to improve crisis management skills create well prepared managers (Stephenson, 2010; Weick and Sutcliffe, 2007; Resilient Organisations, 2012). Furthermore, as crises are usually unexpected and unpredictable and they evolve in an unknown way, managers must develop their sensemaking capacity (Gilpin and Murphy, 2008) and use their knowledge in novel ways to solve new problems (Resilient Organisations, 2012; Parsons, 2007). Finally, crisis managers must be highly skilled, such as able to discriminate between useful and useless data, in order to make appropriate decisions (Resilient Organisations, 2012).

b) Crisis manager situation awareness and commitment

Failures can occur at any time and in any way and they can go unnoticed. Therefore, crisis managers need to be aware to detect any failure and act as soon as possible (Resilient Organisations, 2012; Parsons, 2007). As Weick and Sutcliffe (2007) state, HROs need to be preoccupied with failure because any lapse could have severe consequences. As Shaw el al. (2009) state, it is also essential to be able to understand the implications of these warning signals to respond in the most efficient way. Furthermore, it is important also to develop the capacity to anticipate what could happen in order to take measures beforehand (Resilient Organisations, 2012; Parsons, 2007). Besides, having committed and engaged crisis managers to improve the resilience level assures

that they would perform their work properly (Weick and Sutcliffe, 2007; Resilient Organisations, 2012). They understand that through this work the CIs' long term success will be achieved (Stephenson, 2010).

4.3.1.2.4 CI Operator Preparation

Operators at the CI must be adequately trained prior to the occurrence of a crisis so they know how to respond when a crisis does occur. Operators should take training courses to know the procedures and protocols that should be followed when an incident or a crisis occurs and develop their response and coordination abilities (Resilient Organisations, 2012). Operators should also be committed with the safety of the company since they can help detecting early warning signals and avoiding a crisis occurrence (Resilient Organisations, 2012; Parsons, 2007). They should be constantly aware about the CI's performance and potential problems in order to ensure a high resilience level (Resilient Organisations, 2012).

This policy has been disaggregated into two sub-policies: operator training and operator situation awareness and commitment.

a) Operator training

Operators at the CI are often the ones who detect a failure and need to respond to it. Having well trained operators through table-top exercises, seminars or emergency drills helps them to rapidly find a problem and know how they should act in order to respond in the most efficient and rapid way (Resilient Organisations, 2012). However, the solution is not always known and in those cases it is important that operators are flexible and able to improvise and adapt to new situations to better address the incident or the crisis (Kahan et al., 2009; Resilient Organisations, 2012; Parsons, 2007). Occasionally, when a crisis occurs the decision making capabilities might be pushed down to those operators with more expertise in the field (Weick and Sutcliffe, 2007; Stephenson, 2010; Parsons, 2007). However, Leveson (2009) points out that decentralized decisions should be made from a system-level perspective in order to be effective in reducing crises and avoid side-effects.

b) Operator situation awareness and commitment

Operators must be committed to the resilience in order to help to improve crisis management (Resilient Organisations, 2012; Parsons, 2007). In addition to this, operators need to be constantly aware of possible incidents (Resilient Organisations, 2012; Parsons, 2007). The preoccupation with failure principle defined by Weick and Sutcliffe (2007) emphasizes the importance of constantly remaining alert to possible incidents that can accumulate to cause a triggering event. As Shaw et al. (2009) state, awareness should not only cover the capacity to detect early warning signals but also, from a more proactive posture, the capacity to understand them and, at a higher level, to be able to predict or anticipate any possible incident before it happens (Resilient Organisations, 2012; Parsons, 2007). Therefore, awareness of the operators to communicate any incident must be high.

4.3.1.3 Economic Resilience

4.3.1.3.1 CI Crisis Response Budget

When a triggering event occurs, resources are needed to absorb the impact and recover to the initial state as soon as possible. CIs should have monetary resources set aside in order to cover repairs and replacements just after the triggering event happens and until an acceptable level of performance that guarantees society's welfare is achieved (Resilient Organisations, 2012). Having this budget allows CIs to buy new components, repair damage sooner, and temporarily hire workers and equipment, thereby reducing the response and recovery times. CIs usually contract for insurance which will be responsible for replacing part of the economic resources needed to repair damages and buy new components.

4.3.2 Resilience policies within the External Resilience

Table 4.3 classifies the complete list of resilience policies and sub-policies within the external resilience. Below, we provide the detailed definition and description of each resilience policy and sub-policy.

Table 4.3: Resilience policies and sub-policies within the external resilience.

Resilience Types	Resilience Dimensions	Resilience Policies	Resilience Sub-policies
EXTERNAL RESILIENCE	Technical Resilience	External Crisis Response Equipment	
	Organizational Resilience	First Responder Preparation	First responder training
			First responder situation awareness and commitment
		Government Preparation	Government situation awareness and commitment
			Government training
			Government communication capacity
			Government leadership capacity
			Coordination of the response agents
		Trusted Network Community	Shared information systems and databases
			Trust and engagement of the participants
		Crisis Regulation and Legislation	Regulations and laws revision and update
			Compliance level of regulations and laws
	Economic Resilience	Public Crisis Response Budget	
	Social Resilience	Societal Situation Awareness	Societal situation awareness and commitment
			Societal training

In the case of the external resilience, four resilience dimensions have been determined: technical, organizational, economic, and social. Within the technical resilience only one policy has been defined. Four policies have been identified in order to improve the organizational resilience. Finally, only one policy has been determined within economic resilience and social resilience.

4.3.2.1 Technical Resilience

4.3.2.1.1 External Crisis Response Equipment

External stakeholders such as first responders, government and society also have an important role during crisis resolution in providing crisis response equipment. This equipment should be reliable to ensure its proper functioning and it should be always available. Furthermore, having redundant equipment would ensure the availability of this equipment when a component or a sub-system gets damaged. CIs should advise external stakeholders about the required equipment, especially in the case when specific equipment is needed. In case of a severe crisis, equipment could also be gathered from foreign countries when extra equipment is needed.

4.3.2.2 Organizational Resilience

4.3.2.2.1 First Responder Preparation

First Responder Preparation corresponds to how first responders (fire fighters, emergency units, policemen, military, etc.) are prepared to face a crisis. Prior to the occurrence of a crisis, they should be trained to know how to absorb and bounce back from a crisis and about the procedures and protocols they must follow in each particular case. Actions such as how to act in dangerous environments and how to organize themselves and coordinate with each other need to be defined before a critical event takes place. Prior to the crisis occurrence they need to learn about the special characteristics of their closest CIs in order to be able to properly respond when a crisis occurs. This specific training should be provided by CIs. After a crisis, everything that went wrong

must be identified, and measures should be enacted so failures do not occur again. First responders should also be committed with the resilience building process of the CI and they should be aware about possible incidents that could lead to crisis.

Two sub-policies have been defined within this policy: first responder training and first responder situation awareness and commitment.

a) First responder training

When a crisis occurs first responders play an important role in responding to the emergency situation and ensuring the safety of the society. Therefore, they have to train and be prepared prior to the crisis in order to be able to respond in the most efficient way (Resilient Organisations, 2012). First responders should have access to the internal and external emergency plans to know how they should perform in case a crisis occurs. Those procedures should be properly defined, distributed to first responders, and understood by all of them. Furthermore, as lessons from previous crises are gathered, these procedures should be updated and tailored to them. Special characteristics of the closest CIs should also be analyzed in order to know how to respond in each case. CIs should also take part defining these procedures and providing the required information concerning special features of CIs.

First responders should also be flexible enough to adapt to a new situation and be able to provide an appropriate response. Not only must they rehearse established response procedures but also it is important to develop their sensemaking and adaptive capacity to be able to perform properly in unknown situations (Weick and Sutcliffe, 2007). Moreover, to promote relationships and coordination among different first responders, they should develop table-top exercises involving all the first responders (Resilient Organisations, 2012; Parsons, 2007). CIs can encourage developing these training exercises in order to improve the training of first responders.

b) First responder situation awareness and commitment

First responders must be constantly aware of possible incidents that could occur (Shaw et al., 2009; Resilient Organisations, 2012; Parsons, 2007).

Furthermore they must be committed to the resilience building process of the CI in order to help to improve crisis management (Resilient Organisations, 2012; Parsons, 2007). First responders are essential in crisis management since they are always part of the response and provide emergency assistance to the workers and society. CIs can influence significantly in the improvement of the first responder situation awareness and commitment level through performing training activities and alerting them of possible crises.

4.3.2.2.2 Government Preparation

The government should be well prepared for crisis management. Prior to a crisis, the government should prepare to detect early warning signals and in order to do that it is important to be aware of the possible incidents that may trigger a crisis (Carrel, 2000; Boin, 2009; Resilient Organisations, 2012; Parsons, 2007). Response procedures should be defined prior to the occurrence in order to know how they should act when a crisis occurs. Furthermore, members of the government need to increase their sensemaking capacity because crises may be uncertain and complex and they have to know how to rapidly interpret the situation and adapt to it (Weick and Sutcliffe, 2007; Boin et al., 2005). Proper communication among the government, the media and the public, providing real information, is essential to avoid misunderstandings and rumors that could increase society's anxiety (Carrel, 2000; Boin, 2009; Parsons, 2007). Furthermore, members of the government are also responsible for coordinating efficiently the network of stakeholders involved in the absorption and recovery activities (Carrel, 2000; Boin, 2009).

Within this policy five sub-policies have been defined: government situation awareness and commitment, government training, government communication capacity, government leadership capacity, and coordination of the response agents.

a) Government situation awareness and commitment

The government should be aware of possible incidents that could lead to a crisis and should be committed to the crisis management process, deploying

resources and showing society the need to be aware of crises (Resilient Organisations, 2012; Carrel, 2000; Parsons, 2007). CIs should play an important role in enhancing the awareness and commitment level of the government by alerting them of the importance of the CIs proper functioning for the welfare of society. Members of the government need to develop their capacity to detect early warning signals, understand them, and also be able to anticipate that an incident may occur in order to take measures before it happens (Shaw et al., 2009; Resilient Organisations, 2012; Parsons, 2007). Furthermore, it is important they allocate resources for improving crisis management skills. Crisis management should be integrated into the mindset of government members in order to detect, respond, and manage crises properly (Carrel, 2000).

b) Government training

It is important that the government is well trained prior to a crisis in order to handle it efficiently. Before a crisis occurrence, crisis management procedures need to be defined (Carrel, 2000; Boin, 2009). The steps that must be followed should be defined before the crisis occurrence to efficiently respond when a triggering event occurs. Who should take part in the crisis cabinet, how the responsibilities should be distributed and the actions that must be developed should be well documented to efficiently respond. CIs should also take part in the development of these procedures since they have more knowledge about the risks and efficient response activities. Furthermore, the members of the government should develop their sensemaking capacity to be able to cope with unplanned situations, without much information and under high pressure (Boin et al., 2005; Boin, 2009; Weick and Sutcliffe, 2007).

c) Government communication capacity

In times of crises, the government is primarily responsible for centralizing all the information gathered from stakeholders and communicating appropriately to all the involved agents. Communication is, therefore, a very important aspect in order to efficiently respond to a crisis and reduce public anxiety (Parsons, 2007). Furthermore, the government should provide real and proper information to the media about the state of the crisis. Society places its

trust in the proper performance of the government in responding to a crisis. Therefore, the government should communicate the state of the situation constantly and with real data in order to gain the confidence of the society (Boin et al., 2005; Carrel, 2000). During the pre-crisis state, the government should develop the capacity to communicate with the media determining the contents that should be communicated, the expressions that should be used and how often the government should provide information about the situation. In this case, CIs can hardly help the government in improving its communication skills.

d) Government leadership capacity

During the crisis, government should be the leader of the society. It has to provide credibility to its words and actions in order that people trust in it (Boin, 2009). When a crisis occurs, the leaders should be able to understand and interpret what is occurring and find a solution without much information and in a stressful situation (Parsons, 2007). Moreover, all the actions carried out should be well-justified and they should lead to an efficient recovery in order to reduce public anxiety. Finally, leaders should take advantage of a crisis occurrence, acquiring and internalizing the lessons learned for future crises and promoting new regulations and laws if they are necessary (Boin et al., 2005). Similarly to government communication capacity sub-policy, CIs can barely influence in the development of this policy.

e) Coordination of the response agents

When a crisis occurs the crisis managers within the government are the main agents responsible for coordinating all the external agents that take part in the absorption and recovery tasks (Boin, 2009). They have to determine the amount of resources that are needed to face the critical situation and according to these needs, first responders and volunteers should be assigned to the corresponding tasks. If the crisis turns out to be very severe, foreign or other external assistance will be required. In this case, crisis managers within the government will be responsible to arrange it and CIs can provide some help (Resilient Organisations, 2012).

4.3.2.2.3 Trusted Network Community

Creating a network of stakeholders (CI owners, regulators, government, etc.) in which agents involved in a crisis can trust each other to share different experiences and lessons learned may improve their crisis management knowledge and the number of collaboration agreements to help in crisis prevention and resolution (Resilient Organisations, 2012; Parsons, 2007). Literature defines Communities of Practice as networks where practitioners involved share common interests and problems, and expand their knowledge and expertise in an area by building tools and interacting with other members (Ruffner et al., 2010; Snyder and de Souza Briggs, 2003). The community should promote research in the field of CI protection and safety to improve CIs resilience level. Furthermore, during the recovery stage, members of the communities should help the CI to bounce back to initial stage more efficiently providing resources and knowledge.

Within this policy two sub-policies define the scope of this policy: shared information systems and databases and trust and engagement of the participants.

a) Shared information systems and databases

Stakeholders involved in the community should share information about previous incidents and identify best practices to facilitate information and operational experience sharing. In order to do that the members within the community should have shared information systems and databases. When an incident or a crisis occurs, lessons learned from this experience should be spread to the rest of the CIs through these systems in order to take measures to prevent a reoccurrence. Furthermore, these information systems facilitate the communication process to inform members about incident occurrences (Snyder and de Souza Briggs, 2003; Resilient Organisations, 2012).

b) Trust and engagement of the participants

It is important that entities within the community trust each other in order to share all the gathered experiences and information. Sharing information and lessons gathered about particular experiences would help crisis managers to

improve their knowledge in the field and in turn, increase the trust among the members of the community (Resilient Organisations, 2012). If some entities do not trust in others they will be more reluctant to share their findings publicly in the community. In order to keep alive this community and promote the information sharing among its experts, it is important that participants are engaged with the community and rely on its participants (Resilient Organisations, 2012). Having good relationships among different organizations ensures that everyone would participate and collaboration agreements will be established in case a crisis occurs.

4.3.2.2.4 Crisis Regulation and Legislation

Legislation is a law approved by a government body such as a parliament congress, state legislature or city council, whereas a regulation is a guideline/directive made by a government agency or other authorities that provides details on how legislation will be implemented and may establish specific minimum requirements to meet. Legislation is broader and more general whereas regulation is more specific and provides further technical and organizational details to implement. Normally, changes are faster and easier in regulations because they do not require so much formality as legislation. Each sector has specific regulations. Having well defined and updated regulations and legislation results in more safe and better prepared infrastructures to avoid a crisis occurrence and better handle it if one does occur. Furthermore, the regulations and laws should be regularly updated and reviewed to identify responsibilities in case a crisis occurs. This sub-policy depends basically on the government's crisis awareness level and CIs can hardly assist on its development.

This policy has been disaggregated in two sub-policies: regulations and laws revision and update and compliance level of regulations and laws.

a) <u>Regulations and laws revision and update</u>

Defining the regulations and laws is not sufficient in this field where new lessons are continuously learned, and new crises and incidents lead crisis

managers to modify and implement new technical and organizational measures. Therefore, it is essential to regularly update regulations and laws, based on committed errors in different sectors, in order to establish new safety measures.

b) Compliance level of regulations and laws

Regulations and laws are established in order to be fulfilled by the CIs and all the involved entities. The follow up of the level of compliance with the regulations and laws must be ensured. Furthermore, some mechanisms such as penalty systems or tight controls should be introduced to guarantee their fulfillment. Establishing adequate penalties for the entities that do not perform properly diminishes the probability of entities taking risks and improves the implementation of safety measures. If penalties are lower than the investment level required by the regulations or laws, companies will tend not to establish them and just pay the required penalty.

4.3.2.3 Economic Resilience

4.3.2.3.1 Public Crisis Response Budget

As in the case of the *CI Crisis Response Budget*, public institutions should have a pool of money set aside in case a crisis occurs, in order to help the stakeholders and society. This extra funding allows organizations, society, and first responders to obtain resources within a reasonable time. Monetary resources will allow performing activities, repairing and rebuilding damaged physical systems and compensating the affected CIs and people. If this pool of money is not enough to cover all the expenses, the government should be able to draw upon extra resources urgently to cope with crises.

4.3.2.4 Social Resilience

4.3.2.4.1 Societal Situation Awareness

Not only should the government and first responders prepare to handle crises but society can also play an important role in a crisis resolution. In order

to improve the resilience level of a nation, capabilities from the whole society are required (Committee on Increasing National Resilience to Hazards and Disasters, 2012). The situation awareness and commitment of society towards avoiding a crisis occurrence reduces crisis probability and reduces the magnitude of the impact, with better ability to respond (Shaw et al., 2009; Resilient Organisations, 2012; Parsons, 2007). In the event of a crisis, volunteers might assist first responders in dealing with the affected people, thus reducing possible adverse effects. The collaboration and information that society can provide may be crucial to enhance crisis management. CIs can influence significantly on the preparation of society by becoming people aware of possible risks and providing courses to deal with critical situations. Two sub-policies have been defined within this policy: societal situation awareness and commitment and societal training.

a) Societal situation awareness and commitment

It is important that society is aware of the possibility of incidents or crises occurrence and committed to crisis management because they can help in improving their resolution providing real information about the affected area (Resilient Organisations, 2012; Parsons, 2007). Society also needs to know that it is exposed to vulnerabilities and therefore, they should be prepared to face critical situations. CIs should have an important role in transmitting this information. However, care must be taken because providing too much information about the risks could create a social alarm which is not desirable. Furthermore, they can assist government or other entities in detecting an early warning signal or even anticipating that something may occur (Shaw et al., 2009; Resilient Organisations, 2012; Parsons, 2007).

b) Societal training

Society can play an important role in crisis resolution. They could help in absorption and recovery activities and also assist first responders in their activities. Moreover, it is important that people are informed about the basic tasks or procedures that they should follow when a crisis occurs to reduce public anxiety and avoid further damage. During the prevention stage, risk

probability can be reduced providing training and informative courses about best-practices and proper behaviors by CIs.

4.4 Influence of the Resilience Policies on Resilience Lifecycle Stages (prevention, absorption, and recovery)

All the policies have different influences on the different stages of the resilience lifecycle. There are some policies which are more effective on preventing a crisis occurrence and there are others which are more important on the recovery phase. In order to assess the influence of each resilience policy, we gathered information from the experts' knowledge.

In the Delphi process, once we completed and improved the list of resilience policies and sub-policies through the first questionnaire, the target of the second questionnaire was to determine the influence of each policy on the three resilience lifecycle stages. Therefore, experts were asked to evaluate from 0 to 5 (0 being low influence and 5 strong influence) the influence of each policy on the three the resilience lifecycle stages.

Although the number of experts in the four fields (academic, transport, energy, and first responders) was not the same, we gave equal weight to the results of all the experts. The answers gathered from all the experts after the second interaction are included in Appendix C. After analyzing the answers, data were ordered in the appropriate way to better interpret the results. A new scale with a more suitable range of values to facilitate the interpretation of the data was defined (see Table A.5 in Appendix C). Based on this new scale, an influence table was built in order to summarize the obtained results and determine the influences of the resilience policies (see Table 4.4). The influence level is assessed through a new scale (Very High, High, Regular, Low, and Very Low) where Very High is the highest influence and Very Low is the lowest influence.

Table 4.4: Resilience policies' influence on the three resilience lifecycle stages.

	Resilience Dimensions	Resilience Policies	Prevention	Absorption	Recovery
INTERNAL RESILIENCE	Technical Resilience	CI Safety Design and Construction	Very High	Very High	High
		CI Maintenance	High	Regular	Low
		CI Data Acquisition and Monitoring System	High	High	High
		CI Crisis Response Equipment	Low	Very High	High
	Organizational Resilience	CI Organizational Procedures for Crisis Management	High	Very High	High
		CI Top Management Commitment	Very High	Very High	High
		CI Crisis Manager Preparation	Very High	Very High	High
		CI Operator Preparation	Regular	Very High	Very High
	Economic Resilience	CI Crisis Response Budget	Low	Regular	Very High
EXTERNAL RESILIENCE	Technical Resilience	External Crisis Response Equipment	Very Low	High	High
	Organizational Resilience	First Responder Preparation	Very Low	High	High
		Government Preparation	Low	High	High
		Trusted Network Community	Low	High	High
		Crisis Regulation and Legislation	Very High	Regular	Regular
	Economic Resilience	Public Crisis Response Budget	Very Low	Regular	Very High
	Social Resilience	Societal Situation Awareness	Low	High	Very High

Based on results in Table 4.4, it can be concluded that during the prevention stage, internal policies are those that most contribute to avoid a crisis occurrence. The CI holds the main responsibility for avoiding a crisis

occurrence, establishing a robust and safe infrastructure, and for raising the crisis awareness level of their workers. On the other hand, during the absorption and recovery stages, the influence of external stakeholders becomes essential. The resilience level of CIs needs to be improved, together with the resilience level of external agents in order to properly handle crises. In particular, *Crisis Regulation and Legislation* policy has the greatest influence during the prevention stage, although it is an external policy. In addition, we can also conclude that during the absorption stage, almost all the policies lead to lessen the magnitude of the impact with the exception of the policies within the economic resilience. Their main influence is during the recovery stage providing resources to bounce back to the initial stage.

Analyzing the results based on the sectors the experts belong (see Table A.4 in Appendix C), it can be seen that there are minor disagreements among sectors' experts regarding some policies. For example, if we focused on *CI maintenance*, academics think that its influence in preventing a crisis occurrence is low, believing that maintenance activities are more important during the absorption and recovery phases. This is contrary to the opinion of the non-academic experts. This difference might be because practitioners might have experienced a crisis situation due to low maintenance level. Another slight difference could be seen regarding *Crisis Regulation and Legislation* policy. Academics believe that this policy helps in recovery whereas the rest of the sectors do not concur. Finally, experts from the transport field agree that the T*rusted Network Community* does not influence the recovery stage, whereas the rest of the experts think that it does. The last difference could lie on the maturity level of these communities in the different sectors. However, the differences are very small and therefore, it is hard to obtain generalizable conclusions.

4.5 Implementation methodology

Once the list of resilience policies and sub-policies was defined the implementation methodology was developed through the survey. Due to the interdependency of the policies and sub-policies, it is important to define the temporal order in which they should be implemented. Some policies require others prior implementation in order to efficiently apply. Therefore, this methodology aims to provide some guidelines about the temporal order in which the policies and sub-policies should be implemented to achieve the highest efficiency in the implementation of this framework in practice. First, the temporal order in which the policies should be implemented was defined. Afterwards, the temporal order in which the sub-policies should be implemented for each resilience policy was determined by the experts. Appendix D collects all the gathered data from experts and how the analysis of the data was carried out in order to define the implementation methodology.

4.5.1 Implementation methodology of the resilience policies

Not all the policies can be implemented at the same moment since some of them require others prior implementation to achieve highest efficiency in their implementation. Therefore, this methodology presents the temporal order in which the policies should be implemented to achieve higher efficiency in the framework's application.

It is hard to define the exact order in which the policies should be implemented. After analyzing the results we concluded that there are some policies that need to be implemented at the beginning of the process since they are required for the implementation of others. In turn, others are placed in the last positions as they necessarily built on previous policies. Finally, there are also some policies which require others implementation but they also affect in the efficiency of others.

Therefore, in order to achieve more realistic and coherent results, data were ordered in a suitable way to better interpret the results. We divided the implementation process into five stages based on a new scale with a more

suitable range of values (see Table A.10 in Appendix D). In the first stage two policies should be implemented. In the second stage, another two should be introduced to the implementation methodology. In the next stage, five new policies will be implemented. In the fourth stage, three new policies and in the last stage four new resilience policies are implemented in the system. Table 4.5 illustrates the implementation methodology of the resilience policies divided into five main stages.

4.5.1.1 First stage

There are two policies that are the driving forces to begin, promote, and encourage the improvement of resilience in the CIs. First, having a safely designed and built infrastructure is essential to improve the resilience of CIs. Second, the commitment of top management towards the resilience building process is vital to allocate resources, promote a resilience based culture, and increase the engagement of the workers.

4.5.1.2 Second stage

Once the first two resilience policies are implemented, two new policies would be added to the previous ones in the second stage. Not only the CI needs to be well designed and built but maintenance activities should also be carried out to ensure the reliability of the components and CIs and avoid the accumulation of errors. Therefore, *CI maintenance* policy should be implemented in this second stage.

Together with technical issues, *CI Organizational Procedures for Crisis Management* should also be developed to properly manage crises. Internally, the CI should prepare to be able to respond to a crisis. Guidelines about what activities should be carried out and responsibilities of each worker need to be well defined in order to cope with crises. Coordination procedures with external stakeholders should also be established to better handle crises.

Table 4.5: The Implementation Methodology of the Resilience Framework.

Resili. Types	Resilience Dimensions	Resilience Policies	1st stage	2nd stage	3rd stage	4th stage	5th stage
INTERNAL RESILIENCE	Technical Resilience	CI Safety Design and Construction					
		CI Maintenance					
		CI Data Acquisition and Monitoring System					
		CI Crisis Response Equipment					
	Organizational Resilience	CI Organizational Procedures for Crisis Management					
		CI Top Management Commitment					
		CI Crisis Manager Preparation					
		CI Operator Preparation					
	Economic Resilience	CI Crisis Response Budget					
EXTERNAL RESILIENCE	Technical Resilience	External Crisis Response Equipment					
	Organizational Resilience	First Responder Preparation					
		Government Preparation					
		Trusted Network Community					
		Crisis Regulation and Legislation					
	Economic Resilience	Public Crisis Response Budget					
	Social Resilience	Societal Situation Awareness					

4.5.1.3 Third stage

In this step, five new policies are introduced. First, *CI Data Acquisition and Monitoring Systems* should be implemented through the infrastructure to get

information about the state of the infrastructure and be able to anticipate any incident. Second, *CI Crisis Response Equipment* has also to be acquired in order to be able to absorb the impact and ensure the safety of the workers. Third, the *CI Crisis Manager Preparation* is introduced in this step since they are the ones responsible for detecting early warning signals, analyzing them and communicating to the corresponding person. They are continuously aware of any possible incident and they have the responsibility for preparing the organization to perform efficiently in face of a crisis. Fourth, the *Government Preparation* should be improved since the government also plays an important role in crisis management. It has the authority and the capacity to increase the external entities' awareness and commitment towards resilience building process and it can afford resources to acquire equipment and help in the crisis resolution. Fifth, together with the fourth policy, the government and its public entities should develop crisis regulations and laws in order to establish the minimum requirements that CIs need to fulfill to ensure their safety and high reliability. It is worth noting that these last two policies should be constantly improved and provided with feedback due to the turbulent environment.

4.5.1.4 Fourth stage

CI Operator Preparation, *CI Crisis Response Budget*, and *First Responder Preparation* policies are implemented in this stage. Once the top management is committed, the crisis management procedures are established, and crisis managers are well prepared, operators should be prepared to face crises. They get training courses and make some table-top exercises and emergency drills to improve their crisis management skills and awareness. Furthermore, the CI has to set aside some monetary resources or contract for insurance to be able to absorb the extra costs that arise from a crisis. Externally, the preparation of first responders must be improved to ensure their proper response in case of a crisis.

4.5.1.5 Fifth stage

Finally, in this last stage, the last external policies are implemented. In order to be able to respond appropriately it is important that external entities have reliable and sufficient response equipment to handle crises (*External Crisis Response Equipment*). Furthermore, a *Trusted Network Community* has to be created where stakeholders share information and experiences with other involved agents and improve their crisis management knowledge. The *Public Crisis Response Budget* is also improved in order to have monetary resources to be able to respond to crises. Finally, the *Societal Situation Awareness* is enhanced since society can help to handle a crisis or also avoiding its occurrence or at least not making it worse. Society should be aware about the crisis occurrence and prepared to cope with crises in the most efficient way.

4.5.2 Implementation methodology of the resilience sub-policies

Within some of the resilience policies several sub-policies have been defined in order to better define the scope of each policy. In this first step, through the implementation methodology, the aim is to define the order in which those sub-policies should be implemented to achieve the highest efficiency in the implementation of each resilience policy. In order to define the implementation methodology of the resilience sub-policies, data gathered from experts were analyzed and the temporal order of the resilience sub-policies for each resilience policy was determined (see Appendix D). Below, the implementation process of each resilience policy is explained.

4.5.2.1 CI Safety Design and Construction

First of all, safety systems are implemented in order to avoid a crisis (see Figure 4.1). Those systems start functioning when an incident occurs in order to avoid its unfolding into a crisis and to carry out the infrastructure to a safe state. Safety systems should be established since the start-up of CIs. Despite having reliable and well maintained systems and components, CIs can fail.

Therefore, it is important to have redundant equipment and systems in order to ensure the critical systems' functioning in light of their disruption. Not only main systems should be duplicated but the functioning of safety systems is also critical and therefore, they should have redundant systems and components. Redundancy is the second sub-policy that should be implemented (see Figure 4.1).

In parallel with the two previous ones, simplicity and loose coupling sub-policy should be implemented (see Figure 4.1). It is important to design and build as simple infrastructure as possible and with loose relationships to reduce vulnerabilities and avoid unintended consequences. Having a complex infrastructure increases the consequences of incidents. Furthermore, tight relationships facilitate the escalation of incidents rapidly leading to a crisis occurrence. Therefore, when introducing safety systems and redundancy measures within the CI, it is important to reduce complexity as much as possible and avoid tight relationships.

Finally, once the design is done and the infrastructure is built it is important to ensure its proper functioning through internal and external audits. This sub-policy is the last one that is implemented within this policy (see Figure 4.1).

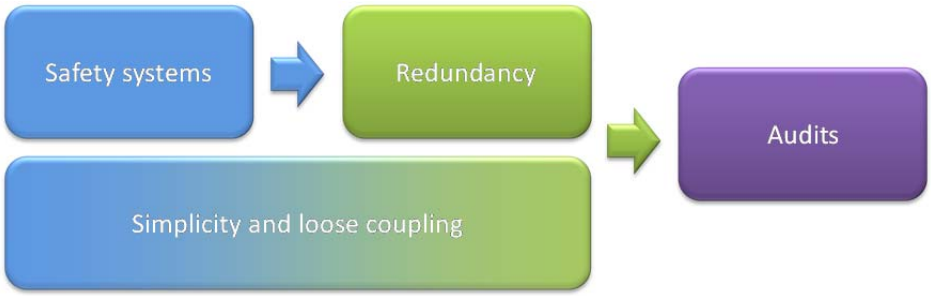


Figure 4.1: The temporal order in which the sub-policies should be implemented within CI Safety Design and Construction policy.

4.5.2.2 CI Maintenance

Preventive maintenance is the first sub-policy that should be implemented (see Figure 4.2). Through these activities the proper state of the infrastructure

and the avoidance of incidents are guarantee. However, failures can still occur and therefore, it is also important to establish a proper corrective maintenance approach to adequately handle them. Thus, corrective maintenance is the second sub-policy that should be implemented within this policy (see Figure 4.2). Having a high level of preventive maintenance would reduce the probability of incidents occurring and therefore, fewer corrective maintenance activities would be required.

Figure 4.2: The temporal order in which the sub-policies should be implemented within CI Maintenance policy.

4.5.2.3 CI Data Acquisition and Monitoring System

In this case, both sub-policies should be implemented simultaneously since both require the other's implementation to properly function (see Figure 4.3). Data acquisition equipment is responsible for gathering data from the infrastructure. This equipment is usually composed of relays and sensors which transmit information to the corresponding place. However, in order to visualize the obtained data, it is essential to have monitoring equipment where the data are displayed. Therefore, simultaneously, adequate equipment to monitor all the gathered information in the most suitable way should be implemented (see Figure 4.3). Monitoring panels with suitable interfaces and alarms alerting of incidents need to be established as well as a data saving system in order to analyze the incidents and extract lessons learned.

Figure 4.3: The temporal order in which the sub-policies should be implemented within CI Data Acquisition and Monitoring Equipment policy.

4.5.2.4 CI Organizational Procedures for Crisis Management

First, it is important to develop crisis management procedures to define how the company and the workers should behave in light of a crisis (see Figure 4.4). This procedures would help coping with crises in the most rapid and efficient way. These procedures should be defined since the start-up of a company because crises can occur any time and company should be prepared to face them.

Second, the management of the incidents of daily life should be implemented as Figure 4.4 shows. These incidents should be detected, reported, analyzed, resolved, and evaluated in order to avoid accumulation of errors and to obtain corrective actions for the future. Evaluation of errors would lead to define new improvement measures and to reduce the likelihood of crises.

Last but not least, organizations should establish coordination agreements and procedures with external stakeholders to get help when a crisis occurs and to respond in the most coordinated way (see Figure 4.4). Responsibilities of each entity should be defined beforehand in order to efficiently response to crises.

Figure 4.4: The temporal order in which the sub-policies should be implemented within CI Organizational Procedures for Crisis Management policy.

4.5.2.5 CI Top Management Commitment

The commitment of the top management towards the improvement of CI's resilience is the driving force for being able to carry out all the possible measures. Top managers should be committed and constantly aware of the possible incidents that could lead to crises. Therefore, top managers' commitment and situation awareness is the first sub-policy that should be implemented (see Figure 4.5). Secondly, activities to promote resilience based culture ought to be established to encourage workers to report incidents and improve the resilience of the organization (see Figure 4.5).

Figure 4.5: The temporal order in which the sub-policies should be implemented within CI Top Management Commitment policy.

4.5.2.6 CI Crisis Manager Preparation

In order to ensure a good preparation level of crisis managers and take advantage of training exercises, crisis managers need to have high situation awareness and commitment level towards crisis occurrence. Crisis managers are the main responsible for detecting early warning signals and responding to them rapidly to avoid their escalation. Therefore, they need to be constantly aware of possible incidents and committed with the resilience building process. Once this is achieved, they also need to train their skills to better perform their job (see Figure 4.6). Not only table-top exercises and emergency drills must be

developed in this second step but also their sensemaking capacity needs to be trained to properly perform in unplanned situations.

Figure 4.6: The temporal order in which the sub-policies should be implemented within CI Crisis Manager Preparation policy.

4.5.2.7 CI Operator Preparation

Operators should be aware of the importance of crises and committed with the resilience building process. Therefore, first, operators' crisis awareness and commitment should be improved (see Figure 4.7). Once this is achieved, second, operators should be trained in order to acquire skills to efficiently deal with crises (see Figure 4.7). Training courses would allow them to know and understand the procedures to handle crises and develop their sensemaking capacity to cope with unexpected and unpredictable crises.

Figure 4.7: The temporal order in which the sub-policies should be implemented within CI Operator Preparation policy.

4.5.2.8 First Responder Preparation

In this case, both sub-policies, first responder situation awareness and commitment and first responder training, should be implemented simultaneously (see Figure 4.8). Since the beginning, first responders are sufficiently trained to properly respond to crises and by default they have a sufficiently high awareness and commitment level to successfully complete their job. Their job basically consists on responding to crises and ensuring the safety of the society. Therefore, they are constantly aware and committed with

the crisis management. They are also properly trained to deal with crises since this is part of their studies.

Figure 4.8: The temporal order in which the sub-policies should be implemented within First Responder Preparation policy.

4.5.2.9 Government Preparation

Government plays an important role in the crisis management process. When the crisis spreads through the whole society, the government usually takes the responsibility for managing the resolution process. Therefore, first, the government needs to be aware in order to anticipate incidents and prevent their escalation to severe crises (see Figure 4.9). Furthermore, it should be committed with the crisis management process in order to deploy resources and promote prevention and preparation activities. Second, it should enhance its leadership capacity since, in case of severe crises, the government is responsible for leading crisis response (see Figure 4.9).

Communication activities are also of utmost importance since during times of crises the government has to communicate all the information to the stakeholders and also to the public and media. Therefore, this policy should be implemented in the third position (see Figure 4.9). Fourth, the government should train in order to know how they should deal with a crisis (see Figure 4.9). Procedures should be established to define the responsibilities and actions each entity should perform in face of a crisis. Finally, the government is also in charge of the coordination of response agents that take part in the crisis resolution (see Figure 4.9). Therefore, it should be prepared to coordinate them in the most efficient way and also to gather help from foreign agents when national resources are not enough.

Figure 4.9: The temporal order in which the sub-policies should be implemented within Government Preparation policy.

4.5.2.10 Trusted Network Community

Sharing information and knowledge with agents involved in the crisis management process enhances considerably the crisis management knowledge and coordination activities among the entities. However, trust and engagement are necessary to share experiences and lessons learned with external agents. Therefore, first, trust and engagement among the participants should be increased (see Figure 4.10). Once this is achieved, information systems and databases need to be implemented to facilitate the information and knowledge sharing among the participants of the network (see Figure 4.10).

Figure 4.10: The temporal order in which the sub-policies should be implemented within Trusted Network Community policy.

4.5.2.11 Crisis Regulation and Legislation

First, it is important to periodically review and update the regulations and laws taking into account the lessons learned from previous crises (see Figure 4.11). Regulations and laws should be well defined and updated in order to be useful for CIs. Second, the fulfillment of these regulations and laws needs to be guaranteed by establishing different mechanisms such as inspections or penalty systems (see Figure 4.11).

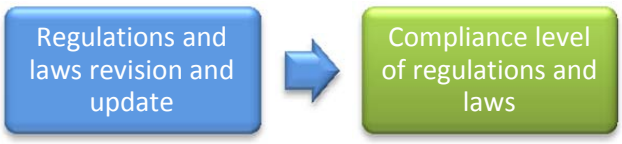


Figure 4.11: The temporal order in which the sub-policies should be implemented within Crisis Regulation and Legislation policy.

4.5.2.12 Societal Situation Awareness

Society can help significantly in the crisis management but in order to be helpful it is essential that citizens are aware of crisis occurrence and committed with the safety of the society. Therefore, first, it is important to increase the situation awareness and commitment of the society to help in the resilience building process (see Figure 4.12). Second, some training activities should be provided to the society to know how they can help and what kind of activities they can perform to improve resilience and reduce vulnerability (see Figure 4.12).

Figure 4.12: The temporal order in which the sub-policies should be implemented within Societal Situation Awareness policy.

4.6 Conclusions

This research contributes to the literature by presenting a resilience framework, a detailed description of how the resilience level of CIs can be improved from a holistic point of view. This framework transfers the theoretical features of the resilience concept to the practice in order to integrate the resilience aspects within the general management of CIs.

Through GMB workshops, multiple case studies, and Delphi process, a set of resilience policies and sub-policies very closely related to the general management issues of CIs are defined. This research also provides the influence

level of each policy on the three stages of the resilience lifecycle (prevention, absorption, and recovery) to facilitate crisis managers understanding the influence level of each policy.

Finally, the implementation methodology is developed gathering data from experts through the survey method. A five stage methodology is defined in order to implement the resilience policies. Furthermore, the temporal order in which the sub-policies should be implemented for each resilience policy is provided. The aim of this methodology is to achieve a high efficiency in the implementation of the resilience policies and sub-policies.

5 Validation of the Resilience Framework for CIs

This section presents the validation process of the resilience framework for CIs. The aim of the validation process was to confirm the framework provides value to CIs in order to improve their resilience level. Three characteristics were analyzed to validate the suitability of this framework: completeness, usefulness, and relevancy. Two studies were carried out in two different CIs: the first study was carried out in a nuclear plant and the second one in a water distribution company.

Already implemented resilience measures were gathered from both CIs and classified by resilience policies and sub-policies in order to justify the completeness of this framework. The framework was also useful for both CIs since it provided some improvement areas to enhance their resilience level. Finally, evidence and examples were gathered for all the policies and sub-policies what advocate the relevancy of the defined resilience policies and sub-policies.

5.1 Introduction

Once the resilience framework was developed, mostly based on experts' knowledge, the validation process was carried out. First of all, it is important to define what validation stands for since validation and verification concepts are often mixed. Validation determines whether a conceptual model is an accurate representation of the system under study whereas verification ensures that the model performs as intended (Kleijnen, 1995). The following two questions clarify the difference among these two concepts: "Is the model right?" (this defines verification) and "Is the right model?" (this defines validation). A model is developed for a specific purpose or application and its validity affirms if this model fulfills this purpose (Sargent, 1998). The required accuracy depends on the model's purpose. Validation process is a costly and very time-consuming activity therefore, evaluations and tests are conducted until sufficient confidence is achieved (Sargent, 1998).

The aim of the resilience framework for CIs is to help crisis managers to enhance the resilience level of CIs. Therefore, the purpose of our validation was to affirm that this framework provides value to crisis managers in the CI's resilience building process. Our validation process focused on determining if the resilience framework accomplishes the following three main characteristics:

- *Completeness:* the framework should collect all the possible resilience building measures to be complete. This framework has been defined holistically covering all the resilience dimensions and involving internal and external stakeholders.
- *Usefulness:* this framework should allow CIs to discover improvement areas to enhance their resilience level.
- *Relevancy:* it is fundamental to verify that all the defined policies and sub-policies are suitable and relevant for building up the CIs resilience level.

Two case studies in two different CIs were carried out to perform this validation. Examples and evidence to improve the resilience level already implemented in the CIs were gathered. Afterwards, these evidence and

examples were classified by resilience policies and sub-policies. This chapter explains the results obtained in both cases and the general conclusions of this validation process.

5.2 Results from Case Studies

Two case studies were carried out to validate the framework. The first one was carried in a nuclear plant in Southern Europe. This study lasted six months and information from different sources (interviews, internal documents, operating and organizational procedures, archival records, and direct observation) was gathered. The second one was performed in a water distribution company in Southern Europe. This study was not as extent as the previous one and in this case we were only able to get information from interviews with the general manager.

Following, the evidence and examples from both cases classified by resilience policies and sub-policies are presented.

5.2.1 CI Safety Design and Construction

In order to analyze this policy we focused on the physical safety systems of the infrastructure. These systems are the ones that start operating when an incident occurs in order to prevent escalation of the incident or absorbing the impact if a crisis occurs.

In the case of the nuclear plant, the most critical part is the core of the reactor. Therefore, all the systems are prepared to avoid or absorb this event. In total, there are thirteen frontal systems that are activated eventually in order to stop or mitigate the incident and eight support systems that provide support to the frontal systems.

Taking into account the three resilience lifecycle stages defined in the literature, we classified the systems according to the stage in which they are applied. Some systems are responsible for mitigating both internal and external incidents that may lead to core damage in the worst case. Others are

responsible for absorbing the impact and avoiding releases to the outside when the core is damaged (see Table 5.1).

Table 5.1: Frontal systems that prevent core damage and absorb the impact.

Objective of the system	Frontal system	Prevention	Absorption
Reactivity control	Reactor Protection System (RPS)	X	
	Reactor Pump Trip System (RPT)	X	
	Alternate Rod Insertion (ARI)	X	
	Liquid Poison Addition system (LPAS)	X	
Cool the core when the pressure in the vessel is high	High Pressure Coolant Injection System (HPCIS)	X	
	Condensate and Feedwater System (C&FS)	X	
Cool the core when the pressure in the vessel is low	Low Pressure Coolant Injection (LPCI)	X	X
	Low Pressure Core Spray System (LPCSS)	X	X
Pressure control	Automatic Depressurization System (ADS)	X	X
	Manual Depressurization System (MDS)	X	X
Residual heat removal	Shutdown Reactor Cooling System (SRCS)	X	
	Isolation Condenser (IC)	X	
	Venting (V)	X	X
Containment of releases	Primary containment		X
	Secondary containment		X
	Isolation System (IS)		X

The recovery phase depends on the final situation of the nuclear plant. After the Fukushima accident, the plant has acquired some portable equipment

to use in case the normal safety systems are completely damaged or inoperable due to crises.

Nowadays, nuclear plants evaluate their risk of having a serious accident through the methodology of Probabilistic Risk Assessment (PRA). This methodology was originated in the aerospace sector in the 1960s (Bedford and Cooke, 2001). The methodology consists of quantifying the risk of having a crisis taking into account the possible initiating events and the probability of safety systems to fail in mitigating these events.

The nuclear plant identifies the possible incidents that could occur in the plant and assesses the capacity of the plant to mitigate them through these safety systems. However, this methodology presents some limitations regarding resilience. This methodology is rigid and provides little flexibility to act since it only evaluates the capacity to face expected crises but it does not provide any information to handle unexpected and extraordinary critical threats (e.g., a giant tsunami as at Fukushima nuclear plant or a direct bomb attack on a plant). Although evaluating the risk level of a system is important, it is also essential to prepare for managing unexpected and unpredictable situations. Moreover, it is difficult to identify all the initiating events that could occur and it is also almost impossible to identify all the combinations of failure that could lead to crises. Therefore, our framework helped the nuclear plant to open this perspective and to realize about the weaknesses in this aspect.

In the case of the water distribution company there is not such a critical part that takes the utmost importance. The infrastructure of this CI covers the following parts of the water distribution network: dams, tubes from dams to water purification centers, water purification centers, tubes from water purification centers to water tanks, and water tanks of the towns. The most critical events that could lead to major crises are the ones listed below and for most of them the company has safety systems to stop its escalation or procedures to respond to these events:

- *Chlorine leakage in the purification plant:* there are some redundant systems to resist the emissions and avoid releases to the outside.

- *Dam breach:* there is not any procedure established.
- *Breakage of an important water pipe that supplies an important area of a province:* there are some procedures to create a bypass in the broken tranche to supply water to the affected area.

In both cases, in order to evaluate the safety level of their CI, they focus on identifying the possible triggering event and evaluating the capacity of the CI to withstand this event. However, little is done to deal with unexpected and unpredictable situations.

5.2.1.1 Safety systems

In the nuclear plant, the frontal systems are mainly responsible for mitigating an initiating event that could lead to core damage and absorbing the impact when the core gets damaged. Support systems, on the other hand, are the ones that provide support to the frontal systems for their functioning. In addition to them, there are also other significant systems (Standby Gas Treatment System (SGTS), Control Room Habitability (CRH), Essential Cool Water (ECW), Neutron Monitoring System (NMS), Control Rod Drive (CRD), primary containment, and secondary containment) that help to mitigate the core damage or absorb it when a crisis occurs, avoiding releases to the outside.

Furthermore, there are other safety systems that assist in mitigating other types of events such as fires or floods. In the case of fires, the following ones are some examples of the identified systems: automatic detection system, fire-resistant doors, penetration seals in fire-resistant barriers, firefighting unit, and covering on the electrical transmission lines. In the case of floods, some examples of the identified systems include penetration seals, curbs, and drainage valves. Furthermore, within each safety system there are many safety subsystems and elements that ensure the proper functioning of the systems.

In the water distribution company, there are several safety components and systems placed throughout the whole supply infrastructure to avoid crises. Throughout the distribution tubes there are valves to control the flow pressure.

The tubes are oversized to be able to transport a higher flow in critical situations. In dams, water purification centers, and water tanks of the towns the elements are oversized to be able to withstand higher quantity of water in periods of peak demand.

5.2.1.2 Redundancy

Redundancy can be applied at many levels: system-level, subsystem-level, and component-level.

In the nuclear plant we found examples at all these levels. At system-level, within the frontal systems, there are some systems which are redundant such as Reactor Protection System (RPS) and Alternate Rod Insertion (ARI). RPS system inserts the control rods in order to control the radioactivity level in the core. In case the RPS system fails, the ARI system is responsible for introducing the control rods in the core.

Furthermore, within each system there is evidence of redundant subsystems or components that increase the reliability level of the system. Almost all the cooling systems have two redundant lines to supply water to the core. Furthermore, there are two sources of water supply from which the system can obtain water: condensate storage tank (CST) and suppression chamber. More specifically, within Low Pressure Coolant Injection (LPCI) system, each redundant line to supply water to the core has two redundant pumps to ensure the functioning of the system in light of a failure in one pump.

The setting up of the systems depends on the manual or automatic signals that are transmitted through the logic of the system. This logic is a set of electrical circuits composed basically of cables and relays which are responsible for gathering the information and transmitting it to the monitoring systems. Within this logic, there are redundant relays and lines to transmit information in order to ensure its proper functioning in case a component fails. Furthermore, there are redundant sources of power (grid power, diesel generators, and DC batteries) to provide power to the whole system.

In the water distribution company all the critical components of the dams, water purification centers, and water tanks of the towns are duplicated to ensure the functioning of the system in light of a failure in one component. In dams, all the metal components are duplicated. There is a power unit that sets in motion the emergency generators in case of a power outage. If this power unit fails they have butane cylinders to activate the generators. Furthermore, the tubes within the dam are duplicated. In water purification centers, there are also power units and butane cylinders to guarantee the availability of power when an outage occurs. Due to the importance of water quality, the system for dosing of reagents is duplicated. Finally, within the water tanks of the towns, there are two tanks to store water.

5.2.1.3 Simplicity and loose coupling

In the case of the nuclear plant, nowadays almost all the frontal systems require electrical power (alternating current (AC) or direct current (DC)) for their functioning. However, after the Fukushima accident, it has been demonstrated that there can be some situations in which the power energy is not available and therefore, the systems are not able to function. In order to avoid this situation, the nuclear plants are obliged to have portable equipment to be able to perform the basic emergency activities such as cooling of the core. These systems do not depend on the electrical power and therefore, their functioning is possible despite the absence of electrical power. Regarding the power system, the power supplies to the pumps of the redundant lines are done from two independent electrical divisions to guarantee their functioning in case of a loss of one electrical division.

In the same vein, the water distribution company is very dependent on the availability of the electrical power for its functioning. Therefore, they have power units and butane cylinders in case of a power outage. In order to verify power units' proper functioning, the company tests their functioning once a month and they keep them operating for the whole day. Reagents are also essential to ensure good water quality. A prolonged strike of transporters could

hardly affect their availability. Therefore, this company has a large quantity of safety stock of reagents.

5.2.1.4 Audits

Generally, there are two types of audits: internal audits which are the ones carried out by the workers of the CI and external audits which are performed by external entities.

In the case of the nuclear plant, these audits are conducted at intervals between one month and six years. Table 5.2 summarizes the internal audits performed within the nuclear plant and the objective of each audit.

Table 5.2: Internal audits within the nuclear plant.

Internal Audits	Objective
Internal audits by Quality department	Audits performed to the personnel and sections of the nuclear plant.
Audits to suppliers by Quality department	Audits performed to the external suppliers.
Periodical inspections plan	Detection, evaluation, and correction of the deficiencies in the facilities, equipment, and processes in order to maintain the plant in optimal condition, to safeguard the safety of the workers, and to minimize the environmental impact.
Supervision planning	Promote the professional level of the personnel and increase the quality level of the work achieving an improvement in the radiological protection safety, in labor risk prevention, and in the environmental aspects.

Within the external audits, the ones carried out by the national Nuclear Security Council (NSC) are the most important ones. Table 5.3 summarizes the main external audits carried out within the nuclear plant and the objective of each audit.

Table 5.3: External audits within the nuclear plant.

External Audits	Objective
Inspections of NSC	Inspection of the overall functioning of the nuclear plant
National Association for Standardization and Certification: ISO 14001	Environmental management system's audit
OSART (IAEA)	Operational security audit
SCART (IAEA)	Safety culture analysis
PROSPER (IAEA)	Analysis of the operational experience program's treatment
PEER REVIEW (WANO)	Identify improvement and strengthen fields within the nuclear industry
FOLLOW UP (WANO)	Follow up of the Peer Review
NEIL	Audit and evaluation of the fire safety within the nuclear plant

In the case of the water distribution company, they do not perform internal audits periodically. Through maintenance activities, they ensure the compliance level of safety and reliability of the infrastructure. Regarding external audits, they only have audits at the start-up of the company to guarantee the compliance of the safety and reliability requirements of the infrastructure. Minor modifications carried out after this phase are not supervised by any external agent.

5.2.2 CI Maintenance

In both cases, through maintenance activities they make sure that the system's physical components are in an adequate and reliable state to ensure their proper functioning.

During the prevention stage, preventive and corrective maintenance activities are carried out to avoid a failure and in case it occurs, to repair rapidly to avoid further damage. When a serious incident occurs (a serious incident is

an incident that may lead to a severe crisis) some specific maintenance activities should be performed to avoid its unfolding into a crisis.

During the absorption stage workers at the maintenance department have to develop specific recovery activities to diminish as much as possible the consequences arising from the crisis. Those activities are, in general, within corrective maintenance. The maintenance activities in the recovery period depend on the final state of the infrastructure. Different activities will be carried out depending on the severity of the crisis and the part which has been damaged.

5.2.2.1 Preventive maintenance

Within preventive maintenance several types of maintenance can be determined: predictive maintenance (activities of diagnosis or continuous or periodical monitoring which help in forecasting the evolution of the system's behavior or anticipating a failure), periodical maintenance (activities scheduled based on number of hours of functioning), and evolutive maintenance (activities should be adapted to new requirements and risks to assure a proper functioning and performance).

Another important issue is determining the frequency of these activities. Experience and historical data could help in determining how often each activity should be performed. Furthermore, there may be other requirements that can motivate a change in the preventive maintenance schedule, for example, regulation, management of the lifetime of the technology, internal or external operational experience, and manufacturers' recommendations.

In the nuclear plant, they define three different types of preventive maintenance: predictive maintenance, periodical maintenance, and planned preventive maintenance (activities which are performed as a result of the gathered data from preventive maintenance, periodical maintenance or due to an occurrence of an incident).

Bearing in mind the high degree of expertise of this nuclear plant, the frequencies of the preventive maintenance activities are defined based on their

experience. First of all, they evaluate the historical data taking into account the amount of corrective actions which have been required. If this amount is higher than a threshold-limit then they reschedule the preventive activities. After that, they evaluate the state of the equipment and bearing in mind the obtained results they decide to reschedule it or not.

Moreover, the nuclear plant uses a data base from the Electric Power Research Institute (EPRI) which allows the plant to evaluate procedures of other nuclear plants in order to adjust their schedule of preventive maintenance activities.

The water distribution company characterizes two types of preventive maintenance: predictive maintenance and preventive maintenance. Through a computer based information system they establish the frequency, the quantity, and the point where preventive maintenance activities should be performed. Furthermore, based on the information gathered through key maintenance indicators, they evaluate the effectiveness of the preventive maintenance plan and they reestablish the plan to improve it.

5.2.2.2 Corrective maintenance

These activities should be prioritized depending on their severity level. The priority would establish the order in which these activities should be performed.

The nuclear plant defines two types of corrective maintenance: corrective with failure (immediate or imminent loss of functioning of a system), and deferred corrective without failure (the system is able to continue its functioning but requires an intervention to avoid a failure). The corrective with failure is the type with higher urgency because the system is inoperable. Deferred corrective without failure, however, is not so urgent, so it will be performed based on the availability of the plant's resources. Related to maintenance, one of the most used indicators is the one in which they compare the number of activities carried out within preventive maintenance with the ones performed within corrective maintenance. The objective of the nuclear

plant is to have at least 60% preventive maintenance and at most 40% corrective maintenance.

In the water distribution company case, they do not distinguish between urgent and not so urgent activities but when they report a corrective maintenance activity in the system, its priority, and urgency level are established.

5.2.3 CI Data Acquisition and Monitoring System

Setting up the required sensors to gather information from the CI and installing adequate software and interfaces within the control panel to monitor the CI performance are some of the main activities that should be carried out in order to achieve a high implementation level of this policy.

In the nuclear plant, in order to prevent a crisis occurrence, there are several guidelines for data gathering, transmission and use of monitoring instrumentation distributed across the plant to control all the required parameters of the CI. During the absorption stage, the critical instrumentation is required to control procedures, control the vessel, and the primary and secondary containment. This instrumentation complies with RG 1.97 "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants" which is the regulation corresponding to monitoring instrumentation. In addition, a Post-accident Sampling System was identified as an information gathering piece of equipment to take samples in different points of the nuclear plant and evaluate them. There is not any specific instrumentation for the recovery phase. However, after the Fukushima nuclear accident, some portable equipment has been acquired to evaluate the dose of radiation.

In the water distribution company, there are several sensors established within the whole distribution network to gather critical data for the proper functioning. All the information gathered by these sensors is transmitted to the water purification centers and to the Control and Monitoring Center to detect anomalies and take actions to avoid their escalation. When a crisis occurs, the

same instrumentation is used to gather information about the evolution of the infrastructure during the absorption and recovery stages.

5.2.3.1 Data acquisition equipment

First, it is important to determine the critical parts of the CI to define what data are needed and identify the specific data to ensure their proper functioning. Furthermore, measuring specific variables that can anticipate other kind of threats such as natural disasters is recommended.

In general, the nuclear plant uses the following types of instrumentation to gather data: pressure instrumentation, flow instrumentation, temperature instrumentation, water level instrumentation, position instrumentation, neutron flux instrumentation, radioactivity of novel gases, and electrical power supply instrumentation. There are also other types of instrumentation such as the meteorological station, radiation level instrumentation, and seismic instrumentation.

In the water distribution network the following data is gathered through the following sensors: flow pressure, flow rate, water quality, contamination level, etc. In this case, they do not have other types of instrumentation to measure climatological or geological data. However, they are in direct contact with the meteorological center of the country to receive information in case of extreme weather condition.

5.2.3.2 Information monitoring equipment

In the nuclear plant, the gathered data are displayed in different places such as control panels in the plant and panels in the control room and also saved in the information system called Plant Data Information System. Table 5.4 summarizes the flow of the information.

Table 5.4: The flow of information and characteristics of each stage.

Stage in the information flow	Characteristics
Data gathering	Data gathering through Programmable Logic Controller (LPC)
Data Processing	Transfer of data to the proper calculation points
	Calculation of composed points
	Alarm evaluation
	Digital filtering
Storage of the processed data	Transitional
	Historical
	Alarms
	Events
Display of the data to the user	Real and historical data

There are some set points in the instrumentation where the system evaluates the obtained data verifying the appropriateness of it. They check if the data are within the proper range of values and if not, alarms are triggered to notify the workers about the problem. Furthermore, the alarms are displayed in different colors depending on the severity of the situation in order to facilitate the workers the interpretation of the situation and taking proper actions.

In the water distribution company, the gathered data are displayed in two places: on the control panel in the water purification centers and on the control panel in the Control and Monitoring Center. Furthermore, these data are also saved in the information system in order to be able to obtain information in the future.

The alarms at the control panel are classified in two groups, "100 Alarms" and normal alarms, based on the severity of the problem. "100 Alarms" are those alarms that warn of severe incidents and they require acting upon them immediately in order to solve the problem and avoid a crisis. On the other hand, the normal alarms warn of minor incidents which do not require such a quick response.

5.2.4 CI Crisis Response Equipment

During the prevention stage, the CI has to procure of emergency equipment that helps the workers to mitigate the escalation of incidents and ensure their safety. For the absorption stage, the same material would usually be used but in this case the aim is to reduce the magnitude of the impact due to the crisis. For the recovery stage the same equipment could be used to ensure the safety of the workers.

The nuclear plant includes a long list of emergency materials to respond to an incident and ensure the safety of the workers. Some examples of these materials are: communication systems, breathing equipment, lighting equipment, special clothes for radiation protection, evaluation and analysis means, radiation measuring devices, medical equipment, and means of transport. This material is distributed over different places, some within the nuclear plant and others outside the physical boundaries of the nuclear plant.

The water distribution company also has all the required equipment such as medical equipment, protection equipment, and communication systems, for the safety of the workers and for being able to cope with crises. Furthermore, fire hydrants are within the whole network for the firefighters.

5.2.5 CI Organizational Procedures for Crisis Management

During the prevention stage, the aim of both CIs is to avoid the unfolding of an initiating event into crisis. In order to prevent that, the studied CIs have several procedures such as operating procedures and organizational procedures that help to avoid their escalation. Furthermore, an information system is established in both CIs in other to track all the incidents and gathered lessons learned. They have also developed coordination procedures with external stakeholders such as first responders to be able to efficiently respond when a crisis occurs. In the absorption stage, the aim of CIs is to absorb the impact. Some specific operating procedures assist on achieving this objective. At the organizational level, guidelines provided by the emergency plan should be

carried out. Both, the nuclear plant and the water distribution company have operating and organizational procedures defined for absorbing the impact.

Finally, for the recovery phase, some specific procedures should be defined to facilitate this process. The nuclear plant does not have any specific procedure to this final stage due to the unpredictable characteristic of this period. However, after the Fukushima accident, they have started developing some specific procedures that define the guidelines for this period. In the water distribution company, the steps that should be carried out in the recovery phase are explained in the internal emergency plan.

5.2.5.1 Crisis management procedures

In the nuclear plant, both types of procedures (operating procedures and organizational procedures) can be found. The operating procedures are the following ones: alarm procedures, Operating Procedures (OP), Abnormal Operating Procedure (AOP), Emergency Operating Procedure (EOP), Severe Accident Guideline (SAG). Some of them are used in the prevention stage whereas others are used in the absorption stage. After the Fukushima accident, they are developing new procedures and improving the old ones based on the lessons learned from the accident. Similarly to technical systems, these procedures have been defined taking into account the already identified crises but they lack to provide more general procedures to be applicable for the unplanned situations.

Within the procedures of the organization, there are basically two emergency plans: On-Site Emergency Plan and Off-Site Emergency Plan. Within the On-Site Emergency Plan four different categories have been defined depending on the stage of the crisis (see Table 5.3). Within each category different guidelines are defined for members of each department.

Table 5.5: On-site Emergency Plan categories classified by resilience lifecycle stages.

Resilience lifecycle stages	On-site Emergency Plan categories
Prevention	Category I: Pre-alert
	Category II: On-site alert
	Category III: On-site emergency
Absorption	Category IV: General emergency
Recovery	End of the emergency

Within the Off-Site Emergency Plan there are also some guidelines defined in order to know the actions that each entity should perform in case of a crisis. This plan covers all the stakeholders (internal and external) involved in the crisis management process.

The water distribution company also divides into two types of procedures: operating procedures and organizational procedures. Operating procedures define the guidelines that should be followed in the event of an alarm condition. Regarding the organizational procedures, there is an Internal Emergency Plan where the procedures that should be followed are defined for each possible scenario. This procedure not only considers internal stakeholders but also external ones such as firefighters and police.

5.2.5.2 Incidents management and evaluation

CIs should have an incident reporting system to track all the failures and incidents that occur and to ensure their proper management. Information system can be a useful tool in order to properly manage incidents. Furthermore, this tool allows gathering data after an event in order to assess the management of incidents and defining some improvement areas.

The nuclear plant has a Corrective Action Programme (CAP) implemented in which workers report all the incidents that occur in the nuclear plant in order to identify them, to establish a priority index depending on the severity level, to identify the causes of the incident, to establish responsibility for solving the problem, and a deadline for its resolution. This system allows the nuclear plant to immediately identify a problem and provide a solution as well

as to find improvements for the nuclear plant through the direct involvement of the personnel. Besides, it helps to correct small failures before they accumulate. After a crisis, all the generated documents are analyzed by the operation groups that took part in the emergency resolution to identify improvement areas and lessons learned for the next crises.

The water distribution company also has an incident reporting system to document all the incidents. When an incident is reported in the system, a priority index is established, a responsible is designated, and an indicative deadline is assigned. Afterwards, a follow up is carried out in order to verify that the incident has been completely solved. Furthermore, the causes are deeply analyzed and corrective actions are defined to avoid its occurrence again. A difference compared to the nuclear plant is that in the water distribution company only authorized people have access to the incident reporting system whereas in the nuclear plant, in principle, everyone can access to this system.

5.2.5.3 Coordination procedures with external stakeholders

Within the nuclear plant, there are some procedures defining coordination with the external stakeholders. These procedures determine responsibility for making contact with external agents as well as the corresponding telephone numbers. When a crisis occurs, the nuclear plant should contact the following external agents: local emergency services (hospitals, policy, firefighters, etc.), government organizations (NSC, Local Government, Government department of Nuclear Energy, national power network company, etc.), external technical support organizations (General Electric, Tecnatom, and INPO), and the national Nuclear Plants Association.

In the same vein, the water distribution company has also some coordination agreements with external stakeholders such as firefighters and police. When a crisis occurs the members at the water distribution company have some procedures to communicate with external stakeholders and alert of the problem. The firefighters have all the required information (maps, infrastructure's characteristics, etc.) to efficiently respond in face of a crisis.

5.2.6 CI Top Management Commitment

During the prevention stage, high crisis awareness level of the top management is important to create a resilience based culture among the CI workers. Furthermore, the incentives or promotion activities established to enhance the resilience level of the CIs helps in the detection of early warning signals and responding to them efficiently. For the absorption and recovery stages also a high awareness level of the top management assists in better preparing the workers at the CI to respond to a crisis in the most efficient and rapid way.

5.2.6.1 Top Manager commitment and situation awareness

In both cases, the management seems to be completely committed to the resilience improvement process. In the case of the nuclear plant, they affirmed that the safety of the plant is the every day's preoccupation. In the water distribution company the general manager affirmed us that the safety of the workers is the maximum priority for the company. Furthermore, they are always establishing new measures to promote a resilience based culture within the CI and to reinforce appropriate attitudes and behaviors within the company. They also promote the coordination of several departments to be more prepared for the time when something occurs. Finally, they integrate the crisis management process within the general management of the CI to cover all the organization.

5.2.6.2 Activities to promote resilience based culture

The nuclear plant under study has a reporting system implemented in the organization to collect workers' proposals to improve the safety of the nuclear plant. Furthermore, all the workers at the nuclear plant receive a bonus if at the end of the year the number of suggested proposals is greater than the threshold value. With this system the nuclear plant achieves a high number of proposals to improve the resilience level of the CI.

The water distribution company affirmed that top managers evaluate and appreciate the contributions of the workers in the areas of improvement and maintenance. However, the general manager did not specify how top management promotes this contribution from the workers.

5.2.7 CI Crisis Manager Preparation

In both, the nuclear plant and the water distribution company, the responsibility for crisis management changes from one stage to another. In the case of the nuclear plant, during the prevention stage, the shift manager and the assistant to the shift manager are responsible for ensuring the proper functioning of the reactor and detecting any early warning signal that could lead to a crisis. However, when a crisis occurs, the main responsibility for operating the reactor lies within the Severe Accidents Management Team. In the field of overall management of the organization, the On-Site Emergency Plan director is the main person responsible for preparing the workers and providing training about the On-site Emergency Plan prior to a crisis occurrence. Furthermore, during the absorption and recovery period he has also the main responsibility for establishing measures within the overall management of the organization.

In the case of the water distribution company, during the prevention stage there are two operators at the Control and Monitoring Center controlling the information gathered from the infrastructure and ensuring the proper functioning of it. When they detect an early warning signal, they immediately warn their supervisor of what it happening but they do not make any decision. The supervisor is the one who has the authority to make decisions and he will be in charge of the crisis management.

5.2.7.1 Crisis manager training

The nuclear plant establishes different training programs depending on the crisis manager type. The crisis managers related to operational activities of the nuclear reactor perform basically three types of training activities: training activities in the nuclear plant, seminars, and training with the simulator. The

nuclear plant has a control room simulator which is similar to the normal control room and they carry out different training activities simulating different stages within the crisis management process. These training activities are conducted in five day session, twice a year. The training of the crisis managers related to the overall management of the nuclear plant consists of two types: general emergency training and specific emergency training. All the training activities are related to the On-Site Emergency Plan.

In the water distribution company, operators at the Control and Monitoring Center are the responsible for interpreting the gathered data and detecting early warning signals to avoid a crisis occurrence. These operators receive special training to be able to perform this task. Normally, they are people with previous experience in water purification centers. On the other hand, crisis managers are responsible for operating the distribution network and managing the organization in case of a crisis. They receive training about the response procedures to know how they should act in each case. The general manager affirmed that these response procedures are perfectly known by the crisis managers of the company.

However, both, crisis managers at the nuclear plant and crisis managers at the water distribution company, lack training about the management of unexpected and unplanned situations. They do not perform any training activities to develop their sensemaking skills (Gilpin and Murphy, 2008) despite their importance in the current context where crises might create unpredictable situations and no procedure might be suitable to handle them.

5.2.7.2 Crisis manager situation awareness and commitment

Based on the direct observations carried out in the nuclear plant and on the interviews with managers, we concluded that crisis managers at the nuclear plant are constantly aware of the possible incidents that could lead to a crisis. Furthermore they develop their skills to be able to understand the implications of the early warning signals and also to anticipate any threat that could unfold during a crisis. Crisis managers are committed to the resilience of the CI and

they are aware of the risk inherent in the company and their responsibility in avoiding a crisis.

Crisis managers and operators controlling the proper functioning at the water distribution company are also aware of the importance of detecting incidents in order to avoid their escalation or even anticipating them. The general manager confirmed us that crisis managers are perfectly aware of their responsibility and the top management also reminds them continuously to ensure their alertness. They are also committed to the resilience building process because they are aware of the importance of adequate water distribution service for the welfare of society.

5.2.8 CI Operator Preparation

Prior to the crisis occurrence, the aim of both CIs is to train operators to respond efficiently when a crisis occurs. Furthermore, during the prevention stage, operators at the CIs are constantly aware of any little incident that could lead to a crisis. When a crisis strikes, operators at the nuclear plant and water distribution company are prepared to carry out the emergency procedures to respond in the most appropriate and rapid way.

5.2.8.1 Operator training

The nuclear plant provides two type of crisis management training to the operators. Initially, extensive training is provided to new operators at the CI. Afterwards, operators receive continuous training to update their crisis management skills. The training provided to the operators develops the following topics: labor risk prevention, human factors, safety based-culture, and general emergency management. Furthermore, operators in direct contact with the nuclear reactor receive special training about the management of the nuclear reactor in an emergency situation. Finally, once a year, general simulation exercises are carried out to put into practice the emergency procedures learned in the training courses.

In the case of the water distribution company, they develop a training plan taking into account the company needs every year. Most of the times these training activities are more focused on productivity issues rather than on management of crises. However, every year they perform the most important table-top and training exercises such as the ones for the case of chlorine leakage.

5.2.8.2 Operator situation awareness and commitment

Operators at the nuclear plant are encouraged to propose new ideas or measures that help to improve the resilience level of the CI. Around 30% of the workers propose new improvement measures every year.

The general manager at the water distribution company ensured that operators are committed to the improvement of resilience and aware of the importance of having a safe and reliable infrastructure for the welfare of society.

5.2.9 CI Crisis Response Budget

During the prevention stage the nuclear plant collects the monetary resources or takes out insurance policies to ensure the monetary resources for the time something occurs. When a crisis occurs, these monetary resources are allocated or the previously hired insurance company covers the costs of response and recovery activities. In the case of the nuclear plant almost all the CI is covered by insurance companies.

The case of the water distribution company is different since this company is public. When a crisis occurs, monetary resources are gathered from the local government so prior to the crisis they do not collect money for the response. Furthermore, most of the important elements at the distribution network are covered by insurance companies. The general manager explained to us that money is not usually a problem; first they respond and then they analyze who should pay for it.

5.2.10 External Crisis Response Equipment

In the case of the nuclear plant, the collection and coordination of the external equipment is carried out from the Operative Coordination Center of the Local Government Representation Department. Furthermore, they can acquire more technical resources through the Nuclear Emergency Plan for Response and Support. The technical resources required by external agents are defined within the Off-Site Emergency Plan. This plan specifies the resources and equipment needed to properly respond to a crisis. Furthermore, the nuclear plant can collect more equipment through the national Nuclear Plants Association.

In the case of the water distribution company, the coordination of this equipment is done by the local first responders group. When a crisis occurs, the water company informs first responders about the situation and they are the ones who allocate the necessary resources to respond efficiently.

5.2.11 First Responder Preparation

The nuclear plant has six fire fighters, one doctor, four nurses, and one person from the radiological protection area permanently at the nuclear plant. In addition to this, four workers from the operation department are also fire fighters. The plant trains military, police, fire fighters, and civil protection workers periodically in order to show them the layout of the CI and the procedures they should carry out when something occurs. The training of the rest of the first responders is carried out through the Off-site Emergency Plan.

In the water distribution company there are no first responders permanently on-site. However, they have direct contact with them. Fire fighters have all the information and design drawings about the distribution network and its peculiarities, and they know perfectly how they should act when something occurs. They have several response procedures in order to know how they should respond when a crisis occurs.

5.2.11.1 First responder training

Through training activities developed within the nuclear plant, first responders gather knowledge in the following aspects:

- Nuclear accident characteristics.
- Off-site emergency plan procedures and the reactor operating procedures that should be carried out if the core is damaged.
- Equipment and resources that should be used during the resolution period.
- Physical preparation needed to respond efficiently to the crisis occurrence.

Table-top simulation exercises put into practice all the knowledge gathered in the training courses. There are partial simulations every year, a general simulation every three years, international exercises and simulation when Civil Protection and Nuclear Security Council (NSC) require them, and application of the Off-Site Emergency Plan every two years.

The water distribution company provides specific training regarding its infrastructure, the layout, and special characteristics to first responders. When updates are introduced in the network first responders are immediately informed in order to have updated information. However, they do not performed table-top exercises at regular intervals.

5.2.11.2 First responder situation awareness and commitment

Through training courses and simulations, both the nuclear plant and the water distribution company work to achieve high awareness and commitment levels of the first responders in order to be ready when a crisis occurs. This information was gathered in both cases based on our interviews with managers and operators.

5.2.12 Government preparation

In the nuclear sector, the government has a specific group called the national Nuclear Security Council (NSC) to control and manage the safety of the nuclear industry. During the prevention stage, NSC verifies the proper state

of the nuclear plant through several audits and revisions of the CI. Members of the council are prepared to know how they should manage a crisis when this occurs since they are responsible for leading it in case of a serious crisis. In the water sector, the government does not have such a specific group to control the safety of the water distribution companies.

During the absorption and recovery stages, the government has to manage, coordinate and lead the response and recovery activities. The government should communicate to the society and ameliorate public anxiety through appropriate activities.

5.2.12.1 Government situation awareness and commitment

Unfortunately, lacking government contacts, we obtain very little evidence about how this is implemented in these particular cases. In the case of the nuclear plant, managers affirmed us that workers from NSC are aware of crisis occurrence and committed with the safety issues. They are always preoccupied with failure and implementing new measures to improve the resilience of nuclear plants. In the case of the water distribution company, the general manager admitted that he did not know about how far the government is committed and aware of the importance of properly managing crises.

5.2.12.2 Government training

The group of experts within the government should provide training courses to the heads of governance and also to the CIs in order to be well prepared if a crisis occurs.

The national NSC is the entity in charge of managing nuclear crises within the Government. This entity is responsible for ensuring proper crisis management measures within the nuclear plant and external entities. When a crisis occurs, it is accountable for managing the crisis and responding to it efficiently. Furthermore, the government has developed an Off-Site Emergency Plan to establish the actions and procedures that should be carried out when a crisis occurs. This plan has different situations depending on the severity level

of the crisis. Table 5.6 relates the categories defined within the On-Site Emergency Plan and the situations identified within the Off-Site Emergency Plan.

Table 5.6: Relationship among the categories within the On-Site Emergency Plan and situations within the Off-Site Emergency Plan.

On-Site Emergency Plan	Off-Site Emergency Plan
Category I: Pre-alert	Situation 0
Category II: On-site alert	Situation 1
Category III: On-site emergency	Situation 2
Category IV: General emergency	Situation 3

For each situation the emergency measures and actions that should be performed within the nuclear plant are defined (see Table 5.7).

In the water sector the government lacks to have a group of experts in this field. However, the water distribution company is a public company; therefore, the company is in direct contact with the government and they are the experts who provide knowledge and advice to the government about the decisions and actions that should be carried out.

Table 5.7: Examples of emergency measures and emergency actions that are implemented in each situation.

	Emergency Measures	Emergency Actions
Situation 0		• Notification and verification of the incident • Declaration of Situation 0 • etc.
Situation 1	• Warn the population • Access control • Response personnel control • Eviction of schools • etc.	• Evaluation and emergency proposals • Activation of Off –Site Emergency Plan • Accreditation and classification of response agents • etc.
Situation 2	• Citizen security and surveillance • Health care and urgent social assistance • Food and water control • etc.	• Emergency evaluation and follow-up • Rotation of response personnel • Operational integration of the means and extraordinary resources • etc.
Situation 3	• Special health care for the personnel in response activities • Evacuation and shelters • Classification and decontamination of people and equipment • etc.	• Evaluation and emergency proposals • Rotation of response personnel • Operational integration of the means and extraordinary resources • etc.

5.2.12.3 Government communication capacity

The group of experts within the government should constantly advise the communication department about how often and what content should be communicated (Carrel, 2000).

The communication strategies are defined by the head of the press section of the Government Representation Department. In the case of the nuclear plant, the NSC advises and provides the necessary support to the government to properly communicate the situation to the society and lead in case of a crisis. After the Fukushima accident, several lessons learned were gathered to improve the communication process such as reinforcement of the society's trust, increase the credibility of regulatory governments, development of communication plans, and implementation of new communication technologies.

In the water distribution company, the company itself is the one who provides the necessary support and advice to properly communicate the situation to the society and to cope with crises. The general manager admitted us that he was unaware of any Government's communication plan.

5.2.12.4 Government leadership capacity

In the case of the nuclear plant, the government takes decisions based on the advice and recommendations provided by the NSC. The NCS is the most knowledgeable group in the nuclear sector and nuclear accidents, therefore, government's decisions are based on the suggestions from the NCS. In the case of the water distribution network, the company itself is the one who provides help to the government.

5.2.12.5 Coordination of the response agents

When a crisis occurs at the nuclear plant, the entities taking part in the crisis management process are basically the following ones: government delegates, head of the press section of the government, members of the NSC to assess technical and organizational aspects, representatives of civil protection,

and first responders. The coordination of these entities that take part in the crisis response is carried out through several procedures defined in the Off-site Emergency Plan.

However, when a crisis occurs in the water distribution company, the emergency department of the government is the one who would coordinate all the entities taking part in the resolution.

5.2.13 Trusted Network Community

The nuclear plant is involved in a community where many national and international nuclear associations also take part, such as the national Nuclear Plants Association, World Association of Nuclear Operators (WANO), and the International Atomic Energy Agency (IAEA).

The water distribution company is member of the Association of Water Supply and Sanitation of its country and it has collaboration agreements with other water distribution companies of the same country.

5.2.13.1 Shared information systems and databases

The nuclear associations share information through their web sites to the nuclear plants. The national nuclear plants, however, share information through NSC which is responsible for updating all the lessons learned based on occurred events.

The Association of Water Supply and Sanitation is the one who shares information and knowledge through their web-sites or through the telephone. When water distribution companies need some information or advice they come to this association and this association suggests them the best alternative.

5.2.13.2 Trust and engagement of the participants

Within the nuclear plant there is a department called Operational Experience which is responsible for sharing and gathering information and lessons learned with external stakeholders and other nuclear plants. They share

knowledge not only with the nuclear associations but also with the rest of the nuclear plants involved in the community. Furthermore, they periodically organize some workshops with all the members of the community in order to discover new improvement areas. However, there is little information sharing with first responders.

The water distribution company usually does not share any experience or lessons learned with other companies. However, at one point, if the company needs to ask for some information to another company or someone asks them for some knowledge they do not usually have any problem to share experiences. Regarding first responders, they are in permanent contact to share all the information about the distribution network and its updates.

5.2.14 Crisis Regulation and Legislation

The group of experts within the government is often responsible for developing the regulations and updating them. In the case of the nuclear plant, the NSC is responsible for developing the specific regulations for the national nuclear industry.

In the case of the water, the government does not have such a group of experts to develop specific regulations and the government is responsible for defining the regulations and laws. In this field, the regulation is focus on water quality, critical components certification, and workers safety.

5.2.14.1 Regulations and laws revision and update

The nuclear sector is a high-risk sector and therefore, safety is of prime importance. This is very well known by the companies and regulators that work in this field. Therefore, they are constantly updating the laws and regulations based on lessons learned from incidents and crises. In the case of the water distribution sector, the laws and regulations are also updated and reviewed periodically taking into account lessons learned from incidents and crises.

5.2.14.2 Compliance level of regulations and laws

In order to ensure that regulations and laws are fulfilled by the CI, in the case of the nuclear plant, an inspector of NSC works full-time in the nuclear plant checking the compliance level. On the contrary, in the case of the water distribution company, there are no on-site inspections and the general manager told us that in principle there is no penalization for not fulfilling the law or the regulation.

5.2.15 Public Crisis Response Budget

This research could not obtain evidence about this policy since public economic issues were unknown for the members of the nuclear plant and water distribution company and we had no opportunity to contact a public member who could give information about this policy.

5.2.16 Societal Situation Awareness

Not only should the government and first responders prepare to handle crises but society can also play an important role in crisis resolution (Committee on Increasing National Resilience to Hazards and Disasters, 2012). Society's awareness and commitment level towards avoiding a crisis occurrence reduces crisis probability and reduces the magnitude of the impact, with better ability to respond (Shaw et al., 2009). Not only during the prevention stage, but also in the absorption and recovery stages the societal crisis awareness level is important to manage crises efficiently.

5.2.16.1 Societal situation awareness and commitment

CIs should inform the society about the risks and should commit the people to help in a crisis management process.

The nuclear plant establishes a plan to continuously communicate with the surrounding community in order to provide real data regarding the safety and reliability level. They also provide evidence about the fulfillment of all the regulatory and legislation issues. Furthermore, to increase the commitment

level of the society and to obtain help from the society when it is required, the nuclear plant performs some social activities and helps in the economic development of the surrounding community such as solidarity activities, development of social environment, and training and education programs.

During the last years, the water distribution company has made a significant effort in changing the culture of water. Before, society was not aware of the importance of water preserving and care. The consumption was much higher and people were not aware of the limitation of this resource. In light of this situation, the water distribution company started providing some training courses about the scarcity and importance of this resource. Now, society is more aware and they take care of its consumption leading to the prevention of incidents and crises. The general manager confirmed that the number of incidents has considerably decreased in the last ten years.

5.2.16.2 Societal training

The CIs should provide training courses to the community regarding how they should behave to prevent crises or help when dealing with crisis. The nuclear plant develops some training activities within the surrounding community in order to prepare it in case something occurs.

In the case of the water distribution company, they provide training regarding the functioning of the water supply and sanitation system and as a result, they commit society with this system. They have a small company which is in charge of providing these training courses to schools, government members, retiree groups, etc. Furthermore, when the water distribution company has to interrupt the water service due to maintenance activities, they warn users about this interruption so that users are able to take appropriate measures.

5.3 Differences between the two case studies

Both case studies present very different CIs with different characteristics regarding the resilience concept. Concerning the infrastructure, in the case of the nuclear plant, the whole plant is concentrated in one geographical area whereas in the case of the water distribution company, the distribution network is dispersed through the whole province. Therefore, implementing some measures can be quite costly in the case of the water distribution company. For example, in the case of the nuclear plant almost all the safety systems have the water supply lines duplicated. However, in the water distribution company, the supply tubes from dams to purification centers and from purification centers to water tanks are not duplicated because the cost would be prohibitive. In both cases, the dependency towards power supply is large and vital for the proper functioning of the CI. Therefore, both companies have several redundant power supply systems to be able to face a power outage. Data acquisition and monitoring systems are also very similar in both cases, since information can be monitored in more than one place, the data is continuously saved, and there are alarms and suitable interfaces to better interpret the data.

Regarding organizational resilience within the CI, there is one main difference between both cases. In the nuclear plant all the workers at the CI receive training courses regarding the emergency plans and procedures in case a crisis occurs. In the case of the water distribution company the operators do not receive training and do not know about the emergency plan; only managers are trained to know how the organization should act when a crisis occurs. Something similar happens with the incidents management and evaluation sub-policy. All the workers at the nuclear plant can report an incident in the system whereas only authorized people are able to do it in the water distribution company.

There are also some important differences in the external resilience. Both cases have strong relationship with first responders. In the case of the nuclear plant some of them are even on-site in order to be able to respond immediately. However, in the case of the water distribution company, they do not perform

table-top exercises or simulations with first responders in order to train for the time a crisis occurs whereas in the case of the nuclear plant they do every year.

Finally, another important difference lies in the ownership of the company. The water distribution company is a public company whereas the nuclear plant is a private company. The government is part of the water distribution company whereas in the case of the nuclear plant the government is an external entity which has no control in the management of the plant. Therefore, the government has its own group of experts in the field of the nuclear sector in order to verify the proper functioning of the nuclear plants and advice the government in times of crisis. In the water field, the government does not have such a group because the plant is public and the members can help and advise in times of crises.

5.4 Discussion of the validation process

As we highlighted at the beginning of this chapter, the aim of this validation process was to assess the completeness, usefulness, and relevancy of the resilience framework. During the validation process, we were able to classify all the resilience building measures and activities that the CIs perform in the framework. All the safety systems, procedures, commitment activities, etc. were perfectly classified in the framework. There was no evidence which could not be classified in the framework; therefore, the completeness of this framework was validated.

Regarding the usefulness characteristic, this validation process has proved that the resilience framework for CIs can provide value to the CIs. In both cases, based on the defined policies and sub-policies, we were able to make some observations and detect some improvement areas to enhance their resilience level.

In the case of the nuclear plant, they are mostly focused on improving the management of already identified hazards reducing their risk probability through improving the technical aspects of the infrastructure and preparing and establishing well defined response and protection procedures for handling

them. They evaluate their capacity to deal with crises assessing the probability of occurrence of already plan critical situations. However, they do not evaluate their overall capacity to cope with crises. Our framework made aware them that they also need to take into account unexpected and unpredictable situations. Therefore, they need also to evaluate their overall capacity to prevent and rapidly absorb a crisis. Furthermore, there were no evidence about how crisis managers and operators develop and train their sensemaking capacity to be able to properly act in unknown situations making decisions without much information and in a stressful situation and using their knowledge in a novel way.

In the case of the water distribution company, more improvement areas were defined. In this case also, they are mostly focused on enhancing the management of known crises without paying too much attention to the preparation of unpredictable crises. Furthermore, although the coordination procedures with external stakeholders are defined, they do not perform any training activities or simulation exercises. Finally, the regulatory and legislation aspects are very "soft" and not precisely defined comparing with the nuclear industry and external audits regarding crisis management issues, are only performed at the start-up of the company.

All this improvement areas were communicated to the managers of both companies and they admitted us that these comments were very useful for them because they made them to think about their current situation and found out new improvement areas to enhance their resilience level. Therefore, the usefulness of this framework to improve the CIs' resilience level was also validated through the case studies.

Finally, this validation process also proved that this framework provides relevant policies and sub-policies to enhance the resilience level. During the case studies, we were able to gather evidence and examples for all the resilience policies and sub-policies. In some of them they have only implemented basic level activities and our framework helps them to find additional improvement areas to improve their resilience level. Therefore, we can conclude that all the

defined resilience policies and sub-policies are relevant to resilience building process and they are applicable in CIs to improve their resilience level.

5.5 Conclusion

Validation determines whether the developed model of framework is adequate to fulfill the defined objective. In our case, the aim of the resilience framework for CIs is to help crisis managers to improve CIs' resilience level taking into account internal and external stakeholders. In order to validate that this framework supports this purpose we evaluated the following three characteristics which are completeness, usefulness, and relevancy through case studies in two different CIs.

The case studies demonstrated that the framework covers all the resilience building activities and highlighted the relevancy of the defined resilience policies and sub-policies to improve the resilience of CIs. Furthermore, these studies affirmed the framework helps to provide insights and improvement opportunities to enhance their resilience level.

However, this validation has also some limitations, especially when providing evidence and examples for external policies. The research was carried out within CIs where we had little contact with external agents. Therefore, there are some sub-policies with little evidence due to the lack of information. Besides, in the case of the water distribution company we were only able to gather information from only one source (interviews with the general manager). Despite the limitations, we consider that this validation confirms the suitability of this resilience framework for CIs to improve the resilience level of the CIs.

6 Conclusions, Limitations and Future Research

This chapter sums up the main results obtained in this research and how the initial objectives have been reached. The process and the outcomes obtained for each sub-objective have been resumed in order to explain the conclusions. Furthermore, it presents the limitations of this research regarding the development and the gathered results, and proposes future steps to address these constraints and improve the resilience framework for CIs.

6.1 Conclusions

CIs are essential for the welfare and proper functioning of the society. Several approaches have been developed in the literature regarding the reliability and safety of CIs. Crisis management has been usually focused on establishing very rigid and specific plans and procedures to prevent crises and respond to them in the most efficient way. However, several recent crises have warned us about the unpredictable consequences of the current crises due to globalization issues, tight interdependences, and the lack of efficiency of the previously defined procedures. Furthermore, crises are even more severe when a CI is affected since they underpin the social and economic sustainability of the society.

Therefore, not only should CIs prepare to face planned triggering event but they also need to prepare for being able to cope with unexpected and unpredictable situations. Resilience provides this adaptive capacity to ensure the safety and reliability of CIs in this complex environment. This research defines resilience as the capacity of a system to prevent a crisis occurrence, absorb the impact when the crisis occurs, and recover to the normal state rapidly. Thus, the aim of crisis managers has become to improve the system's resilience level.

Literature defines several frameworks to define resilient systems' characteristics and to improve the resilience level of systems. However, most of them present some limitations. Some of them just focus on organizational aspects without taking into account other resilience dimensions. Others only concentrate on internal aspects not paying attention to the external involved entities. Furthermore, most of the approaches lack to provide a detailed prescription about what activities (applicable in practice) should be implemented in a system in order to improve the system's resilience level.

In light of this situation, this research aims to provide a holistic framework to improve the CIs' resilience level. This framework has been developed taking into account internal and external stakeholders that are involved in a crisis and covering the four resilience dimensions defined in the literature (technical,

organizational, economic, and social). Furthermore, the policies and sub-policies defined in the framework are applicable in practice to facilitate the implementation of this framework.

In order to reach this main objective, several sub-objectives were defined. Following how each sub-objective has been accomplished is described.

6.1.1 Resilience concept: definition, types and dimensions.

This research defines resilience as a capacity of a system to prevent a crisis occurrence, and when a crisis occurs, the capacity to absorb the impact and recover rapidly to the normal state. In turn, this research characterizes three resilience lifecycle stages: prevention, absorption, and recovery.

This research is focused on major industrial accidents which have been defined as crises that start in a CI and spread through the whole CI network affecting also the society. Therefore, two resilience types have been defined dividing the resilience level of the CI where the triggering event occurs (internal resilience) from the resilience level of the rest of the external involved agents (external resilience). Furthermore, within each resilience type several resilience dimensions have been identified based on the literature. In this way, the first sub-objective was achieved and we established the bases for our research.

6.1.2 Resilience policies and sub-policies

The aim of this research is to provide a framework to improve the CIs' resilience level. In order to achieve this objective, sixteen resilience policies have been defined. These policies have been classified based on the previously defined resilience types and dimensions. Furthermore, in order to better determine the scope and the description of each resilience policy, several sub-policies have been determined for some policies.

The resilience policies have been determined holistically taking into account internal and external stakeholders and covering the four resilience dimensions. Furthermore, they have been defined very closely related to the

general management of CIs in order to facilitate their implementation in practice. These policies and sub-policies were defined based on experts' knowledge and analysis of multiple case studies. Furthermore, the defined policies and sub-policies have been related to other frameworks that have been defined in the literature.

Finally, the examples and evidence about how this set of policies and sub-policies can be implemented in a CI were gathered through two case studies in two CIs. These case studies also allow validating the completeness, usefulness, and relevancy of these policies and sub-policies to improve the CIs' resilience.

6.1.3 Influence of the resilience policies on the resilience lifecycle stages

Once the resilience policies were defined the influence of each policy on the three resilience lifecycle stages was assessed. Some policies influence mostly preventing a crisis occurrence whereas others influence more in the recovery stage. Through the Delphi method the influence of each policy in the three resilience lifecycle stages (prevention, absorption, and recovery) was evaluated by experts. An influence table was developed in order to summarize the results gathered from the experts. The main conclusion gathered from this study was that during the prevention stage the internal policies are the most influential ones avoiding a crisis occurrence whereas during absorption and recovery stages, both internal and external policies influence bouncing back to the normal state. The study also presents some disagreements among some experts regarding the influence of some policies.

This study provides important insights to the crisis managers about the level of influence of each resilience policy and helps them to improve their knowledge regarding resilience aspects and to better understand the resilience framework.

6.1.4 Implementation methodology of the Resilience Framework for CIs

Finally the implementation methodology was defined to efficiently implement this framework in practice. The methodology was developed

through experts' knowledge gathered through a survey. First, in order to efficiently implement each resilience policy, the temporal order in which the sub-policies should be implemented for each policy was determined. Then, a five-step implementation methodology was defined to describe the temporal order in which the resilience policies should be implemented. In the first step two policies are implemented. In the second step, two new policies are added to the previous ones. In the third stage, five new policies are introduced to the ones which have already been implemented. In the fourth stage, three new policies are implemented and in the last one the last four policies are introduced.

This methodology facilitates the implementation of the framework since not all the policies can be implemented at the same time. Furthermore, some policies require others prior implementation. Therefore, this methodology also allows implementing the framework in the most efficient way.

6.2 Limitations of this research

Although the overall goal was achieved, this research presents several limitations. Below, we present the most important limitations.

- This framework aims to be applicable for all CIs, therefore, it presents aggregated resilience policies and sub-policies. When implementing this framework in a specific CI, it needs to be particularized to the specific case and more detailed policies should be defined. Furthermore, the influence of the resilience policies on the three resilience lifecycle stages can differ from one CI to other.
- The list of CIs can vary from one country to another one. There are some sectors which are considered critical in Europe but not in USA such as research sector, and vice versa. Therefore, these differences difficult the identification and explanation of some policies since they might not be suitable for some particular sectors.
- This research has shown that experts might disagree regarding the influence of some resilience policies on the three resilience lifecycle stages.

Experts from some sectors believe that some policies influence more on the prevention stage whereas others think that these policies influence more on the absorption and recovery stages. Therefore, it would be interesting to pursue this diversity of opinion further. The influences also may vary from one sector to other, therefore, specific influence table for each sector might be developed to better represent the reality.

- The resilience framework presents a qualitative approach to improve resilience. The resilience policies and sub-policies define qualitatively the areas which should be improved and the activities that should be carried out to improve the resilience level of CIs. However, it lacks to provide metrics and indicators to assess the resilience level or even to evaluate the improvement of the applied measures.
- The validation phase also presents some limitations especially when providing evidence and examples for external policies. The research was carried out within two CIs (a nuclear plant and a water distribution company) and therefore, we had little contact with external agents. Therefore, there are some sub-policies in the external resilience with little evidence.
- The implementation methodology was developed based on the information gathered from experts through a survey. However, there has not been applied this methodology in practice for the implementation of the resilience policies and sub-policies in a CI.

6.3 Future Research

Based on the limitations of this research, this investigation proposes several steps to perform in the future in order to improve the resilience framework for CIs.

- In order to provide a more quantitative approach for diagnosing and improving the resilience level of CIs, several metrics and indicators should be defined in order to evaluate the resilience policies and sub-policies. Some general metrics and indicators can be defined, but then, due to the

different nature of CIs, specific metrics should be identified for each particular case. This approach would allow evaluating the current resilience level of the CI and also assessing the enhancement provided by applied measures.

- It would be also interesting to know the reason for the diversity of opinions among different sectors on the influence level of some policies on the three resilience lifecycle stages. These arguments might lead to define several influence tables depending on the CI's sector. Therefore, a deeper analysis needs to be performed to better define the influences of the policies on the three resilience lifecycle stages.
- Although the temporal order in which the sub-policies and policies should be implemented has been defined, the relationships among them have not been determined. As a future research, it would be interesting to determine for each policy which ones should be implemented beforehand to efficiently implement this one and which ones would require this policy's implementation to achieve the highest efficiency. Knowing these relationships would provide more insight to the implementation methodology and would provide more flexibility when implementing the resilience framework.
- It would also be important to gather more evidence and examples about how the resilience policies and sub-policies can be implemented in a CI. Having more examples and evidence would facilitate crisis managers the implementation of this framework in practice and would also provide a broader range of alternatives for different kind of CIs. Furthermore, having more evidence and examples would increase the confidence of crisis managers in this framework.
- In order to quantitatively justify the costs of improving the resilience level of CIs, how a good resilience level might reduce the impact of a crisis should be analyzed. Most of the times the benefits of having resilient CIs does not come to light since crises rarely occur. Therefore, resilience building activities have to compete for resources against profit-driven activities which provide immediate results. Assessing the benefits of having

a good resilience level would allow justifying the costs and facilitating the obtaining of resources.

- Finally, through empirical research, the implementation methodology should be applied in practice in order to gather information about its usefulness and correctness. One way could be implementing this framework in a CI from the beginning until a high resilience level is achieved and analyzing the process and improvement points. Another way could be gathering information from resilient CIs about the order in which these policies were implemented and analyzing the errors and improvement areas to enhance the implementation methodology. However, as can be seen in these two examples, empirical research could take several years in order to obtain interesting results.

References

Agency for Healthcare Research and Quality (2008) *Becoming a High Reliability Organization: Operational Advice for Hospital Leaders.* U.S. Department of Health and Human Services. Rockville, USA.

Alexander, D. (2002) *Principles of Emergency Planning and Management*, Oxford University Press, Oxford.

Andersen, D.F., Richardson, G.P. and Vennix, J.A.M. (1997) Group model building: Adding more science to the craft, *System Dynamics Review*, Vol. 13, No. 2, pp. 187-201.

Andersen, D.F., Vennix, J.A.M., Richardson, G.P. and Rouwette, E.A.J.A. (2007) Group Model Building: Problem structuring, policy simulation and decision support, *Journal of the Operational Research Society*, Vol. 58, No. 5, pp. 691-695.

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C. and Vittal, V. (2005) Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance, *IEEE Transactions on Power Systems*, Vol. 20, No. 4, pp. 1922-1928.

Auerswald, P., Branscomb, L.M., La Porte, T.M. and Michel-Kerjan, E. (2005) The challenge of protecting critical infrastructure, *Issues in Science and Technology*, Vol. 22, No. 1, pp. 77-80.

Barr, R. (2010) Iceland's volcanic ash halts flights across Europe, *The Guardian*. Available at: http://www.guardian.co.uk/world/feedarticle/9032564.

Bedford, T. and Cooke, R. (2001) *Probabilistic risk analysis: foundations and methods*, Cambridge University Press, .

Boin, A. (2009) The new world of crises and crisis management: Implications for policymaking and research, *Review of Policy Research*, Vol. 26, No. 4, pp. 367-377.

Boin, A. (2004) Lessons from crisis research, *International Studies Review*, Vol. 6, No. 1, pp. 165-194.

Boin, A., Hart, P., Stern, E. and Sundelius, B. (2005) *The Politics of Crisis Management: Public Leadership under Pressure*, Cambridge University Press, Cambridge.

Boin, A., Lagadec, P., Michel-Kerjan, E. and Overdijk, W. (2003) Critical infrastructures under threat: Learning from the anthrax scare, *Journal of Contingencies and Crisis Management*, Vol. 11, No. 3, pp. 99-104.

Boin, A. and McConnell, A. (2007) Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience, *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 50-59.

Boin, A. and Schulman, P. (2008) Assessing NASA's Safety Culture: The Limits and Possibilities of High-Reliability Theory, *Public administration review*, Vol. 68, No. 6, pp. 1050-1062.

Boin, A. and Van Eeten, M.J.G. (2013) The Resilient Organization, *Public Management Review*, Vol. 15, No. 3, pp. 429-445.

Briguglio, L., Cordina, G., Farrugia, N. and Vella, S. (2009) Economic vulnerability and resilience: Concepts and measurements, *Oxford Development Studies*, Vol. 37, No. 3, pp. 229-247.

Broad, W.J. (2011) Scientists project path of radiation plume, *New York Times*. Available at: http://www.nytimes.com/2011/03/17/science/17plume.html?_r=0.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W. and von Winterfelt, D. (2003) A framework to quantitatively assess and enhance seismic resilience of communities, *Earthquake Spectra*, Vol. 19, pp. 733-52.

Brunner, E.M. and Suter, M. (2008) *International CIIP Handbook 2008/2009*. Center for Security Studies. ETH Zurich.

Brunsdon, D. and Dalziell, E. (2005) Making Organisations Resililent: Understanding the Reality of the Challenge. *Proceedings of the Resilient Infrastructure Conference*, pp. 27-34, Rotorua.

Carrel, L.F. (2000) Training civil servants for crisis management, *Journal of Contingencies and Crisis Management*, Vol. 8, No. 4, pp. 192-196.

Coleman, L. (2004) The Frequency and Cost of Corporate Crises, *Journal of Contingencies and Crisis Management*, Vol. 12, No. 1, pp. 2-13.

Commission of the European Communities (2005) *Green Paper on a European Programme of Critical Infrastructure Protection*. Brussels.

Committee on Increasing National Resilience to Hazards and Disasters (2012) *Disaster Resilience: A National Imperative*. The National Academies Press. Washington, D.C.

Cooke, D.L. and Rohleder, T.R. (2006) Learning from incidents: from normal accidents to high reliability, *System Dynamics Review*, Vol. 22, No. 3, pp. 213-239.

Coombs, W.T. (2007) *Ongoing Crisis Communication: Planning, Managing and Responding*, 2 ed., SAGE publications, Thousand Oaks, CA.

Crichton, M.T., Ramsay, C.G. and Kelly, T. (2009) Enhancing Organizational Resilience Through Emergency Planning: Learnings from Cross-Sectoral Lessons, *Journal of Contingencies and Crisis Management*, Vol. 17, No. 1, pp. 24-37.

Croom, S. (2009) Introduction to Research Methodology in Operations Management. In Karlsson, C. (Eds.), *Researching Operations Management*, pp. 42-83. Routledge: Taylor & Francis, Inc., New York.

Cutter, S.L., Burton, C.G. and Emrich, C.T. (2010) Disaster Resilience Indicators for Benchmarking Baseline Conditions, *Journal of Homeland Security and Emergency Management*, Vol. 7, No. 51.

Dalkey, N. (1969) An experimental study of group opinion, *Futures*, pp. 408-426.

De Bruijne, M. and Van Eeten, M. (2007) Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment, *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 18-29.

De Bruijne, M.L.C. (2006) *Networked reliability: institutional fragmentation and the reliability of service provision in critical infrastructures*, Faculty of Technology, Policy and Management, Delft University of Technology, Netherlands.

Delbecq, A.L., Van de Ven, A.H. and Gustafson, D.H. (1975) *Group techniques for program planning: A guide to nominal group and Delphi processes*, Scott, Foresman and Co., Glenview, IL.

Dempsey, J. and LaFraniere, S. (2011) In Europe and China, Japan's Crisis Renews Fears About Nuclear Power, *New York Times*. Available at: http://www.nytimes.com/2011/03/17/business/global/17atomic.html?pagewanted=all.

Drennan, L. and McConnell, A. (2007) *Risk and Crisis Management in the Public Sector*, Routledge, New York.

Dugdale, J., Bellamine-Ben Saoud, N., Pavard, B. and Pallamin, N. (2009) Simulation and Emergency Management, *Information Systems for Emergency Management*, Vol. 16, pp. 229-253.

Egan, M.J. (2007) Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems, *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 4-17.

Elwood, A. (2009) Using the disaster crunch/release model in building organisational resilience, *Journal of Business Continuity & Emergency Planning*, Vol. 3, No. 3, pp. 241-247.

Eusgeld, I., Nan, C. and Dietz, S. (2011) "System-of-systems" approach for interdependent critical infrastructures, *Reliability Engineering & System Safety*, Vol. 96, No. 6, pp. 679-686.

Farrell, A.E., Lave, L.B. and Morgan, G., 2002. Bolstering the security of the electric power system, http://www.issues.org/18.3/farrell.html.

Fearn-Banks, K. (2007) *Crisis Communications: A casebook approach*, 3rd ed., Erlbaum, Mahwah, NY.

Fink, S. (1986) *Crisis management: Planning for the inevitable*, AMACOM, New York.

Forza, C. (2002) Survey research in operations management: a process-based perspective, *International Journal of Operations & Production Management*, Vol. 22, No. 2, pp. 152-194.

Gibson, C.A. and Tarrant, M. (2010) A 'conceptual models' approach to organisational resilience, *Australian Journal of Emergency Management*, Vol. 25, No. 2, pp. 6-12.

Gilpin, D.R. and Murphy, P.J. (2008) *Crisis Management in a Complex World*, Oxford University Press, Oxford.

Hall, J. (2010) Volcanic ash cloud leaves shops facing shortages of fruit, vegetables and medicine, *The Telegraph*. Available at: http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/7599042/Volcanic-ash-cloud-leaves-shops-facing-shortages-of-fruit-vegetables-and-medicine.html.

Hämmerli, B. and Renda, A. (2010) *Protecting Critical Infrastructure in the EU*. Centre for European Policy Studies, Brussels.

Hernantes, J., Labaka, L., Laugé, A. and Sarriegi, J.M. (2012a) Group Model Building: A collaborative modelling methodology applied to Critical Infrastructure Protection, *International Journal of Organizational Design and Engineering*, Vol. 2, No. 1, pp. 41-60.

Hernantes, J., Labaka, L., Laugé, A. and Sarriegi, J.M. (2012b) Three complementary approaches for crisis management, *International Journal of Emergency Management*, Vol. 8, No. 3, pp. 245-263.

Holling, C. (1973) Resiliency and stability of ecological systems, *Annual Review of Ecological Systems*, Vol. 4, pp. 1-24.

Hollnagel, E. (2011) Prologue: the scope of resilience engineering. In Hollnagel, E. et al. (Eds.), *Resilience Engineering in Practice*, pp. xxix-xxxix. Ashgate, Farnham, England.

Hollnagel, E., Woods, D.D. and Leveson, N. (2006) *Resilience Engineering: Concepts and Precepts*, Ashgate, .

Hopkins, A. (2007) *The Problem of Defining High Reliability Organisations.* National Center Research for OHS Regulation. Camberra, ANU.

Hopkins, A. (2000) *Lessons from Longford: The Esso Gas Plant Explosion*, CCH Australia Ltd., Sydney, Australia.

Hopkins, A. (1999) The limits of normal accident theory, *Safety Science*, Vol. 32, No. 2, pp. 93-102.

Hwang, P. and Lichtenthal, J.D. (2000) Anatomy of Organizational Crises, *Journal of Contingencies and Crisis Management*, Vol. 8, No. 3, pp. 129-140.

Johnsen, S.O. (2010) Resilience in risk analysis and risk assessment. In Palmer, C. and Shenoi, S. (Eds.), *Critical Infrastructure Protection*, pp. 215-227. Springer, Berlin.

Kahan, J.H., Allen, A.C. and George, J.K. (2009) An Operational Framework for Resilience, *Journal of Homeland Security and Emergency Management*, Vol. 6, No. 1.

Kerlinger, F.N. (1986) *Foundations of behavioural research*, 3rd ed., Holt, Rinehart and Winston, New York.

Kleijnen, J.P.C. (1995) Verification and validation of simulation models, *European Journal of Operational Research*, Vol. 82, pp. 145-162.

La Porte, T.R. (1996) High reliability organizations: unlikely, demanding and at risk, *Journal of Contingencies and Crisis Management*, Vol. 4, No. 2, pp. 60-71.

Labaka, L., Hernantes, J., Laugé, A. and Sarriegi, J.M. (2013) Enhancing Resilience: Implementing Resilience Building Policies against Major Industrial Accidents, *International Journal of Critical Infrastructures*, Vol. 9, No. 1/2, pp. 130-147.

Lagadec, P. (2007) Crisis management in the twenty-first century:"unthinkable" events in "inconceivable" contexts. In Anonymous (Eds.), *Handbook of disaster research*, pp. 489-507. Springer.

Lagadec, P. and Rosenthal, U. (2003) Critical networks and chaos prevention in highly turbulent times, *Journal of Contingencies and Crisis Management*, Vol. 11, No. 3, pp. 97-98.

Larsson, S. and Danell, A. (2006) The black-out in southern Sweden and eastern Denmark, September 23, 2003. , Atlanta, GA.

Lecoze, J. and Capo, S. (2006) A Conceptual and Methodological Comparison with the Field of Child Resilience. , Juan-Les-Pins, France.

Lee, A.V., Vargo, J. and Seville, E. (2013) Developing a Tool to Measure and Compare Organizations' Resilience, *Natural Hazards Review*, Vol. 14, No. 1, pp. 29-41.

Lee, B. and Preston, F. (2012) *Preparing for High-impact, Low-probability Events Lessons from Eyjafjallajökull.* Chatham House Report. London, Great Britain.

Lekka, C. (2011) *High reliability organizations: A review of the literature.* Health and Safety Executive. United Kingdom.

Lekka, C. and Sugden, C. (2011) The successes and challenges of implementing high reliability principles: A case study of a UK oil refinery, *Process Safety and Environmental Protection*, Vol. 89, No. 6, pp. 443-451.

Leveson, N., Dulac, N., Marais, K. and Carroll, J. (2009) Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems, *Organization Studies*, Vol. 30, No. 2-3, pp. 227-249.

Linstone, H.A. and Turoff, M. (1975) *The Delphi Method: Techniques and Applications*, Addison-Wesley Pub. Co., Boston, M.A., USA.

Longstaff, P.H. (2005) *Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters, and Complex Technology*, Harvard University, Cambridge MA.

Madsen, P., Desai, V., Roberts, K.H. and Wong, D. (2006) Mitigating hazards through continuing design: The birth and evolution of a pediatric intensive care unit, *Organization Science*, Vol. 17, No. 2, pp. 239-248.

Malhotra, M.K. and Grover, V. (1998) An assessment of survey research in POM: from constructs to theory, *Journal of Operations Management*, Vol. 16, No. 4, pp. 407-425.

Manyena, S.B. (2006) The concept of resilience revisited, *Disasters*, Vol. 30, No. 4, pp. 434-450.

Marais, K., Dulac, N. and Leveson, N. (2004) Beyond normal accidents and high reliability organizations: The need for an alternative approach to safety in complex systems. *Engineering Systems Division Symposium, MIT*, Cambridge.

Marsden, P.V. and Wright, J.D. (2010) *Handbook of survey research*, 2nd ed., Emerald Group Publishing, United Kingdom.

McEntire, D.A. (2005) Why vulnerability matters: Exploring the merit of an inclusive disaster reduction concept, *Disaster Prevention and Management*, Vol. 14, No. 2, pp. 206-222.

McLachlin, R. (1997) Management initiatives and just-in-time manufacturing, *Journal of Operations Management*, Vol. 15, No. 4, pp. 271-292.

McManus, S., Seville, E., Brunsdon, D. and Vargo, J. (2007) Resilience Management: A Framework for Assessing and Improving the Resilience of Organisations, *Resilient Organisations*.

Meredith, J. (1998) Building operations management theory through case and field research, *Journal of Operations Management*, Vol. 16, No. 4, pp. 441-454.

Mileti, D. (1999) *Disasters by Design: A Reassessment of Natural Hazards in the United States*, Joseph Henry Press, Washington, DC.

Mitroff, I. and Anagnos, G. (2000) *Managing Crises Before They Happen: What Every Executive And Manager Needs to Know About Crisis Management*, AMACOM, New York.

Mitroff, I.I., Harrington, L.K. and Gai, E. (1996) Thinking about the unthinkable, *Across the Board*, Vol. 33, No. 8, pp. 44-48.

Moteff, J.D. (2012) *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress.* Congressional Research Service. US.

Multidisciplinary Center for Earthquake Engineering Research (MCEER) (2008) *Engineering Resilience Solutions.* University of Buffalo. USA.

Murray, E. and Shohen, S. (1992) Lessons from the Tylenol tragedy on surviving a corporate crisis, *Medical Marketing and Media*, Vol. 27, No. 2, pp. 14-19.

Myers, K.N. (1993) *Total Contingency Planning for Diasters: Managing Risk... Minimizing Loss... Ensuring Business Continuity*, John Wiley & Sons, Inc., New York.

Nelms, K.R. and Porter, A.L. (1985) EFTE: An interactive Delphi method, *Technological Forecasting and Social Change*, Vol. 28, No. 1, pp. 43-61.

Okoli, C. and Pawlowski, S.D. (2004) The Delphi method as a research tool: an example, design considerations and applications, *Information and Management*, Vol. 42, pp. 15-29.

Parsons, D. (2007) *National Organisational Resilience Framework Workshop: The Outcomes.* Mt Macedon Victoria, Australia.

Pauchant, T.C. and Mitroff, I.I. (1992) *Transforming the crisis-prone organization: Preventing individual, organizational, and environmental tragedies*, Jossey-Bass, San Francisco.

Pearson, C.M. and Clair, J.A. (1998) Reframing Crisis Management, *The Academy of Management Review*, Vol. 23, No. 1, pp. 59-76.

Pearson, C.M. and Mitroff, I.I. (1993) From crisis prone to crisis prepared: a framework for crisis management., *The academy of management executive*, Vol. 7, No. 1, pp. 48-59.

Perrings, C. (2001) Resilience and sustainability. In Folmer, H. et al. (Eds.), *Frontiers of Environmental Economics*. Edward Elgar, Cheltenham.

Perrow, C. (1994) The limits of safety: the enhancement of a theory of accidents, *Journal of Contingencies and Crisis Management*, Vol. 2, No. 4, pp. 212-220.

PERROW, C., ed, 1984. *Normal Accidents: Living with High Risk Technologies.* New Jersey, USA: Princeton University Press.

Quarantelli, E.L. (2006) Catastrophes are different from disasters: some implications for crisis planning and managing drawn from Katrina, *Understanding Katrina: Perspectives from the social sciences*, pp. 1-7.

Repenning, N.P. and Sternman, J.D. (2001) Nobody Ever Gets Credit for Fixing Problems that Never Happendened: Creating and Sustaining Process Improvement, *California Management Review*, Vol. 43, No. 4, pp. 64-88.

Resilient Organisations (2012) Resilience Indicators, Last access (June, 2013). Retrieved from: http://www.resorgs.org.nz/Content/what-is-organisational-resilience.html.

Rich, E., Sveen, F.O., Qian, Y., Hillen, S.A., Radianti, J. and Gonzalez, J.J. (2009) Emergent Vulnerability in Integrated Operations: A Proactive Simulation Study of Risk and Organizational Learning, *International Journal of Critical Infrastructure Protection*, Vol. 2, pp. 110.

Richardson, B. (1994) Socio-technical disasters: profile and prevalence, *Disaster Prevention and Management*, Vol. 3, No. 4, pp. 41-69.

Richardson, G.P. and Andersen, D.F. (1995) Teamwork in group model building, *System Dynamics Review*, Vol. 11, No. 2, pp. 113-137.

Rinaldi, S.M. (2004) Modeling and simulating critical infrastructures and their interdependencies. *Proceedings of 37th Hawaii international conference on system sciences*, Washington DC, USA.

Roberts, K.H. (1993) Cultural characteristics of reliability enhancing organizations, *Journal of Managerial Issues*, Vol. 5, No. 2, pp. 165-181.

Roberts, K.H. (1990) Some Characteristics of one type of High Reliability Organization, *Organization Science*, Vol. 1, No. 2, pp. 160-176.

Roberts, K.H. and Bea, R. (2001) Must accidents happen? Lessons from high-reliability organizations., *The Academy of Management Executive*, Vol. 15, No. 3, pp. 70-78.

Roberts, K.H. and Rousseau, D.M. (1989) Research in nearly failure-free, high-reliability organizations: having the bubble, *Engineering Management, IEEE Transactions on*, Vol. 36, No. 2, pp. 132-139.

Rochlin, G.I. (1993) Defining "high reliability" organizations in practice: a taxonomic prologue. In Roberts, K.H. (Eds.), *New challenges to understanding organizations*, pp. 11-32. Macmillan, New York.

Rochlin, G.I., La Porte, T.R. and Roberts, K.H. (1987) The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea, *Naval War College Review*, pp. 76-90.

Roux-Dufort, C. (2007) Is Crisis Management (Only) a Management of Exceptions?, *Journal of Contigencies and Crisis Mangement*, Vol. 15, No. 2, pp. 105-114.

Roux-Dufort, C. (2009) The Devil Lies in Details! How Crises Build up Within Organizations, *Journal of Contingencies and Crisis Management*, Vol. 17, No. 1, pp. 4-11.

Rowe, G. and Wright, G. (1999) The Delphi technique as a forecasting tool: issues and analysis, *International Journal of Forecasting*, Vol. 15, No. 4, pp. 353-375.

Ruffner, J.W., Brodie, A.C., Holiday, C.L. and Isenberg, T.H. (2010) Selecting and Utilizing Metrics for an Internet-Based Community of Practice. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, pp. 1254-1258, Nevada, U.S.

Sagan, S.D. (2004) The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security, *Risk Analysis*, Vol. 24, No. 4, pp. 935-946.

Sargent, R.G. (1998) Verification and validation of simulation models. , pp. 121-130.

Sarriegi, J.M., Rich, E., Laugé, A., Labaka, L. and Hernantes, J. (2012) Creating and Testing Holistic Crisis Management Strategies: The Crisis Management Balanced Scorecard and Systems Modelling. In Aschenbruck, N. et al. (Eds.), *Communications in Computer and Information Science*, pp. 261-264. Springer, Heidelberg, Germany.

Sarriegi, J.M., Sveen, F.O., Torres, J.M. and Gonzalez, J.J. (2008) Towards a research framework for critical infrastructure interdependencies, *International Journal of Emergency Management*, Vol. 5, No. 3/4, pp. 235-249.

Seville, E., Brunsdon, D., Dantas, A., Le Masurier, J., Wilkinson, S. and Vargo, J. (2008) Organisational resilience: Researching the reality of New Zealand organisations, *Journal of business continuity & emergency planning*, Vol. 2, No. 2, pp. 258-266.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.J. (2009) The impact of information richness on information security awareness training effectiveness, *Computers & Education*, Vol. 52, No. 1, pp. 92.

Shrivastava, P., Mitroff, I.I., Miller, D. and Miclani, A. (1988) Understanding industrial crises, *Journal of Management Studies*, Vol. 25, No. 4, pp. 285-303.

Shrivastava, S., Sonpar, K. and Pazzaglia, F. (2009) Normal accident theory versus high reliability theory: a resolution and call for an open systems view of accidents, *Human relations*, Vol. 62, No. 9, pp. 1357-1390.

Skulmoski, G.J., Hartman, F.T. and Krahn, J. (2007) The Delphi Method for Graduate Research, *Journal of Information Technology Education*, Vol. 6.

Smith, D. (1990) Beyond contingency planning: towards a model of crisis management, *Organization & Environment*, Vol. 4, No. 4, pp. 263-275.

Snyder, W.M. and de Souza Briggs, X. (2003) *Communities of Practice: A New Tool for Government Managers.* IBM Center for The Business of Government. Virginia, U.S.

Solomon, D.J. (2001) Conducting web-based surveys, *Practical assessment research and evaluation*, Vol. 7, No. 19.

Stephenson, A. (2010) *Benchmarking the Resilience of Organizations*, University of Canterbury, New Zealand.

Stephenson, A., Vargo, J. and Seville, E. (2010) Measuring and comparing organisational resilience in Auckland, *The Australian Journal of Emergency Management*, Vol. 25, No. 2, pp. 27-32.

Tellis, W., 1997. Introduction to Case Study, http://www.nova.edu/ssss/QR/QR3-2/tellis1.html.

Turner, B.A. (1976) ‹br />The Organisational and Inter-Organisational Development of Disasters, *Administrative Science Quarterly*, Vol. 21, No. 3, pp. 378-397.

U.S. House of Representatives (2006) *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina.* U. S. Government Printing Office. Washington DC.

Union for the Coordination of Transmission of Electricity (UCTE) (2004) *Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy.* Italy.

United Nations International Strategy for Disaster Reduction (2009) *Teminology in Disaster Risk Reduction.* Geneva, Switzerland.

US-Canada Power System Outage Task Force (2004) *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations.* US Department of Energy & Canada Ministry of Natural Resources.

Van de Walle, B. and Turoff, M. (2008) Decision support for emergency situations, *Information Systems and E-Business Management*, Vol. 6, No. 3, pp. 295-316.

Van Stralen, D., Daniel, A., Rao, R., Calderon, R., Clemments, P., Kausen, B. and Roberts, K.H. (2005) High Reliability Organization Methods Facilitate Initiation of Mechanical Ventilation in A Pediatric Nursing Home.: 111-S, *Critical Care Medicine*, Vol. 33, No. 12, pp. A28.

Vennix, J.A.M. (1996) *Group Model Building Facilitating Team Learning Using System Dynamics*, John Wiley and Sons, Chichester, England.

Vogus, T.J. and Sutcliffe, K.M. (2007) Organizational resilience: Towards a theory and research agenda. *Systems, Man and Cybernetics, 2007.ISIC.IEEE International Conference on*, pp. 3418-3422.

Voss, C., Tsikriktsis, N. and Frohlich, M. (2002) Case Research in operations management, *International Journal of Operations & Production Management*, Vol. 22, No. 2, pp. 195-219.

Waller, M.J. and Roberts, K.H. (2003) High reliability and organizational behavior: finally the twain must meet, *Journal of Organizational Behavior*, Vol. 24, No. 7, pp. 813-814.

Weick, K.E. and Roberts, K.H. (1993) Collective mind in organizations: Heedful interrelating on flight decks, *Administrative Science Quarterly*, Vol. 38, No. 3, pp. 357-381.

Weick, K.E. and Sutcliffe, K.M. (2007) *Managing the Unexpected: resilient performance in an age of uncertainty*, 2nd ed., Calif.: Jossey-Bass, San Francisco.

Weick, K.E. and Sutcliffe, K.M. (2001) *Managing the Unexpected: Assuring High performance in an Age of Complexity*, .

Westrum, R. (2006) A Typology of Resilience Situations. In Hollnagel, E., Woods, D.D. and Leveson, N. (Eds.), *Resilience Engineering: Concepts and Precepts*, pp. 55-65. Ashgate.

World Nuclear Association (2013) Fukushima Accident 2011, Last access (June, 2013). Retrieved from: http://world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Fukushima-Accident-2011/#.UbwM8vn7CAk.

Wybo, J.L. and Lonka, H. (2002) Emergency management and the information society: how to improve the synergy?, *International Journal of Emergency Management*, Vol. 1, No. 2, pp. 183-190.

Yin, R.K. (2009) *Case study research: Design and methods*, 4th ed., SAGE Publications, Incorporated, Thousand Oaks, USA.

Yin, R.K. (1994) *Case Study Research: Design and Methods*, 2nd ed., Sage publications, Thousand Oaks, CA.

Yin, R.K. (1989) *Case Study Research: Design and Methods*, Rev. ed., Sage publications, Newbury Park, CA.

Yin, R.K. (1984) *Case Study Research: Design and Methods*, 1st ed., Sage publications, Beverly Hills, CA.

Zainal, Z. (2007) Case study as a research method, *Jurnal Kemanusiaan*, No. 9, pp. 1-6.

Zeiler, D. (2011) Japan Supply Chain Disruptions Hit Auto, Electronics Industries, *Seeking alpha*. Available at: http://seekingalpha.com/article/259974-japan-supply-chain-disruptions-hit-auto-electronics-industries.

Zimmerman, M.A. and Arunkumar, R. (1994) Resiliency research: Implications for schools and policy, *Social Policy Report*, Vol. 8, No. 4, pp. 1-17.

Zobel, C.W. (2010) Representing perceived tradeoffs in defining disaster resilience, *Decision Support Systems*, Vol. 50, No. 2, pp. 394-403.

Appendix A: GMB Workshops

This chapter presents the resilience policies obtained after the GMB workshops. These policies are classified based on the resilience dimensions defined in the literature.

Resilience policies and sub-policies after the GMB workshops

Table A.1 resumes the policies gathered from the SEMPOC documentary reports classified by sectors.

Table A.1: Resilience policies identified by the experts during the SEMPOC project's workshops.

Resilience Dimension	Sector	Resilience Policies
Technical Resilience	System state	Maintenance
		Infrastructure adequacy & redundancy
Organizational Resilience	Crisis Preparation & Coordination	Internal Training
		External Training: first responders, society
	Crisis Learning	Lessons Learned
		Information exchange
Social Resilience	Legal & Regulatory	Legal & Regulatory Issues
	Public Opinion	Communication via media

B Appendix B: Multiple Case Studies

This chapter presents the resilience policies and sub-policies defined after the Multiple Case Studies. Within each resilience policy several sub-policies were identified in order to better define and limit the scope of each policy.

Resilience policies and sub-policies after the multiple case studies

Table A.2 resumes the second version of the resilience policies and sub-policies defined after multiple case studies analysis. In this case, several sub-policies were defined for each policy in order to better determine the scope of each resilience policy.

Table A.2: The Resilience Framework after the multiple case studies.

Resilience Types	Resilience Dimensions	Resilience Policies	Resilience Sub-policies
INTERNAL RESILIENCE	Technical Resilience	CI Design and Construction	Redundancy
			Security measures
			Audits
		CI Maintenance	Preventive maintenance
			Corrective maintenance
		CI Data Acquisition and Transmission System	Data acquisition
			Information transmission equipment
	Organizational Resilience	CI Capacity for Crisis Detection, Communication and Analysis	Emergency management personnel training
			Coordination among stakeholders
			Incidents management
		CI Workforce Training and Commitment	Workers training
			Emergency action protocols
			Coordination among stakeholders
	Economic Resilience	CI Crisis Budget	Crisis response and recovery resources
EXTERNAL RESILIENCE	Technical Resilience	Public Crisis Response Equipment Availability	First aid equipment availability
			Emergency equipment of other CI's
			Quality of the available equipment
	Organizational Resilience	First Responders Training	First responder personnel training
			Coordination among stakeholders
			Availability of first responders
		Government preparation	Emergency protocols
			Communication capacity
			Leadership capacity
			Coordination among stakeholders
	Economic Resilience	Public Crisis Budget	Crisis response and recovery Resources
	Social Resilience	Societal preparation	Volunteers in response activities
			Society's behavior in crisis response
		Legal and Regulatory Issues	Regulations revision and update
			Compliance level of the regulations

Appendix C: Delphi Process

This chapter provides further information regarding the Delphi Process. The two questionnaires which were used to gather information are attached in this chapter. The data obtained from this process and how the data were analyzed are explained in detail.

Resilience policies and sub-policies: 1st questionnaire

Following, the first questionnaire is attached to show the format and the questions asked to the experts.

RESILIENCE DYNAMICS

1st questionnaire

tecnun
Universidad de Navarra
Escuela de Ingenieros

1st questionnaire

1 Introduction

The welfare of society has grown exponentially in recent decades in almost every country throughout the world. Advances in health, education, energy, communication, etc. have given rise to significant improvements in our quality of life. At the same time this has also increased our dependency on the infrastructures that support these services, which have become a critical part of our daily lives. Consequently, the concept of Critical Infrastructure (CI) has been created to define assets which are essential for the functioning of our society such as power generation, and healthcare. Thus, current daily life has become absolutely dependent on the stable and highly reliable service of a wide range of CIs. Modern CIs are becoming increasingly more interdependent locally, regionally, and globally.

Crises are complex systems in which many agents are interconnected and their interactions are not known. Crisis management is composed of individual elements such as crisis managers, society, organizations, other CIs, first responders, etc. The state of each element is unstable, they are continually evolving and consequently it is very difficult to predict how a variation in one element could affect the others. Therefore, it is essential not to analyze each component separately but to consider all the elements as a whole, with their corresponding interactions, in order to have a more realistic and holistic picture of the situation.

Many times, previously established contingency plans and mitigation activities are not enough or adequate to face this turbulent environment. Since crises are unpredictable, to be able to predict which part of the system will be damaged and how the event will spread through other sectors often proves to be difficult, if not impossible.

In light of this complex environment, success belongs to organizations, groups, and individuals who are resilient. They are able to recognize, adapt to and absorb variations, changes, disturbances, disruptions and surprises, especially disruptions that fall outside of what the system is designed to handle. These organizations are often referred to as High Reliability Organizations, which are defined as organizations that are successful avoiding catastrophes and responding and recovering as soon as possible reducing impacts.

The best way of improving resilience is to combine the identification of risks with the ability to respond effectively when a crisis actually occurs. In this research resilience is the ability of the system to reduce the failure probability, reduce the consequences from failures (abrupt reduction of performance), and to reduce the time to cover all actions that reduce losses from hazards.

Some authors break resilience down into four dimensions:

- Technical resilience: The ability of the organization's physical system to perform properly when subject to a crisis.

1st questionnaire

- Organizational resilience: The capacity of crisis managers to make decisions and take actions that leads to a crisis being avoided, or at least to a reduction of its impact.
- Economic resilience: The ability of the entity to face the extra costs that arise from a crisis.
- Social resilience: The ability of society to lessen the impact of a crisis by helping first responders or acting as a volunteer.

The aim of crisis managers is to boost the system's resilience level in order to reduce the impacts of a crisis. But how can we build up a resilient system? What actions should be implemented in order to improve the system's resilience level?

The aim of this research is to provide crisis managers with tools for a better understanding of how system resilience can be improved, can be measured and can behave in face of a crisis. The aim is not making a crisis assessment, i.e. quantifying the reduction of impacts depending on the system's resilience level. Rather, the purpose is to analyze the characteristics and dynamics of the resilience, i.e. trying to understand the causal structure and dynamic behaviour of resilience. In other words, identifying what technical, organizational, economic and social factors contribute to increasing the resilience level and to reduce the consequences of an impact at a particular point in time.

This framework provides decision-makers with critical insights that can prevent crisis from occurring within organizations and systems, and also to promote safer behaviours and greater adaptability.

2 Resilience types

In the case of major industrial accidents, there are some focal assets where the triggering event occurs: a ship, a nuclear plant, a grid power plant, the chemical industry, etc. Additionally, as crises may become serious and affect a large number of people, the government needs to cooperate with the damaged industry or even lead the crisis resolution in the most appropriate way. Therefore, we divide the resilience level of an overall system into two different resilience types: an internal resilience, which refers to the resilience level of the owner of the focal element/CI, and an external resilience, which corresponds to the resilience level of the rest of involved agents (the government, first responders, other CIs and society).

Based on this classification, we identified some dimensions within each type of resilience. We divided internal resilience into three dimensions: technical resilience, organizational resilience and economic resilience. External resilience, on the other hand, has been broken down into four dimensions: technical resilience, organizational resilience, economic resilience and social resilience (see Figure 1).

Resilience Dynamics 4

1st questionnaire

Internal Resilience	External Resilience
Technical Resilience	Technical Resilience
Organizational Resilience	Organizational Resilience
Economic Resilience	Economic Resilience
	Social Resilience

Figure 1: Resilience types and dimensions in the case of a major industrial accident.

3 Resilience Policies

Resilience policies refer to the actions implemented in order to increase the system's resilience level. By applying these resilience policies, the system's resilience level will be enhanced, and consequently it will be able to reduce the potential impact.

3.1 Resilience policies for Internal Resilience

Figure 2 shows the resilience policies identified for the case of Internal Resilience.

Internal Resilience	
Technical Resilience	CI Design and Construction CI Maintenance CI Data Acquisition and Transmission System
Organizational Resilience	CI Capacity of Crisis Detection, Communication and Analysis CI Workforce Training and Commitment
Economic Resilience	CI Crisis Budget

Figure 2: Resilience policies within the internal resilience.

The description of each policy and the identified sub-policies in order to evaluate the level of each policy in each moment are defined in the next section.

3.1.1 Technical Resilience

3.1.1.1 CI Design and Construction

CI Design and Construction refers to the level of quality, robustness, redundancy and security of the design and construction of the infrastructure or element that the CI is responsible for.

The infrastructure should meet all normative specifications and requirements. To know what specifications the element's design should meet, it is essential to precisely define its purpose, the risk level of the area against any potential threat, the aspects and characteristics of the surroundings and how these surrounding aspects contribute to the security level of the infrastructure.

Moreover, many infrastructures include additional security systems that should be designed to properly work in critical situations. Finally, care has to be taken not to introduce new vulnerabilities into the system when updates are introduced.

Sub-policies:

1st questionnaire

- Redundancy: The redundancy level of the system such as how many redundant systems each critical component has.
- Security measures (Voluntary and Required): The level of security measures (the required and voluntary) that the system integrates in order to avoid a crisis occurrence.
- Audits (External and Internal): The deep assessment that needs to be carried out in order to evaluate the security level of the system.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5 where:

- 1 means that there is no influence
- 2 means that the influence is low
- 3 means that the influence is moderate
- 4 means that the influence is considerable
- 5 means that the influence is strong

Note: If for any reason, you prefer not to answer a question, feel free to leave it blank.

QUESTIONS		1-5	COMMENTS / ANSWERS
Redundancy	Influence level in the policy		
Security measures	Influence level in the policy		
Audits	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

3.1.1.2 CI Maintenance

Not only should the CI be well designed but high quality maintenance activities also need to be performed periodically in order to improve the system's performance and reliability. These activities include repairing damaged parts, renewing old equipment with reliable components, updating technical features to comply with new legislation, etc. In performing these activities, we make sure that the system's elements are in an adequate and reliable condition and consequently the CI's technical resilience level will improve.

Sub-policies:

- Preventive maintenance: The maintenance of equipment and systems before failure occurs or before it develops into a major incident.
- Corrective maintenance: The maintenance activities carried out after the failure occurrence in order to avoid the next one.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Preventive maintenance	Influence level in the policy		

1st questionnaire

Corrective maintenance	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

3.1.1.3 CI Data Acquisition and Transmission System

This policy has to do with the quality, reliability and effectiveness of the sensors and computer equipment that should be set up in order to supervise and control the CI. Setting up the required sensors to gather information from the system and implementing adequate software to control the system are some of the main activities that should be carried out in order to achieve a high implementation of this policy. Through this equipment, it is possible to collect information from the system and transfer it to the central station to guarantee the proper functioning of the system. This way, if a failure does occur, the central station is immediately alerted in order to confront the situation.

Sub-policies:

- Data Acquisition: The extension of the infrastructure which is sensorized in order to detect warning signals early and the quality and reliability level of the sensors.
- Information transmission equipment: The quality, reliability and effectiveness of transmission equipment for sending the warning signals to the operators.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Data Acquisition	Influence level in the policy		
Information transmission equipment	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

Questions referring to the technical resilience level:

Evaluate the influence of each policy in the technical resilience level from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
CI Design and Construction	Influence level in the technical resilience		
CI Maintenance	Influence level in the technical resilience		
CI Data Acquisition and Transmission System	Influence level in the technical resilience		
Propose another possible policy to precisely evaluate the technical resilience level of the critical infrastructure			

1st questionnaire

3.1.2 Organizational Resilience

3.1.2.1 CI Capacity for Crisis Detection, Communication and Analysis

CI Capacity of Crisis Detection, Communication and Analysis corresponds to the capacity of operators to detect, communicate and analyze a crisis, and to propose new preventive measures for the future. The activities carried out when this policy is implemented are training courses so operators are able to detect anomalous signals, communicate them to crisis managers, and then analyze them to establish new preventive measures. These operators are in charge of verifying the proper functioning of the entire system. Firstly, the operators should be able to detect and interpret the data provided and identify the problem. Then, the incident will be communicated to crisis managers who will analyze its origin and consequences in order to identify the measures that must be taken to solve it and to prevent it from happening again. Lessons learned from previous crisis needs to be implemented to avoid a crisis occurrence.

Sub-policies

- Emergency management personnel training: Training courses to improve the crisis management skills of emergency management personnel.
- Coordination among stakeholders: Working in a coordinated and continuously communicative manner with other agents (including government and first responders) can significantly reduce the time needed to respond to a crisis, and consequently fewer negative effects will appear.
- Incidents management: When an incident occurs, they are communicated and deeply analyzed introducing the necessary corrective actions not to occur again. Lessons learned from crises lead to develop new measurements to avoid occurring again.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Emergency management personnel training	Influence level in the policy		
Coordination among stakeholders	Influence level in the policy		
Incidents management	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

3.1.2.2 CI Workforce Training and Commitment

Workers and managers at the CI must be adequately trained prior to the occurrence of a crisis so they know how to prevent a crisis occurrence and how to respond when a

crisis does occur in emergency situations. Workers should take training courses to know the procedures and protocols that should be followed when something unexpected occurs and to gain the skills they need to improve their response and the ability to coordinate with other stakeholders. Managers also need to improve their planning and foresight processes to be able to prevent a crisis occurrence and also their capacity for making decisions and taking corresponding actions in critical and stressful situations. In addition to this, they also have to train their sense making capacity in order to be able to understand the unexpected event, adapt to it, and make the correct decisions in a stressful situation and without much information. Responding on-time and working in a coordinated manner can significantly reduce the time needed to respond to a crisis, and consequently fewer negative effects will appear.

Sub-policies:

- Workers training: Training courses to improve workers skills to plan, make decisions, respond and recover from a crisis.
- Emergency action protocols: Previously defined protocols help workers and managers to know how they should behave when a crisis occurs and what decisions need to be made. This indicator refers to how these protocols are established and their availability level.
- Coordination among stakeholders: Working in a coordinated and continuously communicative manner with other agents (including government and first responders) can significantly reduce the time needed to respond to a crisis, and consequently fewer negative effects will appear.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Workers training	Influence level in the policy		
Emergency action protocols	Influence level in the policy		
Coordination among stakeholders	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

Questions referring to the organizational resilience level:

Evaluate the influence of each policy in the organizational resilience level from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
CI Capacity for Crisis Detection, Communication and Analysis	Influence level in the organizational resilience		

1st questionnaire

CI Workforce Training and Commitment	Influence level in the organizational resilience		
Propose another possible policy to precisely evaluate the organizational resilience level of the critical infrastructure			

3.1.3 Economic Resilience

3.1.3.1 CI Crisis Budget

CIs should have resources set aside in order to cover repairs and replacements just after the incident happens and until an acceptable level in the society's welfare is achieved, should a crisis occur. This allows entities to increase their economic resilience level and consequently to buy new components, repair damage sooner, and temporarily hire workers and equipment, thereby reducing the response and recovery times. When this pool of money is reduced or even emptied, the response to the critical situation will take longer.

Sub-policies:

- Crisis response and recovery resources: It refers to the monetary resources needed to face response and recovery activities.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Crisis response and recovery resources	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

Questions referring to the economic resilience level:

Evaluate the influence of the policy in the economic resilience level from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
CI Crisis Budget	Influence level in the economic resilience		
Propose another possible policy to precisely evaluate the economic resilience level of the critical infrastructure			

3.2 Resilience policies for External Resilience

Figure 3 shows the resilience policies identified for the case of External Resilience.

1st questionnaire

External Resilience	
Technical Resilience	Public Crisis Response Equipment Availability
Organizational Resilience	First Responders Training Government Preparation
Economic Resilience	Public Crisis Budget
Social Resilience	Societal Preparation Legal and Regulatory Issues

Figure 3: Resilience policies within the external resilience.

3.2.1 Technical Resilience

3.2.1.1 Public Crisis Response Equipment Availability

The availability, quality, redundancy, reliability and security level of the technical equipment of the public bodies, first responders and society is essential in order to face a crisis, repair the damages, respond to emergency situations, introduce alternative emergency devices to replace the damaged ones, etc.

Purchasing the necessary equipment, maintaining them properly and updating them are some examples of the activities that should be carried out in this policy. Having high quality equipment allows first responders, government and society to respond rapidly, reducing the impact of the crisis.

Sub-policies:

- First aid equipment availability: The availability of the first aid equipment to face crises.
- Emergency equipment of other CIs: The amount of the emergency equipment that other CIs have in case a crisis occurs.
- Quality of the available equipment: The quality of the emergency equipment that other CIs have in case a crisis occurs.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
First aid equipment availability	Influence level in the policy		
Emergency equipment of other CIs	Influence level in the policy		
Quality of the available equipment	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

Questions referring to the technical resilience level:

1st questionnaire

Evaluate the influence of the policy in the technical resilience level from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Public Crisis Response Equipment Availability	Influence level in the technical resilience		
Propose another possible policy to precisely evaluate the technical resilience level of the public entities			

3.2.2 Organizational Resilience

3.2.2.1 First Responders Training

First Responder Training has to do with how first responders (fire fighters, emergency units, policemen, etc.) are prepared to face a crisis. Prior to the occurrence of a crisis, they should be trained to know how to respond to and solve a crisis and the procedures and protocols they must follow. Actions such as how to act in dangerous places and how to organize themselves and coordinate with each other such as Table-Top exercises need to be defined before the critical event takes place. After a crisis, everything that went wrong must be identified, and measures should be enacted so they do not occur again.

First responders must be prepared and trained to act independently and effectively in dire circumstances. They must feel capable of operating with initiative and performing their tasks. They should be instilled with a set of core values, ethics and priorities that will guide them in their decisions and actions. Potential responders should be trained to assess when emergency plans need to be activated.

Sub-policies:

- First responder personnel training: The first responders level of training for responding to a crisis.
- Coordination among stakeholders: Working in a coordinated and continuously communicative manner with other agents (including government and workforce) can significantly reduce the time needed to respond to a crisis, and consequently fewer negative effects will appear.
- Availability of first responders: The number of available first responders that can be allocated to the crisis and help society to return to the previous state.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
First responders personnel training	Influence level in the policy		
Coordination among stakeholders	Influence level in the policy		
Availability of first responders	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate			

1st questionnaire

this policy	

3.2.2.2 Government preparation

In a crisis, a government's main roles are to properly communicate the situation to the public and give advice about how they should behave, and to lead and coordinate all the entities that take part in dealing with and solving the crisis. Proper communication between the government and the public, where the government tells the public what they should do and how the resolution of the crisis is progressing, will diminish the public's anxiety, and as a result, the impact. When leading a crisis it is essential to increment their sense making because crises are uncertain and complex. Therefore, crisis managers need to understand the critical situation and adapt to it rapidly. Coordination among different entities is also essential to reduce the response and recovery time and the possible impact. All the entities taking part in managing the crisis should act in the most coordinated way in order to effectively reduce its impact.

Sub-policies:

- Emergency protocols: Protocols to be applied in an emergency situation by the government. These protocols should be updated and followed when a crisis occurs.
- Communication capacity: Government is primarily responsible for communicating and informing the public about the state of the crisis and providing advice in critical situations. This capacity should be developed during the pre-crisis state.
- Leadership capacity: Often the government will be called upon to lead the crisis resolution. Coordinating all the stakeholders, informing the public about the current state, and making decisions, and taking the appropriate actions are all responsibilities the government needs to be prepared to handle before the crisis occurs.
- Coordination among stakeholders: Working in a coordinated and continuously communicative manner with other agents (including first responders and workforce) can significantly reduce the time needed to respond to a crisis, and consequently fewer negative effects will appear.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Emergency protocols	Influence level in the policy		
Communication capacity	Influence level in the policy		
Leadership capacity	Influence level in the policy		
Coordination among stakeholders	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate			

1st questionnaire

this policy	

Questions referring to the organizational resilience level:

Evaluate the influence of each policy in the organizational resilience level from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
First Responders Training	Influence level in the organizational resilience		
Government preparation	Influence level in the organizational resilience		
Propose another possible policy to precisely evaluate the organizational resilience level of the public entities			

3.2.3 Economic Resilience

3.2.3.1 Public Crisis Budget

As in the case of CI Crisis Budget, the public institutions should have a pool of money set aside in case a crisis occurs in order to help the stakeholders and society. This extra funding allows organizations, society and first responders to get resources in a reasonable way. If this pool of money is reduced because it is used, the government should fill it again although it might take some time to happen.

Sub-policies:

- Crisis response and recovery resources: The monetary resources needed to face response and recovery activities.

Questions:

Evaluate the influence of the sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Crisis response and recovery resources	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

Questions referring to the economic resilience level:

Evaluate the influence of the policy in the economic resilience level from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Public Crisis Budget	Influence level in the economic resilience		
Propose another possible policy to precisely evaluate the economic resilience level of the public entities			

1st questionnaire

3.2.4 Social Resilience

3.2.4.1 Societal preparation

Not only should the government and first responders prepare to respond to a crisis but society can also play an important role in crisis resolution. In the event of a crisis, elderly people may need assistance, hospitals can become overcrowded.. This often leads to an increase in demand for human resources including volunteers to repair damage.

Training the public would allow citizens to assist society during a crisis, thus reducing possible adverse effects. Public awareness is a very important factor in order for society to prepare for the crisis. Having a good level of public preparation in the face of a crisis directly influences social resilience, and in turn reduces the impact.

Sub-policies:

- Volunteers in response activities: Volunteers can cooperate in the response and recovery activities as well as help vulnerable people.
- Society's behavior in crisis response: During the crisis, complying with the recommendations is essential to recover as soon as possible.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Volunteers in response activities	Influence level in the policy		
Society's behavior in crisis response	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

3.2.4.2 Legal and Regulatory Issues

Legal and Regulatory issues relates to the level of development of the laws and regulations relating to crises. More developed and better defined laws and regulations ensure that companies and organizations will take the needed preventative measures, and will better define their protocols for crisis management.

The regulations that private companies should meet, the regulations for the first responders and regulations for the public must ensure everyone is more prepared for the crisis and this should reduce impact. Not only should the regulations be defined, but it is also necessary to update them continuously. Having well defined and updated regulations would allow each agent to know what its responsibilities are in order to respond in the most coordinated and effective way.

Sub-policies:

- Regulations revision and update: Not only are regulations developed but also they have to be reviewed and updated continuously to be effective when a crisis occurs.

1st questionnaire

- Compliance level of the regulations: The extent in which the regulations are fulfilled in critical and non-critical situations.

Questions:

Evaluate the influence of each sub-policy in the policy from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Regulations revision and update	Influence level in the policy		
Compliance level of the regulations	Influence level in the policy		
Propose another possible sub-policy to precisely evaluate this policy			

Questions referring to the social resilience level:

Evaluate the influence of each policy in the social resilience level from 1 to 5.

QUESTIONS		1-5	COMMENTS / ANSWERS
Societal preparation	Influence level in the social resilience		
Legal and Regulatory Issues	Influence level in the social resilience		
Propose another possible policy to precisely evaluate the social resilience level of the society			

Resilience policies and sub-policies: comments gathered from the experts

Regarding resilience policies, different types of comments were obtained from the experts during the Delphi process. Besides, experts proposed three new policies to improve the resilience framework. Some comments were related to the title of the policy. For example, in the case of *Public Crisis Response Equipment Availability*, they argued that the quality of the equipment also contributes to resilience. They also noted that equipment may be owned and deployed by private entities, such as hospitals. Therefore, they suggested modifying the title of this policy to *External Crisis Response Equipment*. The titles of *CI Design and Construction*, *CI Data Acquisition and Transmission System*, *CI Workforce Training and Commitment*, *CI Crisis Budget*, *Legal and Regulatory Issues*, *First Responders Training*, *Public Crisis Budget* and *Societal Preparation* were also modified based on the proposals obtained from the experts.

The expert panel also recommended that we divide *CI Capacity for Crisis Detection, Communication and Analysis* into two policies. We were considering the preparation aspects of the crisis managers together with organizational procedures to manage crises. To be consistent with other policies related to preparation and taking into account that procedures are for all the workers at the CI, experts suggested that we split it into two policies: *CI Crisis Manager Preparation* and *CI Organizational Procedures for Crisis Management*. In addition, they suggested that *Crisis Regulation and Legislation* policy be categorized within organizational resilience. The experts believed that this policy should be located in the same space as *Government Preparation* since laws and regulations are developed and managed by the government or a public entity from a government.

Finally, the experts' panel proposed including three new resilience policies in the initial list: *CI Crisis Response Equipment*, *CI Top Management Commitment*, and *Trusted Network Community*. The first refers to the emergency equipment that the CI should have when a crisis occurs to absorb the impact and ensure the safety

of the workers at the CI. The second one emphasizes the need of the commitment of CI's top managers with respect to crisis management in order to deploy resources and encourage workers to create a safe CI. The third one describes the community network that should be established within each sector to share lessons learned and experiences and to establish collaboration agreements to help each other in case a crisis occurs.

Table A.3 compares the initial list of resilience policies with the improved list of resilience policies based on the experts' comments gathered through the Delphi process.

Table A.3: Comparison of the initial list of resilience policies and the improved list of resilience policies.

Resilience Types	Resilience Dimensions	Resilience Policies before the Delphi process	Resilience Policies after the Delphi process
INTERNAL RESILIENCE	Technical Resilience	CI Design and Construction	CI Safety Design and Construction
		CI Maintenance	CI Maintenance
		CI Data Acquisition and Transmission System	CI Data Acquisition and Monitoring System
			CI Crisis Response Equipment
	Organizational Resilience		CI Top Management Commitment
		CI Capacity for Crisis Detection, Communication and Analysis	CI Organizational Procedures for Crisis Management
			CI Crisis Manager Preparation
		CI Workforce Training and Commitment	CI Operator Preparation
	Economic Resilience	CI Crisis Budget	CI Crisis Response Budget
EXTERNAL RESILIENCE	Technical Resilience	Public Crisis Response Equipment Availability	External Crisis Response Equipment
	Organizational Resilience	First Responders Training	First Responder Preparation
		Government Preparation	Government Preparation
			Trusted Network Community
			Crisis Regulation and Legislation
	Economic Resilience	Public Crisis Budget	Public Crisis Response Budget
	Social Resilience	Societal Preparation	Societal Situation Awareness
		Legal and Regulatory Issues	

Regarding sub-policies, there were many comments related to their title and their scope. In addition, several new sub-policies were proposed to include in the resilience framework. Finally, regarding the policies with just one sub-policy, experts proposed to eliminate these sub-policies because they did not provide any value and they were just repeating the explanation given at the corresponding policy.

Influence of the resilience policies on the resilience lifecycle stages: 2nd questionnaire

After carrying out two iterations of the first questionnaire, the second questionnaire was sent to experts to evaluate the influence level of each resilience policy on the three resilience lifecycle stages. Below, the questionnaire sent to experts is attached.

RESILIENCE DYNAMICS

2nd questionnaire

tecnun
Universidad de Navarra
Escuela de Ingenieros

Resilience Dynamics 2

2nd questionnaire

The aim of this second questionnaire is to evaluate the influence of each resilience policy and resilience dimension in the overall resilience level and its effect on diminishing impacts.

1 Technical Resilience within the Internal Resilience

Evaluate each statement from 1 to 5 where:

- 1 means that there is no influence
- 2 means that the influence is low
- 3 means that the influence is moderate
- 4 means that the influence is considerable
- 5 means that the influence is strong

Note: If for any reason, you prefer not to answer a question, feel free to leave it blank.

1.1 CI Safety Design and Construction

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

1.2 CI Maintenance

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

1.3 CI Data Acquisition and Monitoring System

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

Resilience Dynamics 3

2nd questionnaire

1.4 CI Crisis Response Equipment

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

1.5 Technical resilience within the internal resilience

Evaluate (table below) the proportion of the influence of each policy in the technical resilience level.

CI Safety Design and Construction	CI Maintenance	CI Data Acquisition and Monitoring System	CI Crisis Response Equipment	Internal - Technical Resilience
____	_____	_____	____	100%

Please think of this scenario although it is not very realistic. The levels of CI maintenance, CI data acquisition and monitoring system and CI Crisis Response Equipment are extremely high but nothing is done in the CI safety design and construction policy.

CI Safety Design and Construction level	CI Maintenance level	CI Data Acquisition and Monitoring System level	CI Crisis Response Equipment
0%	100%	100%	100%

In light of this situation, evaluate the level of the technical resilience of the CI:

- ☐ 0%
- ☐ About 75%
- ☐ Other. Specify how much: _____

Comments:

2 Organizational Resilience within the Internal Resilience

Evaluate each statement from 1 to 5 (being 1 no influence and 5 strong influence).

2.1 CI Organizational Procedures for Crisis Management

QUESTIONS	1-5	COMMENTS / ANSWERS

2nd questionnaire

This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

2.2 CI Top Management Commitment

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

2.3 CI Crisis Managers Preparation

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

2.4 CI Operators Preparation

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

2.5 Organizational resilience within the internal resilience

Evaluate (table below) the proportion of the influence of each policy in the organizational resilience level.

Resilience Dynamics 5

2nd questionnaire

CI Organizational Procedures for Crisis Management	CI Top Management Commitment	CI Crisis Managers Preparation	CI Operators Preparation	Internal - Organizational Resilience
_____	_____	_____	_____	100%

Please think of this scenario although it is not very realistic. The level of CI Top Management Commitment, CI Crisis Managers Preparation, and CI Operators Preparation are extremely high but nothing is done in the CI Organizational Procedures for Crisis Management policy:

CI Organizational Procedures for Crisis Management	CI Top Management Commitment	CI Crisis Managers Preparation	CI Operators Preparation
0%	100%	100%	100%

In light of this situation, evaluate the level of the organizational resilience of the CI:

- ☐ 0%
- ☐ About 75%
- ☐ Other. Specify how much: _____

Comments:

3 Economic Resilience within the Internal Resilience

Evaluate each statement from 1 to 5 (being 1 no influence and 5 strong influence).

3.1 CI Crisis Response Budget

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

2nd questionnaire

4 Technical Resilience within the External Resilience

Evaluate each statement from 1 to 5 (being 1 no influence and 5 strong influence).

4.1 External Crisis Response Equipment

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

5 Organizational Resilience within the External Resilience

Evaluate each statement from 1 to 5 (being 1 no influence and 5 strong influence).

5.1 First Responders Preparation

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

5.2 Government Preparation

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

5.3 Trusted Network Community

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		

2nd questionnaire

This policy has a strong influence in reducing the time/resources needed for recovery		

5.4 Crisis Regulation and Legislation

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

5.5 Organizational resilience within the external resilience

Evaluate (table below) the proportion of the influence of each policy in the organizational resilience level.

First Responders Training	Government Preparation	Trusted Network Community	Crisis Regulation and Legislation	External - Organizational Resilience
_____	_____	____	___	100%

Please think of this scenario although it is not very realistic. The level of Government Preparation, Trusted Network Community, and Crisis Regulation and Legislation are extremely high but the level of First Responders preparation is very low:

First Responders Training	Government Preparation	Trusted Network Community	Crisis Regulation and Legislation
0%	100%	100%	100%

In light of this situation, evaluate the level of the organizational resilience of the public entities:

- ☐ 0%
- ☐ About 75%
- ☐ Other. Specify how much: _____

Comments:

6 Economic Resilience within the External Resilience

Evaluate each statement from 1 to 5 (being 1 no influence and 5 strong influence).

2nd questionnaire

6.1 Public Crisis Response Budget

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

7 Social Resilience within the External Resilience

Evaluate each statement from 1 to 5 (being 1 no influence and 5 strong influence).

7.1 Societal Situation Awareness

QUESTIONS	1-5	COMMENTS / ANSWERS
This policy has a strong influence in reducing the crisis probability		
This policy has a strong influence in reducing the crisis impact once the triggering event has occurred		
This policy has a strong influence in reducing the time/resources needed for recovery		

8 Questions about the overall resilience

8.1 Overall resilience level

Evaluate (table below) the proportion of the influence of each resilience type in the overall resilience level.

Internal Resilience	External Resilience	Resilience
_____	_____	100%

Please think of this scenario although it is not very realistic. The level of external resilience is extremely high but level of internal resilience is zero:

Internal Resilience	External Resilience
0%	100%

In light of this situation, evaluate the overall resilience level:

- ☐ 0%
- ☐ About 50%
- ☐ Other. Specify how much: _____

2nd questionnaire

Comments:

8.2 Internal resilience level

Evaluate (table below) the proportion of the influence of each resilience dimension in the internal resilience.

Technical Resilience	Organizational Resilience	Economic Resilience	Internal Resilience
_____	_____	_____	100%

Please think of this scenario although it is not very realistic. The levels of organizational and economic resilience are extremely high but level of technical resilience is zero:

Technical Resilience	Organizational Resilience	Economic Resilience
0%	100%	100%

In light of this situation, evaluate the level of the internal resilience:

- ☐ 0%
- ☐ About 66%
- ☐ Other. Specify how much: _____

Comments:

8.3 External resilience level

Evaluate (table below) the proportion of the influence of each resilience dimension in the external resilience.

Technical Resilience	Organizational Resilience	Economic Resilience	Social Resilience	External Resilience
_____	_____	_____	_____	100%

Please think of this scenario although it is not very realistic. The levels of organizational, economic and social resilience are extremely high but level of technical resilience is zero:

Technical Resilience	Organizational Resilience	Economic Resilience	Social Resilience

2nd questionnaire

Resilience Dynamics 10

0%	100%	100%	100%

In light of this situation, evaluate the level of the external resilience:

- ☐ 0%
- ☐ About 75%
- ☐ Other. Specify how much: _____

Comments:

Influence of the resilience policies on the resilience lifecycle stages: data gathered from experts

Table A.4 summarizes the results obtained after the second iteration of the second questionnaire and the arithmetic mean of the experts' evaluations. The experts are classified by the sectors depending on their field: Sector A: Academic (5 experts); Sector B: Transport (2 experts); Sector C: Energy (4 experts); and Sector D: First Responders (4 experts).

Table A.4: Results of the second round of the second questionnaire.

Resilience Policies	Resilie. stages	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Exp. 6	Exp. 7	Exp. 8	Exp. 9	Exp. 10	Exp. 11	Exp. 12	Exp. 13	Exp. 14	Exp. 15	Arith. mean
Sector		A					B		C				D				
CI Safety Design and Construction	Prev	5	4	3	1	5	4	4	5	4	5	5	5	5	5	5	4.3
	Abs	5	4	5	5	4	4	3	3	4	4	5	4	4	5	3	4.1
	Rec	5	4	5	5	4	4	3	2	3	3	5	2	5	3	3	3.8
CI Maintenance	Prev	4	3	3	1	4	5	4	5	4	5	1	4	5	5	5	3.9
	Abs	4	2	4	4	4	3	2	2	3	4	2	2	4	4	3	3.1
	Rec	4	2	4	5	2	3	1	3	2	3	2	2	3	4	3	2.9
CI Data Acquisi. and Monitoring System	Prev	4	5	4	1	3	3	4	4	4	4	2	5	5	5	5	3.9
	Abs	4	3	4	3	5	4	4	4	2	5	2	4	5	5	5	3.9
	Rec	4	3	5	3	4	5	2	4	5	3	3	4	4	3	5	3.8
CI Crisis Response Equipment	Prev	3	2	4	1	2	3	4	2	3	4	3	3	3	2	3	2.8
	Abs	4	5	5	4	4	5	4	4	4	5	4	5	5	4	4	4.4
	Rec	3	4	5	4	4	3	5	4	3	4	4	3	5	4	4	3.9
CI Organizatio. Procedures for Crisis Managers	Prev	4	3	4	4	4	5	5	4	4	4	3	3	4	5	4	4.0
	Abs	4	4	5	5	5	4	4	4	4	4	3	4	5	4	4	4.2
	Rec	4	3	5	4	5	4	5	4	5	3	2	3	5	1	4	3.8
Top Management Commitment	Prev	5	4	4	5	4	5	5	4	4	5	4	5	4	5	4	4.5
	Abs	4	4	5	5	5	4	5	4	5	4	3	4	5	4	5	4.4
	Rec	4	3	5	4	4	4	4	4	5	3	3	3	5	1	3	3.7
CI Crisis Manager Preparation	Prev	4	2	4	5	4	5	5	4	4	5	3	5	3	5	3	4.1
	Abs	4	4	5	5	5	4	4	4	5	4	3	4	5	5	5	4.4
	Rec	4	3	5	5	4	4	5	4	5	3	2	3	5	1	5	3.7
CI Operator Preparation	Prev	5	2	4		5	4	4	4	3	1	2	4	4	1	2	3.2
	Abs	4	5	4	4	4	4	3	3	5	5	3	3	4	5	5	4.1
	Rec	4	4	5	4	4	4	2	5	5	4	4	2	5	5	5	4.1
CI Crisis Response Budget	Prev	4	4	2	2	2	4	4	4	3	1	1	4	3	0	3	2.7
	Abs	4	3	2	4	4	4	3	4	4	3	1	3	3	5	5	3.5
	Rec	4	5	5	4	4	4	3	5	5	5	3	3	5	5	5	4.3
External Crisis Response Equipment	Prev	4	1	3	4	3	3	4	2	1	1	1	1	2	1	3	2.3
	Abs	4	1	3	4	5	3	4	4	3	5	1	5	3	5	5	3.7
	Rec	4	3	1	2	3	3	4	4	5	3	4	3	5	5	5	3.6
First Responder Preparation	Prev	4	3	5	4	3	2	1	4	1	1	1	1	3	0	2	2.3
	Abs	4	5	3	4	5	4	4	4	3	5	1	4	5	5	4	4.0
	Rec	4	4	4	4	5	3	4	3	5	4	4	4	4	2	4	3.9
Government Preparation	Prev	5	4	4	4	4	3	3	4	3	1	1	1	2	1	4	2.9
	Abs	5	3	4	4	4	3	4	5	3	5	2	5	4	5	4	4.0
	Rec	5	5	2	4	3	3	3	4	5	4	4	4	5	5	4	4.0
Trusted Network Community	Prev	5	4	2	2	3	4	3	4	1	4	1	4	3	3	3	3.0
	Abs	5	4	3	4	4	2	4	5	2	3	2	2	5	5	4	3.6
	Rec	4	3	4	4	5	2	3	4	2	3	4	3	5	4	5	3.7
Crisis Regulation and Legislation	Prev	5	4	4	4	4	3	4	5	4	5	5	3	4	5	4	4.3
	Abs	5	2	5	5	2	3	2	3	4	3	5	2	2	5	2	3.3
	Rec	4	4	4	5	3	3	1	3	2	4	3	2	2	5	2	3.1
Public Crisis Response Budget	Prev	5	0	3	2	1	3	2	2	2	1	1	4	3	0	5	2.3
	Abs	5	1	4	4	4	4	4	4	3	5	1	2	3	4	4	3.5
	Rec	4	4	4	4	4	3	3	5	5	4	4	3	5	5	5	4.1
Societal Situation Awareness	Prev	5	4	4	3	4	4	1	2	1	1	1	4	2	4	5	3.0
	Abs	5	3	4	5	4	4	4	2	4	4	2	3	3	5	5	3.8
	Rec	4	4	5	5	5	4	4	5	2	5	4	2	5	4	5	4.2

In order to facilitate the interpretation of the data obtained and determine more exactly the influence of each resilience policy, a new scale based on the range of values obtained was defined. The new scale is divided into seven levels and each level is defined using the following ranges of values (see Table A.5).

Table A.5: Range of values in the new scale.

Level	Range of Values
Extremely Low	0-2.0
Very Low	2.1-2.5
Low	2.6-3.0
Regular	3.1-3.5
High	3.6-4.0
Very High	4.1-4.5
Extremely High	4.6-5.0

The final results, based on the new scale defined in Table A.5, are presented in Table 4.4 in section 4.4.

Appendix D: Survey

This chapter provides details about the questionnaire and the analysis of the obtained data during the survey. The results obtained from the survey are summarized in this chapter in order to justify the implementation methodology for the Resilience Framework for CIs.

Survey: questionnaire

Below, the questionnaire sent to expert in the survey is shown.

CI RESILIENCE DYNAMICS: implementation methodology

Leave survey | Continue later

This research presents a framework which aims to improve the resilience level of Critical Infrastructures (CIs). It consists of 16 major resilience policies and several lower level sub-policies that should be implemented in order to improve the resilience level of the system. These policies have been classified taking into account if the policy helps to directly improve the resilience level of the CI (internal resilience) or assists external agents (external resilience) such as government, first responders, etc. Both internal and external resilience have been classified into four dimensions based on the resilience dimensions defined in the literature:
- technical
- organizational
- economic
- social (external only)

Below, we define the major resilience policies and lower level subpolicies. Note that not all the policies have sub-policies. The aim of this survey is to define the most desirable order of implementing the set of sub-policies for each major policy that will contribute to easing the implementation of this major policy. Afterwards, the aim is to define the order in which the major resilience policies should be implemented to achieve the highest efficiency. Please, read through the definition of the major resilience policies before answering the questions. Your answers will not ever be identified by name. If for any reason, you prefer not to answer a question, feel free to leave it blank.

***1. Write your name in the following box**

***2. For about how many years have you been working in crisis management?**

- Less than one year
- 1 - 4 years
- 5 - 9 years
- More than 10 years

INTERNAL RESILIENCE

TECHNICAL RESILIENCE

Policy 1: CI Safety Design and Construction

The infrastructure of the CI should be as safe as possible to avoid a crisis occurrence and absorb the magnitude of the impact efficiently. Having redundant systems increases the safety level of the CI since redundancy assists in maintaining the functioning of the infrastructure in case of a failure in a component or in a system. The infrastructure should also be robust to resist the impact in light of a threat as well as flexible to be able to adapt to extreme situations when the occasion demands. However, having a complex system with many additional redundant and safety systems is difficult for management of the system and control of its functioning. Therefore, the design of the CI should have a proper level of complexity to guarantee a high safety level for the system. In turn, the design should meet the existing normative specifications and requirements.
Within this policy four sub-policies have been defined: safety measures, redundancy, simplicity and loose coupling, and audits.

3. For the four sub-policies of CI Safety Design and Construction indicate which of the sub-policies need to be done first, second, third, and fourth by placing the numbers 1 to 4 in each appropriate box below.

	Order
Safety Systems	Choose one
Redundancy	Choose one
Simplicity and loose coupling	Choose one
Audits	Choose one

4. Comments:

Policy 2: CI Maintenance

Not only should the CI be well designed and built but high quality maintenance activities also need to be performed periodically in order to guarantee a high level of reliability. Having a good level of maintenance helps to withstand incidents and also to reduce the magnitude of the impact and the time to recover. In performing these activities, we make sure that the system's physical components are in an adequate and reliable state to ensure their proper functioning.
Within this policy two sub-policies have been defined: preventive maintenance and corrective maintenance.

5. For the two sub-policies of CI Maintenance indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
Preventive maintenance	Choose one
Corrective maintenance	Choose one

6. Comments:

Policy 3: CI Data Acquisition and Monitoring System

Having systems to monitor the state of the CI would help to ensure the proper state of the CI. Setting up the required sensors to gather information from the CI and installing adequate software and interfaces within the control panel to monitor the CI performance are some of the main activities that should be carried out in order to achieve a high implementation level of this policy. To ensure the proper functioning of these systems, it is important to have reliable components and systems to gather and monitor the required data properly. Furthermore, having redundant systems would ensure the availability of the data to verify the proper state of the system.
Within this policy two sub-policies have been defined: data acquisition equipment and information monitoring equipment.

7. For the two sub-policies of CI Data Acquisition and Monitoring System indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
Data acquisition	

equipment	Choose one
Information monitoring equipment	Choose one

8. Comments:

Policy 4: CI Crisis Response Equipment

CI Crisis Response Equipment refers to the emergency equipment that the CI should have when a crisis occurs to absorb the impact and ensure the safety of the workers at the CI. Emergency equipment should be reliable to ensure its proper functioning when it is required. Furthermore, the CI should make sure that this equipment is always available to use when a crisis occurs. This emergency equipment may be vital in some cases to diminish the impact and ensure the safety of the workers in times of crises. This equipment should be properly maintained and updated, taking into account the specifications and requirements of manufacturers.

ORGANIZATIONAL RESILIENCE

Policy 5: CI Organizational Procedures for Crisis Management

CI organizational procedures for crisis management corresponds to the capacity of the organization to continuously assure the proper functioning of the CI. It includes the proper management of incidents and crisis situations and the ability to coordinate with external stakeholders such as government and first responders. Therefore, it is important to develop crisis management procedures in order to have the response actions and the responsibilities of each worker well defined before a triggering event occurs. This would lead to absorption and recovery in a more coordinated and efficient way.
Within this policy three sub-policies have been defined: coordination procedures with external stakeholders, crisis management procedures, and incidents management and evaluation.

9. For the three sub-policies of CI Organizaitonal Procedures for Crisis Management indicate which of the sub-policies need to be done first, second and third by placing the numbers 1 to 3 in each appropriate box below.

	Order
Coordination procedures with external stakeholders	Choose one
Crisis management procedures	Choose one
Incidents management and evaluation	Choose one

10. Comments:

Policy 6: CI Top Management Commitment

Top managers should be committed to the resilience building process and they have to promote a resilience based culture, attitudes and values within the CI. They are responsible for deploying resources to promote the workers' commitment and training. In addition to this, top managers' agreement is necessary to establish the required technical measures to prevent a crisis occurrence and absorb the impact. Having an adequate level of leadership capacity is also important to provide more confidence to workers.
Within this policy two sub-policies have been defined: top managers' commitment and situation awareness and activities to promote resilience based culture.

11. For the two sub-policies of CI Top Management Commitment indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
Top managers' commitment and situation awareness	Choose one
Activities to promote resilience based culture	Choose one

12. Comments:

Policy 7: Crisis Managers Preparation

Crisis managers preparation corresponds to the capacity of crisis managers to detect early warning signals, communicate to the stakeholders and analyze the triggering event to propose new preventive measures for the future. In addition to this, they also have to train their sensemaking capacity in order to be able to understand an unexpected event, adapt to it, and make the correct decisions in a stressful situation and without complete information. Moreover, crisis managers need to develop their mindfulness capacity to continuously be aware of incidents or crises that can occur not only on their CI but also in other CIs. Thus, not only would managers learn from crises that occur within their own boundaries, but also they could improve their resilience level by adopting lessons learned and establishing measures gathered from other CIs' incidents and crises.
Within this policy two sub-policies have been defined: crisis managers training and crisis managers' situation awareness and commitment.

13. For the two sub-policies of CI Crisis Managers Preparation indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
Crisis managers training	Choose one
Crisis managers' situation awareness and commitment	Choose one

14. Comments:

Policy 8: CI Operators Preparation

Operators at the CI must be adequately trained prior to the occurrence of a crisis so they know how to respond when a crisis does occur. Operators should take training courses to know the procedures and protocols that should be followed when a triggering event occurs. They should also gain the skills they need to improve their response and coordination abilities.
Within this policy two sub-policies have been defined: operators training and operators' situation awareness and commitment.

15. For the two sub-policies of CI Operators Preparation indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
Operators training	Choose one
Operators' situation awareness and commiment	Choose one

16. Comments:

ECONOMIC RESILIENCE

Policy 9: CI Crisis Response Budget

When a triggering event occurs, monetary resources are needed to absorb the impact and recover to the initial state as soon as possible. CIs should have monetary resources set aside in order to buy new components, repair damage quickly, and temporarily hire workers and equipment, thereby reducing the response and recovery time. CIs usually contract for insurance which will be responsible for providing part of the economic resources needed to repair damages and buy new components, etc.

EXTERNAL RESILIENCE

TECHNICAL RESILIENCE

Policy 10: External Crisis Response Equipment

External stakeholders such as first responders, government and society have also an important role dealing with the crisis resolution. They can help by the crisis resolution providing crisis response equipment to cope with the crisis. This equipment should be reliable to ensure its proper functioning and it should be always available. Furthermore, having redundant equipment would ensure the availability of this equipment when a component or a system gets damaged. In case of a severe crises, this equipment also could be gathered from foreign countries when extra equipment is needed.

ORGANIZATIONAL RESILIENCE

Policy 11: First Responders Preparation

First Responders Preparation corresponds to how first responders (fire fighters, emergency units, policemen, military, etc.) are prepared to face a crisis. Prior to the occurrence of a crisis, they should be trained to know how to absorb and bounce back from a crisis and the procedures and protocols they must follow in each particular situation. Actions such as how to act in dangerous environments and how to organize themselves and coordinate with each other need to be defined before a critical event takes place. After a crisis, everything that went wrong must be identified, and measures should be enacted so failures do not occur again.
Within this policy two sub-policies have been defined: first responders training and first responders' situation awareness and commitment.

17. For the two sub-policies of First Responders Preparation indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
First responders training	Choose one
First responders' situation awareness and commiment	Choose one

18. Comments:

Policy 12: Government Preparation

The government should be well prepared for crisis management. Prior to the crisis, the government should prepare to detect early warning signals and in order to do that it is important to be aware of the possible incidents that may trigger a crisis. Procedures should be defined prior to the occurrence in order to know how they should act when a crisis occurs. Furthermore members of the government need to increase their sensemaking capacity because crises may be uncertain and complex and they have to know how to interpret the situation and adapt to it rapidly. Proper communication between the government, the media and the public, providing real information, is essential to avoid misunderstandings and rumors that could increase the society's anxiety. Furthermore, members of the government are also responsible for coordinating efficiently the network of stakeholders involved in the absorption and recovery activities.
Within this policy five sub-policies have been defined: government's situation awareness and commitment, government training, government communication capacity, government leadership capacity, and coordination of the response agents.

19. For the five sub-policies of Government Preparation indicate which of the sub-policies need to be done first, second, third, fourth and fifth by placing the numbers 1 to 5 in each appropriate box below.

	Order
Government's situation awareness and commitment	Choose one
Government training	Choose one
Government Communication capacity	Choose one
Government Leadership capacity	Choose one
Coordination of the response agents	Choose one

20. Comments:

Policy 13: Trusted Network Community

Creating a network of stakeholders (CI owners, regulators, government, etc.) in which agents involved in a crisis can trust each other to share different experiences and lessons learned may improve their crisis management knowledge and the number of collaboration agreements to help in the crisis prevention and resolution. These networks provide many advantages to CIs such as time saving, reduction of errors, increase in productivity, and reduction in duplication of effort. The network should promote research in the field of CI protection and safety to improve CIs resilience level. During the recovery stage, having created these network may also benefit the CI since members of the network would help the CI to bounce back to the initial stage more efficiently.
Within this policy two sub-policies have been defined: shared information systems and databases and trust and engagement of the participants.

21. For the two sub-policies of Trusted Network Community indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
Shared information systems and databases	Choose one
Trust and engagement of the participants	Choose one

22. Comments:

Policy 14: Crisis Regulation and Legislation

Legislation is a law passed by a government body such as a parliament congress, state legislature or city council whereas, a regulation is a rule made by a government agency or other authorities that provides details on how legislation will be implemented and may establish specific minimum requirements to meet. Legislation is broader and more general whereas regulation is more specific and provides more details about how the legislation will be implemented. Having well defined and updated regulations and legislation would provide safer and better prepared infrastructures to avoid a crisis occurrence and to better handle it if one does occur. Furthermore, the regulations and laws should be regularly updated and reviewed to identify the responsibilities in case something happens.
Within this policy two sub-policies have been defined: regulations and laws revision and update and compliance level of regulations and laws.

23. For the two sub-policies of Crisis Regulation and Legislation indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
Regulations and laws revision and update	Choose one
Compliance level of regulations	Choose one

24. Comments:

ECONOMIC RESILIENCE

Policy 15: Public Crisis Response Budget

As in the case of the CI Crisis Response Budget, the public institutions should have a pool of money set aside in case a crisis occurs, in order to help the stakeholders and society. This extra funding allows organizations, society and first responders to get resources within a reasonable time. Monetary resources will allow performing activities, repairing and rebuilding damaged physical systems and supporting the affected CIs and people. If this pool of money is not enough to cover all the expenses, the government should be able to draw upon extra resources urgently to cope with the crisis.

SOCIAL RESILIENCE

Policy 16: Societal Situation Awareness

Not only should the government and first responders prepare to handle crises but society can also play an important role in crisis resolution. Societal situation awareness and commitment level towards avoiding a crisis occurrence reduces the crisis probability and reduces the magnitude of the impact, with better ability to respond. In the event of a crisis, volunteers would assist first responders dealing with the affected people, thus reducing possible adverse effects. The collaboration and information that society can provide may be crucial to enhance the crisis management.
Within this policy two sub-policies have been defined: societal situation awareness and commitment and societal training.

25. For the two sub-policies of Societal Situation Awareness indicate which of the sub-policies need to be done first and second by placing the numbers 1 and 2 in each appropriate box below.

	Order
Societal situation awareness and commitment	Choose one
Societal training	Choose one

26. Comments:

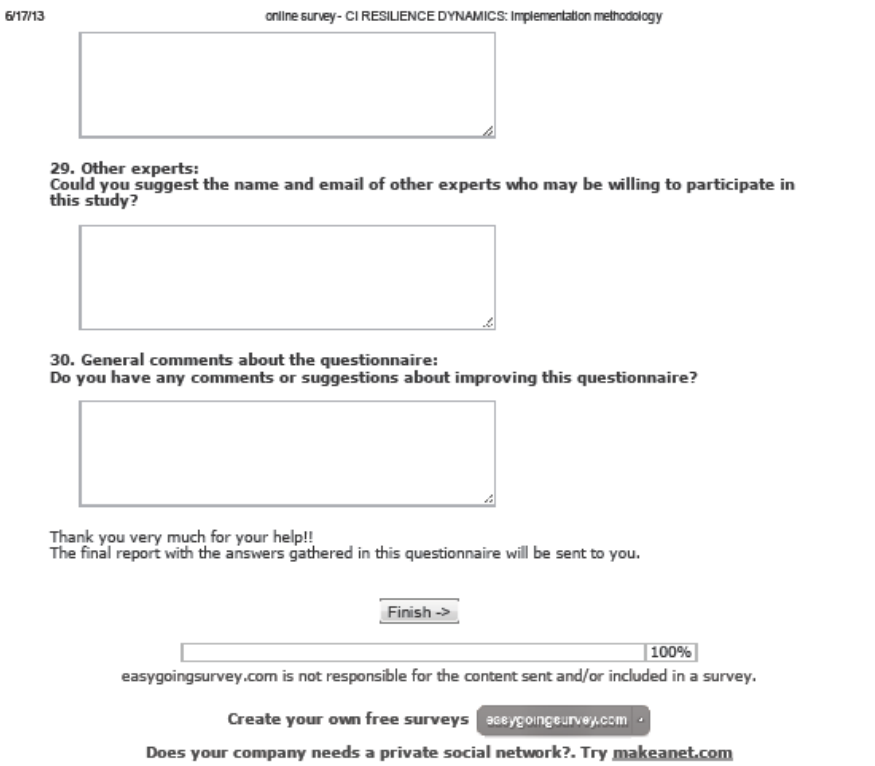
STRUCTURING THE RESILIENCE POLICIES

Now the aim is to define the order in which the major resilience policies should be implemented to achieve the highest efficiency when implementing this framework in a CI.

27. Define in which order, by placing the numbers 1 to 16 in the appropriate box, you believe the resilience policies should be implemented to achieve the highest efficiency. To facilitate this task, we recommend you order the first 5, then the last 5, and finally, the ones in the middle.

	Order
CI Safety Design and Construction	Choose one
CI Maintenance	Choose one
CI Data Acquisition and Monitoring System	Choose one
CI Crisis Response Equipment	Choose one
CI Organizational Procedures for Crisis Management	Choose one
CI Top Management Commitment	Choose one
CI Crisis Managers Preparation	Choose one
CI Workforce Preparation	Choose one
CI Crisis Response Budget	Choose one
External Crisis Response Equipment	Choose one
First Responders Preparation	Choose one
Government Preparation	Choose one
Trusted Network Community	Choose one
Crisis Regulation and Legislation	Choose one
Public Crisis Response Budget	Choose one
Societal Situation Awareness	Choose one

28. Comments:



6/17/13 online survey - CI RESILIENCE DYNAMICS: Implementation methodology

29. Other experts:
Could you suggest the name and email of other experts who may be willing to participate in this study?

30. General comments about the questionnaire:
Do you have any comments or suggestions about improving this questionnaire?

Thank you very much for your help!!
The final report with the answers gathered in this questionnaire will be sent to you.

Finish ->

100%

easygoingsurvey.com is not responsible for the content sent and/or included in a survey.

Create your own free surveys easygoingsurvey.com

Does your company needs a private social network?. Try makeanet.com

Survey: analysis of the data

Implementation methodology of the resilience sub-policies

Table A.6 and Table A.7 summarizes the results obtained from the survey. The percentages represent how many times each sub-policy has been placed in each stage. The mode value has been highlighted for each sub-policy. For each stage different colors have been used (turquoise for the first stage, yellow for the second stage, green for the third stage, blue for the fourth stage, and pink for the fifth stage). Furthermore, the last column represents the mean stage for each sub-policy. The mean stage is the average stage for each sub-policy and it has been calculated based on the following equation:

$$Mean\ stage = \frac{1 * percentage\ stage\ 1 + 2 * percentage\ stage\ 2 + \cdots}{percentage\ stage\ 1 + percentage\ stage\ 2 + \cdots}$$

The sub-policies within each policy have been ordered based on the mean stage (placing at the first position the one with the lowest value and in the last position the one with the highest value) and the same color system has been used to highlight the stage of each sub-policy.

Table A.6: Percentage of how many times each sub-policy (within internal resilience) has been placed in each stage. The last column represents the mean stage for each sub-policy.

Resilience Policies	Resilience Sub-policies	Stages					
		1	2	3	4	5	Mean
CI Safety Design and Construction	Safety measures	43%	17%	35%	4%		2
	Redundancy	22%	39%	17%	22%		2,39
	Simplicity and Loose Coupling	30%	22%	22%	26%		2,43
	Audits	13%	22%	22%	43%		2,96
CI Maintenance	Preventive maintenance	96%	4%				1,04
	Corrective maintenance	4%	96%				1,96
CI Data Acquisition and Monitoring System	Data Acquisition Equipment	73%	27%				1,27
	Information monitoring equipment	27%	73%				1,73
CI Organizational Procedures for Crisis Management	Coordination procedures with external stakeholders	4%	43%	52%			2,48
	Crisis management procedures	70%	26%	4%			1,36
	Incidents management and evaluation	26%	30%	43%			2,17
CI Top Management Commitment	Top manager situation awareness and commitment	83%	17%				1,17
	Activities to promote resilience based culture	17%	83%				1,83
CI Crisis Manager Preparation	Crisis manager training	32%	68%				1,68
	Crisis manager situation awareness and commitment	73%	27%				1,27
CI Operator Preparation	Operator training	48%	52%				1,52
	Operator situation awareness and commitment	57%	43%				1,43

Table A.7: Percentage of how many times each sub-policy (within external resilience) has been placed in each stage. The last column represents the mean stage for each sub-policy.

Resilience Policies	Resilience Sub-policies	Stages					
		1	2	3	4	5	Mean
First Responder Preparation	First Responder Training	55%	45%				1,48
	First Responder situation awareness and commitment	50%	50%				1,48
Government Preparation	Government situation awareness and commitment	52%	17%	9%	13%	9%	2,08
	Government training	13%	17%	17%	17%	35%	3,43
	Government communication capacity	9%	22%	35%	26%	9%	3,04
	Government Leadership capacity	30%	35%	13%	17%	4%	2,30
	Coordination of the response agents	0%	9%	30%	22%	39%	3,91
Trusted Network Community	Shared information systems and databases	23%	77%				1,77
	Trust and engagement of the participants	82%	18%				1,18
Crisis Regulation and Legislation	Regulations and laws revision and update	77%	23%				1,23
	Compliance level of regulations and laws	27%	73%				1,73
Societal Situation Awareness	Societal situation awareness and commitment	83%	17%				1,17
	Societal training	22%	78%				1,78

In most cases the mode stage corresponds to the position of the sub-policy taking into account the mean stage. However, there are some sub-policies were this is not fulfilled for example in simplicity and loose coupling, incidents management and evaluation, and government training. In the case of simplicity

and loose coupling, we believe that this policy should be applied in parallel with safety systems and redundancy, since safety systems and redundancy might increase the complexity of the system and therefore, care must be taken to avoid this as much as possible. In the case of the other two sub-policies (incidents management and evaluation, and government training) the stage of these sub-policies is established based on their position taking into account the mean values.

There is a particular case in which we disagree with experts and we change the order proposed by the experts. When ordering the sub-policies within the *CI Data Acquisition and Monitoring System* policy, experts defined that first data acquisition equipment should be implemented and then, information monitoring equipment should be established. However, we think that both sub-policies should be implemented simultaneously. First, it is important to know what information is needed to ensure the proper state of the CI and then, the equipment to acquire data and to monitor the information should be implemented, simultaneously. Therefore, our belief is that both sub-policies should be applied at the same time.

Finally, there is another special situation which is the F*irst Responder Preparation* policy since experts established that both sub-policies should be implemented simultaneously. Therefore, both sub-policies have been placed in the first stage.

The implementation methodology of the resilience sub-policies within each resilience policy is explained in section 4.5.2.

Implementation methodology of the resilience policies

Similarly to the implementation methodology of the sub-policies, Table A.9 summarizes the results obtained for the implementation methodology of the policies from the survey. In this case, experts were asked to order from one to sixteen (since there were sixteen policies) the temporal order in which the resilience policies should be implemented in order to achieve the highest efficiency in the implementation of the Resilience Framework for CIs. However, in order to facilitate the data analysis process and obtain more coherent results, we aggregate these sixteen steps into five phases based on the relationship presented in Table A.8. Therefore, the first three policies were placed in the first stage, the next three policies were placed in the second stage, the policies in the seventh, eighth, and ninth steps were placed in the third stage, the policies in the tenth, eleventh, and twelfth position were placed in the fourth stage and the last four were placed in the fifth stage (see Table A.8).

Table A.8: Relationship among the order provided by the experts and the stages defined for the analysis of the data.

Order provided by experts	New stages for the analysis of the data
1, 2, 3	1st stage
4, 5, 6	2nd stage
7, 8, 9	3rd stage
10, 11, 12	4th stage
13, 14, 15, 16	5th stage

The percentages in Table A.9 represent how many times each policy has been placed in each stage. The mode value has been highlighted for each policy. For each stage different colors have been used (turquoise for the first stage, yellow for the second stage, green for the third stage, blue for the fourth stage, and pink for the fifth stage). Furthermore, the last column represents the mean stage for each policy. In this case the policies have not been ordered from one to sixteen because it is hard to define the exact order in which the policies should be implemented.

Table A.9: Percentage of how many times each policy has been placed in each stage. The last column represents the mean stage for each policy.

Resilience Types	Resilience Policies	Stages					
		1	2	3	4	5	Mean
Internal Resilience	CI Safety Design and Construction	59%	27%	5%	0%	9%	1,73
	CI Maintenance	27%	23%	27%	9%	14%	2,59
	CI Data Acquisition and Monitoring System	18%	27%	23%	9%	23%	2,91
	CI Crisis Response Equipment	5%	36%	32%	14%	14%	2,95
	CI Organizational Procedures for Crisis Management	18%	45%	18%	14%	5%	2,41
	CI Top Management Commitment	55%	9%	18%	14%	5%	2,05
	CI Crisis Manager Preparation	14%	23%	32%	14%	18%	3
	CI Operator Preparation	5%	18%	27%	36%	14%	3,36
	CI Crisis Response Budget	5%	14%	45%	27%	9%	3,23
External Resilience	External Crisis Response Equipment	0%	5%	5%	36%	55%	4,41
	First Responder Preparation	9%	18%	23%	32%	18%	3,32
	Government Preparation	27%	14%	14%	18%	27%	3,05
	Trusted Network Community	5%	5%	9%	36%	45%	4,14
	Crisis Regulation and Legislation	27%	23%	5%	18%	27%	2,95
	Public Crisis Response Budget	5%	9%	14%	9%	64%	4,18
	Societal Situation Awareness	23%	5%	5%	14%	55%	3,73

Alternatively, in order to define the implementation methodology of the policies we divided the implementation process into five stages. A new scale based on the range of mean values was defined (see Table A.10).

Table A.10: Range of values in the new scale.

Range of mean values	Stage
1 - 2,4	1st
2,4 - 2,8	2nd
2,8 - 3,2	3rd
3,2 - 3,6	4th
3,6 - 5	5th

Based on the new scale, the stage in which each policy should be implemented was defined (see Table A.11).

Table A.11: The mean value and the stage in which each policy is implemented in the implementation methodology.

Resilience Types	Resilience Policies	Mean value	Stage
INTERNAL RESILIENCE	CI Safety Design and Construction	1,73	1st
	CI Maintenance	2,59	2nd
	CI Data Acquisition and Monitoring System	2,91	3rd
	CI Crisis Response Equipment	2,95	3rd
	CI Organizational Procedures for Crisis Management	2,41	2nd
	CI Top Management Commitment	2,05	1st
	CI Crisis Manager Preparation	3	3rd
	CI Operator Preparation	3,36	4th
	CI Crisis Response Budget	3,23	4th
EXTERNAL RESILIENCE	External Crisis Response Equipment	4,41	5th
	First Responder Preparation	3,32	4th
	Government Preparation	3,05	3rd
	Trusted Network Community	4,14	5th
	Crisis Regulation and Legislation	2,95	3rd
	Public Crisis Response Budget	4,18	5th
	Societal Situation Awareness	3,73	5th

In order to order the policies, in most of the cases the mode stage corresponds to the stage of the policy within the implementation methodology (see Table A.9). *CI Maintenance*, *CI Data Acquisition and Monitoring System*, *CI Crisis Response Equipment*, *CI Crisis Response Budget*, *Government Preparation*, and *Crisis Regulation and Legislation* are the ones where the two values do not correspond (see Table A.9). In the cases of *Government Preparation* and *Crisis Regulation and*

Legislation the results are very distributed over the all the stages. There are some experts that think that these policies should be implemented in the first stages whereas others believe that they should be implemented in the last ones. The mean stage, however, corresponds to the third stage (see Table A.9). Therefore, both policies have been placed in the third stage (see Table A.11). Regarding the *CI Maintenance* policy although the mode values are the first stage and the third stage, the mean stage is the second stage (see Table A.9). Therefore, we place it in the second stage (see Table A.11). In the cases of *CI Data Acquisition and Monitoring System* and *CI Crisis Response Equipment*, the mode values are in the second stage but later stages have also high percentages (see Table A.9). Therefore, the mean value is higher in both cases and consequently these policies are implemented in the third stage (see Table A.11). Finally, similarly to the previous cases, *CI Crisis Response Budget* has the mode value in the third stage but due to higher percentages in the next stages the mean stage is higher (see Table A.9). Therefore, this policy will be implemented in the fourth stage (see Table A.11).

The implementation methodology of the resilience policies is further explained in section 4.5.1.

Publications

In this chapter the publications achieved as a result of this research are included. The publications are classified by the different types of publications: conference publications, journal publications, and book chapters.

Conference Publications

Authors: Leire Labaka, Josune Hernantes, Ana Laugé, & Jose Mari Sarriegi.

Title: Three Units of Analysis for Crisis Management and Critical Infrastructure Protection.

Conference: International Conference on Information Systems for Crisis Response and Management (ISCRAM).

Place and date of the Conference: Lisbon, Portugal. May 2011.

Authors: Josune Hernantes, Leire Labaka, Ana Laugé, & Jose Mari Sarriegi.

Title: Eliciting knowledge about crises from 3 different perspectives.

Conference: The International Emergency Management Society Workshop (TIEMS).

Place and date of the Conference: Alés, France. June 2011.

Authors: Leire Labaka, Josune Hernantes, Ana Laugé, & Jose Mari Sarriegi.

Title: Policies to Improve Resilience against Major Industrial Accidents.

Conference: 6th International Conference on Critical Information Infrastructures Security (CRITIS).

Place and date of the Conference: Lucerne, Switzerland. September 2011.

Authors: Ana Laugé, Leire Labaka, Josune Hernantes, & Jose Mari Sarriegi.

Title: Gestión de crisis: Resiliencia e impactos.

Conference: 50th ANNIVERSARY CONFERENCE Engineering: Science and Technology.

Place and date of the Conference: San Sebastian, Spain. June 2012.

Journal Publications

Authors: Josune Hernantes, Leire Labaka, Ana Laugé, & Jose Mari Sarriegi.

Title: Group Model Building: A collaborative modelling methodology applied to critical infrastructure protection.

Journal: Intenational Journal of Organisational Design and Engineering.

Year: 2012 **Volume:** 2 **Pages:** 41-60

Authors: Josune Hernantes, Leire Labaka, Ana Laugé, & Jose Mari Sarriegi.

Title: Three complementary approaches for crisis management.

Journal: International Journal of Emergency Management.

Year: 2012 **Volume:** 8 (3) **Pages:** 245-263

Authors: Leire Labaka, Josune Hernantes, Ana Laugé, & Jose Mari Sarriegi.

Title: Políticas para Mejorar la Resiliencia ante Grandes Accidentes.

Journal: Revista de Ingeniería e Industria (DYNA).

Year: 2012 **Volume:** 87 (5) **Pages:** 518-525

Authors: Leire Labaka, Josune Hernantes, Ana Laugé, & Jose Mari Sarriegi.

Title: Enhancing resilience: implementing resilience building policies against major industrial accidents.

Journal: International Journal of Critical Infrastructures.

Year: 2013 **Volume:** 9 (1/2) **Pages:** 130-147

Authors: Josune Hernantes, Eliot Rich, Ana Laugé, Leire Labaka, & Jose Mari Sarriegi.

Title: Learning before the storm: Modeling multiple stakeholder activities in support of crisis management, a practical case.

Journal: Technological Forecasting & Social Change.

Year: 2013 **Volume:** In Press **Pages:**

Authors: Leire Labaka, Josune Hernantes, Eliot Rich, & Jose Mari Sarriegi.

Title: Resilience Building Policies and their Influence in Crisis Prevention, Absorption and Recovery

Journal: Journal of Homeland Security and Emergency Management.

Year: 2013 **Volume:** In Press **Pages:**

Book Chapters

Authors: Josune Hernantes, Ana Laugé, Leire Labaka, & Jose Mari Sarriegi.

Chapter Title: Vulnerabilidad y Resiliencia de la Cadena de Suministro.

Book Title: Diseño y Gestión de Cadenas de Suministros Globales.

Editors: Ander Errasti.

Year: 2012 **Place:** San Sebastian, Spain **Pages:** 349-369

Authors: Leire Labaka, Josune Hernantes, Ana Laugé, & Jose Mari Sarriegi.

Chapter Title: Resilience: Approach, Definition and Building Policies.

Book Title: Communications in Computer and Information Science.

Editors: Nils Aschenbruck, Peter Martini, Michael Meier, & Jens Tölle.

Publisher: Springer.

Year: 2012 **Place:** Heidelberg, Germany **Pages:** 509-512
