2014 47th Hawaii International Conference on System Science

Implementation methodology of the resilience framework

Leire Labaka[1, 2]
llabaka@tecnun.es

Tina Comes[2]
tina.comes@uia.no

Josune Hernantes[1]
Jhernantes@tecnun.es

Jose Mari Sarriegi[1]
jmsarriegi@tecnun.es

Jose J. Gonzalez[2]
jose.j.gonzalez@uia.no

[1] TECNUN–University of Navarra

[2] Centre for Integrated
Emergency Management, University of Agder

Abstract

Failure of Critical Infrastructures (CIs) can have severe consequences for our societies. Therefore, CI resilience has attracted increasing attention in industries and policy-making. However, empirical studies on CI resilience are rare. In particular, research on the implementation of policies aiming at an improvement of CI resilience is lacking. Using Group Model Building combined with the Delphi method, and surveys we have developed a framework to improve CI resilience. This research identifies policies to enhance CI resilience against major industrial accidents across four dimensions (technical, organizational, economic and social) and proposes a temporal order to ensure that the benefit of policy implementation can be maximized.

1. Introduction

Critical Infrastructures (CIs) are essential, since they support economic growth and social sustainability of societies. CIs are defined as physical or virtual systems, services and assets, that are vital for the welfare of society, and whose a disruption has severe impacts on the health, security, safety or economic well-being of citizens and the effective functioning of the government [1, 2]. Therefore, their reliability and safety are of paramount importance. Along with technical and organizational progress in the last decades, CIs are more interlaced and complex than ever before. As a result, they are also increasingly hard to manage and maintain. Furthermore, current CIs are more and more interdependent. Failures cascade across CIs, and do not respect organizational or national borders, making the management of CIs even more challenging.

Resilience and vulnerability represent two related approaches to understanding the response of systems and actors to changes, which can be trends (such as global warming) or shocks (such as extreme weather events [3]. Their respective origins in ecological and sustainability science, engineering, or risk management explain the continuing differences in the discussions about both terms. This research defines *resilience* as the capacity of a system to withstand a potentially harmful event (e.g., flood, storm), or, if the event impacts the system, the capacity of the system to absorb the impact and recover rapidly. The literature characterizes the following four dimensions [4-6]:

- *Technical resilience* refers to the capacity of an organization's physical system to perform sufficiently well when exposed to a hazard event.
- *Organizational resilience* refers to the capacity of crisis managers to make decisions and take actions that avoid a crisis or reduce its impact.
- *Economic resilience* relates to the capacity of the organization to balance the extra costs from a crisis.
- *Social* resilience refers to the ability of society to reduce the impact of a crisis, e.g., help to first responders or act as volunteers.

To improve the resilience of CIs one needs to determine which policies must be applied in practice bearing in mind the four resilience dimensions. Furthermore, owing to the interdependency of the policies, the temporal order of these policies is crucial and it should be determined for best effect.

When a crisis occurs, the response depends on CI resilience and the decisions and actions of external stakeholders such as government, first responders, and society. Therefore, and due to the interdependences of modern CIs, coordination is essential for efficient and

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.26

effective crisis response. Coordination requires that trust among all actors must be developed before the crisis occurs. Enhancing the resilience level of the whole system has become a main concern of current crisis managers [7-10]. The literature provides much information about the definitions of vulnerability and resilience concepts and design principles that CIs should follow in order to be resilient. However, the literature largely fails to address how these principles should be transformed and applied in practice. Most vulnerability frameworks use static indicators derived from statistical data and assuming that resilience and vulnerability are sufficiently stable concept, which are not prone to sudden changes and shifts [11]. Communities or societies are, however, complex systems and characterised by dynamic behaviour, non-linearity and emergence. Along with the increasing pace of societal changes updating and adaptation of resilience assessments becomes increasingly important [12]. Boin and Van Eeten [13] corroborate our conclusion claiming that few empirical studies have been carried out on the implementation of resilience principles.

The scope of this research is major industrial accidents: crises that start in one CI and rapidly spread through the CI network with severe consequences on the socio-economic system.

To lay the foundations for this work, section two provides the background reviewing several frameworks and approaches aiming at improving CI resilience. Then, we present the results of this paper: first, we present a set of resilience policies aiming at enhancing the resilience level of the overall system classified by the resilience dimensions defined in the literature and illustrate their application (section three). Second, we propose a temporal order in which these resilience policies should be implemented to account for the dynamics (section four). Section five summarizes the main conclusions of this research and outlines future steps to improve the implementation methodology.

2. Resilience building frameworks

Since the late 1970s, accidents such as the Bhopal disaster (1984), the Three Mile Island nuclear accident (1979), and the Chernobyl nuclear accident (1986) raised awareness and elicited grave concerns regarding the safety and reliability of complex and high-risk technological companies. This preoccupation led to two schools of thought: Normal Accident Theory (NAT) and later, High Reliability Theory (HRT). Both are used to analyze reliability, safety and crisis management in complex and high-risk technological organizations, but they came to different conclusions. NAT states that interactive complexity and tight coupling make the occurrence of crises unavoidable [14].

In response to this approach, HRT argues that organizations can take proactive measures that can help to avoid crises [15, 16]. This group of scholars calls High Reliability Organizations (HROs) those organizations that operate complex and high-risk technologies and manage to remain accident free for long periods of time. HRT defines several characteristics and processes that help organizations to reach and maintain high reliability level and safety records [15-17]: deference to expertise, management by exception, climate of continuous training, several communication channels, and redundancy.

HROs are known for the capability to absorb and recover from errors as well as to foresee possible errors that might happen. This is achieved because HROs have the capability to comprehend and discover potential threats, defined as *mindfulness* [18]. Weick and Sutcliffe [18] define five principles to reach the state of mindfulness: preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience, and deference to expertise.

Despite the importance of NAT and HRT to address the issue of reliability and safety of organizations, both have limitations in their definitions and descriptions. Several authors criticize that the main features and characteristics of both theories are poorly explained [19, 20]. NAT explains the problems of the current organizations but it does not provide any solution to deal with these issues [21]. Further, Hopkings [20] highlights five limitations of NAT: only applies to a small number of crises, its main features are poorly explained, there are some crucial aspects that seem to be wrong, recent efforts to improve the theory fail, and lacks provision of policies to deal with crises. Concerning HRT, its principles are quite theoretical and difficult to implement in practice and it does not provide guidelines about how these principles could be implemented in practice [13]. Finally, most of the principles focus on enhancing the organizational resilience without providing sufficient guidance to improve the other dimensions of resilience.

Recently, related to HRT, several authors have developed frameworks to improve the resilience level of companies.

Regarding organizations, a research group in New Zealand called “Resilient Organisations” develops a resilient framework to build up the organizations´ resilience level. This framework is composed of thirteen resilience indicators grouped into three attributes: leadership and culture, networks, and change ready [22]. In the same vein, Parsons describes eight key attributes of resilience organizations based on a workshop conducted by Trusted Information Sharing Network´s Community of Interests [23]: awareness, agility and flexibility, change readiness, interdependency knowledge, integration, culture and values, leadership and communications. The framework proposed by the 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). Furthermore, these authors do not describe the path forward developing resilient systems.

Johnsen [24] 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 fulfill to be resilient: graceful and controlled degradation, management of margins, common mental models, redundancy, flexibility, reduction in complexity, and reduction of coupling. Nonetheless, as in the earlier cases, the processes, the order, and transformations required to create resilience building activities are not specified.

From a more holistic point of view, Kahan et al. [25] 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, robustness, consequence mitigation, adaptability, risk-informed planning, risk-informed investments, harmonization of purposes, comprehensiveness of scope. Externally, Cutter et al. [26] 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 focus on social resilience and, therefore, they do not provide specific policies for CI providers. Furthermore, little is stated about how to improve these indicators.

The literature presents a broad set of works discussing principles about how to improve the resilience level of organizations. However, it is hard to find a detailed prescription for crisis managers about how these principles can be implemented in in practice and which methodology to use. In addition, almost all the principles still focus on activities within the boundaries of the CI, neglecting the role of external agents and their influence on improving the CIs resilience.

In light of this situation, this research aims to present a holistic framework to help CIs to improve their resilience level. This framework provides a set of tangible policies that should be implemented in the whole system to increase their resilience level. A policy should be understood as actions or measures to achieve a strategic goal. Furthermore, the temporal order in which those policies should be implemented is defined in order to achieve high efficiency in the framework's implementation.

3. Resilience Framework for CIs

This research defines two resilience types (internal resilience and external resilience) since the resilience level of the CI where the triggering event occurs could be different to the resilience level of the rest of the external entities. Thus, internal resilience refers to the resilience level of the CI whereas external resilience refers to the resilience associated with involved external agents, such as government, first responders, and society.

In order to improve the resilience dimensions already defined in the literature (technical, organizational, economic, and social), this research defines several resilience policies referring to internal and external stakeholders. These policies were obtained through several iterations of applying different research methods. First, through Group Model Building (GMB) workshops in the context of power cuts, a few selected resilience policies were defined [27, 28]. GMB is a collaborative method which enables integrating fragmented knowledge, initially residing on the minds of different agents, into aggregated models [29-31]. Fourteen multidisciplinary experts took part in the three workshops which were arranged in the context of a European project called SEMPOC[1].

Afterwards, this list of policies was improved and extended to other sectors through multiple case studies of different past major industrial accidents [28, 32]. The causes of the triggering events, and correctly or badly established measures were analyzed in order to complete the initial list of policies.

Finally, through a Delphi method the final list of the policies was obtained [28, 33]. Delphi is a systematic and iterative process for structuring a group communication process in order to obtain a consensus about a complex problem [34-36]. Fifteen multidisciplinary experts from different sectors (academics, transport, energy, and first responders) took part in the process and two different questionnaires with different aims and content were used [28, 33].

[1] www.sempoc.eu

As a result of this process the final list of resilience policies was obtained. These policies have been classified based on the four resilience dimensions. In the following, the resilience policies are described.

3.1. Technical Resilience

Within this dimension five resilience policies have been defined. The first four are within the internal resilience since they assist in improving the resilience level of the CI. The last one is placed within the external resilience because it allows improving the technical resilience level of the external stakeholders.

3.1.1. CI Safety Design and Construction. This policy refers to the safety level of CI to avoid a crisis occurrence and absorb the magnitude of the impact efficiently. Having safety sub-systems and redundant components and sub-systems allow preventing a crisis occurrence and ensuring the functioning of the CI [4, 24]. However, having a complex system with many additional redundant and safety systems makes it difficult to manage the system and to control its functioning [14, 19, 37]. Therefore, when designing the CI, it is important to reduce complexity and tight relationships. Finally, internal and external audits should be carried out to ensure the proper functioning of the CI.

3.1.2. CI Maintenance. Not only should the CI be well designed and built, but high quality maintenance activities must also be performed periodically in order to guarantee a high level of reliability 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.

3.1.3. 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.

3.1.4. CI Crisis Response Equipment. This policy 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 and should be available to be able to use it when a crisis occurs.

3.1.5 External Crisis Response Equipment. External stakeholders such as first responders, government and society should also have reliable and adequate equipment to cope with crisis. Furthermore, having redundant equipment would ensure the availability of this equipment when a component or a subsystem 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.

3.2. Organizational Resilience

Eight policies (the first four within the internal resilience and the next four within the external resilience) have been defined in order to improve the organizational resilience. Below, we present the policies related to this resilience dimension:

3.2.1. CI Organizational Procedures for Crisis Management. This policy corresponds to the preparation and the capacity of the organization to deal with crises and incidents as well as the ability to coordinate with external stakeholders such as government and first responders. CIs should develop crisis management procedures and coordination procedures with external stakeholders in order to have the response actions and the responsibilities of each worker well defined before a crisis occurs.

3.2.2. 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 and to establish the required technical measures to prevent a crisis occurrence and absorb the impact.

3.2.3. CI Crisis Manager Preparation. Crisis managers' 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, managers also have to develop their sensemaking capacity [38], which refers to be ability to understand an unexpected event, adapt to it, and make the correct decisions in a stressful situation and without complete information.

3.2.4. 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 response procedures and protocols and develop their response and coordination abilities [22]. Operators should also be committed with the safety of the company since they can help detecting early warning signals and avoiding a crisis occurrence [22].

3.2.5. First Responder Preparation. This policy refers 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 learn about the special characteristics of their closest CIs in order to be able to properly respond when a crisis occurs. 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.

3.2.6. Government Preparation. The government should be well prepared for crisis management. The government should be aware of the possible incidents that could lead to a big crisis and should be committed to the crisis management process. The government should develop response procedures and acquire leaderships and communication skills to manage and inform properly in case of a crisis [39, 40]. Furthermore, members of the government are also responsible for coordinating efficiently the network of stakeholders involved in the absorption and recovery activities [39, 40].

3.2.7. 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 experiences and lessons learned may improve their crisis management knowledge and the number of collaboration agreements to help in crisis prevention and resolution [22, 41-43]. These networks should promote research in the field of CI protection and safety to improve CIs resilience level.

3.2.8. Crisis Regulation and Legislation. This policy refers to the maturity level and compliance level of the regulations and laws. 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. Furthermore, the regulations and laws should be regularly updated and reviewed to identify responsibilities in case a crisis occurs.

3.3. Economic Resilience

In this case only two policies are defined, the first one for the internal resilience and the second one for the external resilience.

3.3.1. 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 cover repairs and replacements just after the triggering event happens and until an acceptable level of performance that guarantees society's welfare is achieved [22].

3.3.2. Public Crisis Response Budget. As in the case of the CI Crisis 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.

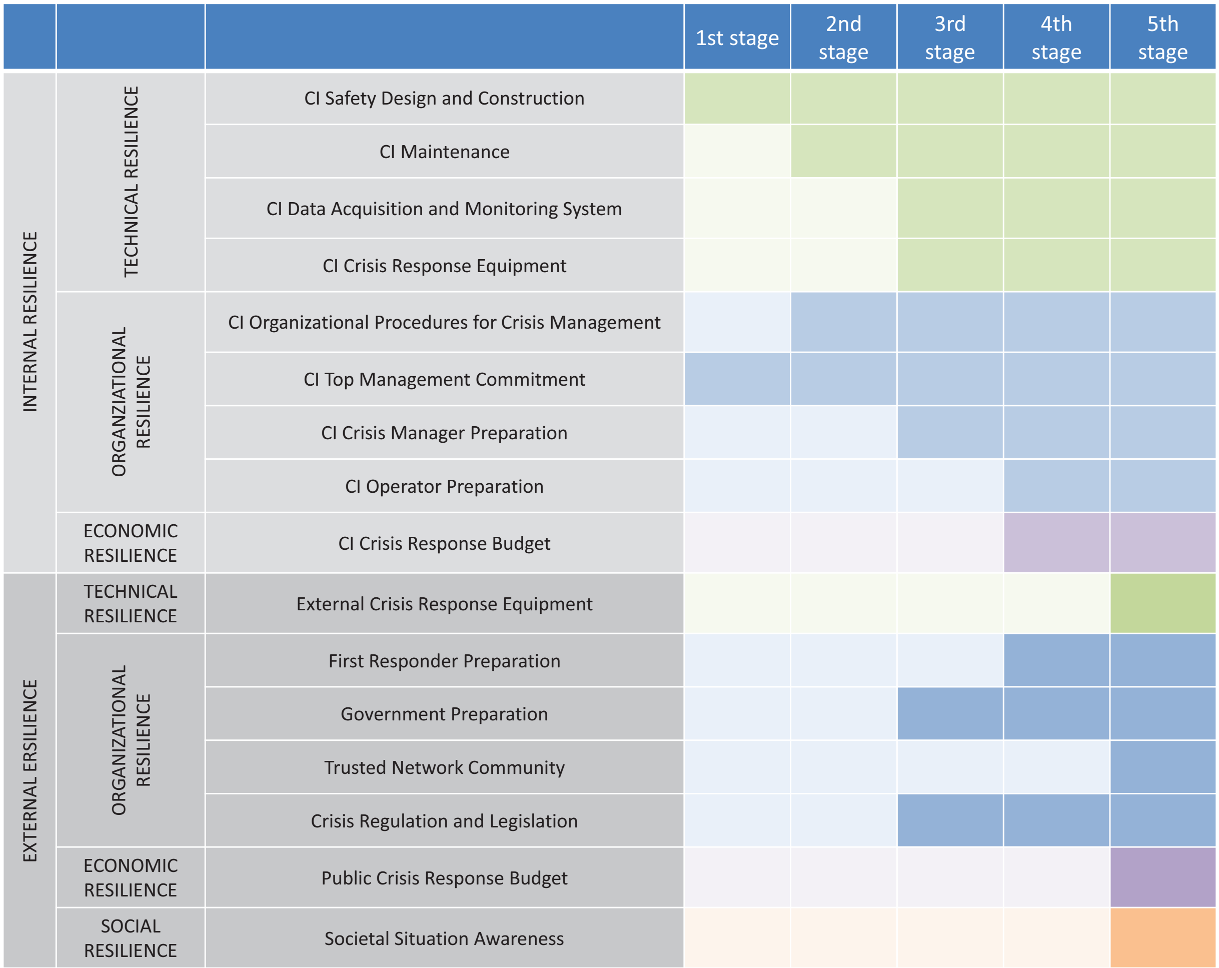
3.4. Social Resilience

In this case, only one policy classified within the external resilience is defined in order to improve the social resilience.

3.4.1. 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. 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 [22, 44]. Furthermore, the collaboration and information that society can provide may be crucial to enhance crisis management.

4. Implementation methodology of the Resilience Framework

Starting from the list of resilience policies, an implementation methodology is presented to efficiently implement this list of policies in practice. Methodology should be understood as a design process for the development of a group of practices or procedures [45, 46]. Due to scarce resources and time pressure, it is impossible to implement all policies simultaneously. Indeed, some policies require others prior implementation to efficiently implement them.



			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			🟩	🟩	🟩
	ORGANZIATIONAL 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 ERSILIENCE	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					🟧

Figure 1: The Implementation Methodology of the Resilience Framework.

Therefore, the aim of this step was to define the temporal order in which the policies should be implemented to achieve high implementation in its application.

In order to do that, information was gathered from experts through the survey methodology. Twenty-five experts from different field such as academic, transportation, energy, water, telecommunication and media, first responders, and safety consultancy took part in this process [28]. The experts were asked to provide the temporal order in which the policies should be implemented in practice in order to achieve a high efficiency in their implementation.

Once the data were gathered, we analyzed them to define the optimal order of implementation [28]. After analyzing the results we concluded that there were some policies that need to be implemented at the beginning of the process since they are required for the proper implementation of others. In turn, others were placed in the last positions as they necessarily built on previous policies.

Therefore, in order to achieve a more realistic and coherent order, we divided the implementation process into five stages. 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.

Figure 1 illustrates the implementation methodology of the resilience policies divided into five main stages.

4.1. 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.

4.2. 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.

4.3. Third stage

In this step, five new policies are introduced. First, CI data acquisition and monitoring system 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 effectively 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.

4.4. 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 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 (Public Crisis Response Equipment). Furthermore, a trusted community network has to be created where stakeholders share information and experiences with other involved agents and improve their CM 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 has to be aware about the crisis occurrence and prepared to cope with crises in the most effective way.

5. Conclusions, Limitations and Future research

This research proposes a set of resilience polices that CI providers could implement in order to enhance their resilience. These policies acknowledge that CIs are an essential part of the wider socio-economic system and that CI crisis management requires a coordinated effort embracing actions of external stakeholders such as first responders, government, and society. Furthermore, this research defines an implementation methodology that supports crisis managers who need to prioritize and implement a set of policies in practice. The policies should be implemented in an adequate sequence so as to maximize efficiency and effectiveness.

However, this implementation methodology still has several limitations. It is yet unclear how to best determine the end of each stage. Furthermore, (direct and indirect) cause-effect relations among the resilience policies should be established to provide more insights about which policies require others prior implementation and to identify further relevant environmental impacts.

Our research will continue to complete the implementation by gathering information about (i) measures or conditions that define the end of each stage, and (ii) the relations between implementation policies and policies and environment that determine requirements of each policy.

6. References

[1] S.M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies", Proceedings of 37th Hawaii international conference on system sciences. Washington DC, USA, 2004.

[2] Commission of the European Communities. Green Paper on a European Programme of Critical Infrastructure Protection, Brussels, 2005.

[3] T. Cannon and D. Müller-Mahn, "Vulnerability, resilience and development discourses in context of climate change", Natural Hazards, Springer, 2010, Vol. 55, pp. 621-635.

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

[5] Multidisciplinary Center for Earthquake Engineering Research (MCEER). Engineering Resilience Solutions, University of Buffalo, USA, 2008.

[6] C.W. Zobel, "Representing perceived tradeoffs in defining disaster resilience", Decision Support Systems, Elsevier, 2010, Vol. 50, pp. 394-403.

[7] De Bruijne, MLC. Networked reliability: institutional fragmentation and the reliability of service provision in critical infrastructures. Netherlands: Faculty of Technology, Policy and Management, Delft University of Technology; 2006.

[8] A. Boin and A. McConnell, "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience", Journal of Contingencies and Crisis Management, Blackwell Publishing Ltd, 2007, Vol. 15, pp. 50-59.

[9] M. De Bruijne and M. Van Eeten, "Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment", Journal of Contingencies and Crisis Management, Wiley Online Library, 2007, Vol. 15, pp. 18-29.

[10] B. Hämmerli and A. Renda. Protecting Critical Infrastructure in the EU, Centre for European Policy Studies, Brussels, 2010.

[11] J. Birkmann. Measuring vulnerability to natural hazards, TERI Press, New Delhi, 2006.

[12] P. Trucco, E. Cagno, and M. De Ambroggi, "Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures", Reliability Engineering & System Safety, Elsevier, 2012, Vol. 105, pp. 51-63.

[13] A. Boin and M.J.G. Van Eeten, "The Resilient Organization", Public Management Review, 2013, Vol. 15, pp. 429-445.

[15] K.H. Roberts and D.M. Rousseau, "Research in nearly failure-free, high-reliability organizations: having the bubble", Engineering Management, IEEE Transactions on, IEEE, 1989, Vol. 36, pp. 132-139.

[16] K.H. Roberts and R. Bea, "Must accidents happen? Lessons from high-reliability organizations.", The Academy of Management Executive, Academy of Management, 2001, Vol. 15, pp. 70-78.

[17] K.H. Roberts, "Some Characteristics of one type of High Reliability Organization", Organization Science, 1990, Vol. 1, pp. 160-176.

[18] K.E. Weick and K.M. Sutcliffe. Managing the Unexpected: resilient performance in an age of uncertainty, Calif.: Jossey-Bass, San Francisco, 2007.

[19] N. Leveson, N. Dulac, K. Marais, and J. Carroll, "Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex

systems", Organization Studies, SAGE Publications, 2009, Vol. 30, pp. 227-249.

[20] A. Hopkins, "The limits of normal accident theory", Safety Science, 1999, Vol. 32, pp. 93-102.

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

[22] Resilient Organisations. Resilience Indicators. 2012. from http://www.resorgs.org.nz/Content/what-is-organisational-resilience.html.

[23] D. Parsons. National Organisational Resilience Framework Workshop: The Outcomes, Mt Macedon Victoria, Australia, 2007.

[24] S.O. Johnsen, "Resilience in risk analysis and risk assessment", Springer, 2010, pp. 215-227.

[25] J.H. Kahan, A.C. Allen, and J.K. George, "An Operational Framework for Resilience", Journal of Homeland Security and Emergency Management, Berkeley Electronic Press, 2009, Vol. 6,

[26] S.L. Cutter, C.G. Burton, and C.T. Emrich, "Disaster Resilience Indicators for Benchmarking Baseline Conditions", Journal of Homeland Security and Emergency Management, Berkeley Electronic Press, 2010, Vol. 7,

[27] J. Hernantes, L. Labaka, A. Laugé, and J.M. Sarriegi, "Group Model Building: A collaborative modelling methodology applied to Critical Infrastructure Protection", International Journal of Organizational Design and Engineering, 2012, Vol. 2, pp. 41-60.

[28] Labaka, L. Resilience Framework for Critical Infrastructures. San Sebastian: University of Navarra; 2013.

[29] G.P. Richardson and D.F. Andersen, "Teamwork in group model building", System Dynamics Review, Wiley Online Library, 1995, Vol. 11, pp. 113-137.

[30] D.F. Andersen, J.A.M. Vennix, G.P. Richardson, and E.A.J.A. Rouwette, "Group Model Building: Problem structuring, policy simulation and decision support", Journal of the Operational Research Society, 2007, Vol. 58, pp. 691-695.

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

[32] L. Labaka, J. Hernantes, A. Laugé, and J.M. Sarriegi, "Enhancing Resilience: Implementing Resilience Building Policies against Major Industrial Accidents", International Journal of Critical Infrastructures, 2013, Vol. 9, pp. 130-147.

[33] L. Labaka, J. Hernantes, E. Rich, and J.M. Sarriegi, "Resilience Building Policies and their Influence in Crisis Prevention, Absorption and Recovery", Journal of Homeland Security and Emergency Management, 2013, Vol. 10,

[34] N. Dalkey, "An experimental study of group opinion", Futures, 1969, pp. 408-426.

[35] H.A. Linstone and M. Turoff. The Delphi Method: Techniques and Applications, Addison-Wesley Pub. Co., Boston, M.A., USA, 1975.

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

[37] S.D. Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security", Risk Analysis, Wiley Online Library, 2004, Vol. 24, pp. 935-946.

[38] D.R. Gilpin and P.J. Murphy. Crisis Management in a Complex World, Oxford University Press, Oxford, 2008.

[39] L.F. Carrel, "Training civil servants for crisis management", Journal of Contingencies and Crisis Management, Wiley Online Library, 2000, Vol. 8, pp. 192-196.

[40] A. Boin, "The new world of crises and crisis management: Implications for policymaking and research", Review of Policy Research, Wiley Online Library, 2009, Vol. 26, pp. 367-377.

[41] J.W. Ruffner, A.C. Brodie, C.L. Holiday, and T.H. Isenberg, "Selecting and Utilizing Metrics for an Internet-Based Community of Practice", Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2010.

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

[43] E. Wenger, R.A. McDermott, andW.M. Snyder. Cultivating communities of practice: A guide to managing knowledge, Harvard Business School Press, Boston, Massachusetts, 2002.

[44] R.S. Shaw, C.C. Chen, A.L. Harris, and H.J. Huang, "The impact of information richness on information security awareness training effectiveness", Computers & Education, Elsevier Science Ltd., 2009, Vol. 52, pp. 92.

[45] "Methodology". Merriam-Webster Dictionary. 2013. from http://www.merriam-webster.com/dictionary/methodology.

[46] "Methodology". The American Feritage Dictionary of the English Language. 2011. from http://www.ahdictionary.com/word/search.html?q=methodology&submit.x=61&submit.y=22.