Policies to Improve Resilience against Major Industrial Accidents

Leire Labaka, Josune Hernantes, Ana Laugé, and Jose Mari Sarriegi

University of Navarra, TECNUN,
Paseo Manuel Lardizabal 13, 20018 San Sebastián, Spain
{llabaka,jhernantes,alauge,jmsarriegi}@tecnun.es

Abstract. A major industrial accident is an unpredictable event which triggers a disruption in a Critical Infrastructure (CI). This disruption can spread through other sectors, affecting not only the CI where the triggering event takes place but the whole society as well. In the case of major industrial accidents, system resilience consists of both the resilience of the CI (internal resilience) and resilience of society (external resilience). Resilience is the system's ability to reduce the probability of failure, the consequences from failure and the response and recovery time. However, little is known about how to achieve a high resilience level. In this paper, using the information gathered from experts and examining several major industrial accidents, we derive twelve policies that enhance the system's resilience level. The definitions of these policies are clarified through real case examples where the consequences of their use or lack of use are explained.

Keywords: Resilience, Critical Infrastructure, Crisis Management, Major Industrial Accidents, Resilience Policies.

1 Introduction

A major industrial accident can be defined as a crisis that starts in a Critical Infrastructure (CI) due to a disruption in the infrastructure or an element, such as an oil spill, a power outage, an aircraft crash or a nuclear accident. One of the main characteristic of current CIs is their interdependency. A crisis that starts in one sector may spread through the CIs' networks rapidly. For example, if a blackout occurs, the hospitals cannot carry out their current activities and the industries have to stop their production unless they dispose an autonomous power generation. Therefore, a crisis that starts in a particular CI spreads through the whole society affecting a great amount of people.

According to Rinaldi [1] there are four different types of CI interdependencies:

1. *Physical*: If the state of each CI depends upon the material output(s) of other CI.
2. *Cyber*: If the state of a CI depends on information transmitted through the ICT (Information and Communication Technologies) infrastructure.

S. Bologna et al. (Eds.): CRITIS 2011, LNCS 6983, pp. 187–199, 2013.

3. *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.
4. *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.

Thus, CIs cannot be considered as isolated entities but as a network of interconnected and interdependent elements. Bearing the importance of proper functioning of CIs for society's welfare in mind, we enhance the need for preparation and prevention measures.

Normally, the crisis is caused by an unpredictable event which can not have been foreseen. We cannot know when the triggering event will occur, which part of the system will be damaged and how it will spread through other sectors. Thus, this makes crisis prevention and preparation a challenging task.

This paper's main purpose is to break down the identified resilience types into resilience policies that crisis managers can implement in order to build up the system's resilience level. We do this through a study of major industrial accidents and also considering the information gathered from three workshops with experts.

The second section introduces the resilience concept and defines the two types of resilience that we have identified. Resilience policies that enhance the resilience level are presented in the third section and in the fourth one the influence of each policy on the crisis impact is defined. Finally, the main conclusions of the paper and the future work are proposed.

2 Resilience

Resilience is an essential concept when managing crises. It can be defined as the ability of the system to reduce the probability of failure, reduce the consequences from failure and reduce the time taken to cover all the response and recovery actions [2].

Some authors [2,3] break resilience down into four dimensions:

- *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.

Taking this definition and the various dimensions into account, we could say that a high level of resilience contributes to preventing the occurrence of a crisis and reducing its impact if one does occur.

The aim of crisis managers is to boost the system's resilience level to reduce the impacts from a crisis. However, how can we build up a resilient system? What actions should be implemented in order to improve the system's resilience level? Despite having a very clear general definition of resilience, there are many difficulties in breaking down this general perspective and putting it into practice.

System resilience is built up by implementing some preventive and preparatory measures such as improving the design of infrastructures and increasing maintenance levels or training operators to respond in the most effective and coordinated way. 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. But, what are the policies that can be applied? How does each policy help to reduce the impact of a crisis? Due to resource scarcity, however, deciding how much should be invested in mitigation is a very challenging task. Furthermore, the influence of each policy varies depending on the triggering event.

2.1 Resilience Dimensions in Case of Major Industrial Accidents

In the case of major industrial accidents, there is some focal asset where the triggering event occurs: a ship, a nuclear plant, a power grid 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 resiliencies: 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 Fig. 1).

3 Resilience Policies

We organised three workshops in San Sebastian (Spain) to gather information with experts from different institutions such as energy companies, first responders, civil protection, health care, and organizations for CIs protection. Furthermore, we analyzed real cases from literature to get further information. Based on all this data we have identified different resilience policies that can be applied in order to improve the resilience dimensions. Afterwards, we have refined these policies to make clear the definition of each of them, which have been subsequently validated using some real examples.

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

Fig. 1. Resilience types and dimensions in the case of a major industrial accident

The real cases analyzed illustrate the consequences of having a low or high level -or degree of effective implementation- of each policy. In some cases it can be seen that a low level of some policies led to the accident, whereas in others, a high level of them helped in its resolution.

It is important to highlight that it is much more complicated to obtain evidences about the efficiency of the policies when they have been correctly implemented and they have been successful avoiding or reducing the impacts of the crises.

3.1 Policies Applied to Internal Resilience

For technical resilience, three different resilience policies have been defined for each CI: CI Design, CI Maintenance, and CI Data Acquisition and Transmission Systems. To enhance organizational resilience, the following two policies can be implemented: CI Capacity for Crisis Detection, Communication and Analysis and CI Workforce Training. Finally, only one policy, which is called CI Crisis Budget, has been defined to build up the economic resilience of an organization (see Fig. 2).

Internal Resilience	
Technical Resilience	CI Design CI Maintenance CI Data Acquisition and Transmission Systems
Organizational Resilience	CI Capacity of Crisis Detection, Communication and Analysis CI Workforce Training
Economic Resilience	CI Crisis Budget

Fig. 2. Resilience policies within the internal resilience

CI Design. CI Design 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, to increase the security level of the system, many infrastructures include additional security systems that should be designed in order to properly work in critical situations. Therefore, the design and construction of these security systems should be carried out consciously to make sure they are operational during the crisis. Finally, not only should the infrastructure design be reliable and robust but also care has to be taken not to introduce new vulnerabilities into the system when updates are introduced.

Two real cases that illustrate the potential catastrophic consequences due to inappropriate infrastructure design are the cases of Ford Motor Company and the DC-crash in Paris. In the 70s, the Ford Motor Company launched the Pinto model to compete with Japanese models. The narrow schedule for its design in addition to considerations of trunk space and manufacturing costs led engineers to place the gas tank between the differential and the rear bumper. In this position, a rear-end collision might push the gas tank forward into the differential, where the exposed bolts could rupture the tank, possibly leading to a fire or explosion. This serious design error cost Ford millions of dollars in legal settlements to accident victims in addition to untold damage to its reputation [4]. The other example was the DC-10 crash that occurred in Paris in 1974. In this case, a defectively designed rear cargo door blew open at an altitude of 12,000 feet, triggering cabin depressurization [5].

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.

The critical nature of maintenance in preventing crises is clear as can be shown in the following example. In 1979, a DC-10 crashed in Chicago because of a maintenance problem. An improper maintenance procedure caused the left engine to break loose, severing control cables in the wing, and making it impossible for the pilots to control the airplane [5].

CI Data Acquisition and Transmission Systems. 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.

The Canadian Blackout and the Spanair aircraft accident are two real cases in which the triggering event could not be avoided because the data acquisition and transmission systems did not work properly.

The Canadian Blackout that occurred in 2003 supports the fact that this policy helps preventing crises from occurring [6]. During a period of hot weather, many air conditioners were being used and the electricity demand increased considerably, leading to peaks in the electricity supply. The communication systems did not work as expected, and consequently grid managers did not receive the information about what was happening in real-time. As a result, managers were not aware of the critical state of the power grid and therefore, were not able to take action to prevent or mitigate the blackout.

In the same vein, in the case of the Spanair aircraft accident that occurred in Spain (2008) killed 154 passengers. The data from investigation showed that the takeoff manoeuvre took place with the flaps and slats retracted because the early warning system that should have detected the incorrectly positioned wing flaps failed to alert the crew to the problem [7].

CI Capacity of 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, proposing 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 whole system. Firstly, the operators should be able to detect and interpret the data provided, identifying 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.

The following two real cases manifest the importance of this policy to avoid the occurrence of a crisis. In 1977, the runway collision in Tenerife happened because of an occurrence of uncontrollable circumstance and an accumulation of human errors. The control tower and the crews of both planes were unable to see one another due to a sudden fog. Miscommunication between the tower and one of the airplanes caused the airplanes to collide [5].

In the case of the Italian power outage of 2003, the operators were unconscious of the urgency regarding the overload of the San Bernardino line. They were unaware of the fact that the overload on San Bernardino was only allowable for about fifteen minutes. Ten minutes after the trip ETRANS (Swiss network operator) called GRTN (Italian network operator) to decrease imports by 300MW. This measurement was completed by GRTN within 10 minutes. Despite the efforts,

it was insufficient to relieve the overload and consequently San Bernardino line disrupted [8].

CI Workforce Training. Workers 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. 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. In addition to this, they also have to train their sensemaking 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.

The Italian Blackout and the Chernobyl accident are two clear examples in which the negative consequences due to human errors can be illustrated. In 2003 in Italy, some electrical grid operators took inappropriate and ineffective measures, which added nine minutes to the time it took to solve the problem. This mismanagement was consequence of lack of training and it led to the disruption in the Sils-Soazza line and the Mettlen-Lavorgo line, disconnecting them from the grid [8,9].

Human error was one of the main causes of the Chernobyl accident. Technicians wanted run an experiment on the main reactor's main turbine in order to verify whether in the event of a power cut turbines would be able to supply enough power to the pumps before the standby diesel generators took over. When they began with the test, they suddenly realized that the reactor was working in unstable conditions but they ignored the situation and carried out the experiment until the reactor exploded [5,10].

CI Crisis Budget. CIs should have resources set aside in order to cover repairs and replacements, 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.

The recent BP Oil Spill is a good example that shows how the CI should possess some extra resources to be able to face the extra costs that arise from an accident.

The pool of money that BP has for emergencies seems to be enough to cover this severe incident. At the time of the Gulf oil spill, BP set up a $20 billion trust fund in order to satisfy the claims, which is plenty since until May 2011 they have only had to pay around $6 billion [11].

3.2 Policies Applied to External Resilience

Within the external resilience level we defined four dimensions. The policy that could help to improve technical resilience is having technical equipment available to first responders. First Responder Training and Government Preparation

allow crisis managers to improve the organizational resilience. Having a large Public Crisis Budget for extra costs arising from a crisis allows all the expense of recovery and response activities to be covered. Finally, training society for crisis management and having well defined and updated regulations enhance the social resilience level (see Fig. 3).

External Resilience	
Technical Resilience	Equipment Availability for First Responders
Organizational Resilience	First Responders Training Government Preparation
Economic Resilience	Public Crisis Budget
Social Resilience	Societal Preparation Legal and Regulatory issues

Fig. 3. Resilience policies within the external resilience

Equipment Availability for First Responders. 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.

The following three examples expose how important is the availability of this equipment not to worse the critical situation and to increase the technical resilience level of the society.

During the gas leak in Bhopal, first responders realized there were serious problems because there were not effective emergency medical facilities or adequate transport for emergency evacuations [12]. The Exxon Valdez oil spill is another example in which there was a lack of equipment to deal with an oil spill of such magnitude and a long time was needed to get it [13].

Mendez-Martnez [14] claim that in the case of Prestige oil spill, the lack of adequate systems for prevention and response, led the Spanish government to accept several equipment offers from other nations which caused delays and a less efficient response.

First Responder 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 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.

The Bhopal accident and Exxon Valdez oil spill are two accidents where first responders lacked training and as a result the impact increased.

According to Bisarya and Puri, when the Bhopal accident occurred, the Mayor and the Chief Police of Bhopal recognized that they were not prepared to face such a crisis. They did not have the proper information about the storage of hazardous and dangerous materials in the plant or about their side effects. Furthermore, they found lack of coordination among company and emergency services [12]. In the case of Exxon Valdez oil spill, the first responders lacked the training to handle such major spills, and as a result the response time was longer than expected and consequently there was a large adverse impact [13].

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 sensemaking capacity because crises are uncertain and complex. Therefore, crisis managers need to understand the critical situation and adapt to it rapidly [15]. 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.

The following three examples describe the importance of the government preparation in the effective crisis management. The government's inability to communicate and coordinate all the stakeholders related with crisis response and to get help from other nations will result in longer recovery times and greater impact, as was the case during the Exxon Valdez oil spill [13]. In the case of Prestige oil spill, although many experts said that the best alternative was to move the ship to the coast because of adverse weather, the stormy sea and the critical condition of the vessel, the Spanish authorities instead ordered to it be removed from the shore, and as a result the strength of the high seas crashed the vessel completely, spilling all the oil and increasing the resulting environmental damage [14].

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.

Two mining accidents explained below illustrate how having extra public money allocated for crises can lead to a satisfactory resolution.

The government's level of commitment may lead to totally different consequences for similar accidents. In the case of the San José mining accident that occurred in Chile in 2010, the high amount of resources invested by Chile's government allowed a rescue system to be built, which consequently saved the lives of all the miners. On the contrary, the Mexican government's attitude was different in the Pasta de Conchos mining accident. In this case, the government did not help in the rescue, and as a result 65 miners died [16].

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 and so they need more personnel resources and some volunteers to repair damage.

Training the public would allow citizens to assist society during a crisis, thus reducing possible adverse effects. Society's awareness is very important factor in order to society 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.

In the case of the Prestige oil spill, the good practice of this policy enhanced in the response. Not only did volunteers help to clean the Galician cost, but they also brought about greater involvement from institutions and the government [17].

Legal and Regulatory Issues. Legal and Regulatory issues relate to the maturity level of the crisis regulations in order to take preventive measures and define protocols to know the responsibilities that each entity has when facing a crisis.

The regulations that private companies should meet, the regulations for the first responders and regulations for the public would allow everyone to be more prepared for the crisis and reduce possible impact. Indeed, 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.

The Chernobyl accident and the Italian Outage are two examples that highlight the need of a policy to improve crisis management.

The ability to deal with the Chernobyl accident was affected by the lack of proper regulation and the unstable political situation in the country. The regulations were mainly focused on the immediate response and lacked information about the post emergency period. Thus, the tragedy's consequences needed more time to be solved leading to a significant increase of the impact [18].

The Italian Outage [9] shows that having different regulations in Swiss and Italy lead to a longer resolution period. Thus, a unified legal and regulatory framework throughout Europe is necessary to ensure the security of grid operation and supply in Europe. Having different regulations in Swiss and Italy led to a longer resolution period.

4 The Influence of Policy Implementation Level on Crisis Impact

Not all the policies implementation level affects a crisis at the same point of its lifecycle. Even though all of them have some influence during the whole process, several policies are more successful at preventing a crisis whereas others mostly influence in the response and recovery period and also reduce impact (see Fig. 4).

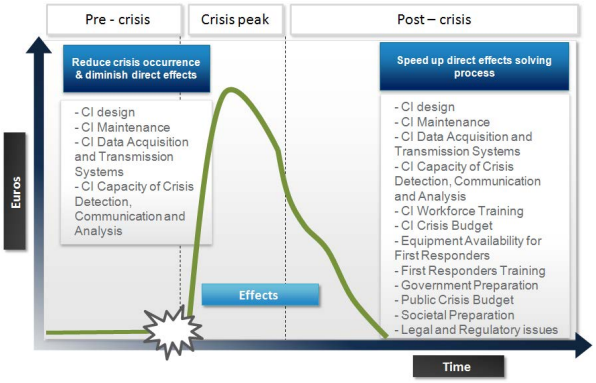

Fig. 4. The influence of the policies throughout the whole lifecycle of a crisis

High level of CI Design, CI Maintenance, CI Data Acquisition and Transmission Systems, and CI Capacity of Crisis Detection, Communication and Analysis help to prevent the occurrence of a crisis. If our CI design is robust and secure enough and it is well maintained, it may be able to withstand some major hazards and prevent the triggering event from taking place. Moreover, if our data acquisition and transmission system is the appropriate one, we will be able to detect early warning signals and take measures to keep a crisis from occurring. Finally, the good level of detection, communication and analysis policy helps us to correctly interpret the signals we are receiving from the system and communicate threats to the managers so they can take the corresponding measures.

In the case of reducing impact, all the policies have an influence. Having a good level of all policies will allow all stakeholders to be more prepared to respond and recover from a crisis.

5 Conclusions and Future Work

Resilient Critical Infrastructures reduce the probability of incidents and crises occurring, and if they do occur, the impact will not be so significant. As a consequence, building resilience has become the most promising strategy in crisis management. This work-in progress research attempts to present and illustrate how this can be done with examples of twelve policies that contribute to this resilience building process. Bearing in mind these policies and their consequences will provide new insights to CI security managers.

However, this research is still incipient as we have not defined how each policy implementation level and system's resilience level can be quantified yet. Moreover, the influence of each policy into the overall system's resilience level needs to be also evaluated. As resources are scarce, in most cases it is impossible to implement all the policies. Therefore, knowing before the crisis which policy is the most efficient in diminishing impact would allow prioritizing them.

References

1. Rinaldi, S.M.: Modeling and simulating critical infrastructures and their interdependencies. In: Proceedings of 37th Hawaii International Conference on System Sciences. IEEE Computer Society, Washington, DC (2004)
2. Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., von Winterfelt, D.: A framework to quantitatively assess and enhance seismic resilience of communities. Earthq. Spectra 19, 733–752 (2003)
3. Multidisciplinary Center for Earthquake Engineering Research (MCEER): Engineering Resilience Solutions (2008)
4. Fleddermann, C.B.: Engineering Ethics. Prentice Hall (2004)
5. Manion, M., Evan, W.M.: Technological catastrophes: their causes and prevention. Technology in Society 24, 207–224 (2002)
6. US-Canada Power System Outage Task Force: Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (2004)
7. Comisión de Investigación de Accidentes e Incidentes de Aviación Civil: Accident involving aircraft McDonnell Douglas DC-9-82 (MD-82), registration EC-HFP, operated by Spanair, at Madrid-Barajas airport on 20 August 2008 (2008)
8. Union for the Coordination of Transmission of Electricity (UCTE): Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy (2004)
9. CRE and AEEG: Report on the Events of September 28th, 2003 culminating in the separation of the Italian Power System from the other UCTE Networks (2004)
10. Dörner, D.: The Logic of Failure. Addison-Wesley, Massachusetts (1997)
11. British Petroleum: Public Claims Status, `http://responsedata.bp.com/files/PublicClaimsStatusTracking05052011v2.pdf` (retrieved on 2011)
12. Bisarya, R.K., Puri, S.: The Bhopal gas tragedy - A perspective. J. Loss Prev. Process Ind. 18, 209–212 (2005)
13. Skinner, S.K., Relly, W.K.: The Exxon Valdez Oil Spìll (1989)
14. Méndez-Martínez, C.: Libro Blanco sobre el Prestige. Gobierno del Principado de Asturias, Oviedo (2003)

15. Boin, A., McConnell, A.: Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. J. Conting. Crisis Manag. 15, 50–59 (2007)
16. Taniguchi, H.: El rescate de mineros en Chile revive las heridas del accidente en México, México (2010)
17. García-Mira, R., Real, J.E., Uzzell, D.L., San Juan, C., Pol, E.: Coping with a threat to quality of life: the case of the Prestige disaster. Revue Européenne de Psychologie Appliquée/European Review of Applied Psychology 56, 53–60 (2006)
18. Demin, V.F., Yatsalo, B.I.: Chernobyl Lessons Learned for Post-Emergency Response. IRPA 10 (2000)