Reliability Engineering and System Safety 141 (2015) 92–105

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Resilience framework for critical infrastructures: An empirical study in a nuclear plant

Leire Labaka*, Josune Hernantes [1], Jose M. Sarriegi [2]

TECNUN—University of Navarra, Paseo Manuel Lardizabal, 13, 20018 San Sebastian, Spain

ARTICLE INFO

Available online 17 March 2015

Keywords:
Resilience
HRO
Crisis management
Empirical research
Case study
Nuclear power plant

ABSTRACT

The safety and proper functioning of Critical Infrastructures (CIs) are essential for ensuring the welfare of society, which puts the issue of improving their resilience level at the forefront of the field of crisis management. Most of the resilience-building principles defined in the literature do not cover all the dimensions that make up resilience and most of them only focus within the boundaries of the CI, neglecting the role of the external agents that also have an influence on enhancing resilience. Furthermore, most of the principles that are present in the literature are theoretical and difficult to implement in practice.

In light of this situation, the aim of this research is to present a holistic resilience framework for critical infrastructures in order to improve their resilience level by taking into account internal and external agents and covering all the resilience dimensions. Furthermore, this framework has been defined in close collaboration with the general management of CIs to facilitate its implementation in practice. Finally, in order to illustrate the value added of this framework it was implemented in a nuclear plant.

1. Introduction

Currently, Critical Infrastructures (CIs) underpin the economy, safety, and social sustainability of modern society, and therefore, providing highly reliable service is paramount for the welfare of society [1,2]. CIs are defined as systems, services and assets that are vital for the welfare of society, and whose disruption or destruction has severe impact on the health, security, safety or economic well-being of citizens and on the effective functioning of government [3,4].

CIs have grown in size and complexity in order to provide a high level of reliability and safety in their services, but in doing so they have also inadvertently increased their vulnerability. Furthermore, the number of agents involved in a crisis affecting critical infrastructure has increased, which has led to an increase in the complexity of crisis management. In addition to the agents involved in the resolution of the affected CI, external stakeholders such as government, first responders, and society also play an important role in managing crises. In order to properly deal with crises, their adequate preparation is of utmost importance.

Recent terrorist attacks and natural disasters that threaten the proper functioning of CIs have increased concern about the reliability and safety level of CIs [1,5], making the creation of resilient CIs that are able to cope with crises an issue of paramount importance in the field of crisis management [1,6–8].

There are several definitions of resilience in the literature, each reflecting a different disciplinary perspective [9–11]. However, almost all the definitions can be characterized by the following pillar capacities: preventive capacity, absorptive capacity and recovery capacity [12–14]. We define resilience as the capacity of a system to prevent the occurrence of a crisis, and when a crisis does occur, the capacity to absorb the impact and to efficiently recover the normal state of operation. The literature characterizes the following four dimensions of resilience [15–17]:

- Technical resilience: This refers to the ability of the organisation's physical system to perform properly when subject to a crisis.
- Organisational resilience: This refers to the capacity of crisis managers to make decisions and take actions that lead to the avoidance of a crisis or at least to a reduction of its impact.
- Economic resilience: This refers to the ability of the CI to absorb 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 volunteers.

* Corresponding author. Tel.: +34 943 219877x2574.
E-mail addresses: llabaka@tecnun.es (L. Labaka), jhernantes@tecnun.es (J. Hernantes), jmsarriegi@tecnun.es (J.M. Sarriegi).
[1] Tel.: +34 943 219877x2491.
[2] Tel.: +34 943 219877x2492.

http://dx.doi.org/10.1016/j.ress.2015.03.009
0951-8320/

Several authors argue that these dimensions are often studied separately without taking into account their interrelationship [18,19]. As a result of this weakness sociotechnical models were developed in which they interrelate technical aspects and the stakeholders involved in crisis management, such as legislators, government agencies, insurance companies, top managers, crisis managers and system operators [20]. If we analyze resilience dimensions independently they could be assessed as satisfactory, but crisis could be originated due to the lack of integration of these dimensions, i.e. a valve could be the right one but operators might not have the required training for its proper use [20].

Recently, in a step that moves the application of resilience forward, a new paradigm called resilience engineering has emerged within the field of crisis management. Resilience engineering focuses on developing tools and methods that improve resilience. More specifically, resilience engineering looks for tools and methods that improve the overall capacity of CIs to create processes that are robust but flexible, to monitor and revise risk models, and to use resources proactively in the face of disruptions or on-going production and economic pressures [21]. A distinctive feature of resilience engineering is its emphasis on how success is obtained, which is by being able to understand and foresee when a system may lose its stability rather than focusing on errors [22].

The literature provides a broad set of works that discuss general characteristics and principles for improving the resilience level of systems [9,13,23]. Several quantitative and qualitative models that assess the resilience level of systems [9,24–26] are also found in the literature. However, these models have limitations in their implementation [27]. Furthermore, it is harder to find empirical research on how resilience improvement principles can be implemented in practice [27,28]. The lack of comprehensive resilience assessment models and of practical guidelines for implementation means that CIs have still not fully adopted the concept of resilience in their processes, despite the potential benefits that resilience presents in terms of safety and costs. Because of the theoretical nature of current resilience frameworks [13] and because the principles of resilience noted in the literature are limited to describing their meaning and advantages and do not provide specific activities or actions for their practical implementation [28,29], crisis managers have difficulties determining which activities or policies they should carry out to improve the resilience level of their CIs [30].

Given the above gaps, the present research develops a resilience framework that helps CIs to improve their resilience level. The framework is composed of sixteen resilience policies and several sub-policies that any type of CI should implement in order to improve its resilience engineering. In order to confirm that the framework provides value to crisis managers to improve the resilience level of CIs, a case study was carried out in a nuclear plant. Nuclear plants are one of the most resilient CIs because they operate in a high-risk environment where any failure could lead to highly detrimental effects. As a consequence, their resilience level is high and it is constantly being improved. This paper explains the implementation of the resilience framework in a nuclear plant and highlights the results and the value added by this implementation. The following section describes the literature on resilience engineering principles and assessment methods, and then presents the contribution of this research. Section 3 presents our research methodology, and Section 4 explains the resilience framework developed in this research. Section 5 and 6 illustrate the results obtained in the case study and finally, Section 7 highlights the conclusions and limitations of our research and proposes future steps in order to improve the framework.

2. Resilience engineering principles and assessment

The literature contains several definitions of resilience as well as several resilience-building principles [11]. These principles help to identify the policies that should be implemented in order to enhance the resilience level of a CI, and they also indicate what factors should be assessed to estimate a CI's resilience level. Prior and Hagmann [27] describe five reasons for measuring resilience: characterising resilience, raising resilience awareness, allocating resources for resilience, building resilience, and assessing resilience policy performance.

Some authors [15–17] define the following characteristics as being the main features of the resilience building process: robustness, resourcefulness, redundancy, and rapidity. Bearing in mind these four characteristics, Cimellaro et al. [26] present a framework for the analytical quantification of disaster resilience based on a system's functionality level and recovery time. However, recent literature [11] has defined resilience more as a process than an outcome since the outcome not only depends on the resilience level but also on the magnitude of the hazard. Concentrating more on the approach that considers resilience-building as a process, Francis and Bekera [25] discuss the diversity of factors and dimensions that are been related to the concept of resilience, and all of them are summarized in terms of three main capacities: absorptive capacity, adaptive capacity, and restorative capacity. These capacities are the base of their definition of a resilience metric that assesses the resilience level of CIs. Nevertheless, the analytical framework proposed by Cimellaro et al. [26] as well as the resilience metric defined by Francis and Bekera [25] can only be used when a crisis occurs, since the parameters are defined based on the system's performance level. In fact, they are barely able to assess the degree of resilience improvement in the absence of a crisis situation.

At the organisation level, a research group in New Zealand called Resilient Organisations defines a framework composed of thirteen resilience indicators for the improvement of the resilience level of companies [31]. In a similar vein, High Reliability Organisations (HROs) are defined as organisations that operate complex and high-risk technologies and manage to remain accident free for long periods of time, while simultaneously achieving highly variable and demanding production goals. Weick and Sutcliffe [32] and Lekka [33] define several principles that organisations should apply in order to improve their resilience level and become HROs. The framework proposed by the Resilient Organisations group, as well as the principles of HROs, focus on organisational management, without taking into account other resilience aspects, such as technical or social and external aspects. Concentrating on industrial processes, Dinh et al. [13] define several resilience strategies, principles and factors and through a case study they illustrate how these principles and factors help to create more resilient industries.

In looking more deeply at the concept of resilience engineering, although the literature does not have a widely accepted set of principles, various studies define the following principles as having the potential to improve resilience engineering [9,23,34]: top-level commitment, just culture, learning culture, awareness, preparedness, flexibility, and opacity. Taking these seven principles as a basis, Shirali et al. [23] propose a method for the quantitative assessment of resilience engineering based on the data obtained from a questionnaire given to employees that addressed these principles. In another study, Costella et al. [9] reduce the resilience engineering principles to four (top management commitment, flexibility, learning, and awareness), and based on these principles they define a method for assessing a health and safety management system (MASH).

Leveson et al. [19,20] stress the importance of the integration of different socio-technical factors in order to improve resilience. They propose a model of accident causation (STAMP) based on system theory. STAMP integrates resilience dimensions including organizational, social, economic and technical aspects. The model