RESILIENCE CAPACITIES ASSESSMENT FOR CRITICAL INFRASTRUCTURES DISRUPTION

Anoop Sharma
(815748)

Supervisor
Prof. Paolo Trucco

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science (Laurea Magistrale) in Civil Engineering for Risk Mitigation



POLITECNICO
MILANO 1863

The Department of Civil and Environmental Engineering
Politecnico di Milano
Italy
2017

ACKNOWLEDGEMENT

I would like to thank my advisor Professor Paolo Trucco, whose expertise and guidance help made this work possible. My special thanks goes to Professor Dr. Boris Petrenj, He was readily available to answer any of my queries and showed considerable forbearance with me. It was a great pleasure working with him. I would also like to thank my parents, whose steadfast support has helped me grow as an individual. A special thanks, goes to all my professors and lecturers at Politecnico di Milano, whose invaluable guidance and teaching helped me in my studies. Lastly, I'd like to convey my thanks to all my friends and family, they helped me silently in background without them life would be a lot less fun.

ASTRATTO

La resilienza delle infrastrutture critiche è oggi uno degli elementi chiave per poter assicurare non solo continuità operative ma anche per garantire la disponibilità di beni vitali per le nostre società by leading to disruptions. Negli ultimi anni l'approccio della protezione delle infrastrutture critiche si è spostato dalla mera protezione alla resilienza. Il metodo basato sulla resilienza si fonda sull'assunto che non tutti gli eventi distruttivi che coinvolgono i sistemi di infrastrutture critiche possono essere prevenuti. Da qui la necessità di creare sistemi di infrastrutture critiche più resilienti che possano assorbire e ricostituirsi dopo potenziali shock, in quanto è fondamentale educare la società ad affrontare eventi inaspettati.

Il presente progetto di tesi si propone di valutare la capacità delle infrastrutture critiche durante potenziali scenari di distruzione per la protezione delle infrastrutture critiche (PIC) attraverso la creazione di un framework e di un software. A seguito di uno studio sulla letteratura in merito, è stato sviluppato un framework completo di software per la valutazione delle capacità in diversi scenari. Vengono inoltre forniti una guida al software per la selezione delle funzionalità all'interno dell'organizzazione e un manuale per l'utente finale. Per la validazione il sistema pilota è stato applicato in casi di blackout in Lombardia, Italia. In conclusione, sono state discusse strategie di resilienza in casi di blackout basati su analisi GAP e sulla capacità di costruzione a livello regionale e a livello operativo.

Keywords: Protezione delle infrastrutture critiche; Resilienza; Gestione dell'emergenza; Capacità; Analisi GAP

ABSTRACT

The resilience of critical infrastructure (CI) systems has become one of the key elements to assure not only the continuity of operations but also the availability of vital functions for our societies by leading to disruptions. In recent days CI protection is being moved from a focus on protection to a focus on resilience. Resilience approaches build on the assumption that not all disruptive events involving CI systems can be prevented and that there is a need to create more resilient CI systems which can absorb and recover from potential shocks, as there is a need to better prepare the societies to face the unexpected.

This thesis project aims at to assessing resilience in critical infrastructure in potential disruption scenarios relevant for CIP through creating a framework and tool. After literature review, A frame work along with tool has been developed to assessment of capabilities in different scenarios. The guide to select capabilities within organization and a user guide of the tool for end user is also described. For validation of tool pilot application is performed for blackout scenario in Lombardy region of Italy. Finally, resilience strategies for blackout scenarios are discussed based on GAP analysis along with Capacity building on regional level and operational level.

Keywords: Critical infrastructure protection; resilience; Emergency management; capabilities; GAP Analysis

Contents

CHAPTER 1 – INTRODUCTION 1
1.1. Critical Infrastructure and its importance 1
1.1. Sectors of Critical infrastructure 3
1.1.1. American sectors of critical infrastructure as per Presidential Policy Directive 21 3
1.1.2. European critical infrastructure sectors 4
1.2. Critical Infrastructure Protection (CIP) 4
1.3. Resilience: Definition and terminology 5
1.4. Emergency Management (EM) 7
1.5. Aim and Scope of the thesis 9
CHAPTER 2 – STATE OF THE ART 11
2.1. Terminology 11
2.1.1. Incident, Accident, crisis, emergency, disaster and catastrophe 11
2.2. Critical Infrastructure Resilience 13
2.3. EMERGENCY MANAGEMENT: 21
2.4. Capability-based planning 24
CHAPTER 3 – THE RESILIENCE CAPACITY ASSESSMENT FRAMEWORK 26
3.1. Resilience Capacity 26
3.1.1. Capability compounds 30
3.1.2. Capabilities data model 31
3.2. The Resilience capacity assessment 32
3.2.1. The scope of the Resilience capacity assessment 38
Chapter 4: Identifying the capabilities in Critical infrastructure: 40
4.1. Classification of Capabilities 40
4.2. Identification of capabilities in EM cycle mission areas: 42
4.3. Capability building cycle and Gap Analysis 60
CHAPTER 5- IMPLEMENTATION OF THE SW TOOL 62
5.1. Description of a model 62
5.2. The Relational Database Model 63
5.2.1. Programming Environment (Microsoft Access) 64
5.3. description of tool and End User guide 65
5.3.1 System description: 66
5.3.2. Characterization: 72

5.3.3. Resilience assessment and analysis 73
CHAPTER 6- PILOT APPLICATION IN LOMBARDY REGION 76
6.1. Blackout event 76
6.2. CI operators participating in Thematic Task Force 77
6.2.1. Capacity classification 77
6.2.2. Capability assessment 78
6.2.3. Intra-organisational Gap Analysis: 79
6.3. Blackout resilience strategies: 80
6.4. Pilot case's Blackout resilience strategy 82
6.4.1. Degree of alignment between Operators' Improvement Plans and actual map in strategy number 2. 82
6.4.2. Gap Analysis for strategy 2: 83
6.5. Capacity Discussion & Capacity building on regional level and operational level: 84
References: 86

List of Figures

Figure 2.1-1 Terminology 13
Figure 2.3-1 EXAMPLES OF DIVIDING THE EM CYCLE INTO PHASES 22
Figure 2.3-2 PRINCIPLES OF EMERGENCY MANAGEMENT 22
Figure 2.3-3 Crisis Management Phases 23
Figure 2.3-4 APPROACH TO BUILDING AND SUSTAINING NATIONAL PREPAREDNESS GOAL 24
Figure 3.1-1 MEASURE OF RESILIENCE - CONCEPTUAL DEFINITION 26
Figure 3.1-2 The resilience triangle showing three major capacities that make up the resilience capacity of a system 28
Figure 3.1-3 System resilience capacities that contribute to the ability of a system to prevent, absorb, adapt to, and/or rapidly recover from a potentially disruptive event 29
Figure 3.1-4 System features that may contribute to the system resilience 30
Figure 3.1-5 Capability Data Model 32
Figure 3.2-1 BUILDING SYSTEM RESILIENCE 35
Figure 3.2-2 INTER-ORGANIZATIONAL MODEL 36
Figure 3.2-3 COUPLING RESILIENCE CAPABILITY SOLUTIONS TO SPECIFIC CIS 38
Figure 4.1-1 CLASSIFICATION OF CAPABILITIES 42
Figure 4.2-1 Flow chart for identity fication of capabilities 43
Figure 4.2-2 Protection and Integrated Capabilities 45
Figure 4.3-1 CAPACITY BUILDING CYCLE 61
Figure 5.1-1 model 63
Figure 5.2-2 model relationship diagram 65
Figure 5.3-1 overview of tool 66
Figure 5.3-2 System description 66
Figure 5.3-3 Edit organization 67
Figure 5.3-4 edit capabilities 68
Figure 5.3-5 edit hazard threats 69
Figure 5.3-6 Edit Infrastructures 71
Figure 5.3-7 accident specification 72
Figure 5.3-8 Edit asset vulnerability 73
Figure 5.3-9 resilience assessment 74
Figure 5.3-10 Assessment of capabilities 75
Figure 6.2-1 Pi chart of Intra-organizational Gap in terms of Operators' improvement plan 80
Figure 6.4-1 improvement plan 84

List of tables

Table 2.3-1 time frame for each phase 23
Table 3.2-1 RESILIENCE CAPABILITIES' SPACE 33
Table 3.2-2 Ranking resilience solutions for implementation/enhancement 38
Table 3.2-3 THE SCOPE OF THE READ PROJECT IN THE RESILIENCE CAPABILITIES' SPACE 39
Table 4.2-1 Capabilities by Mission Area 44
Table 4.2-2 CAPABILITY MAPPING ASSESSMENT SCALE 60
Table 5.3-1 Hazard Classification 69
Table 6.2-1 the standard template 77
Table 6.2-2 Capacity classification 78
Table 6.2-3 standard assessment 78
Table 6.2-4 Intra-organizational Gap in terms of Operators' improvement plan 79
Table 6.2-5 gap analysis 79
Table 6.2-6 resilience capacity in em phases 80
Table 6.3-1 Strategic Objective for Strategy no. 1 81
Table 6.3-2 Capability Mapping of Actual Map by Strategic Objective 81
Table 6.3-3 Strategic Objective for Strategy no. 2 82
Table 6.3-4 Capability Mapping of Actual Map by Strategic Objective 82
Table 6.4-1 Degree of alignment between Operators' Improvement Plans and actual map 83

CHAPTER 1 – INTRODUCTION

Functioning of today's societies is relying on a sustainable, efficient, safe, and reliable operation of infrastructure systems that are critical for the economy and the society. Considering this fact, negative side effects of any problem or delay in data collection, access, usage, and propagation do not abide by the quality of decision- making but should also influence the quality of Emergency response. To maximize the potential advantages of infrastructure investment, and minimize its social and environmental costs in the future, intelligent systems are adapted to the current critical infrastructures. There are two factors that play a main role in all phases of emergency management: Information sharing and collaboration, which enables simplified and efficient prevention of, response to and recovery from all hazards.

1.1. Critical Infrastructure and its importance

"Critical infrastructures" is a term used to describe systems or assets that are essential for the functioning of a society and economy. But in Broadway, Despite the numerous attempts, there is still no universal definition of critical infrastructure, or at least a definition that provides a classification suiting the characteristics of each nation. Generally, A critical infrastructure is often identified as that infrastructure whose incorrect functioning, even for a limited time, may negatively affect the economy of individual subjects or groups, involving economic losses and/or even expose people and things to a safety and security risk [Lewis, 2013]. however, the definition of critical infrastructure varies slightly from country to country. There are few definitions below with different perspective.

The definition of critical infrastructure (CI) accepted by Australia is "those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defense and ensure national security." (national guidelines protection critical infrastructure from terrorism)

Responding to a parliamentary inquiry, the Austrian federal chancellor defined critical infrastructures as “natural resources, services, information technology facilities, networks, and other assets which, if disrupted or destroyed would have serious impact on the health, safety, or economic wellbeing of the citizens or the effective functioning of the Government.” This definition conforms to the definition elaborated by the EU. [Brunner and Suter, CIIP Handbook 2008-09]

Accordingly, the Hungarian definition of the concept of critical infrastructure corresponds to the definitions of the EU as formulated in the Green Paper of the EU Commission. Critical Infrastructures, as per the Hungarian Green Book, are defined as interconnected, interactive, and interdependent infrastructure elements, establishments, services, and systems that are vital for the operation of the national economy and public utilities to maintain an acceptable level of security for the nation, individual lives, and private property, as well as concerning the maintenance of the economy, the public health services, and the environment. [Brunner and Suter, CIIP Handbook 2008-09]

In the US, critical infrastructures are defined according to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism [USA PATRIOT ACT 2001]: “the term ‘critical infrastructure’ means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” [USA PATRIOT Act (H.R. 3162)]

The Communication of the Commission of the European Communities (EU Commission) on Critical Infrastructure Protection in the Fight Against Terrorism, adopted on 20 October 2004, provides a definition of critical infrastructures (CI), enumerates the critical sectors identified, and discusses the criteria for determining potential CI. In the Communication, CI are defined as follows: “Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy and key government

services.” [Critical Infrastructure Protection in the Fight against Terrorism (Brussels, 20 October 2004]

1.1. Sectors of Critical infrastructure

1.1.1. American sectors of critical infrastructure as per Presidential Policy Directive 21

On February 12, 2013, the President issued PPD-21, Critical Infrastructure Security and Resilience, which explicitly calls for the development of an updated national plan. The directive builds on the extensive work done to date to protect critical infrastructure, and describes a national effort to share threat information, reduce vulnerabilities, minimize consequences, and hasten response and recovery efforts related to critical infrastructure. It also identifies 16 critical infrastructure sectors. [Department of Homeland Security, 2013]

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

1.1.2. European critical infrastructure sectors

The Green Paper on EPCIP identifies the following critical sectors and their products and services: [European Programme for Critical Infrastructure Protection, 2005]

- Energy (Oil and Gas Production, Refining, Treatment and Storage, including Pipelines; Electricity Generation; Transmission of Electricity, Gas, and Oil; Distribution of Electricity, Gas, and Oil),
- Information and Communication Technologies (ICT) (Information System and Network Protection; Internet; Provision of Fixed Telecommunications; Provision of Mobile Telecommunications; Radio Communication and Navigation; Satellite Communication; Broadcasting),
- Water (Provision of Drinking Water; Control of Water Quality; Stemming and Control of Water Quantity),
- Food (Provision of Food and Safeguarding Food Safety and Security),
- Health (Medical and Hospital Care; Medicines, Serums, Vaccines, and Pharmaceuticals; Bio-Laboratories and Bio-Agents),
- Financial System (Payment Services/Payment Structures (private); Government Financial Assignment), • Public and Legal Order and Safety (Maintaining Public and Legal Order, Safety and Security; Administration of Justice and Detention),
- Civil Administration (Government Functions; Armed Forces; Civil Administration Services; Emergency Services; Postal and Courier Services),
- Transport (Road Transport; Rail Transport; Air Traffic; Inland Waterways Transport; Ocean and Short-Sea Shipping),
- Chemical and Nuclear Industry (Production and Storage/Processing of Chemical and Nuclear Substances; Pipelines of Dangerous Goods (Chemical Substances),
- Space and Research.

1.2. Critical Infrastructure Protection (CIP)

Promoted by threats, a new knowledge area known as Critical Infrastructure Protection (CIP) was created to protect CI. 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). 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).

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. Resilience: Definition and terminology

Resilience is derived from Latin word resilio, that means “to jump back”. Most of the literature states that the study of resilience evolved around disciplines of psychology and psychiatry in the 1940s (Waller, 2001; Johnson and Wiechelt, 2004). but originally concept of resilience was for, some say ecology (Batabyal, 1998), while other researchers

say physics (Van der Leeuw and Leygonie, 2000). However, today resilience is being applied in many fields, especially disaster & emergency management.

There are different definitions of Resilience, as defined in PPD-21, is “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, it includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.” Having accurate information and analysis about risk is essential to achieving resilience. Resilient infrastructure assets, systems, and networks must also be robust, agile, and adaptable. Mitigation, response, and recovery activities contribute to strengthening critical infrastructure resilience.

However, there are also diverse definitions and perspectives in the literature regarding this concept. There are some definitions that are chronically written below

Author	year	definition
Wildavsky	1988	“Resilience is the capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back.”
Hoiling et al.	1997	resilience is the buffer capacity or the ability to a system to absorb perturbation, or magnitude of disturbance that can be absorbed before a system changes its structure by changing the variables
Mallak	1998	Local resiliency with regard to disasters means that a locale is able to withstand an extreme natural event without suffering devastating losses, damage, diminished productivity, or quality of life without a large amount of assistance from outside the community
Comfort	1999	resilence is The capacity to adapt existing resources and skills to new systems and operating conditions.

Paton et al.	2000	Resilience describes an active process of self-righting, learned resourcefulness and growth the ability to function psychologically at a level far greater than expected given the individual's capabilities and previous experiences.
Kendra & Wachtendorf	2003	The ability to respond to unique and singular events.
Cardona	2003	The capacity of the damaged ecosystem or community to absorb negative impacts and recover from these.
Pelling	2003	The ability of an actor to cope with or adapt to hazard stress.
UNISDR	2005	The capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organising itself to increase this capacity for learning from past disaster for better future protection and to improve risk reduction measures.

1.4. Emergency Management (EM)

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

are predictable, what could be done about it could be well planned, and that anyone could be well trained to respond properly when a emergency 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 emergency occurs. Furthermore, the globalization and tight interrelationships exacerbate the consequences that a disruption in a CI could have. Considering this complex situation, it is difficult to be ready for all kind of possible crises and a different approach needs to be adopted.

Although emergency 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 emergency 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 emergency 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 emergency 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, emergency 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, emergency 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 emergency management has increased and thus, 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 to properly deal with crises. Therefore, coordination activities and cooperation agreements should be established among the involved stakeholders to adequately cope with crises. These stakeholders may have different training, expertise, and mental models. Without measures that join these differences, emergency response will suffer from poor coordination and low integration. Thus, establishing a proper emergency 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 emergency management may be a costly activity and its potential is often not appreciated unless an emergency occurs. Therefore, CIs tend to reduce resources allocated to emergency 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.

1.5. Aim and Scope of the thesis

The main objective of this research is to define Resilience capacity assessment framework and develop tool for CIs, considering internal and external stakeholders, validation and testing of the READ tool to assess resilience capacities in Lombardy region of Italy. Below, the sub-objectives to reach the overall goal of this research are defined:

- To understand the main characteristics of emergency situations involving interdependent critical infrastructure systems.

- To develop a framework that will support identifying, characterizing and assessing the resilience capacities required to prepare, cope and re-cover from these type of disruptions
- To translate it into a software tool. that will help improvement of capabilities in practice
- To test it in a real set-up (pilot application)

This thesis contains State-of-the-art on EM and resilience capacities (the context is how to cope with CI resilience) and Resilience capacity assessment framework (READ framework) and Implementation of the SW tool (description of the tool, the logic, etc.; user guidelines) followed by pilot application in Lombardy region. In the end conclusion is being discussed.

CHAPTER 2 – STATE OF THE ART

This section reviews the literature regarding Emergency management and resilience, it explains the resilience capacity concept in context of CIs. This research posits that resilience covers the whole Emergency management process and presents a more holistic approach than other theories. Therefore, the aim of the CIs is to improve their resilience level to manage emergency efficiently and diminish their occurrence.

2.1. Terminology

2.1.1. Incident, Accident, crisis, emergency, disaster and catastrophe

An incident is defined as an unexpected or unwanted change from normal system behavior which has the potential to cause a crisis (Cooke et al, 2006). Perrow (1984), on the other hand, explained different between incident and accident based on the extension of the damaged part and if the system gets disrupted or not. He pointed that if the damage is limited to 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 2009, United Nations International Strategy for Disaster Reduction stated, “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.” 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.

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 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.

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 because 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; RouxDufort, 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.

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. We can also understand difference between Incident, Accident, crisis, emergency, disaster and catastrophe by following figure.

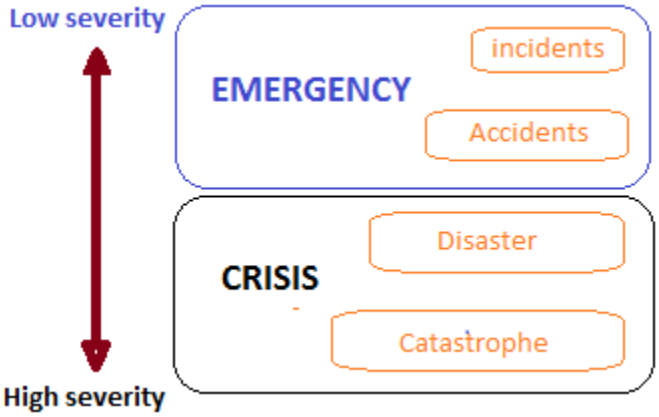

FIGURE 2.1-1 TERMINOLOGY

Mitroff and Anagnos (2000) believe that current emergencies and 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.

2.2. Critical Infrastructure Resilience

the resilience of a CI system is its ability to

- reduce the chances of a disruption of its performance and service to the public,
- absorb the consequences of any disruption if it occurs,

- recover quickly after a disruption by re-establishing normal performance and service, and when relevant, to
- adapt to unforeseen crisis scenarios and possibly significantly different circumstances of operation.

This thesis project ultimately aims at the development of practical tools to assess resilience capacities of CIs, Above, we sought to select only those approaches that are operational and we screened out the others that are not practical. The review disclosed that there are a relatively small number of frameworks of a direct relevance to 'infrastructure resilience'; and it is noticeable that most of them (see, for example, [64]) are either theoretical or conceptual and therefore aim primarily at clarifying and defining interrelated aspects of resilience rather than serving as operational guidance for, for instance, assessments of resilience. Still, a few frameworks have an explicit both theoretical and practical aim and are applicable to different domains, and we have selected two that are cited and used by many authors: first, the MCEER framework for quantitative assessment and enhancement of the seismic resilience of communities [65] developed by researchers at (what was formerly known as) the Multidisciplinary and National Center for Earthquake Engineering Research at Univ. of Buffalo and, second, the Sandia resilience assessment framework applied to infrastructure and economic systems developed by researchers at the Sandia National Lab.

we nevertheless must establish and decide on sound, reasonably precise and practically useable definitions of key concepts such as: critical infrastructure, resilience, resilience capacities, resilience capabilities, performance criteria w.r.t. resilience, resilience measures. In addition, among the several clusters of attributes of resilience which are in use and may be useful for the project are: dimensions of resilience, resilience domains, features of resilient systems.

For an influential and often cited definition of 'critical infrastructure' a good starting point is the EU's Directive on Critical Infrastructures which stipulates that a CI is:

> an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-

being of people, and the disruption or destruction of which would have a significant impact in a Member State because of the failure to maintain those functions

Similarly, the US Dept. of Homeland Security states that

> Critical infrastructures (Cis) are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. CIs are assets or systems that are critical for the maintenance of vital societal functions, providing services that citizens rely on in their daily life – i.e. power and water supply systems, healthcare, transport, electronic communications systems, banking.

These definitions are sufficiently precise for the purpose at hand and there is consensus about core examples of infrastructures that are critical to 'maintaining vital social functions'. Still, there is moderate variation in the ways in which different countries have characterized what infrastructures are "critical" for (i.e. for the maintenance of public safety, social and economic well-being, health, security, public order, the functioning of key national and local government responsibilities ….), which sectors are included and how broadly 'infrastructures' shall be interpreted1. But there is agreement that a range of large-scale sociotechnical infrastructures are "critical" for the continued functioning of key social functions and that these infrastructures therefore must be protected. To identify threats, vulnerabilities and to develop and assess defenses, on the other hand, is an empirical matter and cannot be determined by definitions.

Turning to 'resilience', we put up two of the most cited and discussed contributions, namely the characterization from a group of authors at MCEER (Multidisciplinary Center for Earthquake Engineering Research) and another group at Sandia (Sandia National Laboratories):

Def. 1 (MCEER)· Resilience is the ability of the system to reduce the chances of a shock, to absorb a shock if it occurs (abrupt reduction of performance) and to recover quickly after a shock (re-establish normal performance).

Def. 2 (Sandia)· Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels.

The MCEER definition introduces explicitly what they call the key measures of resilience: “reduced probabilities of shocks”, “reduced consequences from failures” and “reduced time recovery”; and the authors state that a “broad measure of resilience” that captures these key measures can be expressed by formula (1) that is graphically illustrated in literature review:

$$R = \int_{t_0}^{t_1} \big(100 - Q(t)\big)\, dt \qquad (1)$$

where R stands for resilience.

It is also stated in that “resilience must be measured in light of the full set of earthquakes that threaten a community, and therefore must include probabilities of the occurrences of various earthquakes.” That is, when applied to CIs this means that we should consider a representative set of possible emergency scenarios and weigh them all with the probabilities of their occurrence; and then average them. In this way, we can produce an averaged disruption scenario that is modelled as a function Q(t).

In most cases, it is hardly feasible to assess with a reasonable degree of confidence the probabilities of disruptive events. Another point of concern about the MCEER framework is that it deals with known (predicted) disruptive scenarios.

Yet, this “broad measure of resilience” expressed by (1) fails to represent the probabilities of shocks or disruptions – it represents the extent of degradation by time, but it says nothing about the probability that degradation or interruption will occur. At the same time, a shock – such as an earthquake or any other sudden large-scale natural event - is an event the occurrence of which may not be controllable by a CI system.

The MCEER authors suggest that “resilient system is one that displays the “positive” measures of resilience”. The “positive” measure means that the system displays reduced failure probabilities, consequences and/or time recovery compared to other systems similar in functionality or, perhaps, compared to a kind of a reference system. The practical challenge is thus to define a reference system (or a baseline system) to compare with so that we can determine whether the key measures are reduced.

Def. 2 by the Sandia group emphasizes that resilience is determined by a combination of the impact of the event on the system and the time and cost required for the system to recover. It is different from the MCEER definition in that it is conditional on a disruptive event (not necessarily observed, though, possible) and recovery cost (or more general, “recovery effort”) which is another “key” measure of resilience. The “recovery effort”, however, may not be an informative dimension of resilience, as this effort can be reduced by redistributing it to other EM mission areas and preparedness. Still, it may be useful in choosing a cost-beneficial solution among the alternatives (which is beyond the objectives of READ).

Much of the discussion in the literature about resilience contrasts bouncing back from a shock to predefined state to resilience through adaptation – or ‘bouncing forward’. Whether systems or their components bounce back from disturbance or bounce forward and develop resilience in an adaptive manner depends on the system and the way in which the conceptualization of resilience is made. Even for the same system different components of resilience can mean different things. The resilience of some components will necessarily involve the capacity for some form of ‘bouncing back’, while other components within the system may show resilience through adaptation to novel conditions and bouncing forward. For example, for the technical and physical part of the CI the ‘bouncing back’ to normal operations is the primary objective, while for the organizational part adaptation can be seen either as a temporary response strategy or a permanent effect of lessons learned.

The Sandia authors suggest that the objective of enhancing CI resilience is to minimise any reduction in quality of life due to CI disruption [65]. A similar statement of the objective(s) was suggested by Ortwin Renn:

The main objectives for resilience are:

- to guarantee the functional continuity service in times of stress and disaster;
- to limit the extent of and impacts if the service is discontinued;
- to ensure fast recovery if the provider of the service is unable to continue to provide the needed service.

This definition of the resilience objectives seems to be consistent with the MCEER definition and is also a slightly more detailed version of the definition of the objective given in. However, Renn's definition does not articulate the need for resilient systems to reduce the chances of a disruption, nor does it include the ability of the CI to adapt by bouncing back (e.g. during the acute and early restorative phases to unforeseen development of the scenario) or bouncing forward (e.g. adapt in the longer run to new and possibly quite different circumstances of operation).

Dimensions of resilience or system domains

A cluster of resilience categories that has been cited and applied widely was introduced by the MCEER researchers who suggested the following four categories as dimensions of resilience: technical, organizational, social, and economic (TOSE). In the Sandia framework, these categories are called system domains, and it does in fact seem more sensible and consistent to view these four categories as 'dimensions' of the system, the resilience of which can be analyzed and assessed; in contrast, it does not seem appropriate to classify them as dimensions of resilience. So, a CI is a complex socio-technical system that "contains" or must involve these four interrelated domains of activity. Of course, they may also be referred to as system parts or components or subsystems.

Resilience properties

The MCEER framework also nominates robustness, redundancy, resourcefulness, and rapidity as so-called resilience properties. Three of these terms - robustness, resourcefulness and rapidity - describe the ability of a system to do something: the ability to resist change, the ability to find solutions against difficult situations, and the ability to do things with speed and no delay. In contrast, redundancy is the provision (not ability) of

additional or duplicate systems, functionality, equipment, etc. Thus, this pool is heterogeneous and as such should not have a common label.

Like our considerations above about the so-called resilience dimensions (which we proposed to classify as system dimensions), we may also view the present four categories as system attributes rather than features of resilience. They are system characteristics that represent part of the overall resilience of the system. However, the heterogeneity of the concepts raises several questions: is it useful or even coherent to pool them together? If coherent, is the group complete? For example, it may seem we need a property that characterizes the ability to prevent and secure the IC against shocks and interruptions. And how about survivability, susceptibility, vulnerability, adaptiveness and recoverability? Why only those four are suggested in?

The Sandia authors, despite taking as their basis the MCEER framework, avoid using this taxonomy of resilience or system properties. Instead they use “system capacities that determine system resilience”: absorptive capacity, adaptive capacity, and restorative capacity.

We agree: the shift from “resilience properties” to “system capacities that determine system resilience” appears more consistent. Nevertheless, the use of ‘capacities’ does not look appropriate here and seems to be confused with “capabilities” (at least, on some common definitions of these terms - confer with definitions given below). Furthermore, the division of the “capacities” into the three groups is incomplete about Def. 1, since preventive capacities are missing. It should be noted though that the use of these three capacities is consistent and complete in relation to the Sandia definition (Def. 2), as the prevention phase is not included in their definition of resilience.

Capability and capacity

Capability is a feature, faculty, ability or process that can be developed or improved and that enables the execution of given tasks. In this context, it is a collaborative process that can be deployed and through which individual competencies can be applied and made use of for given objectives and goals. The relevant questions for capability is: “How can

we get done what we need to get done?" and "How easily is it to access, deploy or apply the competencies needed?".

The Sandia authors do not use the term 'capability', but they talk about "resilience enhancement features", which are in fact in compliance with the above definition.

Another definition of capability that is common in management and business studies states:

Capability is the ability of an entity (department, organization, person, system) to achieve its objectives, and therefore also and, in relation to its overall mission

Teece, writing in the same tradition (management and business), defines dynamic capability as 'a capability that continuously creates, extends, upgrades, protects, and keeps relevant the enterprise's unique asset base'.

As per Birkie et al. (2014), the concept of dynamic capability "helps refresh existing capabilities" and can be categorized as learning, reconfiguration, integration/coordination and delivery typologies. Dynamic capabilities are linked to the resilience capability base and serve as a complimentary set of capabilities.

Capacity is the power to hold, receive or accommodate. It is about "amount" and "volume". The relevant question related to capacity is "Do we have enough?", and related questions such as "How much is needed?"

Absorptive and adaptive capacities are defined in [Bruneau, et al,2003] as "the degrees to which a system is capable …", which is in line with the definition of capacity given in [Vugrin, et al 2010]

Absorptive capacity is the degree to which a system can automatically absorb the impacts of system perturbations and minimize consequences with little effort.

For example, storage can enhance the absorptive capacity; if a chemical plant is disabled but a large amount of collocated storage of its product is undamaged, customers can continue to be supplied by the stored quantities.

Adaptive capacity is the degree to which the system is capable of self-organization for recovery of system performance levels - and (our addition) for reconfiguring and adjusting to new conditions of operation.

Consider the scenario in which a hurricane destroys many power lines, leaving many customers without electricity. Having customers with their own emergency generators enhances system adaptive capacity because the system can be changed (customers adapt to the disruptive event by generating power from a gasoline fuel source rather than connecting to the electric grid) so that some portion of system performance is regained at a relatively low amount of effort and little or no central coordination.

Restorative capacity is the ability of a system to be repaired easily.

Although all three definitions (absorptive, adaptive and restorative capacity) are given in the same source (E.D. Vugrin, et al 2010), the definition of restorative capacity appears inconsistent with the other two. Absorptive and adaptive capacities are defined in terms of degrees while restorative capacity is defined as the ability (to retain previous service delivery).

Finally, it should be observed that another cluster of characteristics or functions of resilience have been offered: sense, build, reconfigure, re-enhance and sustain. For details the reader is referred to.

2.3. EMERGENCY MANAGEMENT:

In introduction chapter, it shows that there are multiple examples of defining the EM phases very differently. Even the number of the phases may range from three to eight. Recent changes in labelling the phases involve additional words for a better coverage of the critical activities within the phases. For instance, “mitigation” is changed to “mitigation and prevention” to align with the disciplines and practices of risk management, security and loss prevention. The “preparedness” phase is often extended to “preparedness and planning”, to stress the planning activity within the phase (Baird, 2010). The conventional view of the EM set-up is to see it as a cycle of consequent phases. Figure 2.3-1 provides few examples of how the EM cycle can be conceived.

A different account on the EM set-up is due to the Federal Emergency Management



FIGURE 2.3-1 EXAMPLES OF DIVIDING THE EM CYCLE INTO PHASES

Agency (FEMA) of the United States on what phases should be distinguished and how they connect to each other. They do not view the EM as cyclic but as parallel activities, with three of the five (prevention, preparedness, and mitigation) spanning the entire period from pre- to post-incident. “Prevention” is considered as a separate, fifth phase or component of emergency management. For instance, Principles of Emergency Management (FEMA, 2006), an independent study manual produced by FEMA, elaborates on the “five phases of emergency management activities.” Much of the subsequent discussion of the “five phases” in that manual relies on the diagram shown as Figure 2.3-2 below.



FIGURE 2.3-2 PRINCIPLES OF EMERGENCY MANAGEMENT

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

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

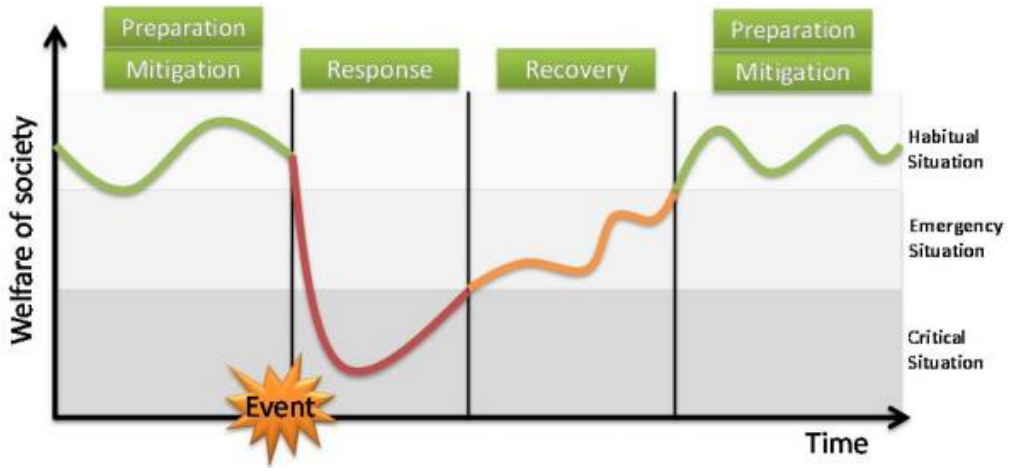

FIGURE 2.3-3 CRISIS MANAGEMENT PHASES

Timely mitigation of impacts in one phase will lead to the transition of a community from one phase to the other. Thus, a community will undergo an effective and within time, post disaster recovery. Such communities portray the traits of a resilient community. Depending on the intensity and type of disaster, Comerio (1998) have provided a time frame for each phase for community recovery (Table 2.3-1).

TABLE 2.3-1 TIME FRAME FOR EACH PHASE

	Disaster Type and intensity		
Phase	Small and concentrated disasters	Large and Complex	
Preparedness	Before Emergency	Before Emergency	
Emergency	t hrs.	One week	
Response and Relief	1 week	Up to 6 months	Overlap
Recovery Phase	Few months to as long as 10 years		

A more drastic parting from the “conventional” EM cycle is expounded in Presidential Policy Directive (PPD-8, 2011) that refers to five mission areas (prevention, protection, mitigation, response and recovery) and the overarching activity called preparedness (see

Figure 2.3-1). Preparedness includes a range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, mitigate, respond to, and recover from incidents.



FIGURE 2.3-4 APPROACH TO BUILDING AND SUSTAINING NATIONAL PREPAREDNESS GOAL

This approach to defining EM preparedness and mission areas appears coherent in the following respects:

- Preparedness refers to all the phases (mission areas) of EM: preparedness to prevent, to protect, to mitigate, to respond and to recover. It does not leave any doubt where preparedness starts and ends with regard to the other phases;
- There is a clear mapping to the pre-incident, incident, and post-incident phases;
- This approach aligns with related disciplines and practices of risk management, security and loss prevention;
- It provides a framework for addressing the all-hazards approach.

Document PPD-8, 2011 gives clear-cut definitions of the mission areas that are given in **Error! Reference source not found.**. We adopt the definition of the EM set-up as it is defined in document PPD-8 (2011) and depicted in Figure 2.3-4.

2.4. Capability-based planning

According to FEMA's Comprehensive Preparedness Guide (2010) capabiltiy based planing is Planning, under uncertainty, to provide capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates

prioritization and choice. Capabilities-based planning addresses uncertainty by analyzing a wide range of scenarios to identify required capabilities. The goal of capability based planning include readiness measures, standards for preparedness assessments and strategies, and a system to assess the orgenazations's overall preparedness to respond to major events. Capabilities, (or the abilities to perform a task), provide the common framework used for relating and comparing disparate elements of an emergency response organization. The objective-based approach, when used alone, may imply a degree of certainty regarding the disaster hazard or threat that not be attainable. This unpredictability is best met by planning to accomplish those objectives which we are capable of achieving [Mark E Keim,2013]. Leonard-Barton (1992) defines dynamic capabilities as the firm's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments. Dynamic capabilities thus reflect an organization's ability to achieve new and innovative forms of competitive advantage given path dependencies and market positions

CHAPTER 3 – THE RESILIENCE CAPACITY ASSESSMENT FRAMEWORK

This section illustrates overview of basic definitions, concepts and Aligning definitions and concepts together in framework. Later framework for Resilience capacity assessment will be explained in this chapter.

3.1. Resilience Capacity

A broad measure of resilience that captures the key measures of resilience can be expressed by the concepts illustrated in Figure 3.1-1 and by its mathematical presentation as formula (1).

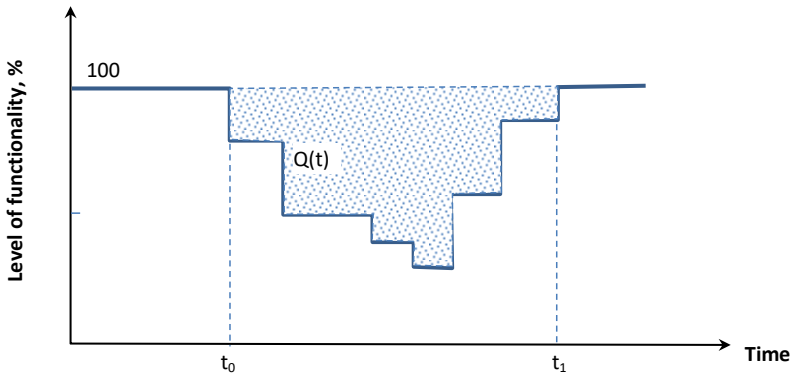

FIGURE 3.1-1 MEASURE OF RESILIENCE - CONCEPTUAL DEFINITION

$$R = \int_{t_0}^{t_1} \big(100 - Q(t)\big)\, dt, \quad \text{---------- (1)}$$

where R stands for resilience.

It is also stated in that “resilience must be measured in light of the full set of earthquakes that threaten a community, and therefore must include probabilities of the occurrences of various earthquakes.” That is, when applied to CIs this means that we should consider a representative set of possible emergency scenarios and weigh them all with the probabilities of their occurrence; and then average them. In this way, we can produce an averaged disruption scenario that is modelled as a function Q(t).

In most cases, it is hardly feasible to assess with a reasonable degree of confidence the probabilities of disruptive events. Another point of concern about the MCEER framework is that it deals with known (predicted) disruptive scenarios.

We further operationalize the definition of a resilience capability of CI as follows:

A resilience capability of CI is a coherent compound of different entities - belonging to one or more of the following three groups: assets (including knowledge systems), resources (including skills of people involved), and practices and routines (including sets of procedures) – that promotes the achievement of resilience objectives.

In 2014 Francis and Bekera proposed resilience paradigm might be implemented via the set of resilience capacities outlined above: absorptive capacity, adaptive capacity, and recovery and restorative capacity. These three pillar capacities give rise to what he called the resilience triangle as illustrated in Figure 3.1-2:

- Preventive capacity: Vugrin et al. define absorptive capacity as the degree to which a system can absorb the impacts of system perturbations and minimize consequences with little effort. In practice, though, it is a management feature depending on configuration, controls, and operational procedures. System robustness and reliability are prototypical pre-disruption characteristics of a resilient system [European Programme for Critical Infrastructure Protection 2005]. Designing a production system with adequate buffer capacity to overcome potential blocking of a production line is, for example, an absorptive endowment. Absorptive capacity is attained through the practice of adverse event mitigation in many systems. Absorptive capacity is the capacity to limit the extent of sudden performance reduction

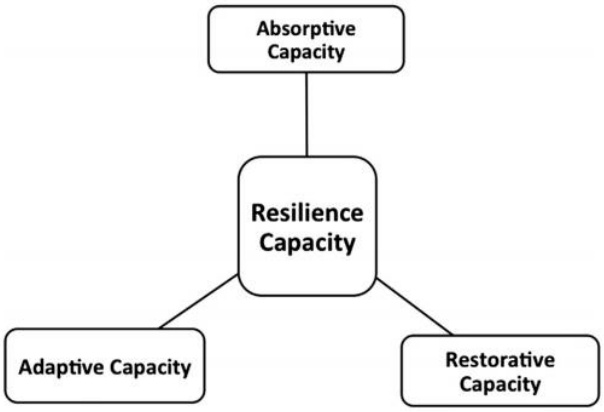

FIGURE 3.1-2 THE RESILIENCE TRIANGLE SHOWING THREE MAJOR CAPACITIES THAT MAKE UP THE RESILIENCE CAPACITY OF A SYSTEM

- Adaptive capacity: While absorptive capacity is the ability of a system to absorb system perturbations, adaptive capacity is the ability of a system to adjust to undesirable situations by undergoing some changes. Adaptive capacity is distinguished from absorptive capacity in that adaptive systems change in response to adverse impacts, especially if absorptive capacity has been exceeded. A system's adaptive capacity is enhanced by its ability to anticipate disruptive events; recognize unanticipated events; re-organize after occurrence of an adverse event; and general preparedness for adverse events.
- Restorative capacity: Restorative capacity of a resilient system is often characterized by rapidity of return to normal or improved operations and system reliability [62]. This capacity should be assessed against a defined set of requirements derived from a desirable level of service or control. In practice, recovery efforts may be daunting because of a likely conflict of interests. More specifically, it may be difficult not only to assess the costs of recovery actions, but stakeholders may not agree on the benefits accrued through recovery. In addition, navigating these tradeoffs might be obscured by mistrust or ambiguity about the trustworthiness of government agents or other citizen stakeholders. Hence restorative capacity may be compromised if inadequate investments are made due to disagreements among stakeholders.

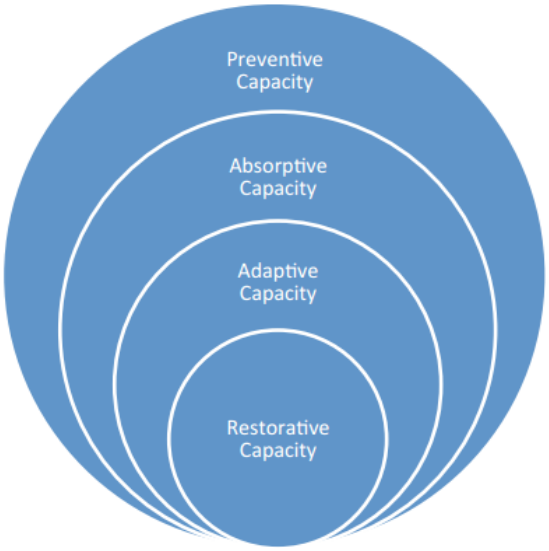

FIGURE 3.1-3 SYSTEM RESILIENCE CAPACITIES THAT CONTRIBUTE TO THE ABILITY OF A SYSTEM TO PREVENT, ABSORB, ADAPT TO, AND/OR RAPIDLY RECOVER FROM A POTENTIALLY DISRUPTIVE EVENT

The resilience features represent the actual infrastructure engineering functional solutions that contribute to one or more of the system capacities. Potential resilience features are (Figure 3.1-4): Robustness, Redundancy, Segregation, Diversity, Training, Governance, Automatic reaction, Rerouting, Human Resources Substitution and so on. In building and evaluating resilience the contribution made by each of these features needs to be considered and evaluated.

It can be difficult to place a specific resilience feature into a single capacity category, and some time they may be contradictory: resilience feature like robustness may enhance absorptive capacity and at the same time make the system more rigid and therefore less flexible for adaptation.

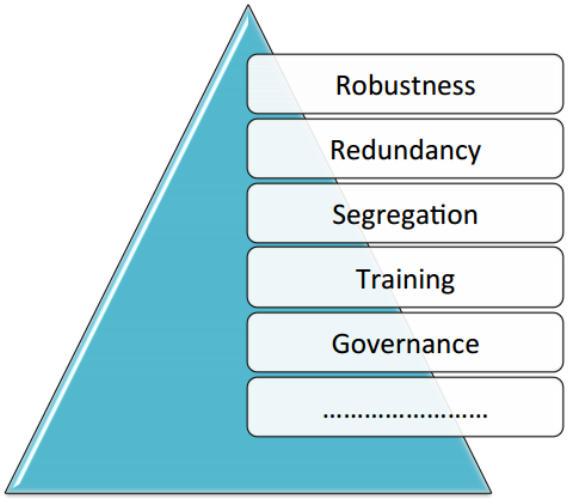

FIGURE 3.1-4 SYSTEM FEATURES THAT MAY CONTRIBUTE TO THE SYSTEM RESILIENCE

3.1.1. Capability compounds

These terms, assets, resources and routines, are used in parts of the literature on management and business as well as that on quality improvement and safety management, but with different meanings. The term ‘asset’ is used to refer to tangible and intangible items that can be owned – and therefore also includes knowledge and information systems. Items that can be owned will by inference have a value to their owners – otherwise there is no point in ownership. By ‘resources’ we aim to capture tools and competencies that make it possible to make use of assets and without which assets may not have their value. Resources include cognitive and social capital and thus the specific skills and competencies that people have for making use of other resources assets. The distinction between assets and resources is context dependent – so what counts as a resource in once context may be assets in another (say, ambulances, software programs). Finally, ‘routines’ refers to both explicit procedures for doing things and to the informal practices people and communities have and which are not articulated in procedures and prescriptions, yet shared as tacit background knowledge and know-how. Short definitions of these terms are the following: [Trucco et al 2016]

Asset: an asset is an item of ownership that has exchange value; includes intangibles such as knowledge systems.

Resource: a resource is tool or competence required to carry out given tasks or achieving given objectives, including making use of assets to achieve individual and shared goals. A specific competence is also a resource.

A routine is defined as the way things are done, possibly codified as an explicit procedure, within a community or social group, a pattern of activities.

As mentioned, in some cases it is not obvious whether a certain item should be classified either as an asset or a resource, and the classification issue must be resolved by convention.

Let us consider a simple example to illustrate the approach.

Assume the following capability is found important for building and maintaining resilience of a system: “Provision of access to required information”. What is this capability compounded from?

Assets: Information (can be paper medium, e-repository, audio records, etc.)

Resource: Examples may be tools such as communication links, computing facilities, competencies to operate and make use of these.

Routines (procedures, prescriptions or tacit background knowledge and know-how): Examples may be instructions for getting access to the target information which may include authorization, credentials for e-access, etc.

3.1.2. Capabilities data model

The Capability data model consists of the Capability classification (explained above), textual description of the capability, descriptors and capability assessment (explained in the following sections)

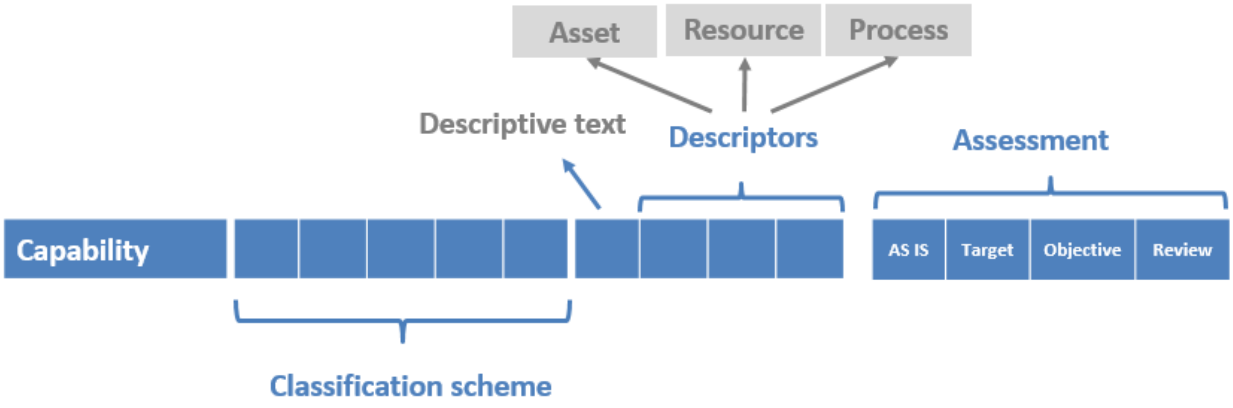

FIGURE 3.1-5 CAPABILITY DATA MODEL

3.2. The Resilience capacity assessment

Distinguishing features of the framework

- A key approach lying in the foundation of the developed framework is a capabilities-based planning approach. It has been adopted by several countries as part of their emergency preparedness work. Presidential Policy Directive (PPD-8, 2011), the Swedish statutory instructions MSBFS (2010) and Houdijk (2010) are the references to this approach of choice. The strategy of the capabilities-based planning is to prepare for a large variety of threats and risks instead of simply preparing for specific scenarios (Lindbom, 2015).
- The break-down of the capabilities into groups is based on the view that preparedness is the overarching set of activities over the emergency mission areas: prevention, protection, mitigation, response and recovery. This is as it is suggested in Presidential Policy Directive (PPD-8, 2011). Adopting this EM set-up we further distinguish core capabilities and preparedness capabilities. Where the former label stands for the capabilities for all five mission areas and the latter covers those capabilities that build and sustain the core capabilities. Preparedness capabilities enable planning, training, exercising, continuously maintaining and sustaining the core capabilities.
- Another distinguishing feature is that we do not consider a capability as an indivisible singleton but an entity composed of three compounds: asset(s), resource(s), and routine(s).

- A CI system is analyzed in four dimensions: technical, organizational, social and economic (TOSE).
- We explicitly divide organizational capabilities into inter- and intra-organizational capabilities, as some inter-capabilities are to be enabled by intra and should not be analyzed as decoupled. Should we also distinguish inter- or intra-physical, social and economic capabilities?
- Finally, all capabilities are grouped into preventive, absorptive, adaptive, and restorative clusters to relate them to the measures of resilience and as a step towards being able to measure the capacity of a CI to prevent a disruption, to absorb. Is this the objective of having this dimension?

On a general level, the space in which resilience capabilities of CIs are defined is restricted to two dimensions: (1) types of the CI subsystems or components (TOSE) and (2) mission areas (prevention, protection, mitigation, response and recovery). Besides this, the space is split into two parts: (1) core capabilities, and (2) preparedness capabilities/activities. Specific solutions or mechanisms that will be identified within this space are resilience capabilities that contribute to making the system resilient, i.e. enhancing at least one of its mission areas or/and preparedness to them. In a tabular form the resilience capability space is shown in fig.

TABLE 3.2-1 RESILIENCE CAPABILITIES' SPACE

	Resilience capability building and sustaining				
	Preparedness activities/capabilities (building and sustaining core capabilities: planning, training, exercising, organising, evaluating/improving)				
Tecnical					
Organisational					
Social					
Economic					
	Prevention	Protection	Mitigation	Response	Recovery
	Core capabilities				

	Prevention	Protection	Mitigation	Response	Recovery
Technical					
Organizational					
Social					
Economic					

Figure 3.2-1 visualizes the approach to building system resilience where it is explicitly shown that capabilities are the aggregates of some or all the following the three components: assets, resources and routines.

In times of a crisis and in a post-crisis phase several emergency responders, authorities and possibly social groups will be involved to cope with and recover from the disruption. They all are external organizations and institutions that in concerted actions with the operator of the CI must respond to the disruption and restore the services. It is not only the intra-capabilities of the CI and its operator that make the CI resilient. The inter-organizational and institutional capabilities enabling concerted actions among all the involved parties play as great role as intra-organizational capabilities. The space in which the resilience capabilities are defined should be refined and complemented by one more dimension classifying the capabilities into inter- and intra-organizational. This dimension

can simply be accommodated by labelling the identified capabilities as belonging to either

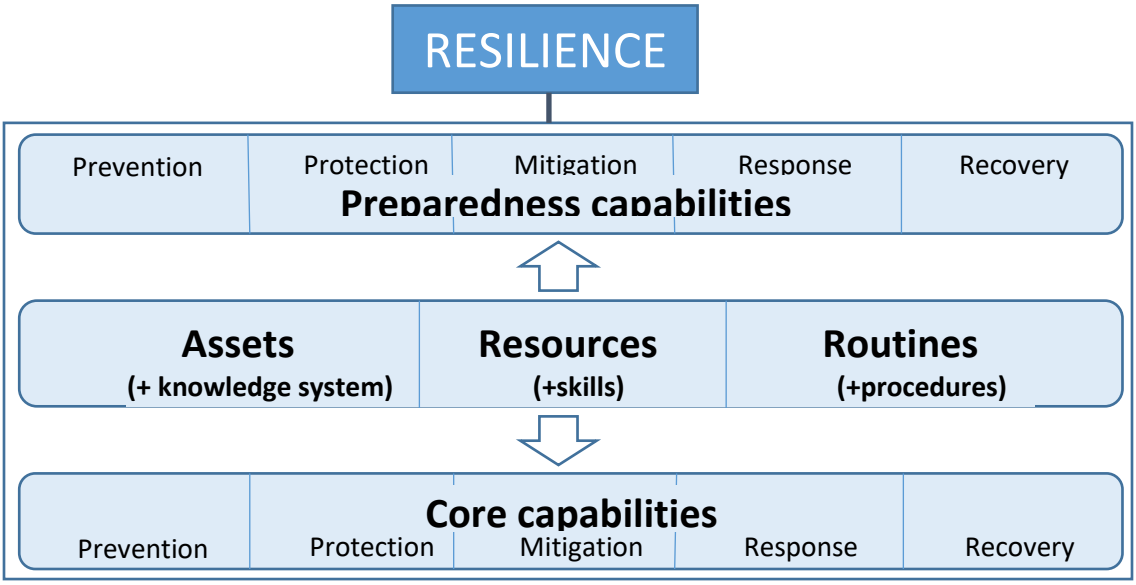

FIGURE 3.2-1 BUILDING SYSTEM RESILIENCE

inter- (labelled by “r”) or intra- (labelled by “a”) capability group.

The interorganizational model of capability building consists in the following. To enable interorganizational relations and activities, there must be interorganizational ‘enablers’ in place. Among many intra-capabilities contributing to the system resilience there are some enablers (capabilities) that allow establishing interorganizational relations and conducting activities. The interorganizational relations can have different gradations that are displayed in Figure 3.2-2.

	INTER-ORGANISATIONAL MODEL (National and cross-border)				
Capabilities	**Independent**	**Coordinate**	**Cooperate**	**Collaborate**	**Meta-organisation**
+ To share **Authority**					
+ To share **Power**					
+ To share **Activities and Resources**					
+ To share **Information**					
Intra-Organisational Resilience					

FIGURE 3.2-2 INTER-ORGANIZATIONAL MODEL

This model will facilitate the identification of inter-organizational resilience capabilities and their intra-enablers. This is potentially a wide-ranging and laborious activity that - if performed in the full scale – must be done for each cell of the resilience capability space

Finally, one more dimension can be distinguished that relates the capabilities to one out of four resilience capacity groups: preventive, absorptive, adaptive and restorative. Accommodating this dimension in the capability space. can be done again by labelling the identified capabilities. The following labels are adopted: “P” for preventive, “B” for absorptive, “D” for adaptive, and “R” for restorative. Thus, each identified capability appearing in the table will be attributed two labels: one saying whether it is inter- or intra-capability while the other indicating a resilience capacity group. For example, “Capability X [r,D]” should be read as “Capability X” is an intra-capability belonging to the adaptive capacity group.

The above sketched approach suggests that the starting point for resilience capability building is to work out an inventory of required capabilities that will populate the capability space. The identification of the capabilities is the key activity to make the framework operational. Then splitting capabilities into assets, resources and routines will help checking their state for each specific application. To be able to work out an exhaustive set of resilience capabilities, additional aids should be provided to guide a purposeful

search and checking activity. These aids can emerge opportunistically and should become subject to scrutiny about their value for our purpose.

The following structured knowledge is a potentially useful help in working out a set of the resilience capabilities of CI:

- Ontologies developed in the THREVI2 project (infrastructure topology and asset taxonomy; and hazard and threat ontology),
- Resilience capabilities and components identified to assess the Resilience Measurement Index of CI,
- Core functions of operational resilience],
- "Resilience properties" (robustness, redundancy, resourcefulness, and rapidity),
- Main barriers and capabilities in crisis information sharing and collaboration.

The inventory of the resilience capabilities will serve as a generic repository to be consulted to find resilience solutions for specific CI systems and the environments. To identify system-specific solutions, system vulnerabilities have to be identified as the next step of the Framework. This exercise is rooted in risk analyses of specific CIs. Mapping the capabilities against the vulnerabilities will provide an overview of what capabilities are in place for the system and what gaps that may exist. This will provide input for bridging the gaps to enhance the resilience.

If further developed, this approach can even provide a richer guidance for resilience capability building. Being able to assess the efficiency of the existing and/or suggested resilience solutions and being able to rank the vulnerabilities will serve as purposeful guidance for action and, in this way, will complete the resilience capability building cycle.

The above described steps are summarized in the two figures (Figure 3.2-3 and Table 3.2-2).

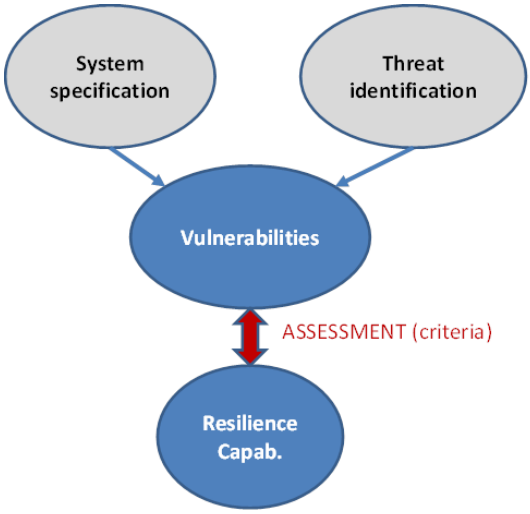

FIGURE 3.2-3 COUPLING RESILIENCE CAPABILITY SOLUTIONS TO SPECIFIC CIS

TABLE 3.2-2 RANKING RESILIENCE SOLUTIONS FOR IMPLEMENTATION/ENHANCEMENT

Vulnerabilities	Preventive	Absorptive	Adaptive	Restorative
	✓		✓	✓
		✓		
		✓	✓	
			✓	
	✓			✓
			✓	✓
	✓	✓		

Prioritized list

An aid in a systematic identification and specification of the vulnerabilities can be the overview suggested in the THREVI2 project.

3.2.1. The scope of the Resilience capacity assessment

The framework delineated in the previous section will require considerable resources to implement, test and validate in the full scale. Given the limited focus of the READ project, the scope of application and test of the framework is similarly limited while keeping with the project objectives.

As shown in Table 3.2-3 the project will work out the inventory of the resilience capabilities within the technical and organizational dimensions of Cis – but involving the social to the extent that application of the capabilities can be understood only in terms of interactions

with the social dimension; hence, some limited effort will be applied to analyses and describe social capabilities in their interaction with the other dimensions.

Within the group of resilience capacities, we limit our analysis and application to absorptive, adaptive and restorative resilience capacities, and so that the capabilities to be identified will cover the three EM mission areas: mitigation, response and recovery.

TABLE 3.2-3 THE SCOPE OF THE READ PROJECT IN THE RESILIENCE CAPABILITIES' SPACE

	Resilience capability building and sustaining				
	Preparedness activities/capabilities (building and sustaining core capabilities: planning, training, exercising, organising, evaluating/improving)				
Technical			The READ main scope		
Organizational					
Social			Complimentary contributions		
Economic					
	Prevention	Protection	Mitigation	Response	Recovery

	Core capabilities				
	Prevention	Protection	Mitigation	Response	Recovery
Technical			The READ main scope		
Organizational					
Social			Complimentary contributions		
Economic					

Chapter 4: Identifying the capabilities in Critical infrastructure:

The terms capability, competency and capacity are often used interchangeably, however:

- Competency usually refers to knowledge, skills or strength at a task and is another word for an individual's expertise.
- Capability has a broader more holistic meaning that takes account of attributes, attitudes and behaviours, and the ability to achieve a certain outcome in the future. In this way organization capability arises from the use and application of an individual's competence.
- Capacity refers to the amount or volume of work, for example 'how much?' and 'how many?'

While people often use the words "ability," "competence," and "capability" interchangeably, we make some distinctions. In technical areas, we refer to an individual's functional competence or to an organization's core competencies; on social issues, we refer to an individual's leadership ability or to an organization's capabilities. In this chapter, we discussed how to identify capabilities in CIs.

4.1. Classification of Capabilities

Capability of an entity (organization, person, system) is a feature, faculty or process that promotes the achievement of its objectives. We further operationalize the definition of a resilience capability of CI as follows: A resilience capability of CI is a coherent compound of different entities - belonging to one or more of the following three groups: assets (including knowledge systems), resources (including skills of people involved), and practices and routines (including sets of procedures) – that promotes the achievement of resilience objectives.

As per Trucco et. Al (2016) Capabilities are classified across five dimensions as we discussed in state of the art chapter:

- EM cycle – Preparedness is considered as the phase where the high-level capabilities are required to improve core capabilities in all the other phases of the cycle. Preparedness refers to all the phases (mission areas) of EM: preparedness to prevent, to protect, to mitigate, to respond and to recover.
- Type of resilience – Technical and Organizational dimensions are within the scope of the project
- Type of actor – Critical Infrastructure Operators and First Responders are considered
- Resilience Capacity to which it contributes:
    - Preventive capacity is the degree to which the system is able to anticipate and prepare for a disruptive event, e.g. by building other capacities, monitoring and sensing, doing risk assessment, etc.
    - Absorptive capacity is the capacity to limit the extent of sudden performance reduction.
    - Adaptive capacity is the degree to which the system is capable of self-organization for coping with the unexpected and to adjust to novel conditions of operation.
    - Restorative capacity is the degree of ease with which the system repairs after a shock or a disruption.
- Organizational level – explains whether the capability is intra- or inter-organizational.

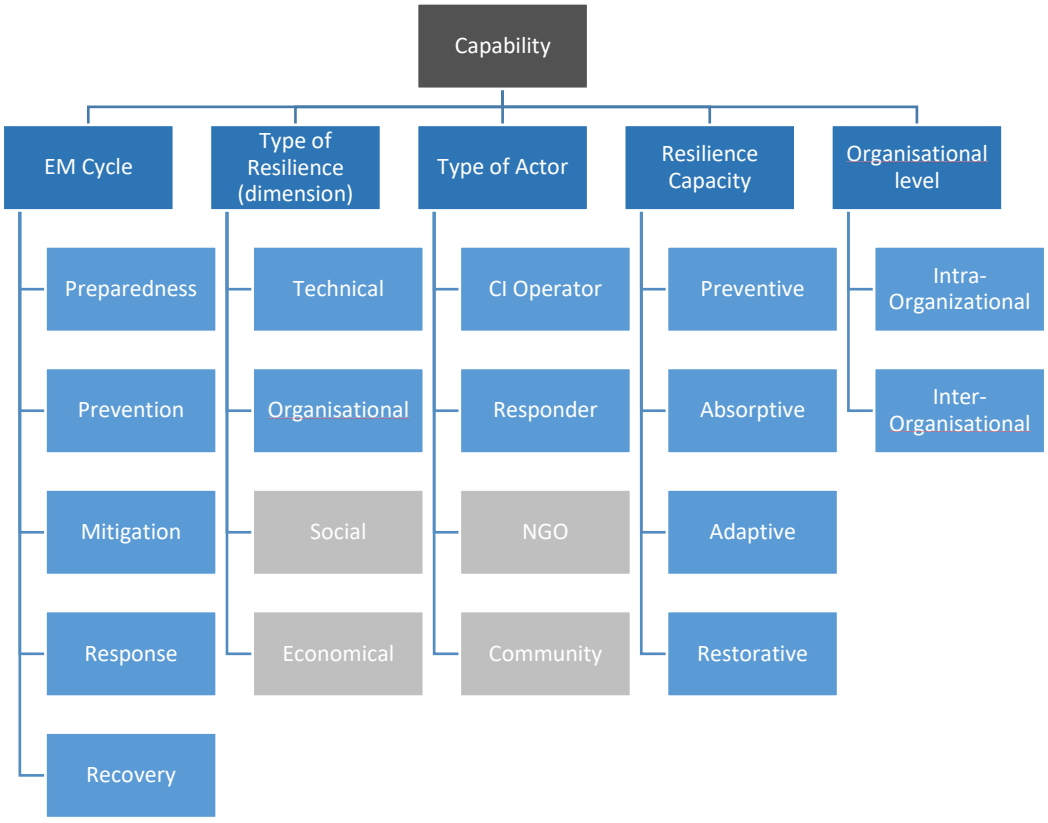

FIGURE 4.1-1 CLASSIFICATION OF CAPABILITIES

4.2. Identification of capabilities in EM cycle mission areas:

Here, Capability is the ability of an entity of CIs to achieve its objectives, and therefore also and, in relation to its overall mission. In this segment of chapter, we look at capabilities of CIs and how organizations can evaluate them and build the ones needed to create intangible value. Through a flowchart Figure 4.2-1. we explain how to do a capabilities audit, which provides a high-level picture of an organization's strengths and areas for improvement. Defining the capabilities of a critical infrastructure can be broken down into the following steps. Beginning with establishing the roles and objectives of the CI. A clear definition is very essential at this stage. This leads us to the next step, where we determine the potential hazards and threats to the functionality of the CI under the consideration. This also acts as the feedback completion for the CI when there are any capabilities update to the CI. Then we move on to classify the mission of the CI in to five areas: Prevention, Protection, Mitigation, Response, and Recovery. Subsequently, we

evaluate the security requirements for the CI using the ECPI procedure. Based on the above risk assessment, the capabilities of the CI are identified. And to complete the feedback loop, a capability assessment is performed for the CI under consideration and the updates are identifying, which then leads us again to the step to determine the potential hazards and threats to the CI.

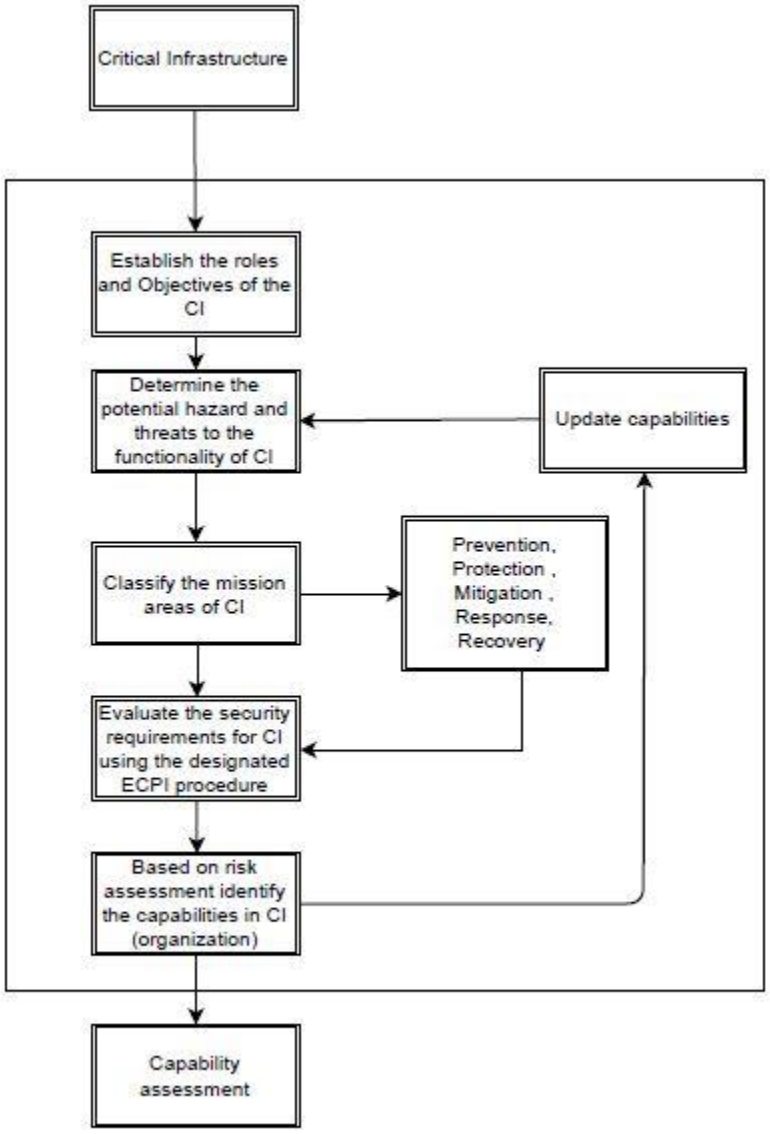

FIGURE 4.2-1 FLOW CHART FOR IDENTITY FICATION OF CAPABILITIES

Each capability is also tied to a capability target, which describes what Allen County wants to achieve as an outcome for each capability and is based on the vulnerability assessment.

Table 4.2-1 provides a list of the core capabilities by mission area as per US Homeland Security's National Protection Goal (2016). Many of these core capabilities exist and are used every day for steady-state protection activities. The approach to further developing and delivering these core capabilities will differ according to and across the mission areas.

TABLE 4.2-1 CAPABILITIES BY MISSION AREA

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Intelligence and Information Sharing, Interdiction and Disruption, Screening, Search and Detection	Intelligence and Information Sharing, Interdiction and Disruption, Screening, Search, and Detection, Access Control and Identity Verification, Cybersecurity, Physical Protective Measures, Risk &resilience assessment, Supply Chain Integrity and Security	Community Resilience building, Threat and Hazard Identification	Logistics and Transportation, Environmental Response/ Health and Safety, Fatality Management, Mass Care Services, Mass Search and Rescue Operations, On-Scene Security and Protection, Operational Communications, Public and Private Services and Resources, Public Health and Medical Services, Situational Assessment	

Protection and Prevention mission areas share three core capabilities: Intelligence and Information Sharing; Interdiction and Disruption; and Screening, Search, and Detection. The cross-cutting core capabilities between mission areas provide opportunities for integration. Prevention and Protection use many of the same capabilities and coordinating structures, including for delivering Intelligence and Information Sharing; Interdiction and Disruption; and Screening, Search, and Detection. Protection and Mitigation share capabilities directly related to risk management. For Protection, the capability is Risk Management for Protection Programs and Activities. For Mitigation, risk management is informed by Long-Term Vulnerability Reduction; Risk and Disaster Resilience Assessment; and Threat and Hazard Identification. (Figure 4.2-2) is a simplified graphic that conceptually illustrates the interconnectedness of all the mission areas. The figure calls specific attention to the connections and shared or related core capabilities that align efforts in the context of Protection and Prevention, as well as Protection and Mitigation. Additionally, Protection is linked to Response and Recovery through various core capabilities such as those pertaining to Infrastructure Systems and relevant coordinating structures.



FIGURE 4.2-2 PROTECTION AND INTEGRATED CAPABILITIES

Collectively, the core capabilities for the Protection mission area provide the foundation for achieving the overarching critical objective for Protection: a homeland that is protected from terrorism and other hazards in a manner that allows American interests, aspirations, and way of life to thrive. we established preliminary targets for each of the Protection mission area core capabilities. The critical tasks associated with the Protection core capabilities are ambitious. They are not tasks for any single jurisdiction or agency; rather, achieving them will require a national effort involving the whole community

1. Planning

Mission Area: All

Description: Conducting a systematic process that engages the whole community, as appropriate, in the development of executable strategic, operational, or community-based approaches to meet defined Protection objectives. Planning includes the development of multidisciplinary plans; their implementation, exercising, and maintenance; and the promotion of planning initiatives.

Critical Tasks:

- Initiate a flexible planning process that builds on existing plans.
- Establish partnerships, facilitate coordinated information sharing between partners, and enable the planning and protection of critical infrastructure within the jurisdiction.
- Implement measures to identify and prioritize critical infrastructure and determine risk.
- Conduct vulnerability assessments, perform risk analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private sector and state partners.
- Implement security, protection, resilience, and continuity plans and programs, train and exercise, and take corrective actions.
- Develop and implement progress measures and communicate adjustments and improvements to applicable stakeholders and authorities.

- Integrate planning for the whole community, including, but not limited to, individuals with disabilities and others with access and functional needs, as well as those with limited English proficiency, and racially and ethnically diverse communities.

2. **Public Information and Warning**

Mission Area: All

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole community using clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard, as well as the actions being taken and the assistance being made available, as appropriate.

Critical tasks:

- Determine requirements for protection stakeholder information and information sharing.
- Determine information sharing requirements and processes to address the communication needs of children; people with limited English proficiency; and individuals with disabilities and others with access and functional needs, including those who are deaf, hard of hearing, blind, or have low vision using appropriate auxiliary aids and services, such as sign language and other interpreters and the captioning of audio and video materials.
- Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, and the public.
- Promptly share actionable measures with the public and among all levels of government, the private sector, and NGOs.
- Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, National Terrorism Advisory System, and social media sites and technology

3. Operational Coordination

Mission Areas: All

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities

Critical tasks:

- Collaborate with all relevant protection partners.
- Determine jurisdictional priorities, objectives, strategies, and resource allocations.
- Establish clear lines and modes of communication among participating organizations and jurisdictions.
- Define and communicate clear roles and responsibilities relative to courses of action.
- Integrate and synchronize the actions of participating organizations and jurisdictions to ensure unity of effort.
- Determine requirements for protection stakeholder operational coordination.
- Coordinate across and among all levels of government and with critical nongovernmental and private sector partners to protect against potential threats, conduct law enforcement investigations, or engage in enforcement and protective activities based on jurisdictional authorities.

4. Intelligence and Information Sharing

Mission Areas: Prevention, Protection

Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats (people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on stakeholders. Information sharing is the ability to

exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.

Critical tasks:

- Monitor, detect, and analyse threats and hazards to public safety, health, and security, which include:
  - Participation in local, state, tribal, territorial, regional, and national education and awareness programs.
  - Participation in the routine exchange of security information including threat assessments, alerts, attack indications and warnings, and advisories among partners.
- Determine requirements for protection stakeholder intelligence, information, and information sharing.
- Develop or identify and provide access to mechanisms and procedures for intelligence and information sharing between the public, private sector, and government protection partners.
- Using intelligence processes, produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include partners in the other mission areas.
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information.

5. Interdiction and Disruption

Mission Areas: Prevention, Protection

Description: Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.

Critical Tasks:

- Prevent movement and operation of terrorists into or within the United States and its territories.
- Ensure the capacity to detect and render safe CBRNE devices or resolve CBRNE threats.

- Interdict conveyances, cargo, and persons associated with a potential threat or act.
- Implement public health measures to mitigate the spread of disease threats abroad and prevent disease threats from crossing national borders.
- Disrupt terrorist financing or conduct counter-acquisition activities to prevent weapons, precursors, related technology, or other material support from reaching its target.
- Enhance the visible presence of law enforcement to deter or disrupt threats from reaching potential target(s).
- Employ wide-area search and detection assets in targeted areas in concert with local, state, tribal, and territorial personnel or other Federal agencies (depending on the threat).

6. Screening, Search and Detection

Mission Area: Prevention, Protection

Description: Identify, discover, or locate threats and/or hazards through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, bio-surveillance, sensor technologies, or physical investigation and intelligence.

Critical tasks:

- Locate risk associated with a potential threat.
- Develop and engage an observant public
- Operate safely in a hazardous environment.
- Consider the deployment of teams and capabilities to enhance local, state, tribal, and territorial efforts, including the use of incident assessment and awareness assets.

7. Access Control and Identity Verification

Mission Area: Protection

Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

Critical tasks:

- Verify identity to authorize, grant, or deny physical and cyber access to physical and cyber assets, networks, applications, and systems that could be exploited to do harm.
- Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities.

8. Cybersecurity

Mission Area: Protection

Description: Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

Critical tasks:

- Implement risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.
- Implement and maintain procedures to detect malicious activity and to conduct technical and investigative-based countermeasures, mitigations, and operations against malicious actors to counter existing and emerging cyber-based threats, consistent with established protocols.

9. Physical Protective Measures

Mission Area: Protection

Description: Implement and maintain risk-informed countermeasures, and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors.

Critical tasks:

- Identify and prioritize assets, systems, networks, and functions that need to be protected.
- Identify needed physical protections, countermeasures, and policies through a risk assessment of key operational activities and infrastructure.
- Develop and implement security plans, including business continuity plans, that address identified security risks.
- Develop and implement risk-based physical security measures, countermeasures, policies, and procedures.
- Implement security training for workers, focused on awareness and response.
- Develop and implement biosecurity and biosafety programs and practices.
- Leverage Federal acquisition programs, as appropriate, to ensure maximum cost efficiency, security, and interoperability of procurements.

10. Risk (& Resilience) Assessment

Mission Area: Protection

Description: Identify, assess, and prioritize risks to inform Protection activities, countermeasures, and investments. Assess risk and disaster resilience so that decision makers, responders, and community members can take informed action to reduce their entity's risk and increase their resilience.

Critical tasks:

- Gather required data in a timely and accurate manner to effectively identify risks.
- Build the capability within communities to analyse and assess risk and resilience.
- Identify, implement, and monitor risk management plans.
- Update risk assessments to reassess risk based on changes in the following areas: the physical environment, aging infrastructure, new development, new mitigation projects and initiatives, post-event verification/validation,

new technologies or improved methodologies, and better or more up-to-date data.

- Validate, calibrate, and enhance risk assessments by relying on experience, lessons learned, and knowledge beyond raw data or models.
- Use risk assessments to design exercises and determine the feasibility of mitigation projects and initiatives.
- Engage in a peer-to-peer mentoring structure that promotes effective practices

11. Supply Chain Integrity and Security

Mission Area: Protection

Description: Strengthen the security and resilience of the supply chain.

Critical tasks:

- Secure and make resilient key nodes, methods of transport between nodes, and materials in transit.
- Analyse key dependencies and interdependencies related to supply chain operations.

12. Community Resilience Building

Mission Area: Mitigation

Description: Enable the recognition, understanding, communication of, and planning for risk and empower individuals and communities to make informed risk management decisions necessary to adapt to, withstand, and quickly recover from future incidents.

Critical tasks:

- Maximize the coverage of the area that has a localized, risk-informed mitigation plan developed through partnerships across the entire community.
- Empower individuals and communities to make informed decisions to facilitate actions necessary to adapt to, withstand, and quickly recover from future incidents.

- Ensure that local and state governments complete a risk assessment that defines localized vulnerabilities and consequences associated with potential natural, technological, and human caused threats and hazards to their natural, human, physical, cyber, and socioeconomic interests.

13. Threats and Hazards Identification

Mission Area: Mitigation

Description: Identify the threats and hazards that occur in the geographic area; determine the frequency and magnitude; and incorporate this into analysis and planning processes to clearly understand the needs of a community or entity.

Critical Tasks:

- Identify the threats and hazards within, in collaboration with the whole community, against a national standard based on sound science.

14. Logistics and Transportation under EM

Mission Areas: Response

Description: Provide transportation (including infrastructure access and accessible transportation services) for response priority objectives, including the evacuation of people and animals, and the delivery of vital response personnel, equipment, and services into the affected areas. Deliver essential commodities, equipment, and services in support of impacted communities and survivors, to include emergency power and fuel support, as well as the coordination of access to community staples. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

Critical tasks:

- Establish physical access through appropriate transportation corridors and deliver required resources to save lives and to meet the needs of disaster survivors.
- Ensure basic human needs are met, stabilize the incident, transition into recovery for an affected area, and restore basic services and community functionality.

- Clear debris from any road, rail, airfield, port facility, waterway for response operations.

15. Environmental Response / Health and Safety

Mission Area: Response
Description: Conduct appropriate measures to ensure the protection of the health and safety of the public and workers, as well as the environment, from all-hazards in support of responder operations and the affected communities.

Critical tasks:

- Identify, assess, and mitigate worker health and safety hazards and disseminate health and safety guidance and resources to response and recovery workers.
- Minimize public exposure to environmental hazards through assessment of the hazards and implementation of public protective actions.
- Detect, assess, stabilize, and clean up releases of oil and hazardous materials into the environment, including buildings/structures, and properly manage waste.

16. Fatality Management Services

Mission Areas: Response
Description: Provide fatality management services, including decedent remains recovery and victim identification, working with local, state, tribal, territorial, insular area, and Federal authorities to provide mortuary processes, temporary storage or permanent internment solutions, sharing information with mass care services for the purpose of reunifying family members and caregivers with missing persons/remains, and providing counselling to the bereaved.

Critical tasks:

- Establish and maintain operations to recover a significant number of fatalities over a geographically dispersed area.

17. Fire Fighting

Mission Area: Response

Description: Provide structural, wildland, and specialized firefighting capabilities to manage and suppress fires of all types, kinds, and complexities while protecting the lives, property, and the environment in the affected area.

Critical tasks

- Provide traditional first response or initial attack firefighting services.
- Conduct expanded or extended attack firefighting and support operations through coordinated response of fire management and specialized fire suppression resources.
- Ensure the coordinated deployment of appropriate local, regional, national, and international fire management and fire suppression resources to reinforce firefighting efforts and maintain an appropriate level of protection for subsequent fires.

18. Mass Care

Mission Area: Response

Description: Provide life-sustaining and human services to the affected population, to include hydration, feeding, sheltering, temporary housing, evacuee support, reunification, and distribution of emergency supplies.

Critical tasks:

- Move and deliver resources and capabilities to meet the needs of disaster survivors, including individuals with access and functional needs.
- Establish, staff, and equip emergency shelters and other temporary housing options (including accessible housing) for the affected population.
- Move from congregate care to non-congregate care alternatives and provide relocation assistance or interim housing solutions for families unable to return to their pre-disaster homes.

19. Mass Search and Rescue Operations

Mission Area: Response

Description: Deliver traditional and atypical search and rescue capabilities, including personnel, services, animals, and assets to survivors in need, with the goal of saving the greatest number of endangered lives in the shortest time possible.

Critical Tasks:

- Conduct search and rescue operations to locate and rescue persons in distress.
- Initiate community-based search and rescue support operations across a wide geographically dispersed area.
- Ensure the synchronized deployment of local, regional, national, and international teams to reinforce ongoing search and rescue efforts and transition to recovery.

20. On-scene Security, Protection and Law Enforcement

Mission Area: Response

Description: Ensure a safe and secure environment through law enforcement and related security and protection operations for people and communities located within affected areas and for response personnel engaged in lifesaving and life-sustaining operations.

Critical tasks:

- Ensure the capacity to communicate with both the emergency response community and the affected populations and establish interoperable voice and data communications between Federal, tribal, state, and local first responders.
- Re-establish sufficient communications infrastructure within the affected areas to support ongoing life-sustaining activities, provide basic human needs, and transition to recovery.

- Re-establish critical information networks, including cybersecurity information sharing networks, to inform situational awareness, enable incident response, and support the resiliency of key systems.

21. Operational Communications

Mission Area: Response

Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations by all means available, among and between affected communities in the impact area and all response forces.

Critical Tasks:

- Deliver medical countermeasures to exposed populations.
- Complete triage and initial stabilization of casualties and begin definitive care for those likely to survive their injuries and illness.
- Return medical surge resources to pre-incident levels, complete health assessments, and identify recovery processes.

22. Public Health, Healthcare and Emergency Medical Services

Mission Area: Response

Description: Provide lifesaving medical treatment via Emergency Medical Services and related operations and avoid additional disease and injury by providing targeted public health, medical, and behavioural health support, and products to all affected populations.

Critical tasks:

- Identify affected populations, groups and key partners in short-term, intermediate, and long-term recovery.
- Complete an assessment of community health and social service needs, and prioritize these needs, including accessibility requirements, based on the whole community's input and participation in the recovery planning process, and develop a comprehensive recovery timeline.
- Restore health care (including behavioural health), public health, and social services functions.

- Restore and improve the resilience and sustainability of the health care system and social service capabilities and networks to promote the independence and well-being of community members in accordance with the specified recovery timeline.

23. Situational Awareness and Decision Making

Mission Area: Response

Description: Provide all decision makers with decision-relevant information regarding the nature and extent of the hazard, any cascading effects, and the status of the response.

Critical tasks

- Deliver medical countermeasures to exposed populations.
- Complete triage and initial stabilization of casualties and begin definitive care for those likely to survive their injuries and illness.
- Return medical surge resources to pre-incident levels, complete health assessments, and identify recovery processes.

24. Natural and Cultural Resources Protection

Mission Area: Response

Description: Protect natural and cultural resources and historic properties through appropriate planning, mitigation, response, and recovery actions to preserve, conserve, rehabilitate, and restore them consistent with post-disaster community priorities and best practices and in compliance with applicable environmental and historic preservation laws and executive orders.

Critical tasks:

- Implement measures to protect and stabilize records and culturally significant documents, objects, and structures.
- Complete an assessment of affected natural and cultural resources and develop a timeline for addressing these impacts in a sustainable and resilient manner.

- Preserve natural and cultural resources as part of an overall community recovery that is achieved through the coordinated efforts of natural and cultural resource experts and the recovery team in accordance with the specified timeline in the recovery plan.

Core Capabilities Evaluation Criteria:

Table describes the criteria used to rate the county's current capabilities across the five solution mission areas. The scores are assigned using a scale of 0 (no capability) to 5 (fully capable).:

TABLE 4.2-2 CAPABILITY MAPPING ASSESSMENT SCALE

Missed	0
Very Low	1
Low	2
Medium	3
High	4
Very high	5

4.3. Capability building cycle and Gap Analysis

The capability building cycle is the process through which the system resilience is enhanced. It consists of four steps (Figure 4.3-1):

- In the first step, the current state of the resilience capabilities is assessed.
- In the second step, a Gap Analysis is performed where the gaps in the capabilities are identified considering the accidents and related system vulnerabilities. Based on the analysis, a target value for each capability is deliberated. Target values aim to cover all the gaps and make the system completely fitting with its exposure to the con-text.

- In the third step, the objectives are set, and the implementation plan is decided upon. Objective values identify the expected improvements to be achieved during the next planning cycle, hence they could be lower than the target values.
- The fourth step (which is also the first step of the next planning cycle) is where the resilience capabilities are reassessed and reviewed after a single improvement cycle.

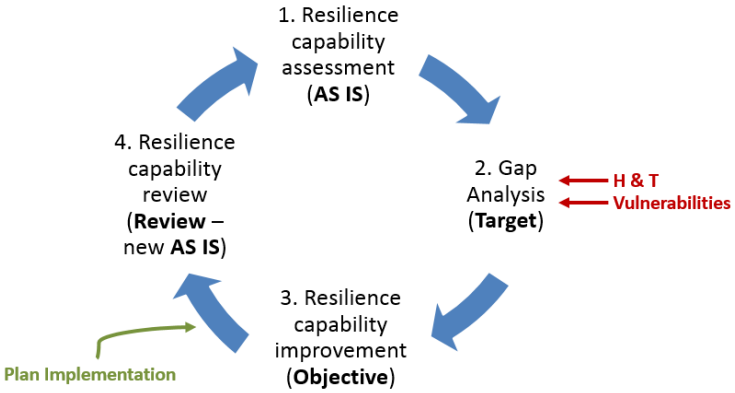

FIGURE 4.3-1 CAPACITY BUILDING CYCLE

The Gap Analysis is not tied to a specific accident but to the overall EM and resilience state, including all involved organizations. It is shown as a matrix (EM phases vs. Resilience Capacities) summarizing the capability gaps (the difference between the Target and the Current level) for each field, considering every Organization-Capability couple. The Gap Analysis shows the analyst a comprehensive picture giving quantitative indicators, enabling him to easily identify the weak points. It is also a clear clue about where the future improvements should be focused, considering EM phases against the resilience capacities. The 'detailed list' option is also able to show the full details on each of the capabilities.

CHAPTER 5- IMPLEMENTATION OF THE SW TOOL

In this chapter, description of model for tool, programing that used, process flowchart., and end user guidelines are explained.

5.1. Description of a model

A model is a representation of a set of components of a system or subject area. The model is developed for understanding, analysis, improvement or replacement of the system. Systems are composed of interfacing or interdependent parts that work together to perform a useful function. System parts can be any combination of things, including organizations, EM information, capacity, software, processes, accident, system description, characterization, resilience assessment. The model describes what a system does, what controls it, what things it works on, what means it uses to perform its functions, and what it the output. this tool is focused on resilience assessment and analysis. In the proposed tool user guidelines are developed to direct the users to four main functions as: system description, characterization, resilience assessment (output). In system description, there are four other components organizations, infrastructures, hazards and threats and capabilities. Like system description, also in characterization there are there component possess where we give property and characterize the system by which are namely Accident specification, asset vulnerability and capacity assessment. In the end phase resilience assessment, we get output as capability analysis and GAP analysis. The aim of this study is to deliver a model to support assessment and analysis of resilience within framework. These main functions user interface is illustrated in Figure

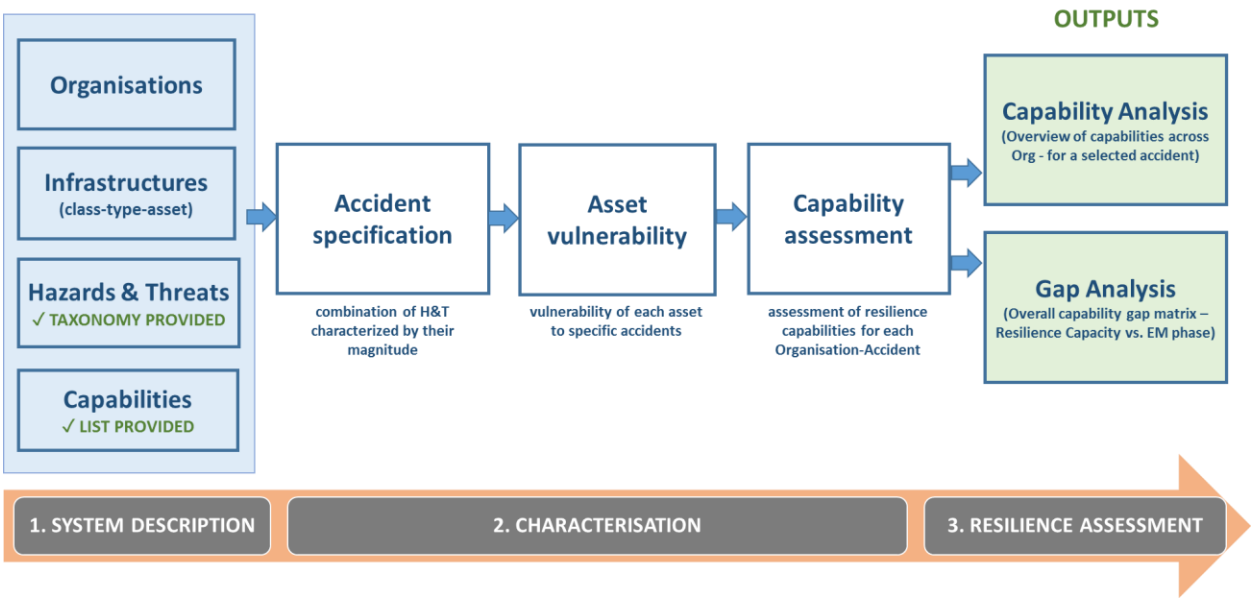

FIGURE 5.1-1 MODEL

5.2. The Relational Database Model

A database is a set of information with regular structure. Its user interface allows data access, searching and sorting routines. A database can be understood as a collection of related files. How those files are related depends on the model used. Early models included the hierarchical model (where files are related in a parent/child manner, with each child file having at most one parent file), and the network model (where files are related as owners and members, similar to the network model except that each member file can have more than one owner). The first databases implemented during the 1960s and 1970s were based upon either flat data files or the hierarchical or networked data models. These methods of storing data were relatively inflexible due to their rigid structure and heavy reliance on applications programs to perform even the most routine processing. The relational model for database management is a database model based on predicate logic and set theory. It was first formulated and proposed in 1969 by Edgar Codd with aims that included avoiding, without loss of completeness, the need to write computer programs to express database queries and enforce database integrity constraints. In 1969, when Codd developed the model, it was thought to be hopelessly impractical, as the machines of the time could not cope with the overhead necessary to

maintain the model. Evidently, hardware since then has come on in huge strides, so that today even the most basic of PCs can run sophisticated relational database management systems. In relational databases, such as Sybase, Oracle, IBM DB2, MS SQL Server and MS Access, data is stored in tables made up of one or more columns (Access calls a column a field). The data stored in each column must be of a single data type such as Character, Number or Date. A collection of values from each column of a table is called a record or a row in the table. Different tables can have the same column in common. This feature is used to explicitly specify a relationship between two tables.

5.2.1. Programming Environment (Microsoft Access)

Access is used by small businesses, within departments of large corporations, and hobby programmers to create ad hoc customized desktop systems for handling the creation and manipulation of data. Access can also be used as the database for basic web based applications hosted on Microsoft's Internet Information Services and utilizing Microsoft Active Server Pages ASP. One of the benefits of Access from a programmer's perspective is its relative compatibility with SQL—queries may be viewed and edited as SQL statements, and SQL statements can be used directly in Macros and VBA Modules to manipulate Access tables. Users may mix and use both VBA and "Macros" for programming forms and logic and offers object-oriented possibilities. Access allows relatively quick development because all database tables, queries, forms, and reports are stored in the database. For query development, Access utilizes the Query Design Grid, a graphical user interface that allows users to create queries without knowledge of the SQL programming language. Microsoft Access can be applied to small projects but scales poorly to larger projects involving multiple concurrent users because it is a desktop application, not a true client-server database. MS Access is chosen for development environment mainly because of availability and user-friendly issues of the program. The aim of developing this program had not been delivering a fully functioning system but to illustrate a real-life example on a relatively small scale of information. Physical relations definitions between MS Access tables for out tool is given below in figure

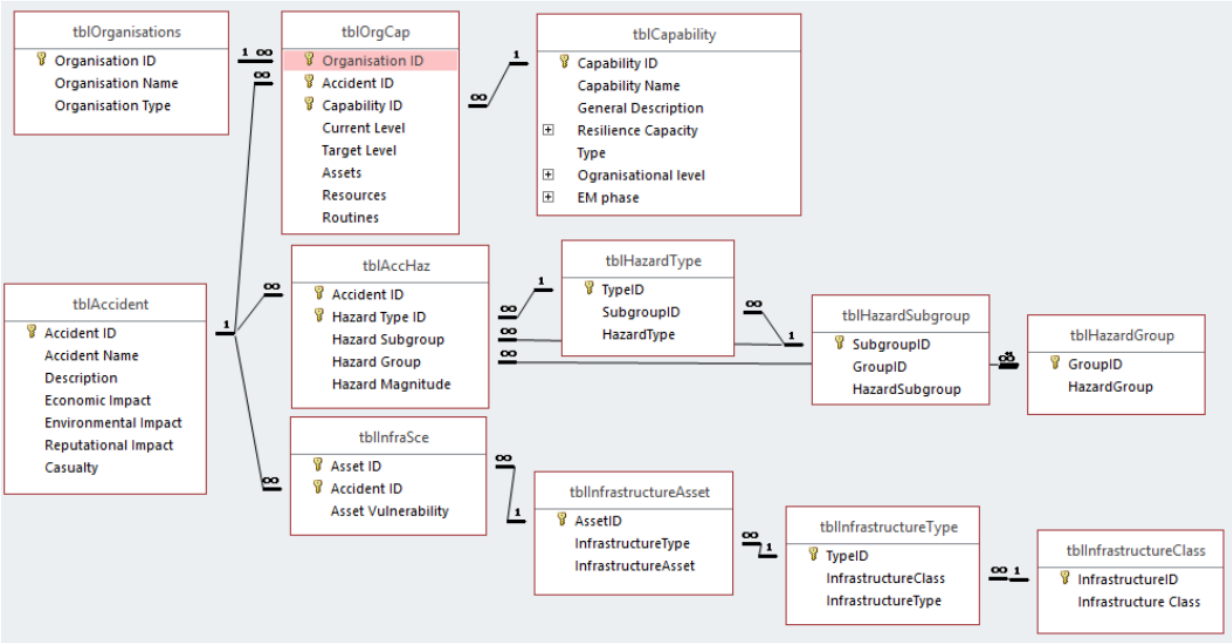

FIGURE 5.2-1 MODEL RELATIONSHIP DIAGRAM

5.3. description of tool and End User guide

To work with a system, the users need to be able to control the system and understand the state of the component of system. In software applications, the end-user interaction with the program is limited with the user interface defined by the developer. So here is the user guide developed that defines an access understanding between user and the tool.

In the proposed tool user guidelines are developed to direct the users to four main functions as: system description, characterization, resilience assessment.

When we open the tool, the 1st view appears consisting four click bars in which edit the system belongs to the system description part, edit accident & edit asset vulnerability belongs to the system characterization part and then finally resilience assessment in which you can carry out resilience analysis and gap analysis as shown in following figure.

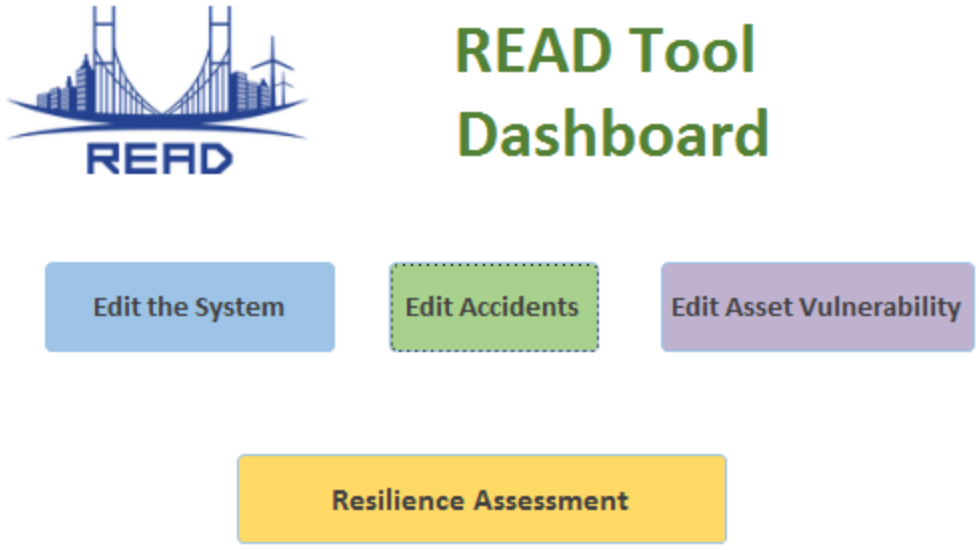

FIGURE 5.3-1 OVERVIEW OF TOOL

5.3.1 System description:

In the system description, we have four parts namely Organizations, capabilities, hazards and threats, and infrastructures. While we click on option “Edit system” we have these four options appeared on the screen as we see in figure below.

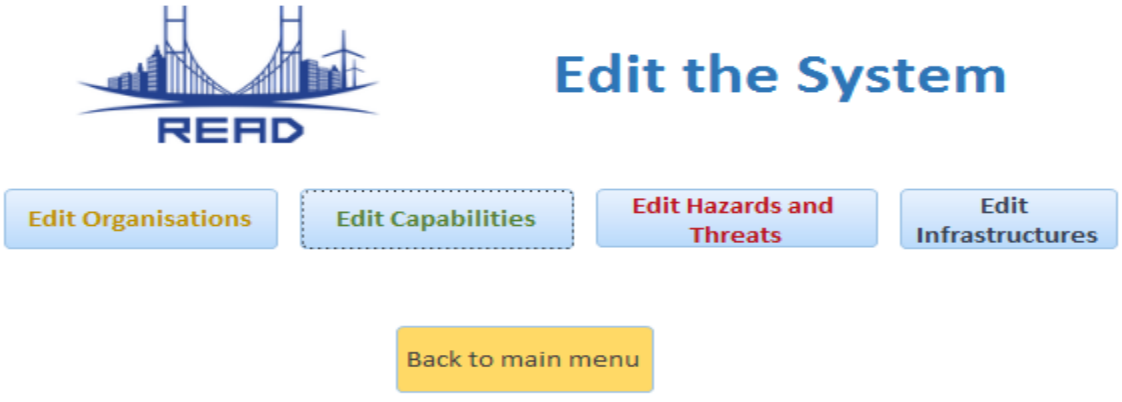

FIGURE 5.3-2 SYSTEM DESCRIPTION

There four parts of system are named in tool as “Edit Organizations”, “Edit Capabilities”, “Edit hazard and threats”, “Edit infrastructure” and “back to main menu”.

“back to main menu” option take you back to main menu and other options are explained below.

A) By clicking on “edit organizations” option, we can create list of organizations by their name and type of organizations by adding new organization in the list. If we have to edit the already existing list, we can use delete option. And by clicking on close option, it will take you to previous menu called “Edit the system”.

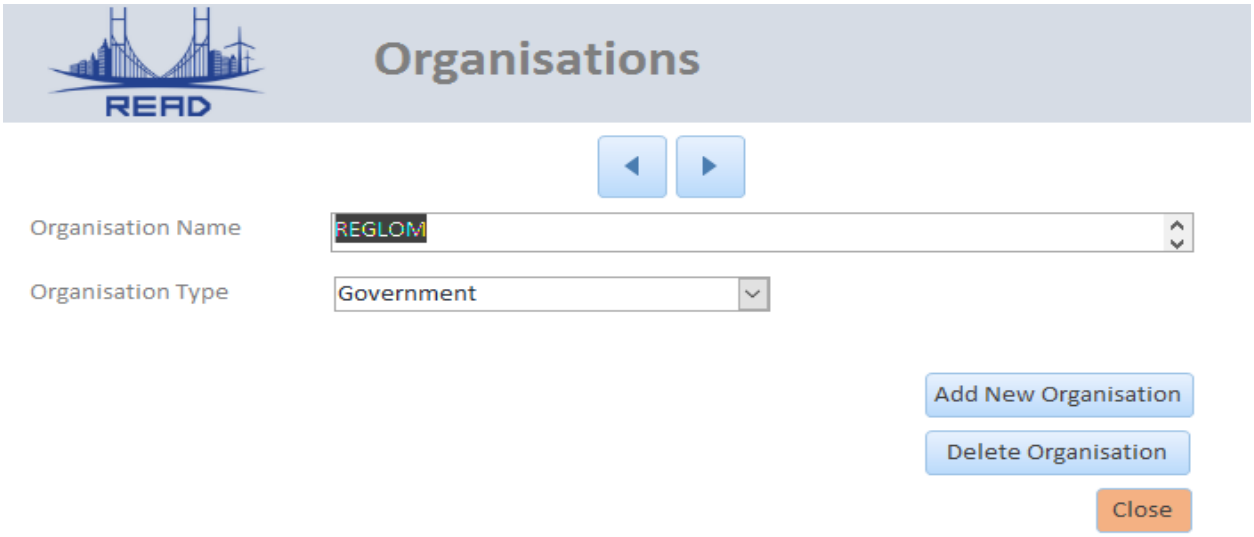

FIGURE 5.3-3 EDIT ORGANIZATION

B) By clicking on “edit Capabilities” option, we can create list of capabilities. And we can also include capabilities’ characteristics by adding their name and type, description, organizational level, EM Phases, and resilient capacity of capabilities. If we do have to edit the already existing list, we can use delete and add options. And by clicking on close option, it will take you to previous menu called “Edit the system”.

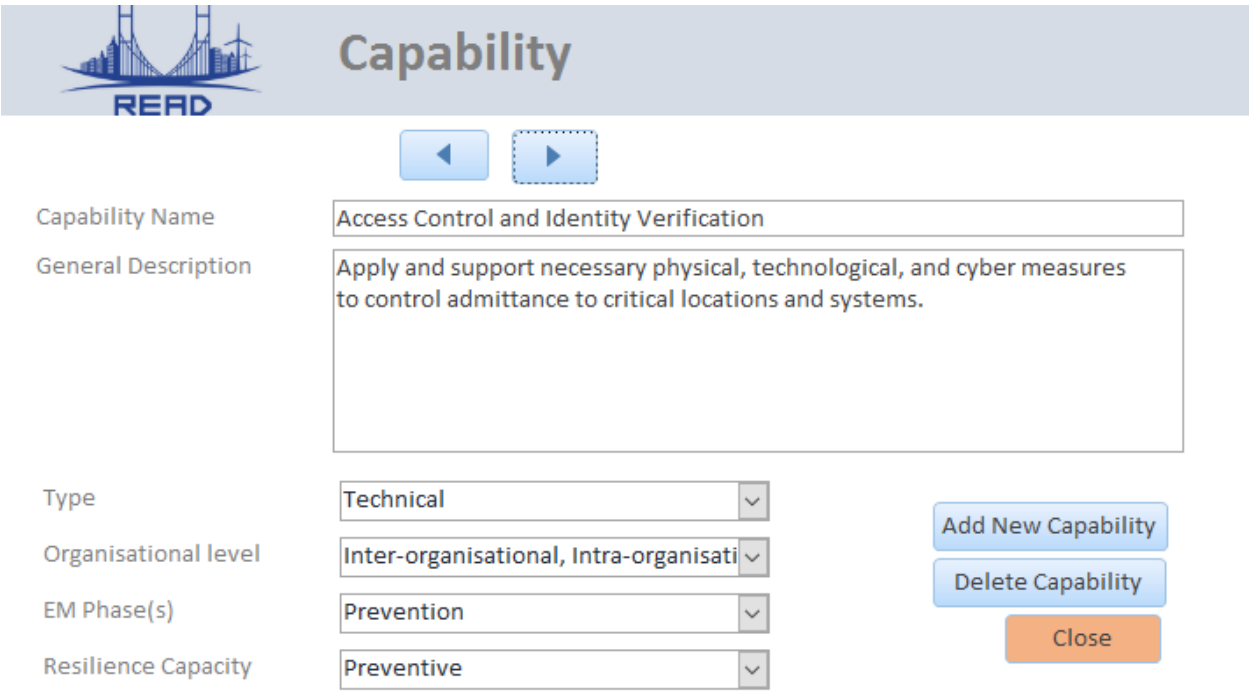

FIGURE 5.3-4 EDIT CAPABILITIES

There are different 24 capabilities which are selected for this framework which are from FEMA's National Preparation Goals (2016) and Types, organismal levels, EM phases and type of resilient capacities are defined in previous chapter for thesis.

C) By clicking on "edit hazards and threats" option, we can add and delete hazard groups, sub hazard groups, & hazard type, snd by clicking on close option, it will take you to previous menu called "Edit the system". Classification of hazard/sub hazard/ hazard types that is being used for our frame work, are given below in the table.

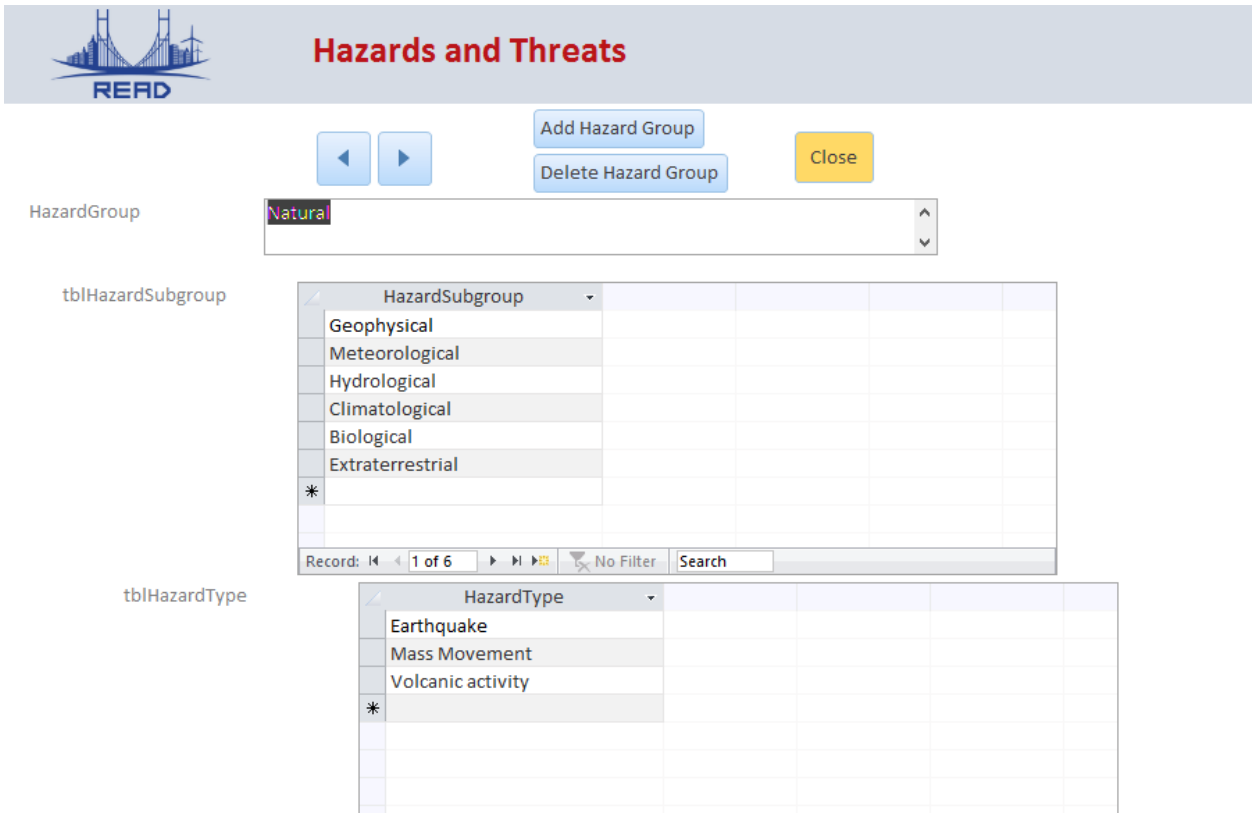

FIGURE 5.3-5 EDIT HAZARD THREATS

TABLE 5.3-1 HAZARD CLASSIFICATION

Disaster Group	Disaster Subgroup	Disaster Main Type
Natural	Geophysical	Earthquake
		Mass Movement
		Volcanic activity
	Meteorological	Extreme Temperature
		Fog
		Storm
	Hydrological	Flood
		Landslide
		Wave action
	Climatological	Drought
		Glacial Lake Outburst

		Wildfire
	Biological	Epidemic
		Insect infestation
		Animal Accident
	Extraterrestrial	Impact
		Space weather
Technological	Industrial accident	Chemical spill
		Collapse
		Explosion
		Fire
		Gas leak
		Poisoning
		Radiation
		Other
	Transport accident	Air
		Road
		Rail
		Water
	Miscellaneous accident	Collapse
		Explosion
		Fire
		Other
Intentional Threats	Terrorism	Cyberterrorism
		Narcoterrorism
		Stampedes
		Crime
		Chemical Agents
		Biological agents
		Nuclear and radiological weapons
		Conventional explosives

	Mass Shootings	School shootings
		Workplace violence
		Hate crimes
	Civil Disobedience	Labor riots
		Race riots
		Political riots

D) By clicking on “Edit Infrastructures” option, we can create list of infrastructure class, infrastructure type and then infrastructure assets. For example, we have infrastructure class “transportation” in which we have types of transport infrastructure i.e. rail, road and airports. In infrastructure assets are name of stations if we choose type of infrastructure “rail”. If we do have to edit the already existing list, we can use delete and add options as shown in figure. And by clicking on close option, it will take you to previous menu called “Edit the system”.

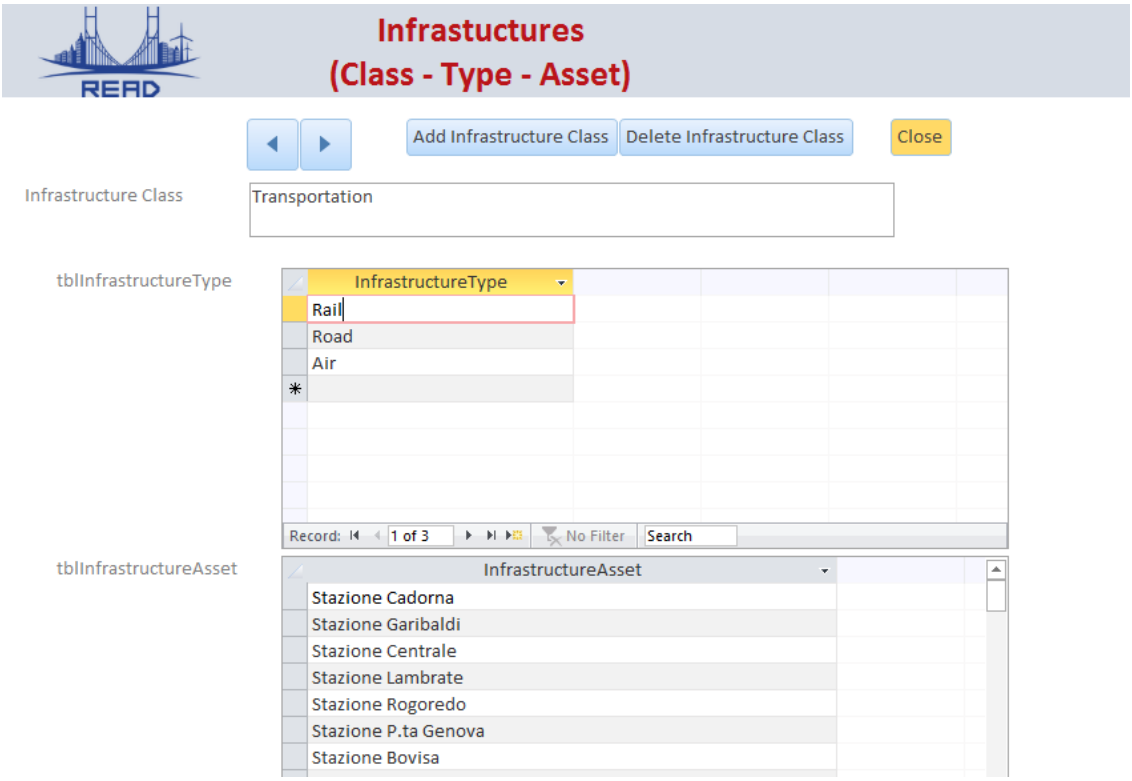

FIGURE 5.3-6 EDIT INFRASTRUCTURES

5.3.2. Characterization:

Characterization of system includes accident, assets vulnerabilities and resilience assessment. On main menu, there are three icons which represents the characterization of system, namely “Edit accident, edit asset vulnerabilities and “resilience assessment”.

A) When we click on “Edit accident”, following window appears which is shown in figure. We can add or remove more or more than one accident here including accident description by clicking add option and delete option. “Edit capabilities” option will take you back in previous section of capabilities. We can also define hazard group/subgroup/type and intensity of accident. Intensity is measured in terms of low, medium, high and very high which is explained in previous chapter. In this section, we also will have to define economic impact, environmental impact, reputational impact and causality in term of low/medium/high/ very high. we can use delete and add options as shown in figure. And by clicking on “done” option, it will take you to previous menu called “Edit the system.

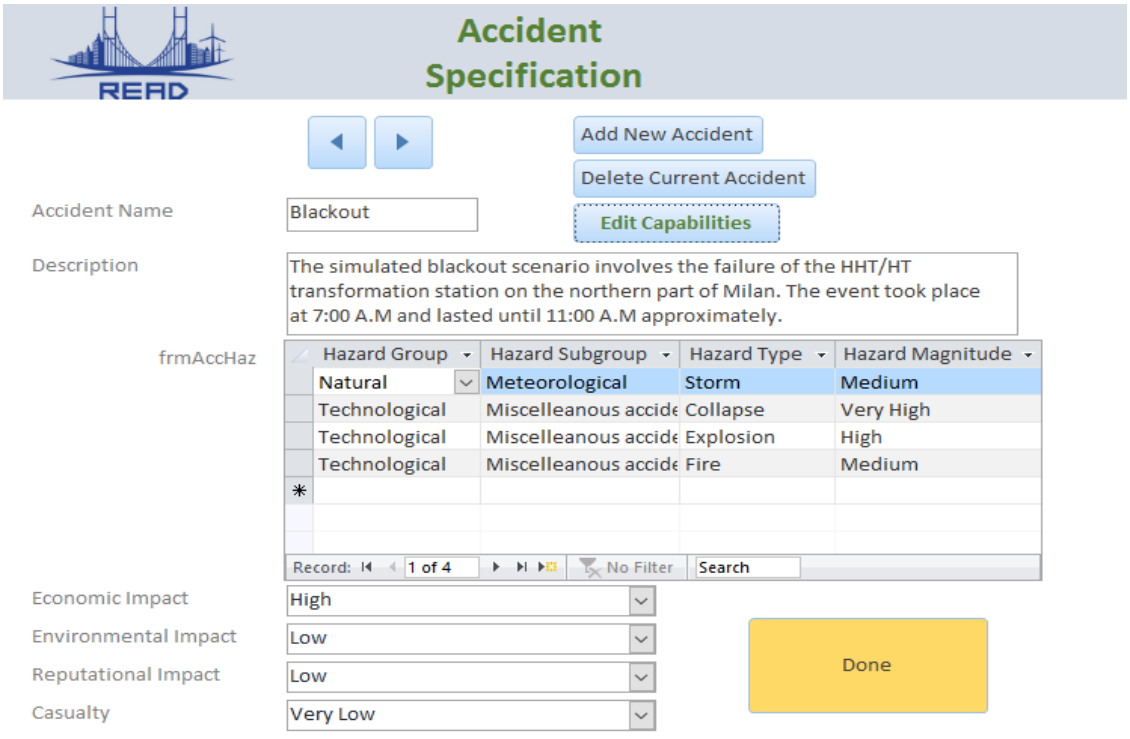

FIGURE 5.3-7 ACCIDENT SPECIFICATION

B) When we click on “Edit asset vulnerability”, following window appears which is shown in figure. We can add or remove more or more than one records of vulnerabilities by using add option and delete option. In this section, we will have to define infrastructure class/type/asset as per example given in figure. we can use delete and add options as shown in figure. Down in the table we have to add in the table type of “accident” and its vulnerability in terms of low/medium/high/very high. And by clicking on “done” option, it will take you to previous menu called “Edit the system”.

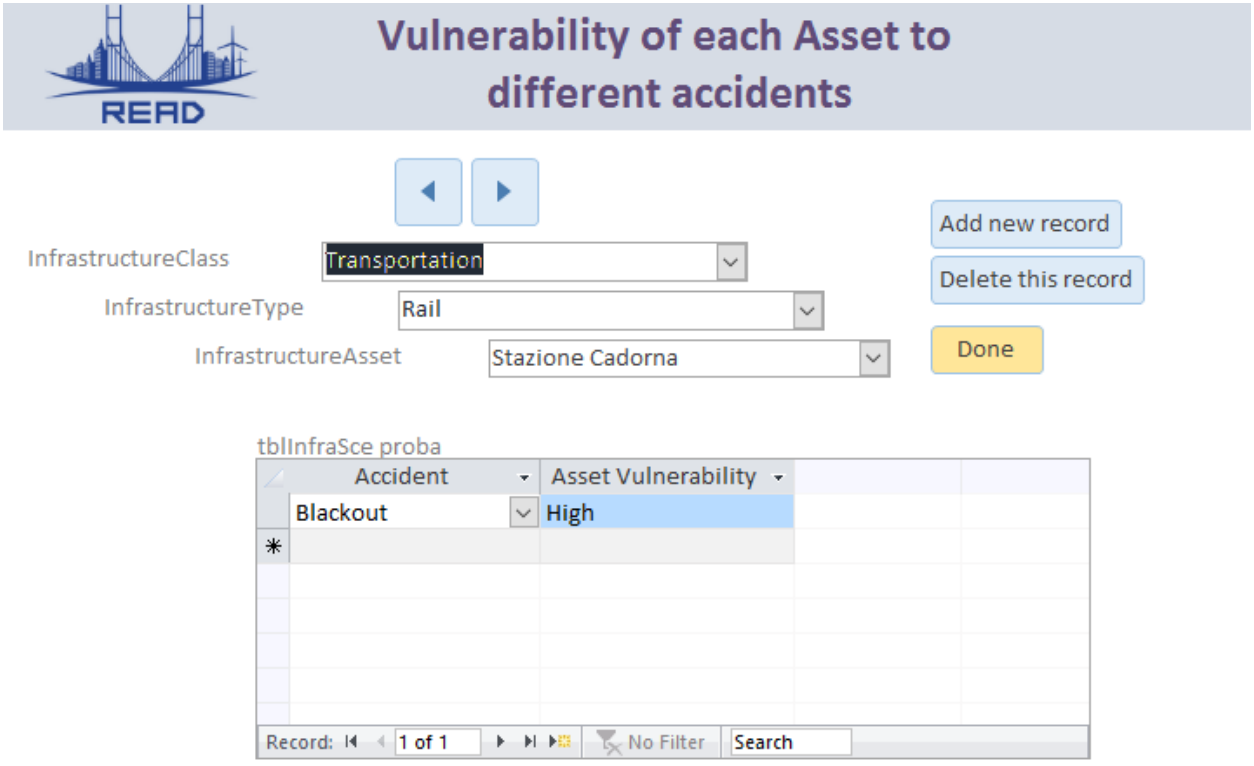

FIGURE 5.3-8 EDIT ASSET VULNERABILITY

5.3.3. Resilience assessment and analysis

This section included capability assessment, capability analysis, and GAP analysis. In which capability assessment is part of characteristics and capability analysis and GAP analysis are part of the Resilience analysis. when we click on “resilience

assessment” on main window of tool the following window appears as shown in figure. It has four options to click and one option to choose event by click. Four options are following “capability assessment”, “resilience analysis”, “gap analysis” and “back to main menu”. capability assessment”, “resilience analysis” and “gap analysis are explained in next segment while by clicking on “back to main menu” option, it will take you to main menu.

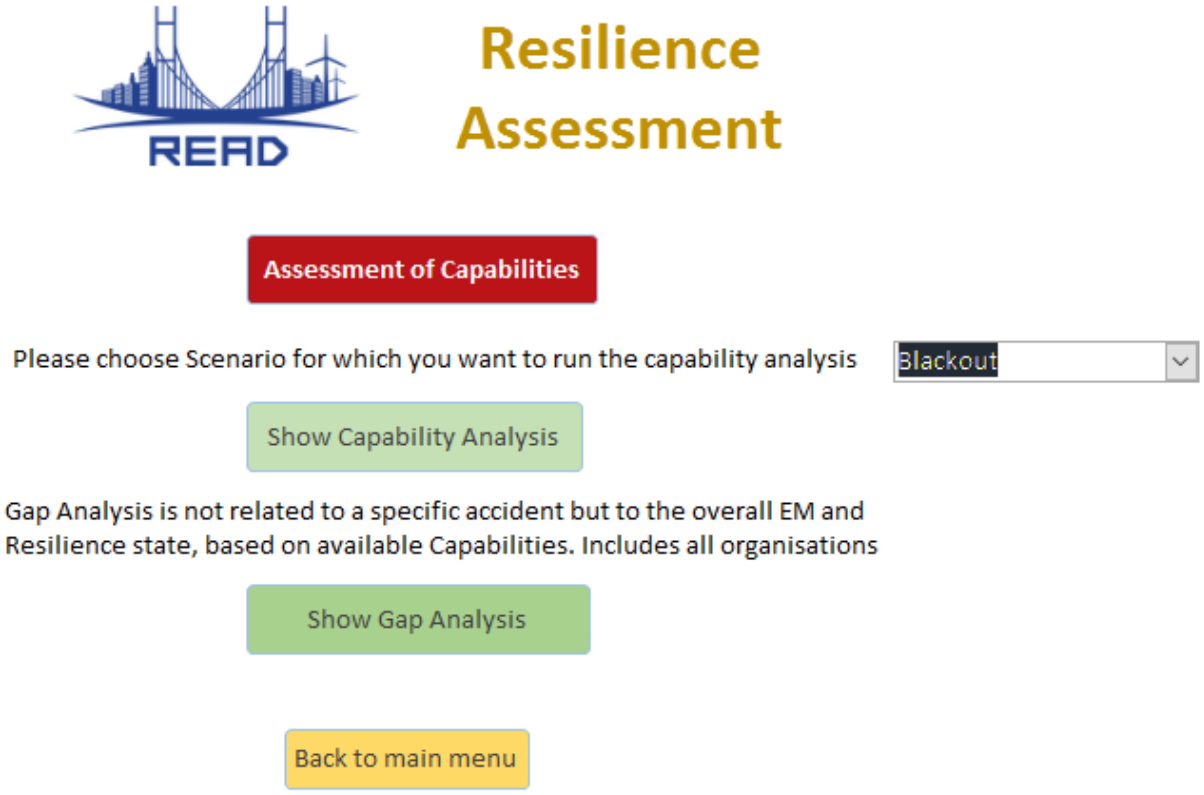

FIGURE 5.3-9 RESILIENCE ASSESSMENT

A) When we click on “Assessment of capabilities”, following window appears which is shown in figure. By clicking on edit organizations, edit accidents and “Edit capabilities” option will take you back in previous section of capabilities, organizations, accidents. Beside that we name the event and pick assets for vulnerabilities. In Individual capacity description, we need to choose organization, capability name, assets. Resources, and routines. List of capabilities is given by the side. section is to be defined as shown in this example taken for blackout event.

Capacity level and target level is measured in terms of low, medium, high and very high which is explained in previous chapter. by clicking on “done” option, it will take you to previous menu called “resilience analysis”.

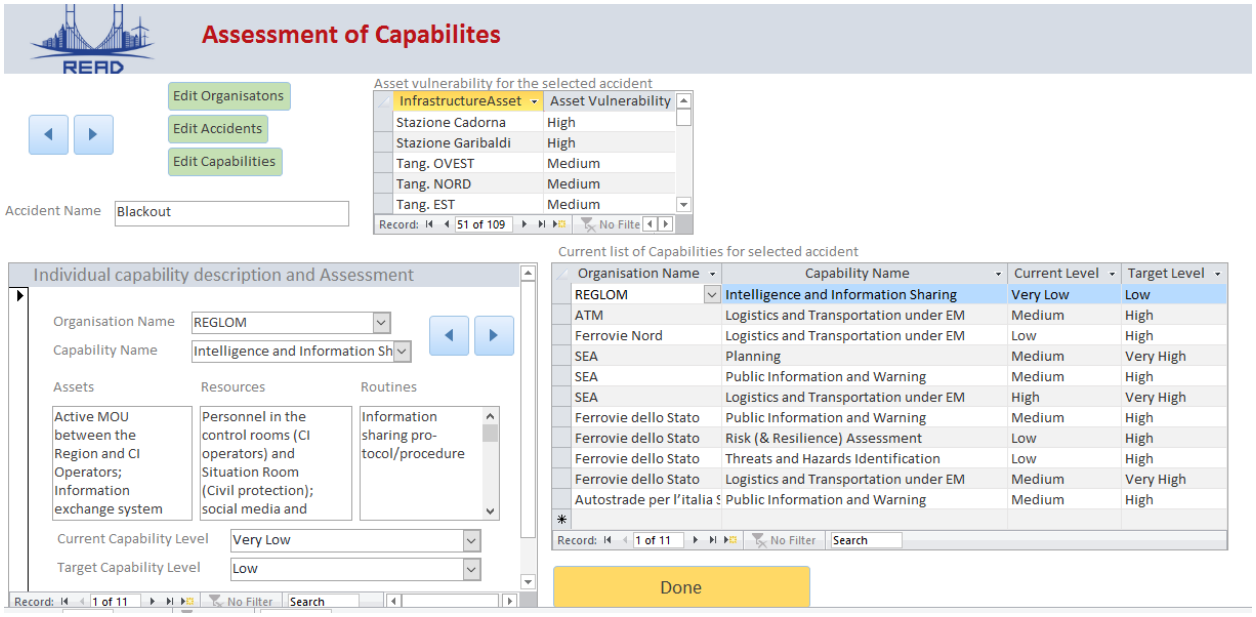

FIGURE 5.3-10 ASSESSMENT OF CAPABILITIES

B) After we are done with capability assessment, we have finished process of characterization of system. Now we are eligible to get results, but clicking on “show Resilience analysis” we get resilience output in table form for scenario we have chosen. And by clicking on “show gap analysis” we get out put in terms of resilience capacity & EM phases matrix. The gap analysis is not related to any specific accident but to the overall EM and resilient state, based on capabilities, and it includes all the organizations. In the gap analysis, maximum gap is selected of each couple organization capability, as the biggest gap across different scenarios. Then the gap analysis is calculating buy summarizing those capabilities maximum gap by resilience capacity and EM phases. Detailed list will be shown by clicking “show detailed list”.

CHAPTER 6- PILOT APPLICATION IN LOMBARDY REGION

The chapter is warmed up by discussing adoption of READ framework in the context of a Thematic Task Force on blackout events is described for eight virtual operators in Lombardy region of Italy.

Thematic Task Force focused on specific accident scenarios, they adopted the same methodological approach, substantially organized into three steps:

- development of vulnerability and resilience studies;
- identification of best practices and innovative solutions for risk mitigation through collaboration between actors, where opportunities for enhancing information sharing were particularly investigated and promoted;
- design, validation and implementation of collaborative emergency plans;

The outcomes of Resilience Assessment, GAP analysis, Capacity assessment are also discussed briefly in this chapter.

6.1. Blackout event

Power grids are the most prominent infrastructure due to the fact that the daily life of modern society is directly or indirectly integrated to electric power consumption. And when it is exposed to failures due to human or natural factors, detecting and repairing failed component of the system can initiate another failure. Hence, modelling and analyzing failure could help understanding of characteristics of blackout distribution on the network and predict the impact of the failure on interconnected systems.

In order to perform pilot application, we have considered two Reference Blackout scenarios

1. Local urban event triggered by a failure in the transmission grid without loss of components

- Assessment time: 1 hour
- TS recovery time: 6 hours

2. Nation-wide blackout, with cross-border effects, triggered by an operating error (e.g. human) of the TSO

- Assessment time: 1 hour
- TS recovery time: 12 hours

6.2. CI operators participating in Thematic Task Force

There are eight different virtual operators considered in this pilot application.

1. Actor-1 [Electricity Operator]
2. Actor-2 [Electricity Operator]
3. Actor-3 [Rail transport Operator]
4. Actor-4 (Tram/Bus/Metro) [Public transport Operator]
5. Actor-5 [Gas distribution Operator]
6. Actor-6 [Transmission System Operator]
7. Actor-7 [Gas distribution Operator]
8. Actor-8 [Rail transport Operator]

6.2.1. Capacity classification

Resilience capacity is identifying and measuring local conditions hypothesized to position a system best for responding to and recovering from a disturbance. In the following pilot application, we have considered twenty-four capacities and classified them according to properties like assets, capacities, Gap between self-assessment and target level as shown in table below. This table was provided to different operators to fill self-assessment of capacities and the target level.

TABLE 6.2-1 THE STANDARD TEMPLATE

CAPABILITY	e-distribuzione (TBA)	Capability															To fulfil during Session I	To fulfill during Session II	
	Assets	EM cycle					Resilience Dimension		Resilience Capacity				Organazational Level		Cross border interction		Self assessment	Target level	GAP
		Preparedness	Prevention	Mitigation	Response	Recovery	Technical	Organizational	Preventive	Assorbtive	Adattativaptive	Ristorative	Intra-organizational	Intra-organizational	yes	No	It is the assessment about current level of capabilities [1 (min) a 5 (max)]	It is the assessment about desirable level of capabilities [1 (min) a 5 (max)]	

Capacity classification can be understanding by following Examples of capabilities of intra organizations in the case application

TABLE 6.2-2 CAPACITY CLASSIFICATION

Organization type	Capability Description	Classification			
		EM Cycle	Resilience Dimension	Resilience Capacity	Organizational Level
Civil Protection	Communication and Information Sharing	Preparedness, mitigation, response, recovery	Technical, organizational	Absorptive Adaptive	Intra-organizational, inter-organizational
Rail operator	Backup Electricity	mitigation, response, recovery	Technical	Absorptive	inter-organizational
Metro Operator	Backup transport means	mitigation, response, recovery	organizational	Absorptive Adaptive Restorative	Intra-organizational, inter-organizational
Airport Operator	Evacuation of passengers	mitigation, recovery	Technical, organizational	Absorptive	Intra-organizational, inter-organizational
Electricity operator	Communication to the public	Preparedness, response, recovery	Technical, organizational	Absorptive Adaptive	inter-organizational

6.2.2. Capability assessment

An assessment is Assessment of the actual level of resilience capabilities and also given on the current and the target (i.e. desired) level of this capability as planned by the corresponding organization. The difference between current and desired capacity level also called GAP analysis. It is important to mention that the capability assessment is done considering the vulnerability of assets to the accident.

The standard assessment scale matrix is defined as:

TABLE 6.2-3 STANDARD ASSESSMENT

		Capability coverage of hazards and threats		
		Single or few	Several	All-hazard
Type of accident event	Simple	1 - Very low	2 - Low	3 - Medium
	Complex	2 - Low	3 - Medium	4 - High
	With cross-border effects	3 - Medium	4 - High	5 – Very High

6.2.3. Intra-organisational Gap Analysis:

After collecting date, Operators' improvement plan with respect to efforts are determined. For example, in given matrix of EM cycle and Resilience capacity if we choose Preventive and preparation. We will get improvement effort are determined in percentage by formulating

$$\text{Operators' improvement} = \frac{\text{Resilience capacity of all operators in selected phase of EM cycle}}{\text{Self assessed Resilience capacity of all operators in all phases of EM cycle}} * 100$$

For example, if we want to determined operator's improvement for preventive capacity in Prevention phase of EM cycle. The total capacity is 41 as we can see in following table and total self-assessment resilience capacity is 416. Hence operator's improvement would be around10% in this block. Same, we can determine for other phases as well.

TABLE 6.2-4 INTRA-ORGANIZATIONAL GAP IN TERMS OF OPERATORS' IMPROVEMENT PLAN

	Preparation	Prevention	Mitigation	Response	Recovery
Preventive	9%	10%	5%	5%	3%
Absorptive	4%	5%	6%	6%	5%
Adaptive	4%	4%	5%	6%	4%
Restorative	4%	4%	5%	6%	6%

TABLE 6.2-5 GAP ANALYSIS

Sum of GAP	Column Labels								
Row Labels	Actor 1	Actor 2	Actor 3	Actor 4	Actor 5	Actor 6	Actor 7	Actor 8	Grand Total
Access Control and Identity Verification	1		1	1	1		0	0	4
Community Resilience Building	1	0	1					0	2
Cybersecurity	1	1	0				0	0	2
Environmental Response / Health and Safety		0				0		0	0
Fatality Management Services								0	0
Fire Fighting		2		1	3		0	0	6
Intelligence and Information Sharing	1					0	0	0	1
Interdiction and Disruption		1				1	1	0	3
Logistics and Transportation under EM							0	0	0
Mass Care								0	0
Mass Search and Rescue Operations								0	0
Natural and Cultural Resources Protection								0	0
On-scene Security, Protection and Law Enforcement								0	0
Operational Communications		0					0	0	0
Operational Coordination		0					0	0	0
Physical Protective Measures			1			2	1	0	4
Planning		1	1			0	0	0	2
Public Health, Healthcare and Emergency Medical Services								0	0
Public Information and Warning		1		0	0			0	1
Risk (& Resilience) Assessment		2	1			0	1	0	4
Screening, Search and Detection				1		1	0	0	2
Situational Awareness and Decision Making		0	1	0	0			0	1
Supply Chain Integrity and Security						1	2	0	3
Threats and Hazards Identification	3	1		0	0	1	1	0	6
Grand Total	**7**	**9**	**6**	**3**	**4**	**6**	**6**	**0**	**41**

In below two different Pi charts presented, they represent share of each capacity GAP in EM cycle, and share of Phases of EM cycles to capacity.

TABLE 6.2-6 RESILIENCE CAPACITY IN EM PHASES

	Preparedness	Prevention	Mitigation	Response	Recovery		Resilience Capacity
Preventive	37	41	21	21	13		133
Absorptive	17	21	25	23	18		104
Adaptive	15	17	18	23	15		88
Restorative	16	14	20	23	22		95
EM Cycle	85	93	84	90	68		420

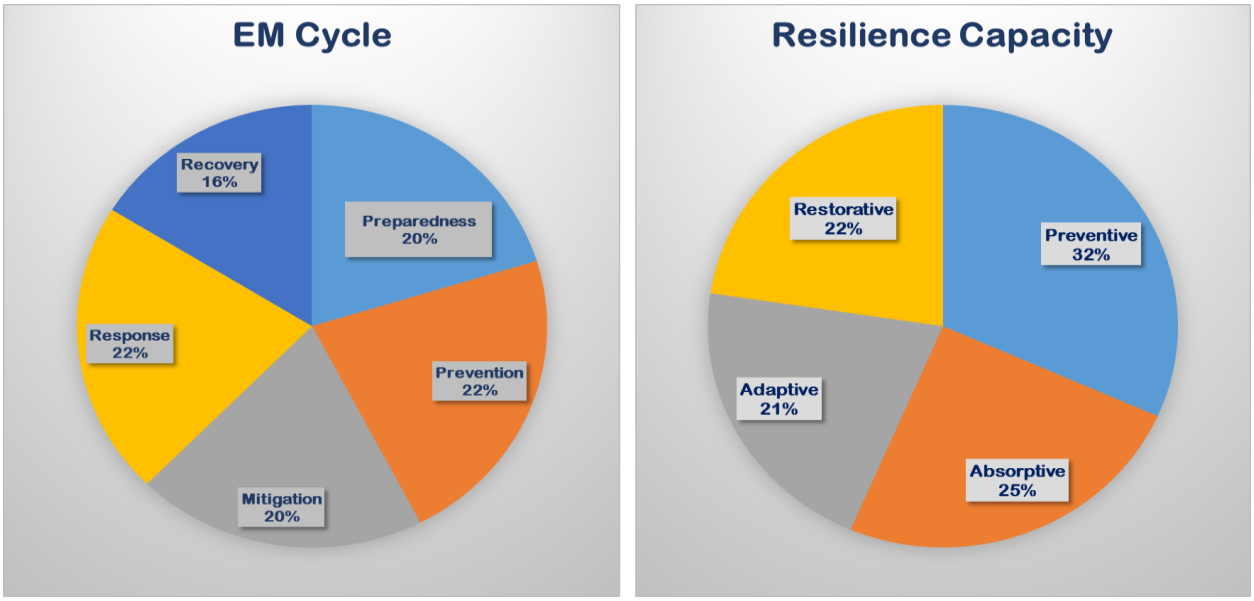

FIGURE 6.2-1 PI CHART OF INTRA-ORGANIZATIONAL GAP IN TERMS OF OPERATORS' IMPROVEMENT PLAN

6.3. Blackout resilience strategies:

To combat problems of capacity resistance, we have to decide strategies, in this case we have two strategies, one is to robust all hazards in electricity infrastructures and selective capabilities in other infrastructures. However, in another strategy, we give importance on adaptive capabilities of all the CI operators to assure rapid service recovery even in emergencies with complex cascading and cross-border effects. For Capability Mapping, following assessment scale is used:

Strategy 1 – in Strategy1 we focus more on robusting the electricity infrastructure by considering all hazard. But also, focus on selective resilience capabilities in other critical infrastructures Because there is a managed propagation of disruptions and disservices. In this strategy, we focus more on preventive, absorptive capacity for preparedness and mitigation, Adaptive for recovery, finally Restorative capacity for mitigation and recovery as highlighted in following table. As per strategic objective, strategic capacities are marked on in actual map which is actual capacity map at current level of operators. By using capability mapping prepared for action plan.

TABLE 6.3-1 STRATEGIC OBJECTIVE FOR STRATEGY NO. 1

	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	***5***	3	***5***	3	0
Absorptive	***4***	0	***4***	3	2
Adaptive	2	0	0	2	***3***
Restorative	2	3	***5***	2	***3***

Strategic obj.	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	5	3	5	3	0
Absorptive	4	0	4	3	2
Adaptive	2	0	0	2	3
Restorative	2	3	5	2	3

Actual map	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	71%	68%	77%	78%	81%
Absorptive	83%	80%	77%	77%	81%
Adaptive	83%	81%	79%	75%	81%
Restorative	81%	81%	77%	76%	76%

TABLE 6.3-2 CAPABILITY MAPPING OF ACTUAL MAP BY STRATEGIC OBJECTIVE

Strategy 2 – in strategy 2 we consider leveraging on adaptive capabilities of all the CI operators to assure rapid service recovery even in emergencies with complex cascading and cross-border effects. In this strategy, we focus more on preventive capacities for recovery, absorptive & adaptive capacities for Response, Adaptive & Restorative for preparedness and recovery, finally Restorative capacity for mitigation and recovery as highlighted in following table. As per strategic objective, strategic capacities are marked on in actual map which is actual capacity map at current level of operators. By using capability mapping prepared for action plan.

TABLE 6.3-3 STRATEGIC OBJECTIVE FOR STRATEGY NO. 2

	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	3	3	3	3	***4***
Absorptive	3	0	3	***4***	2
Adaptive	***5***	0	0	***5***	***5***
Restorative	***4***	3	3	***2***	***4***

TABLE 6.3-4 CAPABILITY MAPPING OF ACTUAL MAP BY STRATEGIC OBJECTIVE

Strategic obj.	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	3	3	3	3	4
Absorptive	3	0	3	4	2
Adaptive	5	0	0	5	5
Restorative	4	3	3	2	4

Actual map	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	71%	68%	77%	78%	81%
Absorptive	83%	80%	77%	77%	81%
Adaptive	83%	81%	79%	75%	81%
Restorative	81%	81%	77%	76%	76%

6.4. Pilot case's Blackout resilience strategy

We chose (Strategy 2) for when we talked most of stakeholders most of them preferred strategy 2 (Leveraging on adaptive capabilities of all the CI operators to assure rapid service recovery even in emergencies with complex cascading and cross-border effects) over strategy 1 [Robust the Electricity Infrastructure («all-hazards») + selective resilience capabilities in another CI] because it's difficult to manage blackout cascades selectively. Other than that, 2nd strategy involves all stakeholders in a more distributed and fair way. And it leverages on actual strengths and CI operators' improvement plans.

6.4.1. Degree of alignment between Operators' Improvement Plans and actual map in strategy number 2.

By aligning actual mat to operator's improvement plan, we can idea how much we need to Improve and which capacities we must work on. As we can see from following alignment, for preparation phase, we have to focus on adaptive and restorative capacities. However adaptive and restorative have capacity capabilities as they are green which mean safer side, but to achieve improvement plan they need to be achieved 4% more

each. Similarly, in recovery phase we need to improve 3%, 4% & 6% to preventive, adaptive and restorative recoveries. In Response phase of EM cycle, improvements are little higher because we can see capacities absorptive & adaptive capacities have relatively low percentage, and we need to improve 6% each to absorptive & adaptive capacities.

TABLE 6.4-1 DEGREE OF ALIGNMENT BETWEEN OPERATORS' IMPROVEMENT PLANS AND ACTUAL MAP

Operator's improvement plans	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	9%	10%	5%	5%	3%
Absorptive	4%	5%	6%	6%	5%
Adaptive	4%	4%	5%	6%	4%
Restorative	4%	4%	5%	6%	6%

Actual map	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	71%	68%	77%	78%	81%
Absorptive	83%	80%	77%	77%	81%
Adaptive	83%	81%	79%	75%	81%
Restorative	81%	81%	77%	76%	76%

6.4.2. Gap Analysis for strategy 2:

In representation of gap analysis is done by Pi charts as shown following, Here a comparison is drawn between Operators' Improvement Plans and the Actual Strategic Weaknesses.

As we can see by comparing resilience capacities of both, preventive and absorptive capacities are more in operators' improvement plan to the Actual Strategic Weaknesses and in the same time adoptive and restorative capacities are less in operators' improvement plan to the Actual Strategic Weaknesses.

When we compare, EM cycle of Operators' Improvement Plans and the Actual Strategic Weaknesses. There's not that much changes except some minor difference between preparedness, prevention and mitigation phases of EM cycle.

However, response phase Weaknesses.

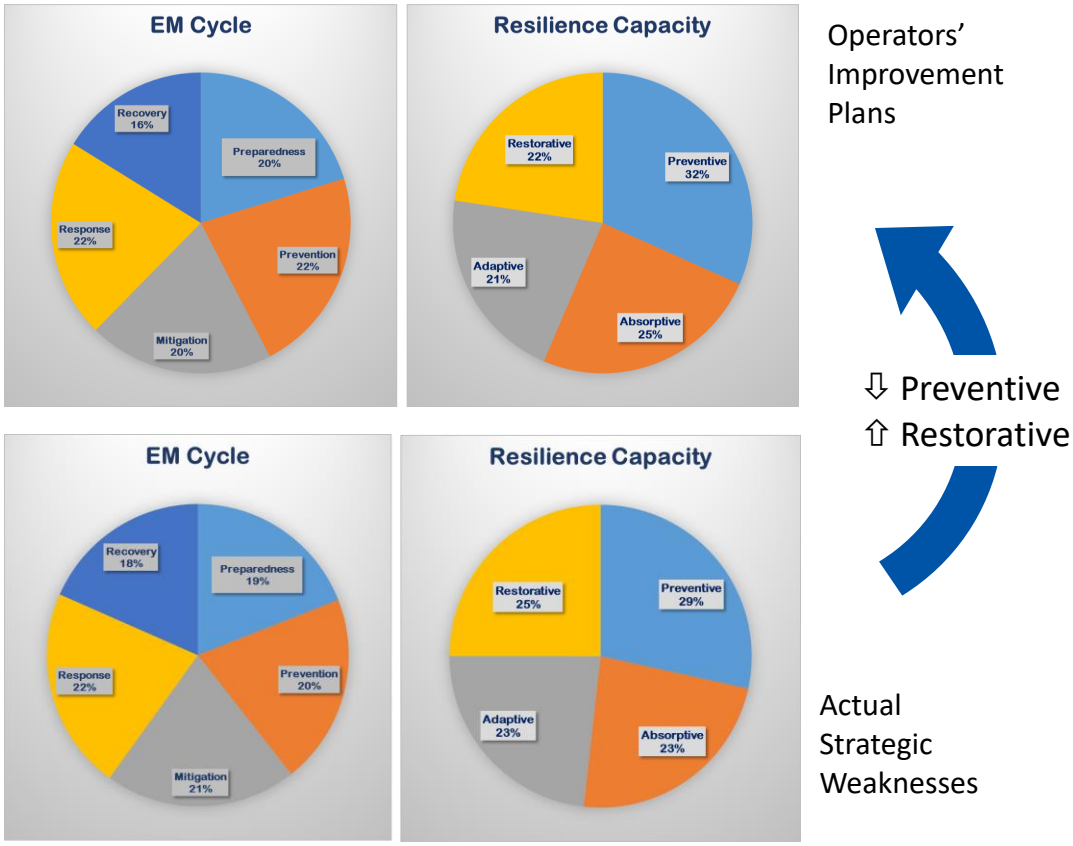

FIGURE 6.4-1 IMPROVEMENT PLAN

6.5. Capacity Discussion & Capacity building on regional level and operational level:

A lack of dialogue between the organizations was acknowledged, and a need for better integrate mutual planning. 'Only by pooling forces together we can be effective', was one of the comments. Consequently, the participants' suggestions included invitation to extend the analysis by involving more actors, not only CI operators, and discovering more ways to support the society. The operators agree that this type of approach helps them to avoid and cope with cascading effects. It is impossible to prevent everything, especially when an impact spreads through different infrastructure systems. There was a recognition of the current weaknesses in response and recovery, since prevention does not help anymore in those situations. Of course, there is no conflict between preventive and responsive capabilities. Operators also recognized that a standardized way of representing interorganizational resilience capacity enables a better mutual

understanding of the strategies and resources that each single organization can mobilize under a certain crisis event. The achievement and updating of such common picture fosters:

- the implementation of collaborative and coordination crisis response practices among operators, going beyond the requirements and plans of Civil Protection authorities;
- benchmarking of good practices and sharing of capacity building efforts. Another recurrent comment from the operators that completed the capacity assessment was that it takes time, even for experts in the field, to understand all the capabilities, check their comprehensiveness, and the level of implementation.

Given the amount of effort needed by the implementation of the pilot study, most operators proposed to continue to use the tool in the context of the PPP for CIR, starting from the new Task Force on CIR against climate change and severe weather events. The shared feeling was that the effort required will reduce by getting used with the tool; the quality of information and decision support will concurrently improve.

References:

1. 1. Lewis, A. M., Ward, D., Cyra, L., and Kourti, N. (2013). European reference network for critical infrastructure protection. International Journal of Critical Infrastructure Protection, 6(1):51–60
2. Bacher, R., Näf, U., Renggli, M., Bühlmann, W., and Glavitsch, H. (2003). Report on the blackout in italy on 28 september 2003. Technical report, Swiss Federal Office of Energy.
3. Stumpp, E.-M. “New in town? on resilience and resilient cities. Cities”, 32(0):164–166. 2013
4. Waller, M. A. (2001). Resilience in ecosystemic context: Evolution of the concept. American Journal of Orthopsychiatry, 71(3):290–297. Available from: http: //dx.doi.org/10.1037/0002-9432.71.3.290.
5. Johnson, J. L. and Wiechelt, S. A. (2004). Introduction to the special issue on resilience. Substance Use & Misuse, 39(5):657–670. Available from: http:// informahealthcare.com/doi/abs/10.1081/JA-120034010.
6. Batabyal, A. A. (1998). The concept of resilience: retrospect and prospect. Environment and Development Economics, null (2):221–262. Available from: http://journals.cambridge.org/article_S1355770X98230129.
7. Van der Leeuw, S. and Leygonie, C. (2000). A long-term perspective on resilience in socio-natural systems. In workshop on System shocks–system resilience, Abisko, Sweden
8. Department of Homeland Security. “National Infrastructure Protection Plan”, Washington, 2013, p. 9.
9. UNISDR (2005). Hyogo framework for 2005–2015: Building the resilience of nations and communities to disasters. Technical report, United Nations International Strategy for Disaster Risk Reduction – Extract from the final report of the World Conference on Disaster Reduction, Kobe, Hyogo, Japan.
10. National guidelines for protection of critical infrastructure from terrorism,” national security department, Australia.

11. http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf
12. USA Patriot Act (H.R. 3162), 107th Congress 1st Session H. R. 3162, In the Senate of The United States October 24, 2001. https://epic.org/privacy/terrorism/hr3162.pdf
13. Commission of the European Communities. Critical Infrastructure Protection in the Fight against Terrorism (Brussels, 20 October 2004), COM(2004)702 final, p. 3. http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf
14. Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM(2005) 576 final, p. 19 & 24
15. 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.
16. Brunner, E.M. and Suter, M. (2008) International CIIP Handbook 2008/2009. Center for Security Studies. ETH Zurich.
17. Hämmerli, B. and Renda, A. (2010) Protecting Critical Infrastructure in the EU. Centre for European Policy Studies, Brussels.
18. Boin, A. and McConnell, A. (2007) Preparing for Critical Infrastructure Breakdowns: The Limits of Emmergency Management and the Need for Resilience, Journal of Contingencies and Crisis Management, Vol. 15, No. 1, pp. 50-59.
19. 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.
20. 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.
21. Fink, S. (1986) Crisis management: Planning for the inevitable, AMACOM, New York.

22. 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.
23. Coombs, W.T. (2007) Ongoing Crisis Communication: Planning, Managing and Responding, 2 ed., SAGE publications, Thousand Oaks, CA.
24. 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.
25. Boin, A. (2004) Lessons from crisis research, International Studies Review, Vol. 6, No. 1, pp. 165-194.
26. 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.
27. 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.
28. 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.
29. 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.
30. PERROW, C., ed, 1984. Normal Accidents: Living with High Risk Technologies. New Jersey, USA: Princeton University Press.
31. United Nations International Strategy for Disaster Reduction (2009) Teminology in Disaster Risk Reduction. Geneva, Switzerland.
32. 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.

33. 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.
34. 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.
35. Pearson, C.M. and Clair, J.A. (1998) Reframing Crisis Management, The Academy of Management Review, Vol. 23, No. 1, pp. 59-76.
36. Coleman, L. (2004) The Frequency and Cost of Corporate Crises, Journal of Contingencies and Crisis Management, Vol. 12, No. 1, pp. 2-13.
37. Turner, B.A. (1976) The Organisational and Inter-Organisational Development of Disasters, Administrative Science Quarterly, Vol. 21, No. 3, pp. 378-397.
38. Coombs, W.T. (2007) Ongoing Crisis Communication: Planning, Managing and Responding, 2 ed., SAGE publications, Thousand Oaks, CA.
39. 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.
40. 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.
41. Pauchant, T.C. and Mitroff, I.I. (1992) Transforming the crisis-prone organization: Preventing individual, organizational, and environmental tragedies, Jossey-Bass, San Francisco.
42. Hwang, P. and Lichtenthal, J.D. (2000) Anatomy of Organizational Crises, Journal of Contingencies and Crisis Management, Vol. 8, No. 3, pp. 129-140.
43. 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.
44. 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.

45. Trucco P., Petrenj B., Kozine I.,& Andersen H. B.(2016) Emergency Management involving Critical Infrastructure Disruptions –operationalizing resilience capabilities deployment., ESREL2016 Glasgow (UK).
46. Baird Malcolm E., (2010) The “Phases” of Emergency Management., Intermodal Freight Transportation Institute (ITFI) University of Memphis (USA)
47. FEMA – Federal Emergency Management Agency. 2006. Principles of Emergency Management, Independent Study, IS230, Washington.
48. Drennan, L. and McConnell, A. (2007) Risk and Crisis Management in the Public Sector, Routledge, New York.
49. Alexander, D. (2002) Principles of Emergency Planning and Management, Oxford University Press, Oxford.
50. Comerio, M.: Disaster hits home: new policy for urban housing recovery. Berkeley: University of California Press. 1998.
51. PPD (2010). Presidential policy directive/ppd 8 critical infrastructure security and resilience
52. Wildavsky, A. (1988). Searching for safety, volume 10. Transaction publishers
53. Hoiling, C., Schindler, D., Walker, B. W., and Roughgarden, J. (1997). Biodiversity in the functioning of ecosystems: an ecological synthesis. Biodiversity loss: economic and ecological issues, page 44.
54. Mallak, L. (1998). Measuring resilience in health care provider organizations. Health Manpow Manage, 24(4-5):148–152. Available from http://europepmc.org/abstract/MED/10346317
55. Comfort, L. (1999). Shared Risk: Complex Systems in Seismic Response. Pergamom Press.
56. Paton, D., Smith, L., and Violanti, J. (2000). Disaster response: risk, vulnerability and resilience. Disaster prevention and Management, 9(3):173–180.
57. Kendra, J. M. and Wachtendorf, T. (2003). Elements of resilience after the world trade center disaster: Reconstituting new york city’s emergency operations centre. Disasters, 27(1):37–53.

58. Cardona, D. O. (2003). The notions of disaster risk: Conceptual framework for integrated management. Technical report, Inter-American Development Bank, Universidad Nacional de Colombia, Istituto de Estudios Ambientales, Manizales.
59. Pelling, M. (2003). The Vulnerability of Cities: Natural Disasters and Social Resilience. Earthscan LLC. Available from: https://books.google.it/books?id=cjjBdCzB-C0C&hl=en
60. , Francis R., Bekera, B., (2014), "A metric and framework for resilience analysis of engineered and infrastructure systems", Reliability Engineering and System Safety, vol. 121, 2014. Pp. 90–103
61. Vugrin ED, Warren DE, Ehlen MA. A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Process Safety Progress 2011;30(3):280–90.
62. Anex RP, Focht W. Public participation in life cycle assessment and risk assessment: a shared need. Risk Analysis 2002;22(5):861–77.
63. 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.
64. M. Tarrant. A 'conceptual models' approach to organisational resilience. The Australian Journal of Emergency Management. Vol. 25, No. 2, pp. 6-12
65. M. Bruneau, et al. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra, V. 19, No. 4, pp. 733-752, November 2003, Earthquake Engineering Research Institute
66. E.D. Vugrin, et al. A Framework for Assessing the Resilience of Infrastructure and Economic Systems. In K. Gopalakrishnan & S. Peeta (Eds.): Sustainable & Resilient Critical Infrastructure Systems, pp. 77-116. Springer-Verlag Berlin Heidelberg 2010.
67. L. Vincent. Differentiating Competence, Capability and Capacity. Newsletter Vol. 16, No. 3. Vincent & Associates, Ltd. 2008.
68. Teece, D.J., Pisano, G. and Shuen, A. (1997) 'Dynamic capabilities and strategic management', Strategic Management Journal, Vol. 18, No. 7, pp.509–533.

69. Teece, D.J. (2007) Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Start. Mgmt. J., 28: 1319-1350.
70. J. Walker and M. Cooper. (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. Security Dialogue. 42(2) 143-160
71. Factsheet. Expressions of Resilience: From 'Bounce Back' to Adaptation. Report of Risk and Resilience Research Group, Center for Security Studies, ETH Zurich, 2012
72. Adger, W.N., S. Agrawala, M.M.Q. Mirza, C. Conde, K. O'Brien, J. Pulhin, R. Pulwarty, B. Smit and K. Takahashi, 2007: Assessment of adaptation practices, options, constraints and capacity. Climate Change 2007: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change, M.L. Parry, O.F. Canziani, J.P. Palutikof, P.J. van der Linden and C.E. Hanson, Eds., Cambridge University Press, Cambridge, UK, 717-743.
73. Birkie S.E., Trucco P., Kaulio M. (2014) Disentangling core functions of operational resilience: a critical review of extant literature. Int. J. Supply Chain and Operations Resilience, Vol. 1, No. 1.
74. Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. Argonne National Laboratory Report, ANL/DIS-13-01, April 2013
75. Petrenj B., Lettieri E. and Trucco P. (2013) Information sharing and collaboration for critical infrastructure resilience – a comprehensive review on barriers and emerging capabilities. Int. J. Critical Infrastructures, Vol. 9, No. 4, pp. 304-329.
76. "Version 2.0 of Comprehensive Preparedness Guide 101: Developing and Maintaining Emergency Operations Plans" Federal Emergency Management Agency, USA (2010)
77. Mark E Keim "An innovative approach to capability-based emergency operations planning" Disaster Health 1:1, 54–62; January/February/March 2013

78. Leonard-Barton, D. (1992). “Core capabilities and core rigidities: A paradox in managing new product development”, Strategic Management Journal, Summer Special Issue, 13, pp. 111–125.
79. “National Protection Goal”, Department of Homeland Security (USA), 2016 https://www.fema.gov/mission-areas
80. “National Protection Framework”, Department of Homeland Security (USA), 2013