Resilience Capacities Assessment for Critical Infrastructures Disruption: READ pilot applications (Part 2)

Paolo Trucco, Boris Petrenj, Carmelo Di Mauro

Abstract:

The study aims at supporting the stakeholders involved in the Emergency Management (EM) activities to tackle the challenges related to scenarios involving interdependent Critical Infrastructure (CI) systems, by building resilience. Our approach to enhancing resilience is capabilities based, which supports the identification, assessment and development of specific capabilities required to prepare to, cope with and recover from CI disruptions within the EM set-up. The primary objective is to enable and foster collaborative EM in the context of Public-Private Collaborations (e.g. interdependent, multi-sectoral, and multi-stakeholder) for CI resilience.
The READ framework and related tool has been tested to support the stakeholders involved in EM and post-stress activities, including CI operators, to assess their own resilience capacities with respect to cross-border disruptions and thus identify the main areas where progress is needed. Two pilot cases were used to validate the READ framework and tool, and to demonstrate the applicability of the approach in the context of regional Public-Private Collaborations for Critical Infrastructure Protection and Resilience with different degree of development and level of maturity, namely Basque Country (Spain) and Lombardy Region (Italy).
The practitioners' feedback from both application cases confirmed the usefulness of such approach and helped to identify areas for future research and improvement.

Keywords: Critical Infrastructure, Resilience, Capability Assessment, Public-Private Partnerships

Biographical notes:

1. Introduction

Critical Infrastructure (CI) can be defined as those assets or systems that are critical for the maintenance of vital societal functions, providing services that society and citizens rely on in their daily life (EC, 2008) - i.e. power and water supply systems, healthcare, transport, electronic communications systems, banking. In the last decade, a shift of emphasis has appeared in both scientific literature and practitioners 'discussion on Emergency Management (EM) when CI are involved, from protecting the systems to maintaining their service continuity and improving resilience (e.g. Setola, Luiijf & Theocharidou, 2016; Petrenj & Trucco, 2014; EC, 2013; PPD-21, 2013; De Bruijne & Van Eeten, 2007). Resilience approaches are built on the assumption that not all the disruptive events involving CI systems can be predicted and prevented. In line with the main body of literature on the subject (Bates & Linkov, 2015; Author et al., 2015), in the context of the present study, CI resilience can be defined as "the ability of a CI system to:

- reduce the chances of a disruption of its performance and service to the public,
- absorb the consequences of any shock or disruption if it occurs,
- recover quickly after a shock or disruption by re-establishing normal performance and service, and when relevant, to
- adapt to unforeseen crisis scenarios and possibly significantly different circumstances of operation".

On top of these four resilience goals there is the overarching *preparedness* goal that is to be understood as "prepare to fulfil the four resilience goals". 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.

The five defined resilience goals are in line with Presidential Policy Directive 8 (PPD-8, 2011) that refers to five mission areas (prevention, protection, mitigation, response and recovery) and the overarching preparedness goal. The document PPD-8 (2011) does not explicitly refer to adaptation. However, the definition of the recovery mission area implies adaptation as a possible post-accident phase.

Beyond definitions, a number of conceptual frameworks have emerged that aim at demonstrating different, interrelated aspects of CI systems' resilience. However, they do not provide any operational guidance for its assessment. A few of the existing frameworks can be viewed as operational and applicable to CI, to assess and improve their resilience. Notable are the MCEER framework for quantitative assessment and enhancement of the seismic resilience of communities (Bruneau, et al. 2003) and the Sandia resilience assessment framework applied to infrastructure and economic systems (Vurgin, et al. 2010). While providing constructive guidelines for resilience assessment, they are loosely coupled to the EM set-ups and activities practiced by EM agencies and emergency responders (e.g. Fox-Lent, Bates & Linkov, 2015; Linkov et al., 2013). Nevertheless, understanding and managing this relationship is of paramount importance when it comes to emergencies involving CI disruptions, both as the trigger or as one of the cascading effects.

To cover the current gaps in knowledge and practice, the present study aims at testing and validating the READ Framework (Author et al., 2015) for the planning and assessment of resilience capacities to cope with disruptions affecting complex CI systems. It was developed in the context of READ (Resilience Capacities Assessment for Critical Infrastructures Disruptions), an EU co-funded research project under the CIPS Action. The framework primarily integrates the resilience capabilities of CI into the Resilience Management (RM) cycle – i.e. *preparedness, prevention, mitigation, response, and recovery* – which allows emergency services to explicitly address resilience improvement measures while planning to cope with CI disruptions. It also goes beyond the EM phases by analysing the resilience capabilities of the long-term adaptation. An overall resilience capability building cycle completes the framework, enabling a systematic implementation of relevant capabilities and making gap analysis with regard to resilience deficits.

The rest of the paper is organised as follows. The next section gives an overview of the READ framework. Section 3 describes the study methodology used for the pilot testing and guides the reader step-by-step through the entire resilience assessment process and subsequent analysis. The results are discussed in Section 4. A final section summarizes the achievements and suggests possible future steps.

2. Overview of the READ Framework

A description of the READ framework, as well as the definition of its constituents, have already been published in Author et al. (2015). In this section, we first summarise the main concepts necessary for a full understanding of the resilience assessment method and tool and then use it to propose a comprehensive resilience capability building cycle.

The READ framework adopts a capabilities-based approach that several countries have employed to plan and prepare for emergency work - see, for example, PPD-8 (2011) and Lindbom et al. (2015a). The strategy of capabilities-based planning is to prepare for a large variety of threats and risks instead of simply preparing for specific scenarios.

2.1 Resilience Capabilities

A *Resilience Capability* of an entity (organization, person, system) is a feature, faculty or process that promotes the achievement of its resilience objectives. The definition of a resilience capability is further deepened and operationalized through the following three related compounds:

- ***asset***, is an item of ownership that has exchange value; includes intangibles such as knowledge systems;
- ***resource***, is a tool, consumable, or human being possessing competences required to make use of assets and achieving given objectives;
- ***routine***, is defined as the way things are done, i.e. the way assets and resources are combined and exploited to achieve a specific resilience objective, possibly codified as an explicit procedure, within a community or social group, a pattern of activities.

The list of 24 basic capabilities included in the READ Framework and their definitions is given in Annex 1.

2.2 Resilience Capacities

Following Vurgin et al. (2010) and Author et al. (2015), the resilience *capacities* can be classified into the following four groups:

- *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 of adjusting to novel conditions of operation
- *Restorative capacity* is the degree of ease with which the system repairs after a shock or a disruption.

A single resilience capability may contribute to more than one capacity; on the other side, a certain level of capacity can be achieved through the contribution and combination of multiple capabilities

The above mentioned four resilience capacities comply well with the typical phases of the RM cycle (*prevention, protection, mitigation, response and recovery*)[1], such as those stated in the Presidential Policy Directive 8 (PPD-8, 2011) that aims at strengthening the security and resilience of the United States. Consistently, the READ Framework implements a RM cycle as defined in the US National Infrastructure Protection Plan (DHS, 2009).

2.4 Classification of capabilities

As EM involves a number of responders that should act in concerted actions under emergencies, two other levels of resilience capabilities should be distinguished: intra-institutional and inter-institutional resilience capabilities (Author et al., 2015). Inter-institutional capabilities should be identified according to what is shared between the organizations involved in concerted actions.

Following the MCEER framework (Bruneau, et al. 2003) we also distinguish among the *Types of CI resilience dimensions (subsystems/components):* (1) **T**echnical, (2) **O**rganisational, (3) **S**ocial, and (4) **E**conomic, (TOSE). This brings us to the final classification of the capabilities according to the four different perspectives (Figure 2). Social and Economical resilience dimensions are however out of scope of the present study.

[1] These phases are referred to as mission areas by FEMA

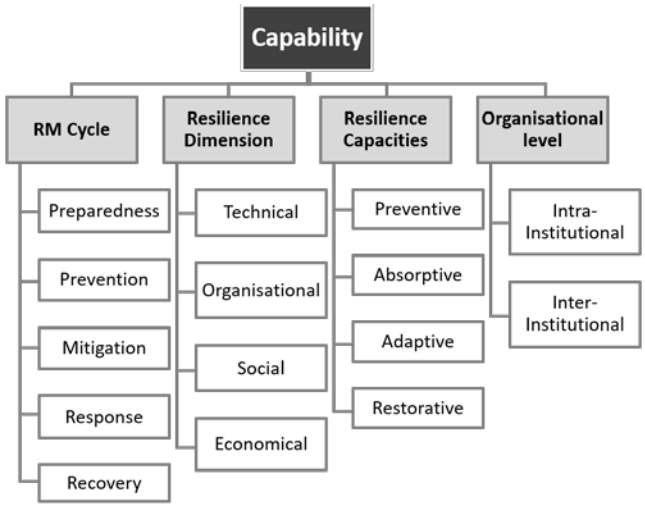

Figure 1: Classification of resilience capabilities

The concepts defined in the previous section allowed us to shape an approach to building and maintaining the resilience of interconnected CI systems (Figure 3). Each of the four (high-level) resilience capacities – preventive, absorptive, adaptive and restorative – is ensured by the availability of particular capabilities. Looking from below, each capability is built from three related compounds: assets, resources, and routines. Further, each single capability contributes to one or more resilience capacities and is used in one or more phases of the RM cycle. A capability can contribute to the resilience of individual organisations as independent ('intra-institutional'), and/or enable different levels of collective approaches ('inter-institutional') through sharing information, activities and resources, power or even authority.

3. Study methodology

In order to validate the READ framework and test the practical feasibility of its approach to building high level resilience capabilities against large disruptions and emergencies involving CI, the study implemented two pilot applications in the context of regional Public-Private Collaborations for Critical Infrastructure Protection and Resilience with different degree of development and level of maturity. The first one consisted of a table-top exercise involving selected stakeholders (emergency managers, civil protection authorities, first responders and CI operators) in the Basque Country (Spain), whereas the second on is connected with the ongoing Lombardy Region (Italy) Public-Private Collaboration and Programme for CI Resilience (Trucco & Petrenj, 2017).

The main stakeholders are CI operators, the emergency management and civil protection authorities, first responders, and the main public authorities in charge of Critical Infrastructure & Resilience (CIP-R) programmes. According to the objectives and features of the READ framework and the corresponding implementation tool, the main benefits and support that target groups are expected to receive are as follows:

- Better characterizing emergency situations involving interdependent CI systems (including transboundary dependencies and cascading effects);
- Systematically identifying, characterizing and assessing the resilience capacities required to prepare, cope and recover from these type of disruptions;
- Guiding capacity building, i.e. improving intra- and inter-institutional practices and capabilities.

3.1 Pilot Case I: Table-top Exercise on large disruptions in the Basque Region

Typically, table-top and other type of exercises should be seen as an integral part of preparedness for major emergencis. The aim of planning and staging exercises is to validate plans, systems, procedures and training, to enable practice of lessons identified and capabilities developed and to test and enhance the overall capability of an organisation to respond. Exercises raise awareness, educate individuals about their roles and the roles of others, and promote co-ordination and cooperation.
In the context of a disaster that involves CI disruptions and cross-border cascades, this aim has to be reconsidered. Scenarios that imply strong cross-border impacts and involve many different countries are not typically considered by the national authorities responsible for civil protection and emergency management. Moreover, private CI operators are not used to be involved in such exercise activities. Considering these aspects, the READ table-top exercise aimed to foster the collaboration among stakeholders to improve their resilience capacities under critical cross-border scenarios. Thanks to its simplicity, the exercise approach can be considered as a valuable approach to face such challenge.

3.1.1 Aim and scope of the READ Table-top exercise

The table-top exercise was organised as a one-day session and held at Tecnalia Headquarters in Bilbao (Spain). The exercise's goal was to test the added value of the framework and the usability for responders and other stakeholders involved in transboundary disasters. This project activity was built upon an interactive framework in which emergency responders and selected international CI operators interplayed with the READ framework and tool. We can distinguish some possible applications of the READ framework and tool in such case:

- **Common knowledge base**: the tool can be used as common base of knowledge in order to share information about the capabilities of each partner involved in the CI disruption response. In particular, it can be useful to assess a specific capability of an operator that needs to be involved in a specific activity.
- **Check list and assessment tool:** the tool can help responders and operators to assess which are the capabilities that require some reinforcement and what are the gaps. In these terms the READ framework can be considered as a check list that drives the investigation and the coordination of the involved actors, with the advantage that it can provide also synoptic representation of the needs and the available capabilities which can help in defining more concrete management strategies and the priorities to fulfil the most relevant capability deficiencies.
- **Lesson learned tool:** all the knowledge collected and stored into the READ framework during the different phases can be used as a valuable information source to stimulate the lesson learning process.

As far as it was possible all the illustrated aspects were considered to drive the design of the table-top exercise.

3.1.2 Table-top exercise design and training package

In order to facilitate the design and the implementation of a table-top exercise dealing with cross-border disruptions, a training package has been developed. In particular, the package illustrates the importance of the training activities in order to improve the resilience of a community, it summarises the main characteristics of any communication process and the main issues that have to be considered in order to design and to rule a table-top exercise. The organisation of the exercise also constituted the opportunity to review and validate the contents of the package. The design process was structured according to the following steps:

1. **Identification of a large scenario** that can generate transboundary impacts: The scenario was elaborated on the basis of a number of real blackout events occurred in the past in Europe. It was assumed that Bilbao, the capital of the province of Biscay in the Basque Country, was the main urban context where a severe storm started to strike the population and the local critical infrastructures. The town lies along a 16km-long estuary, between two mountain ranges to the

north-east and south. As the sea is not far away, tides reach the city and a large part of the urban area is prone to flooding (RESIN, 2015; Basque Government, 2015). Bilbao may therefore be significantly affected by extreme weather events, as it has been occurred several time in the past (e.g. August 1983). The scenario considered that due to extreme weather conditions, a number of electrical substations nearby Bilbao (e.g. substations of Güeñes, Itxaso, ect.) are severely damaged. The impact creates a number of repercussions on population, regional public services, and it generate impacts on the productive system (Figure 4). Impacts also propagate through the border affecting France and, later, other European countries like Italy and Germany.

2. **Review of real past events** in order to consider the characteristics and the attribute of the scenario in relation with the capabilities considered by the READ framework. In particular, the past events where selected considering the accidents that involved critical infrastructures, that impacted an extended portion of territories and that have transboundary propagation of effects (e.g. Italian blackout in September 2003 which affected 56 million people in Italy Switzerland and France for 12 hours; German Blackout in November 2006- western Germany, France, Belgium, Italy, Spain, Austria, the Netherlands and Croatia were without electricity due to a procedural error of the German energy operator.).
3. **Design of the table-top exercise** in role playing. The scenario was described along a sequence of ten time steps. Each time step description reported an update about the evolution of the disaster and the impacts and criticalities that need to be evaluated. Each step was defined in order to stimulate a discussion about a specific capability (or a limited number of them). The Annex 2 lists the sequence of events within this scenario and the related questions that where provided to the participants.

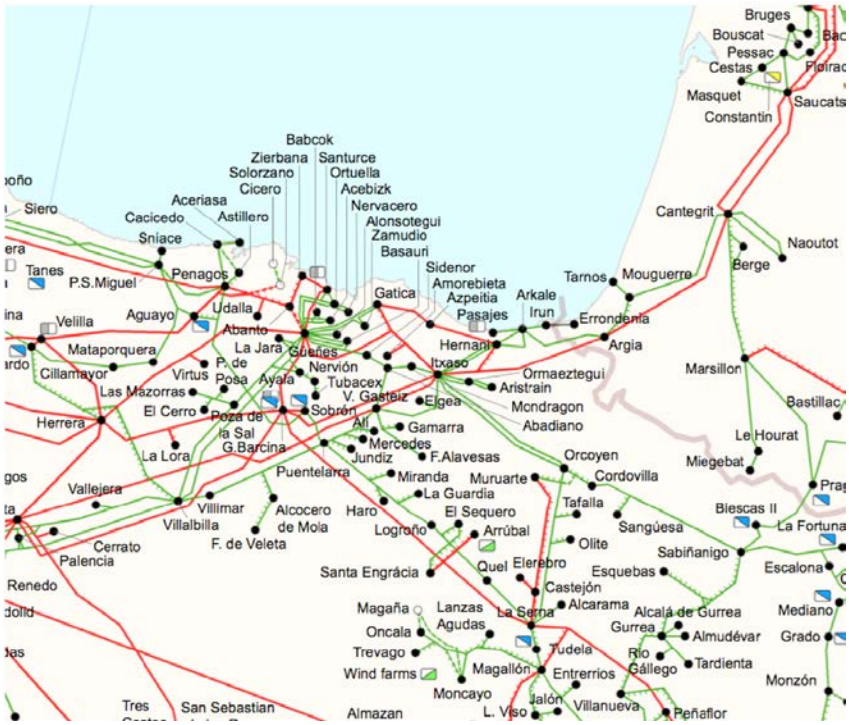

Figure 2: Detail of the electricity grid impacted by heavy storm considered by the scenario

4. **Selection of the experts:** around twenty responders and operators were invited to attend the exercise. An introductory session provided the attendees with general background information

and an overview of the READ framework. A list of relevant past blackout events was distributed in advance; this aimed to stimulate, during the days prior to the exercise, the perception of the participants about the implication of some extreme real events occurred in the past and to increase their awareness about the consequences and the possible complexity of a scenario development.

5. **The participants were trained** in advance about the READ framework and how to use the READ tool.
6. **The validation criteria** for the usability and utility of the READ framework-tool included authors' direct observations during the exercise, and experts' judgement elicitation in the debriefing phase post exercise. In particular, three general questions were addressed to each participant:
   - What do you think could be the added value of the READ tool for your activities and responsibilities?
   - What is the added value of the READ framework to evaluate and plan resilience against major CI disruptions at regional scale?
   - Who should be involved in the process and how the READ tool could be used for the purpose?

3.2 Pilot Case II: Regional Public-Private Collaboration on CIP-R in Lombardy

Lombardy (Lombardia in Italian) is one of the 20 Italian regions, located in the north. A sixth of Italy's population lives in Lombardy (around 10 million citizens) and it accounts for around 20% of Italy's GDP, making it the most populous and richest region in the country and the fourth richest in Europe.
Following the release of the EC Directive 2008/114/EC (EC, 2008), the Lombardy Region Administration expanded the scope of its Integrated Regional Program for the mitigation of major risks (PRIM, Lombardy Region, 2007) and set up a new regional policy on CIP-R, with the aim of promoting and advancing inter-institutional (cross-organisational) collaborations. In light of this logic, from 2010 Lombardy Region has launched a programme of activities aimed at defining a model of integrated and shared management, capable of supporting a higher level of collaboration within the processes of prevention, risk monitoring and emergency management related to the regional CI. The programme, based on a specific Memorandum of Understanding, involves today 16 operators of the energy and transport sectors.

The preliminary study, carried out by a team of academics and consultants in 2011, provided a complete picture of the actual status of the vulnerability of regional CI nodes and the corresponding emergency management processes adopted by the most important CI operators. Thanks to the implementation of a functional simulation model (Trucco et al. 2012) of the regional infrastructural system a systematic vital node analysis was carried out that returned a ranking list of the most critical nodes, or clusters of nodes.

3.2.1 Thematic Task Forces (TTF)

TTF represent the backbone of the programme implementation; they are established and coordinated by a higher level PPP Governance Committee that is formed by the managing directors from all of the organizations that signed the MoU. So far, five TTFs have been established starting from January 2011. One focused on mapping of the information flows and communication channels among actors. Another one focused on developing collaborative procedures for coping with major meteorological events (e.g. heavy snowfall). The third one was in charge to set up collaborative activities in case of large blackout events. The fourth analyzed the regional CI nodes with respect to natural hazards. The objective of the fifth TTF was the definition of a new system for information exchange under emergency, and the identification of the rules for engagement.

As for the TTF 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;

3.2.2 Data sources

All the above mentioned activities and processes are documented by a wide set of documents, databases and SW applications. The data used in the present study was collected from the following sources:

- bilateral agreements (Memorandums of Understanding) between Lombardy Region and CI Operators;
    - reports on the activities and outcomes of TTFs, such as: a catalogue of regional CI nodes; vulnerability and resilience analysis of the regional CI; description of relevant scenarios and analysis of historical cases; mapping of the information flows and communication channels among actors; information exchange system (SUSI) documentation.
- interviews with CI Operators and Directorates of the Lombardy Region involved in the programme.

3.2.3 Pilot implementation of READ

The adoption of the READ framework was tested in the context of a Thematic Task Force on blackout events, over 5 months (Table 1), that involved 15 CI operators (Table 2). Out of them, 8 operators completed the capability assessment so far: 3 transport operators (rail, metro) and 5 energy operators (3 electricity and 2 gas).

Table 1: Pilot-case implementation milestones

Date	**Activity**
September 2016	TTF on blackout kick-off. READ framework and the capability classification scheme introduced.
November 2016	Review of capability descriptions and classification. Capability Assessment scheme adoption. Initial capability assessment (current level).
December 2016	Resilience strategies on regional level – definition and selection. Objective capability assessment (target level).
January 2017	Presentation of the outcomes (analysis). Discussion and validation of the results and READ methodology.

Table 2: CI operators involved in the Lombardy Region pilot case

Operator ID	**Type**	**Participation in meetings**	**Capability Assessment**
1	Public Transport (road and underground)	X	X
2	Electricity distribution	X	X
3	Regional rail transport	X	X
4	National Gas Distribution Network	X	X
5	Italian TSO	X	X
6	Electricity distribution	X	X
7	Local gas distribution	X	X
8	Regional light rail transport	X	X
9	National Rail transport Network	X	

Operator ID	Type	Participation in meetings	Capability Assessment
10	Roads – Highways	X	
11	Roads – Highways	X	
12	Roads – Highways and Motorways	X	
13	Roads – Beltways	X	
14	International Airport operator	X	
15	International Airport operator	X	

4. Findings

4.1 Application of the READ framework within an ad-hoc stakeholder group

The table-top exercise in the Basque Country was used to validate the READ framework-tool involving selected stakeholders without a structured collaboration history, i.e. stakeholder representatives where majority have never worked together before. The participants dealt with the scenario development as described in Annex 2 and provided their valuable feedback on the used approach.
A full working day was dedicated to the table top exercise which took place in October 2016 and involved around 20 participants, including the representatives of the regional and national Critical Infrastructures (Energy, Transport, Water), regional government (Security and Emergency units), police and universities, and the Ministry of Interior (National Center for Critical Infrastructure Protection).
The activities where mainly divided in two different sessions:

- During the morning session, the READ framework was illustrated to the attendees and they were trained to use the READ tool. This activity allowed making a critical review of the capabilities required to face large disasters that disrupt the main CI services. In particular, the experts were asked to list the capabilities required to insure an adequate level of resilience capacity against a large electricity black-out event, on the basis of their own experience and knowledge. This helped to clarify the role of each actor during an emergency and the related capabilities. This session also allowed to make the attendees acquainted with a common set of definition and assumptions that were useful to facilitate the communication.
- The afternoon session was dedicated to the implementation of the table-top exercise; it was conducted describing each time step of the scenario and allowing the participants to review and discuss the actions they would take in that particular emergency situation of the scenario. This allowed to test their emergency plans in an informal way and environment, to clarify roles and responsibilities, and to identify mitigation gaps and preparedness needs to improve their operational capabilities. The READ tool was useful to collect in a consistent way information about the level of capabilities and to analysis them.

Following these activities, the experts were asked to provide some final judgements and feedbacks. Apart from the information gathered by READ tool, the participants where stimulated to report their opinion about the pros and cons of the READ tool using the questions listed in the exercise design description.
CI operators highlighted the value of READ framework, in particular its capacity to encompass the complexity related to the representation of all the attributes that describe the resilience concept. They appreciated the systematic characterisation of the elements that compose the framework and the description of all the logical relationships among them. The experts considered that the framework can constitute a reference approach to map in a common way the different dimensions of the resilience of each actor involved in disaster management. It could facilitate the common understanding of resilience attributes that are still not addressed in an appropriate way or unrecognised or misinterpreted. This interpretation alignment will improve the communication among the actors involved in emergency activities and it will enable the identification of the obstacles to collaboration.

Besides the improvements that can be reached at the organisational and operational level, a collaborative approach will allow to increase the mutual trust and the awareness about common critical issues related to the development of resilience. Regarding this aspect, police officers noted that police forces are not used to work according to an informal approach to share information. Therefore, they consider the framework valuable but its implementation can face some formal obstacles.

All the participants agreed that definition of a strategy to exploit the value the READ framework can be only set by a public authority. This issue become even more relevant when the development of resilience strategy requires the involvement of multinational actors, since cross-border collaboration is associated to number of authorities, laws, protocols, bilateral agreements and other procedures that regulate the collaboration between different countries. It was recognised that before starting any evaluation of obstacles, the READ framework can be used to identify critical disaster scenarios and misalignment and asymmetries between countries, which are called to collaborate to increase their own resilience. In order to overcome some of such constraints, some operators are established as a common company legally registered and recognised in two countries (e.g. Franco-Spanish rail operator). Such operators respect and accomplish all law requirements of the two countries, including in the field of safety and security.

Several operators pointed out at the moment there are so many different plans, i.e. plans based on specific events, that it is difficult to assess how there are coherent each other. Some also argued that the READ framework is rather complex if compared with the resilience dimensions and aspects encompassed by their internal business continuity plans.

Existing experiences of CI collaboration schemes show that important factors are the voluntary dimension of the collaboration, the creation of win-win situations in which all stakeholders see an advantage in collaborating, the need to take time to build a real trust environment with the view to discuss and exchange sensitive information. The exercise demonstrated, once again, the need for resilience-based strategies to address CI disruptions at all scales, the necessity of collaborating with all stakeholders – in particular private operators of infrastructures, and for setting up action plans not limited to CI disruptions but considering the multiple aspects of local and regional resilience against all hazards.

In summary, participants emphasised the fact that the READ framework-tool has the advantage of providing a quite exhaustive representation of the resilience concept applied in the field of CI disaster management. The tool can then facilitate and stimulate a common reference framework at European level that would provide the basis for collaborative (inter-institutional) resilience building. The READ framework can provide a general and common methodological approach that can help the analysis of the available emergency plans in order to remove discrepancies and facilitate the harmonisation of those plans.

4.2 Application of the READ Framework within an established regional CIP-R programme

The second pilot case, involving the public and private actors engaged in the Regional Programme on CIP-R in Lombardy (Italy), demonstrates the applicability of the approach and the use of the tool within a running collaboration programme. It presents the full process of (Figure 3): 1) CI system specification; 2) CI system and environment characterisation; 3) Resilience Capabilities Assessment and Gap Analysis, followed by the joint selection of strategic objectives and analysis of the alignment of operators' improvement actions and plans (as Phase 4).

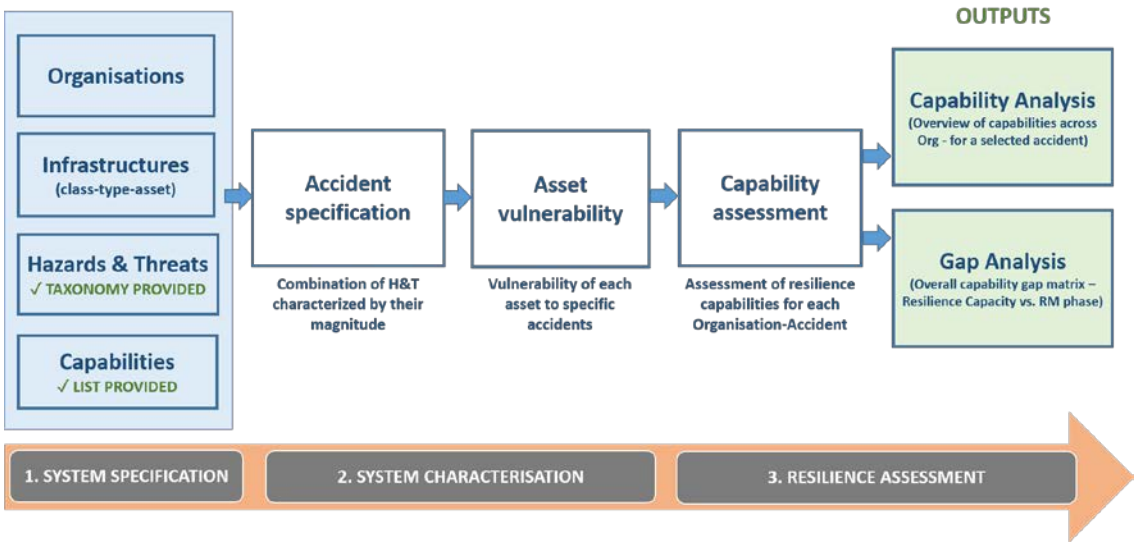

Figure 3: Resilience assessment and gap analysis process

4.2.1 System and environment specification and characterisation (Phases 1 & 2)

In the initial phase, the characteristics of the system under analysis, the organisational and environmental contexts was specified. The description of the physical infrastructure system was based on the nodes defined and included within the Regional CIP-R programme, for which the vulnerability analysis to a blackout event was already available.
Then the types and characteristics of accident events were specified. The reference blackout scenarios were:

- Local urban event triggered by a failure in the transmission grid without loss of components, and characterised by an assessment time of about 1 hour, and an estimated recovery time of the Transmission System of 6 hours;
- Nation-wide blackout, with cross-border effects, triggered by an operating error (e.g. human) of the TSO (Italian or Swiss). It is characterised by an assessment time of about 1 hour, and an estimated recovery time of the Transmission System of 12 hours.

It was described inside the tool in simple terms (Figure 4), while the TTF participants elaborated on it in more detail.

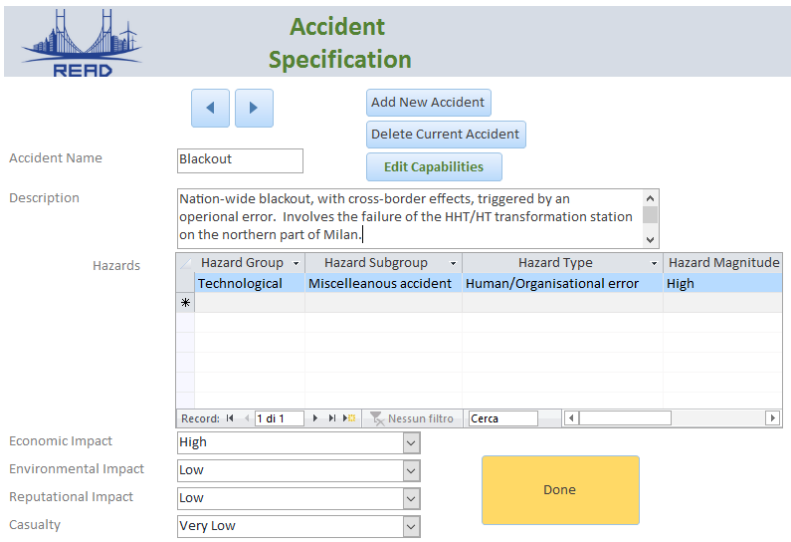

Figure 4: Screenshot of the accident specification

Finally, the Asset Vulnerability Analysis was based on the outputs of the Regional CIP-R programme. Detailed analysis included a timeline with which regional energy and transport infrastructure nodes suffer a deterioration of the service due to the lack of electricity supply. The reports also show the dynamic characteristics of the failure of each node in detail.

4.2.2 Assessment of Resilience Capabilities (Phase 3)

During the second meeting, a review of capability description, classification and an initial capability assessment (current level) were performed.

The comprehensiveness of the predefined capabilities was discussed, as well as the appropriateness of the *Capability Assessment Scale* (Figure 5). The proposed assessment scale considers a combination of capability's coverage of different hazards and trheats on one side, and the complexity of the accident in can cope with on the other. The capability assessment is done considering the vulnerability of assets to the accident in question (as specified in Phase 1). The assessment scale was agreed upon and accepted in the form proposed in the READ framework.

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

Figure 5: Standard Assessment Matrix and Scale

To input the data, the participants had a possibility to use either the READ tool or the template (created in *MS Excel*), translated into Italian. They were also allowed to take the template back home and fill it out within their organisations, and with consultations with the relevant personnel. A few examples of the received assessment are given in Table 3, it is translated from Italian and references to organisations are removed.

4.2.3 Analysis and identification of strategies and actions for improvement (Phase 4)

The first analysis tried to understand where the current operators' efforts are directed to. This was done by looking at their own perceived gap, i.e. where they plan for an improvement in capability levels (Figure 6). Looking at the whole picture, we can see that they mostly target the preventive capacity, prioritising capabilities applicable in preparedness and prevention phases. Looking at the rows and columns in total we can see the spread of their focus by RM cycle (Figure 7 - left) and Resilience Goals (Figure 7 - right).

	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%

Figure 6: Intra-Institutional Gap Analysis (Summary of Operators' improvement plans – effort)

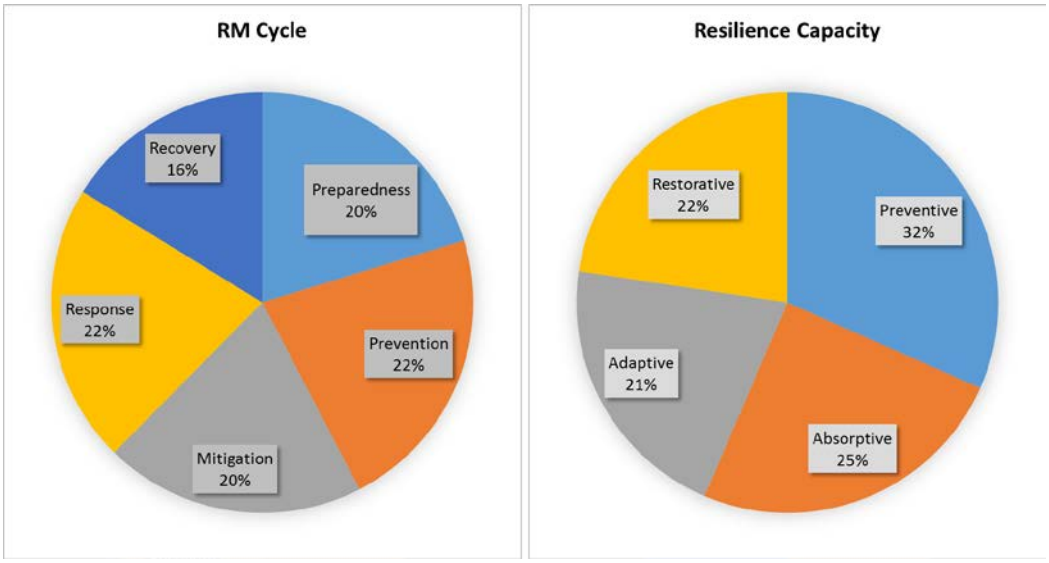

Figure 7: Intra-Institutional Gap Analysis (Summary of Operators' improvement plans – effort) across RM cycle (left) and Resilience Capacities (right)

Table 3: Examples of capability specification (translated from Italian)

Capability	Elements	Context
Operational Coordination	***Assets:*** Emergency Management procedures and involved subjects are stated inside the Operational Intructions document (named IO95) Operating Centers have central role in monitoring and management of our network, which are 24h able to intervene remotely in the execution of the first maneuvers on our medium voltage network and coordinate our operations staff in the field during the fault location operations. In Emergency, at our Operative Centers are activated *Workstations for Operational Assistance* that support Operative Centers in their activity, taking care of information flows as an interface to the *Emergency Workstations* that are activated at the operating units. ***Resources:*** Carrying the distribution activities we have available (on-call) personnel in various units. In warning situations, the number of simultaneously available personnel is appropriately increased. Contracting companies are alerted. In emergency conditions the entire organisation is activated, from the Operational Centers to *Workstations for Operational Assistance*, to *Emergency Workstations*, according to IO95 Where necessary, in the emergency area are sent forces (personnel) from other territories/regions. ***Routines:*** The reference document is IO95	Electricity (Distribution) Operator
Risk Assessment	***Assets:*** Integrated Management System. List of experts in Risk Management ***Resources:*** Management competent in Network Security and Access, with the support of the Directions for Maintenance & Operation and Infrastructure Development ***Routines:*** Standard procedures for Safety, Security and Environmental Risk Management according to EU and national regulations Procedures for Risk Management.	Rail Operator
Public Information and Warning	***Assets:*** IT applications (website, Twitter channel, ...) run until the generators supply power (theoretically infinitely). Sound systems and TV in stations are active for the time necessary to implement possible evacuations (about 1 hour) ***Resources:*** In case of an emergency, in short time the available human resources belonging to the marketing and communications services are organised in shifts. ***Routines:*** In case of an emergency or an accident, information necessary for possible evacuation of the lines are provided immediately. Other information related to the service recovery are communicated in agreement with top management	Public transport operator
Logistics and Transportation under EM	***Assets:*** In case of transport service interruption in the national gas network, there is an emergency service for supplying gas into pipes from cylinder trucks (gas vehicles). ***Resources***: Operation Centers have staff on duty and additional available staff. The dispatching center is manned in shifts. ***Routines***: There are formalised processes for: - Coordinated network management; - Control room activity (Dispatching); - Management of the emergency services on the network; - Business continuity management of Dispatching.	Gas operator

When considering the blackout resilience strategies for the entire region, on a higher (strategic) level, two main approaches are possible.

Strategy 1 – Robust the Electricity Infrastructure («all-hazards») with an addition of selective resilience capabilities in other CI thanks to a managed propagation of disruptions and disservices.
This strategy would require a combination of capabilities as in Figure 8 (top part). When compared to the actual map of the capability (Figure 8, bottom part) we can notice that the gap is on average lower in the important (marked) areas.

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

Figure 8: Strategy 1 - Capability Mapping

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.
This strategy would require a combination of capabilities as in Figure 9 (top part), which is slightly mismatched as the gap appears to be on average higher in the areas with the higher importance.

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

Figure 9: Strategy 2 - Capability Mapping

Since it is difficult to manage blackout cascades selectively, the strategic approach decided by the Regional Government, in agreement with the CI operators, focuses on adaptive capabilities of all the CI operators to assure rapid service recovery even in emergencies with complex cascading and cross-border effects (Strategy 2). Improved collective response (on system level) and an efficient recovery is supported

by promoting and advancing inter-institutional collaboration. It involves all stakeholders in a more distributed and fair way and leverages on actual strengths of CI operators and their improvement plans.
Comparing the degree of the alignment between the operators' current improvement plans and the actual capability map (Figure 10) a dose of discrepancy can be noticed. It becomes more visible when looking at the overall share summed by Resilience Capacities and RM phases (Figure 11). The *preventive capacity* receives a higher attention in the operator improvement plans, than the actual strategic weakness, while *restorative capacity* would require an increased effort to match the actual strategic weakness. It suggests that the improvement plans should slightly shift in favour of better restorative capacity. Looking deeper into some of the hotspots needed to support Strategy 2, we can better see what lays behind the current improvement plans.

		Preparedness	Prevention	Mitigation	Response	Recovery
Operators' improvement plans	**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 Assessment	**Preventive**	71%	68%	77%	78%	81%
	Absorptive	83%	80%	77%	77%	81%
	Adaptive	83%	81%	79%	75%	81%
	Restorative	81%	81%	77%	76%	76%

Figure 10: Degree of Alignment for Strategy 2

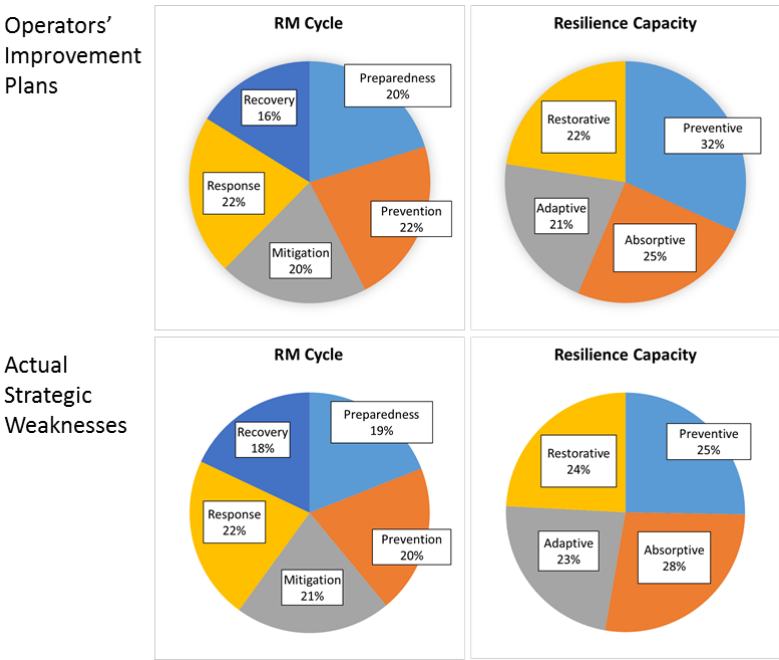

Figure 11: Gap Analysis on the degree of alignment actual strategic weaknesses and operators improvement plans

Operators' improvement plan involving *Response RM phase* and *Absorptive Capacity* combination (Figure 12) shows that different organisations might just work on the same capabilities, potentially neglecting some of the key strategic points. In this case, the improvement plans are mainly focused on *Planning*, *Cybersecurity* and *Interdiction/Disruption* capabilities.

Capability	Op1	Op2	Op3	Op4	Op5	Op6	Op7	Op8	TOTAL
Access Control and Identity Verification									0
Community Resilience Building			1						1
Cybersecurity		1				2			3
Environmental Response / Health and Safety									0
Fatality Management Services									0
Fire Fighting		2							2
Intelligence and Information Sharing									0
Interdiction and Disruption		1	1		1				3
Logistics and Transportation under EM			1						1
Mass Care									0
Mass Search and Rescue Operations									0
Natural and Cultural Resources Protection									0
On-scene Security, Protection and Law Enforcement									0
Operational Communications			1						1
Operational Coordination				1					1
Physical Protective Measures						2			2
Planning	1	1		1	1				4
Public Health, Healthcare and Emergency Med Serv									0
Public Information and Warning		1							1
Risk (& Resilience) Assessment		2							2
Screening, Search and Detection			1						1
Situational Awareness and Decision Making									0
Supply Chain Integrity and Security									0
Threats and Hazards Identification		1							1
Total	1	9	5	2	2	4	0	0	23

Figure 12: Capabilities addressed in Operators' Improvement Plans (Response-Absorb)

A similar situation is visible in the *RM Recovery Phase* and Resilience goal to *Restore* where the same inter-institutional capabilities are mostly marginalised (Figure 13).

Capability	Op1	Op2	Op3	Op4	Op5	Op6	Op7	Op8	TOTAL
Access Control and Identity Verification									0
Community Resilience Building									0
Cybersecurity		1				2			3
Environmental Response / Health and Safety									0
Fatality Management Services									0
Fire Fighting		2							2
Intelligence and Information Sharing									0
Interdiction and Disruption		1			1				2
Logistics and Transportation under EM			1						1
Mass Care									0
Mass Search and Rescue Operations			1						1
Natural and Cultural Resources Protection									0
On-scene Security, Protection and Law Enforcement									0
Operational Communications									0
Operational Coordination			1	1					2
Physical Protective Measures							1		1
Planning		1	1	1	1				4
Public Health, Healthcare and Emergency Med Serv									0
Public Information and Warning		1							1
Risk (& Resilience) Assessment		2							2
Screening, Search and Detection			1						1
Situational Awareness and Decision Making									0
Supply Chain Integrity and Security						1			1
Threats and Hazards Identification						1			1
Total		8	5	2	2	4	1	0	22

Figure 13: Capabilities addressed in Operators' Improvement Plans (Recovery-Restore)

4.2.4 Feedbacks

The final discussion of the presented analysis and the TTF outcomes took place in January 2017, involving the main regional Emergency Management stakeholders (CI operators, Government officials, Emergency managers, Responders, etc.). A lack of inter-institutional dialogue was acknowledged, and a need for more integrated 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 definitely 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.

Operators also recognised that a standardised way of representing intra-institutional resilience capabilities enables a better mutual understanding of the strategies and resources that each single organisation is able to mobilise 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, and also the 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 and distinguish all the capabilities, check their comprehensiveness, and the level of implementation. Given the amount of effort needed by the implementation of the pilot study, the large majority of operators proposed to continue to use the tool in the context of the PPP for CIP-R, starting from the new Task Force on CIP-R 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.

5. Conclusion

The prototype of the READ tool and the READ framework on which the tool is based, were successfully tested and validated. The initial pilot implementation took place in the Basque Country through a table-top exercise focusing on an extreme weather event. It involved the representatives of the CI operators (regional and national), Government and Responders. The second pilot implementation took place in the context of an ongoing public-private collaboration for CIP-R. The main evaluation criteria were experts' and practitioners' feedback on applicability and usefulness of the framework and the tool in the real world set-up (pilot applications).

The participants' feedback from both application cases confirmed the need for such framework and the usefulness of the READ tool for the end-users, expecting their important impact and wide reach. However, a not negligible amount of time and effort are needed to understand the entire framework and the concepts inside, before moving onto the resilience assessment. The practitioners agree that different examples could help them grasp the concepts more quickly. CI operators also see the value in identifying gaps and aligning resilience capabilities between their own different territorial (or also cross-border) units.

Thanks to a unified model and capability classification, different actors were able to represent their resilience and coping capacities in a way that is more understandable by the partners and usable for joint emergency planning. It also demonstrated the power of the proposed approach in fostering multi-agency and multi-stakeholder collaboration, and information sharing. The framework helps the stakeholders to jointly focus their effort and limited resources on those capabilities that would address the gaps under a common resilience strategy. Indeed, the study demonstrated the need of developing strategies based on resilience to address CI disruptions at all scales, the necessity of working in collaboration with all stakeholders for setting up action plans considering local and regional resilience against all hazards.

The feedback helps the further improvement of the READ framework-tool, especially when trying to accommodate different users' needs (Responders, CI operators, Government) and aiming to have an easily understandable assessment process and a user-friendly tool. The next step will be the development of an exercise training package.

Acknowledgements

The material described in this paper is developed as part of EU project 'Resilience Capacities Assessment for Critical Infrastructures Disruptions' (READ) (http://www.read-project.eu/) that was funded with support from the European Commission (Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme) – Directorate-General Home Affairs. This publication [communication] reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

The authors would like to acknowledge the involvement of Igor Kozine in testing the framework. His valuable feedback for the improvement is also gratefully acknowledged.

References

Basque Government (2015). "KLIMA 2050 - Climate Change Strategy Of The Basque Country To 2050", Eusko Jaurlaritzaren Argitalpen Zerbitzu Nagusia Servicio Central de Publicaciones del Gobierno Vasco Donostia-San Sebastián, 1 - 01010 Vitoria-Gasteiz , Report BI 1725-2015, July 2015.

Bruneau, M. et al. (2003). *A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities*. Earthquake Spectra, V. 19, No. 4, pp. 733-752, Earthquake Engineering Research Institute

De Bruijne, M., & Van Eeten, M. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. *Journal of contingencies and crisis management*, *15*(1), 18-29.

Department of Homeland Security (DHS, 2009). National infrastructure protection plan, Washington, DC.

European Commission (2008). Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official J. of the EU*.

European Commission (2013). Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. SWD(2013) 318 final.

FEMA – Federal Emergency Management Agency (2006). Principles of Emergency Management, Independent Study, IS230, Washington

FEMA – Federal Emergency Management Agency, Core Capabilities in the National Preparedness Goal: https://www.fema.gov/core-capabilities, visited on June 21, 2016.

Fox-Lent, C., Bates, M. E., & Linkov, I. (2015). A matrix approach to community resilience assessment: an illustrative case at Rockaway Peninsula. *Environment Systems and Decisions*, *35*(2), 209-218.

Kozine, I & Andersen, H. B. (2015). *Integration of resilience capabilities for critical infrastructures into the emergency management set-up*. Proceedings of The Annual European Safety and Reliability Conference – ESREL 2015 conference, September 2015, Zurich, Switzerland.

Lindbom, H., Tehler, H., Eriksson, K., & Aven, T. (2015b). The capability concept–On how to define and describe capability in relation to risk, vulnerability and resilience. *Reliability Engineering & System Safety*, *135*, 45-54.

Lindbom, H., Tehler, H., Frykmer, T., Uhr, C. (2015a). How can the usefulness of capability assessments be improved? *ESREL Conference 2015*, Zurich, Part of: Safety and Reliability of Complex Engineered Systems (ISBN: 978-1-138-02879-1), pages: , C R C Press LLC.

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., ... & Seager, T. P. (2013). Measurable resilience for actionable policy. Environ. Sci. Technol., 47, 10108-10110

Petrenj, B., & Trucco, P. (2014). Simulation-based characterisation of critical infrastructure system resilience. *International Journal of Critical Infrastructures*, *10*(3-4), 347-374.

Presidential Policy Directive/PPD-8 (2011) Washington, DC: The White House.

Presidential Policy Directive/PPD-21 (2013) Critical infrastructure security and resilience, Washington, DC: The White House.

RESIN (2015). "City Assessment Report Bilbao", Resin - Climate Resilient Cities and Infrastructures Project, EC Horizon2020, Project ID: 653522.

Setola R., Luiijf E., Theocharidou M. (2016) Critical Infrastructures, Protection and Resilience. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control, vol 90*. Springer, Cham

Trucco, P. Cagno, E. & De Ambroggi, M. (2012). Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures, Reliability Engineering & System Safety, Volume 105, September 2012, Pages 51-63, doi:10.1016/j.ress.2011.12.003.

Trucco, P. & Petrenj, B. (2017) "*Resilience of Critical Infrastructures: benefits and challenges from emerging practices and programmes at local level*". In: Linkov, I. & Palma-Oliveira, J. M. (eds.), Resilience and Risk, NATO Science for Peace and Security Series C: Environmental Security, Springer Science+Business Media B.V., Dordrecht, The Netherlands.

Vugrin E.D., Warren E.D., Ehlen M.A. & Camphouse R.C. (2010). 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.

Annex 1: Resilience capabilities

Capability	**General Description**
Planning	Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.
Public Information and Warning	Deliver coordinated, prompt, reliable, and actionable information to the whole community regarding any threat or hazard, as well as the actions being taken and the assistance being made available.
Operational Coordination	Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.
Intelligence and Information Sharing	Provide timely, accurate, and actionable information concerning all hazards and threats. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.
Interdiction and Disruption	Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.
Screening, Search and Detection	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.
Access Control and Identity Verification	Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.
Cybersecurity	Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.
Physical Protection	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.
Risk Assessment	Identify, assess, and prioritize risks to inform Protection activities, countermeasures, and investments.
Supply Chain Integrity and Security	Strengthen the security and resilience of the supply chain.
Community Resilience Building	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.

Capability	**General Description**
Threats and Hazards Identification	Identify the threats and hazards that occur in the geographic area; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of a community or entity.
Logistics and Transportation under EM	Provide transportation (including infrastructure access and accessible transportation services) for 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 vital services. Synchronize logistics capabilities and enable the restoration of impacted supply chains.
Environmental Response / Health and Safety	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.
Fatality Management Services	Provide fatality management services, including decedent remains recovery and victim identification, working with regional and national 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 counseling to the bereaved.
Fire Fighting	Provide structural, wildland, and specialized firefighting capabilities to manage and suppress fires of all types while protecting the lives, property, and the environment in the affected area.
Mass Care	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.
Mass Search and Rescue Operations	Deliver 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.
On-scene Security, Protection and Law Enforcement	Ensure a safe and secure environment through law enforcement and related security and protection operations for people and communities located within affected areas and also for response personnel engaged in lifesaving and life-sustaining operations.
Operational Communications	Ensure timely communications in support of security, situational awareness, and operations among and between affected communities in the impact area and all response forces.

Capability	General Description
Public Health, Healthcare and Emergency Medical Services	Provide lifesaving medical treatment via Emergency Medical Services and related operations and avoid additional disease and injury by providing targeted public health, medical, and phsycological support, and products to all affected populations.
Situational Awareness and Decision Making	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.
Natural and Cultural Resources Protection	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.

Annex 2: Scenario event sequence

Step #	FACT	REQUEST
Step 1	Today at 14.30, the National Meteorological Service inform you that an extreme weather event within three days. The storm has been called READ.	Assess what is your actual level of capability to cope against the READ event
Step 2	Some of your national infrastructure depends of other countries infrastructures. You have been informed the READ event will impact a large part of Europe.	Assess what is your level of international interdependency and evaluate what is your actual level of resilience
Step 3	Review your emergency plan (business continuity plan) to check what are the procedure that need to be implemented in order to be prepared to the READ event	Evaluate what is quality and the efficacy of your emergency plan
Step 4	You have activated the procedures to alert the public (or customers)	Evaluate what is your capability to inform the public
Step 5	At 5.30 it starts to rain; After few hours, the scenario is very critical: some of the urban infrastructures are disrupted	Evaluate what is your capability in order to mitigate the impact of Critical Infrastructures disruptions Identify what are your main functions and priorities that need to be guarantee in order to maintain an acceptable level of operational continuity
Step 6	Some High voltage lines a destroyed by the strong wind; Some Energy production plants are flooded and do not operate The blackout propagates to France and then to the rest of Europe The train do not circulate in the country The airport is closed	Evaluate what are your capabilities to face such impacts What is your capacity to coordinate your activities with other European countries

Step #	FACT	REQUEST
Step 7	Some villages do not have drinkable water and 40 power generators are required to maintain vital emergency services; 500.000 people need to find a shelter; Hospitals in the region have saturated the operational capacity and there are more than 2.000 people that need medical care assistance	Evaluate what are your capabilities to face such issues
Step 8	The READ storm is over. Following heavy winds and rains some recovery measures need be undertaken	Evaluate what is your priorities for returning to the normal situation Identify what are the capabilities needed during the recovering phase and how you interact with the other actors
Step 9	One month is passed. You called to contribute to the lesson learnt process The ministry has defined a working team to learn from the past event and to define an advanced emergency plan In particular, it wants to improve: • the coordination among Public Authorities and Critical Infrastructure Operators; • the international coordination • to define international emergency exercises	Evaluate what is your capability to contribute to such plan
Step 10	END	Dedicate the remaining to time to review