Technical University of Denmark

Emergency Management involving Critical Infrastructure Disruptions: operationalizing the deployment of resilience capabilities

Trucco, P.; Petrenj, B. ; Kozin, Igor; Andersen, Henning Boje

Published in:
Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016

Publication date:
2016

Citation (APA):
Trucco, P., Petrenj, B., Kozin, I., & Andersen, H. B. (2016). Emergency Management involving Critical Infrastructure Disruptions: operationalizing the deployment of resilience capabilities. In Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016 (pp. 548-555)

Emergency Management involving Critical Infrastructure Disruptions: operationalizing the deployment of resilience capabilities

P. Trucco & B. Petrenj
Fondazione Politecnico di Milano, Milan, Italy

I. Kozine & H. B. Andersen
Technical University of Denmark, Kgs. Lyngby, Denmark

ABSTRACT:
Recent developments nurturing the importance of Emergency Management (EM) of Critical Infrastructure (CI) brought a shift of emphasis from protecting the systems to building resilience. Resilience approach is required to cope with inevitable events, ensuring ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. The study proposes a novel approach to integrating the resilience capacities of CI into the EM cycle, which facilitates emergency services and CI operators to collaborate in addressing resilience improvement measures, while planning to cope with CI disruptions. It grounds on a previously published comprehensive framework which reflects the main characteristics of such emergencies (e.g. interdependent, multi-sectoral, multi-stakeholder) and supports the identification, assessment and development of specific technical and organizational capabilities. A pilot application is provided on a real case involving the public and private actors engaged in the Regional Programme on Critical Infrastructure Protection and Resilience (CIP-R) in Lombardy (Italy).

1 INTRODUCTION

Critical infrastructure (CI) may 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 current literature and discussion on Emergency Management (EM) of CI a shift of emphasis has appeared from protecting the systems to maintaining their resilience. Resilience approaches are built on the assumption that not all disruptive events involving CI systems can be prevented. We adopt the following definition of resilience (Kozine & Andersen, 2015): “*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 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”.*

A number of conceptual frameworks have emerged that aim at demonstrating different, interrelated aspects of systems’ resilience rather than serving as operational guidance for assessment of the resilience. Notable are the MCEER[1] 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.

The present study aims at improving the planning and assessment of the resilience capacities to address the challenges raised by disruptions affecting complex CI systems. It was developed in the context of the READ Project[2] (Resilience Capacities Assessment for Critical Infrastructures Disruptions). The stakeholders and beneficiaries of READ are the emergency management and civil protection authorities, first responders, CI operators, and the main public authorities in charge of CIP-R programmes.

[1] MCEER is the Multidisciplinary and National Center for Earthquake Engineering Research at University of Buffalo

[2] The READ Project (http://www.read-project.eu/) is co-funded by the European Commission under the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme.

Our approach integrates the resilience capabilities of CI into the EM cycle (prevention, preparedness, response, and recovery), which allows emergency services to explicitly address resilience improvement measures while planning to cope with CI disruptions. 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 planning of training exercises to enhance CI resilience can also benefit from the approach.

The project supports the stakeholders involved in the EM of Critical Infrastructure disruptions through:

- characterizing transboundary emergency situations involving interdependent CI systems;
- identifying, characterizing and assessing the resilience capacities required to prepare, cope and recover from these type of disruptions;
- improving practices and capabilities.

To practically support READ target groups, the project will provide a tool to effectively assess their resilience capacities (in preparedness, response and recovery phases) and identify the areas where actions and efforts are needed to improve the emergency management set-up.

In the present paper, we focus on the development of the READ tool, grounding on the READ framework that has been validated through an international focus group (Kozine & Andersen, 2015).

The reminder of the paper is organized as follows. The next section gives a short summary of the READ framework. Section 3 describes the case that will be used for the tool pilot testing. Some data collected for this case are used in Section 4 for a realistic demonstration of the tool's structure and functionalities. The final section briefly summarizes the progress and presents the future steps.

2 INTEGRATION OF CI RESILIENCE CAPABILITIES IN THE EMERGENCY MANAGEMENT SET-UP: THE READ FRAMEWORK

The full overview READ framework and the definition of its constituents have already been published in Kozine & Andersen (2015). In this section we summarise the main concepts necessary for a full understanding of the resilience assessment tool.

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. The Framework breaks it down into the following three related compounds: assets, resources, and practices/routines.

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:

- an *asset* is an item of ownership that has exchange value and, more directly, has value to the community and the CI that serves the community; assets include both physical entities as well as intangibles such as knowledge systems;
- 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 *routine/practice* is defined as the way things are done, possibly codified as an explicit procedure or a pattern of activities with no explicit procedure.

2.2 *Resilience capacities*

Following Vurgin et al. (2010) and Kozine & Andersen (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.

2.3 *Emergency Management Cycle*

We adopted the definition of the EM phases given in FEMA (2006) and reported in the following.

Preparedness: The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private-sector and non-governmental organizations to identify threats, determine vulnerabilities, and identify required resources.

Prevention: Actions taken to avoid an incident or to intervene to stop an incident from occurring, actions taken to protect lives and property, and applying intelligence and other information to a range of activities that may include countermeasures.

Mitigation: Activities that are designed to reduce or eliminate risks to persons or property, or lessen the actual or potential effects or consequences of an incident.

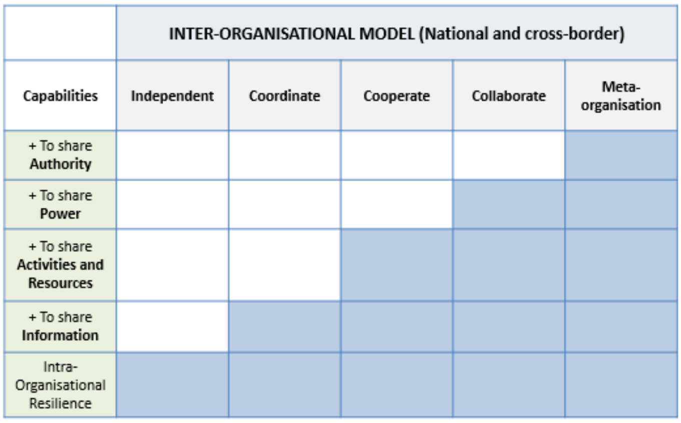
Response: The activities that address the short-term, direct effects of an incident. Response also includes the execution of EOPs and of incident mitigation activities designed to limit the loss of life, personal injury, property damage, and unfavorable outcomes.

Recovery: The development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private-sector, non-governmental, and public assistance programs.

2.4 *Inter-organizational approaches*

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-organizational and inter-organizational resilience capabilities.

Inter-organizational capabilities should be identified according to what is shared between the organizations involved in concerted actions. The READ project suggests the inter-organizational escalation model that helps identify the corresponding resilience capabilities, as suggested by Kozine & Andersen (2015) and depicted in Figure 1. To define inter-organizational resilience capabilities, responders (organizations and organizational units) shall determine their mutual relationships in each of the relevant pairwise relations, and in general, in each of the n-tuple relations of relevance.



	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 1. Levels of inter-organizational approach (taken from Kozine & Andersen, 2015)

2.5 *Classification of capabilities*

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**rganizational, (3) **S**ocial, and (4) **E**conomic, (TOSE).

This brings us to the final classification of the capabilities according to explained four criteria (Figure 2). Social and Economical resilience dimensions are however out of scope of the present study.

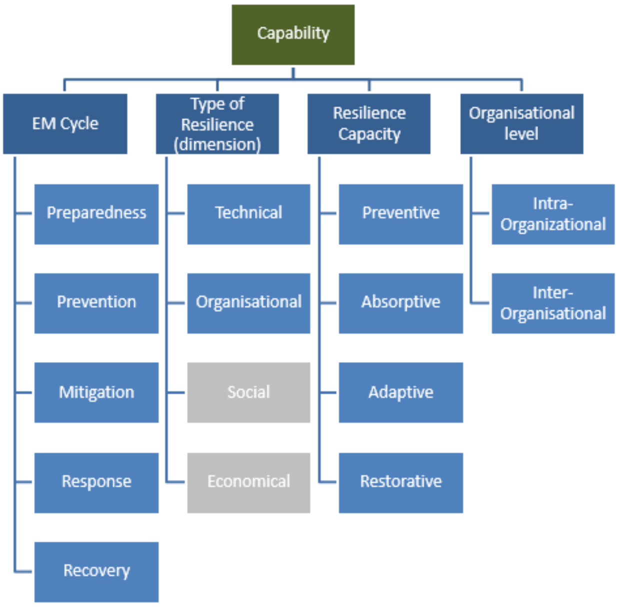


Figure 2. Classification of capabilities

The concepts defined in the previous section allow us now to shape an approach to building and maintaining the resilience of CI (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 practices/routines. Further, each single capability contributes to one or more resilience capacities and is used in one or more phases of the EM cycle. A capability can contribute to the resilience of individual organisations as independent ('intra-organizational'), and/or enable different levels of collective approaches ('inter-organizational') through sharing information, activities and resources, power or even authority.

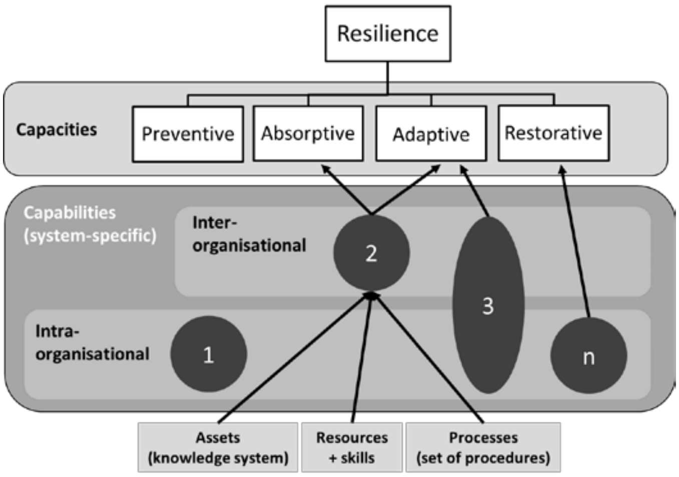


Figure 3. Building system resilience (adapted from Kozine & Andersen, 2015)

3 CASE DESCRIPTION

To test the practical suitability of the READ framework and the functionalities of the tool, the case of Lombardy Region (Italy) Public-Private Collaboration and Programme for CI Resilience has been selected as a pilot case. For the sake of this paper, we did not refer to the full case, which is still in progress, but we selected a reduced piece of collected data for demonstration purposes only. Our aim here is just to describe the applicability of the framework and the functionalities of the related tool by referring to realistic elements and conditions, as reported in the next section.

3.1 *Lombardy Region CIP-R Programme*

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 one of the richest in Europe.

To establish a risk-informed policy making process, the Regional Administration launched in 2007 a four-year research programme named "PRIM – Integrated Regional Program for the mitigation of major risks" (Lombardy Region, 2007). Considering the results of PRIM study, it became evident that hazards identified over the territory, not only can threat the citizen life, but can also cause severe disruptions of infrastructure service continuity inducing wide cascading effects. As a consequence, following the release of the EC Directive 2008/114/EC (EC, 2008), the Lombardy Region Administration decided to set up a preliminary study to investigate critical infrastructures vulnerability and to assess current emergency practices in the sector.

It emerged that there is a great potential for an increase in the flow of shared information regarding criticality and accidents, which can increase efficiency of the invested resources and bring an improvement in the security level. The objective of the Lombardy region policy on CIP-R is therefore not to add new mechanisms or control processes, but to promote and advance inter-institutional and inter-organizational collaboration. 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.

3.2 *Type and characteristics of regional CI systems*

The regional CI systems that have been taken into consideration in the present study include:

- Transport infrastructures:
  - Roads, highways, beltways and related assets (4 operators);
  - Rail – national and regional railway network, major train stations and control centers, metro system (6 operators);
  - Air – the 3 major airports in the region (2 operators);
- Energy infrastructures:
  - Electricity – the main points of connection between the high and medium voltage networks (transmission and distribution), zones of distributed generation, control rooms (3 operators).
  - Gas – main plants and dispatching networks (2 operators).

3.3 *Mapping of emergency management processes and vital node analysis*

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. More specifically, the study focused on:

- Carrying out a census of the most relevant CI nodes; globally more than 200 regional nodes have been identified and documented;

- Analysis of the accidents influencing regional CI and creating a series of historical cases;
- Mapping the Emergency Management organizational models and operational processes of the main CI operators active in the region.

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.

3.4 *Thematic Task-Forces (TTF)*

TTFs represent the backbone of the programme implementation; they are established and coordinated by a higher level PPP Governance Committee which 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 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 TTFs 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;

3.5 *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:
  - 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.

4 THE READ TOOL FOR CAPACITY ASSESSMENT AND PLANNING

In this section, we present the key features and the functionalities of the tool that translates the READ framework for the integration of CI resilience capabilities in the emergency management set-up (the tool prototype was implemented in MSAccess^{TM}).

4.1 *Phase 1: System and environment specification*

In the initial phase, the characteristics of the system under analysis, the organisational and environmental contexts must be specified. In this part, the users should go through a few setup steps, namely:

1) *System definition*, which consists of:
   - Specification of each single organization, classified by type and role;
   - Specification of the technological infrastructure (Classes, Types and Assets);
   - Specification of relevant Hazards & Threats (a default taxonomy is provided, which is editable);
   - Documentation of the existing types of capabilities and their classification (as in Tables 1, 2);
2) *Accident Events Specification*, where different possible future events can be described and documented as the scenario of reference for the next assessment and planning phases (e.g. electrical blackout event, heavy snowfall and flooding event).
3) *Asset Vulnerability Analysis*, where for each asset its vulnerability is defined for each of the accidents of interest.

Table 1: Examples of capability specification

Capability	**Elements**	**Context**
Communication and Information Sharing	***Assets:*** Information exchange system (SUSI); map of multi-actor information flows during disaster management ***Resources:*** Personnel in the control rooms (CI) and Situation Room (Civil protection); social media and other web resources. ***Routines:*** Information sharing protocol and procedure	Regional Government and partners (CI operators)

Capability	Elements	Context
Evacuation of passengers	***Assets:*** Installations of emergency light and ventilation ***Resources:*** Airport personnel and fleets; replacement of transport services using buses ***Routines:*** Evacuation and Emergency procedure; Airport Passenger Contingency Plan	Airport operator
Communicating with the public	***Assets:*** Information to users with all active and passive channels available (various messaging, network, toll free number, SMS, company website). ***Resources:*** Staff and other resources at emergency sites to redirect traffic and intervene. ***Routines:*** Communication plan capable of informing users of the location and type of emergency	Road operator
Backup transport means	***Assets:*** Agreements for replacement services with bus companies wherever possible. ***Resources***: Bus fleets and drivers of road transport companies. ***Routines***: Internal process for back-up service activation and SLA on responsiveness.	Rail operator

4.2 *Phase 2: Assessment of Resilience Capabilities*

After the system specification, the user moves into the 'Resilience Assessment' module of the tool. Referring to a specific accident event at a time, the users assign different types of capabilities to organizations - e.g. ATM, the Urban Transport Company, or Civil Protection -, describing in which way the capability is specifically implemented in each organization (assets-resources-routines). An assessment is also given on the *current* and the *target* (i.e. desired) level of this capability as planned by the corresponding organization (Annex A). It is important to mention that the capability assessment is done considering the vulnerability of assets to the accident in question (as specified in Phase 1). The capability levels are defined as:

- Missing (0);
- Very Low (1);
- Low (2);
- Medium (3);
- High (4);
- Very High (5).

Table 2: Examples of capabilities of different organizations in the case application

		Classification*			
Organization type	**Capability Description**	**EM Cycle**	**Resilience Dimension**	**Resilience Capacity**	**Organizational Level**
Civil Protection	Communication and Information Sharing	Pp, Mi, Re, Rc	T, O	Ab, Ad,	I
Rail operator	Backup Electricity	Mi Re Rc	T	Ab	i
Metro Operator	Backup transport means	Mi, Re, Rc	O	Ab, Ad, Re	i, I
Airport Operator	Evacuation of passengers	Mi Re	T, O	Ab	i, I
Electricity operator	Communication to the public	Pp Re, Rc	T, O	Ab, Ad	i

* EM Cycle = Preparedness (Pp), Prevention (Pv), Mitigation (Mi), Response (Re), Recovery (Rc).
Resilience dimension = Technical (T), Organis. (O)
Resilience Capacity = Preventive (Pr), Absorptive (Ab), Adaptive (Ad), Restorative (Re).
Organizational level = intra-org (i), inter-org (I)

After all the capabilities are assigned to organizations and the assessment completed, it is possible to give an overview of the current state of the overall system. The *Resilience Capacity Analysis* function shows the distribution of specific capabilities throughout the organization types and levels, as well as their compounds for selected accident events.

4.3 *Phase 3: Capability building cycle*

The capability building cycle is the process through which the system resilience is enhanced. It consists of four steps (Figure 4):

1) In the first step the current state of the resilience capabilities is assessed – situation AS IS;
2) 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 context.
3) 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.

4) 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.

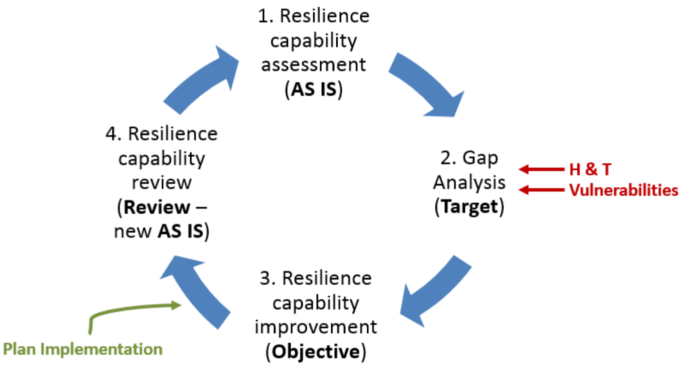

1. Resilience capability assessment (**AS IS**)
2. Gap Analysis (**Target**)
H & T
Vulnerabilities
3. Resilience capability improvement (**Objective**)
4. Resilience capability review (**Review** – new **AS IS**)
Plan Implementation

Figure 4. Capability 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, taking into account every Organization-Capability couple. The *Gap Analysis* shows the analyst a comprehensive picture giving quantitative indicators, enabling him to easily identify the weak points (Annex A). 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.

5 CONCLUSIONS

In this paper, we presented a novel approach to integrating the resilience capacities of CI into the EM cycle, which facilitates emergency services and CI operators to collaborate in addressing resilience improvement measures, while planning to cope with CI disruptions. It grounds on a comprehensive framework (Kozine & Andersen, 2015), which reflects the main characteristics of such emergencies (e.g. interdependent, multi-sectoral, multi-stakeholder) and supports the identification, assessment and development of specific technical and organizational capabilities. The test case we prepared, based on a piece of data collected for preparation of a full pilot case in Lombardy Region (Italy), demonstrates the applicability of the approach and the functionalities of the software tool. The proposed approach and the tool were used to support the preparedness and collaborative planning activities in the context of the public-private partnership on CI Resilience in Lombardy Region. The pilot application shown that, thanks to a unified model and capability classification, different actors – energy or transport operators, first responders, etc. – 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.

In the next steps of the ongoing research project, the tool will be tested in practice in two different contexts:

- the preparedness activities carried out within the Public-Private Collaboration and Programme for CI Resilience in Lombardy Region (Italy);
- a table-top exercise on the assessment of recovery strategies for CI disruption, involving some selected EU stakeholders (emergency managers, civil protection authorities, first responders and CI operators).

ACKNOWLEDGEMENT

This project has been funded with support from the European Commission. 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

REFERENCES

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

Crosby, B.C., & Bryson, J.M. 2005. *Leadership for the Common Good: Tackling Public Problems in a Shared-Power World* (2nd Edition). San Francisco, CA: Jossey-Bass.

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.*

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

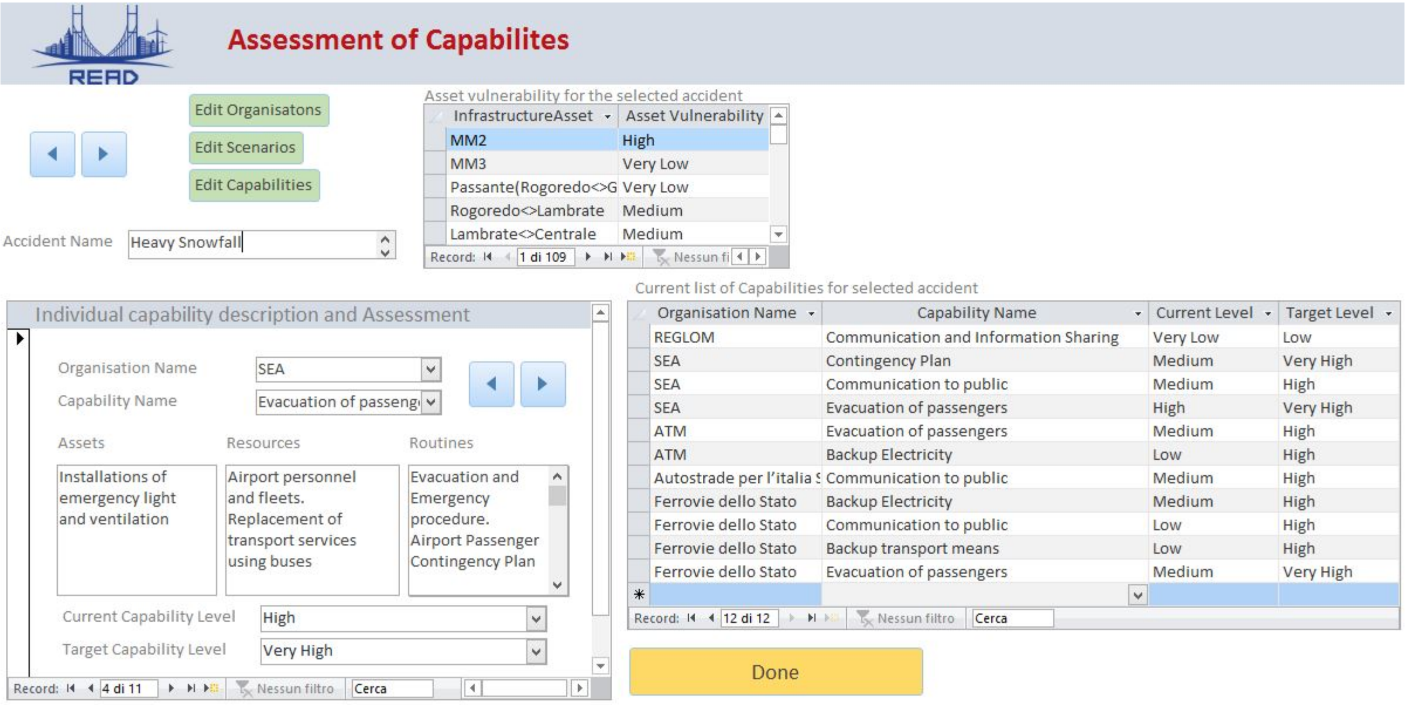
Kozine, I & Andersen, H. B. 2015. *Integration of resilience capabilities for critical infrastructures into the emergency management set-up.* Proceedings of The Annual European Safety and Reliability Conference – ESREL 2015 conference, September 2015, Zurich, Switzerland.

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.

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 A - READ TOOL FUNCTIONALITIES AND USER INTERFACE

A.1. Assessment of resilience capabilities



Assessment of Capabilites

Accident Name: Heavy Snowfall

Asset vulnerability for the selected accident

InfrastructureAsset	Asset Vulnerability
MM2	High
MM3	Very Low
Passante(Rogoredo<>G	Very Low
Rogoredo<>Lambrate	Medium
Lambrate<>Centrale	Medium

Record: 1 di 109

Individual capability description and Assessment

Organisation Name: SEA

Capability Name: Evacuation of passeng

Assets	Resources	Routines
Installations of emergency light and ventilation	Airport personnel and fleets. Replacement of transport services using buses	Evacuation and Emergency procedure. Airport Passenger Contingency Plan

Current Capability Level: High

Target Capability Level: Very High

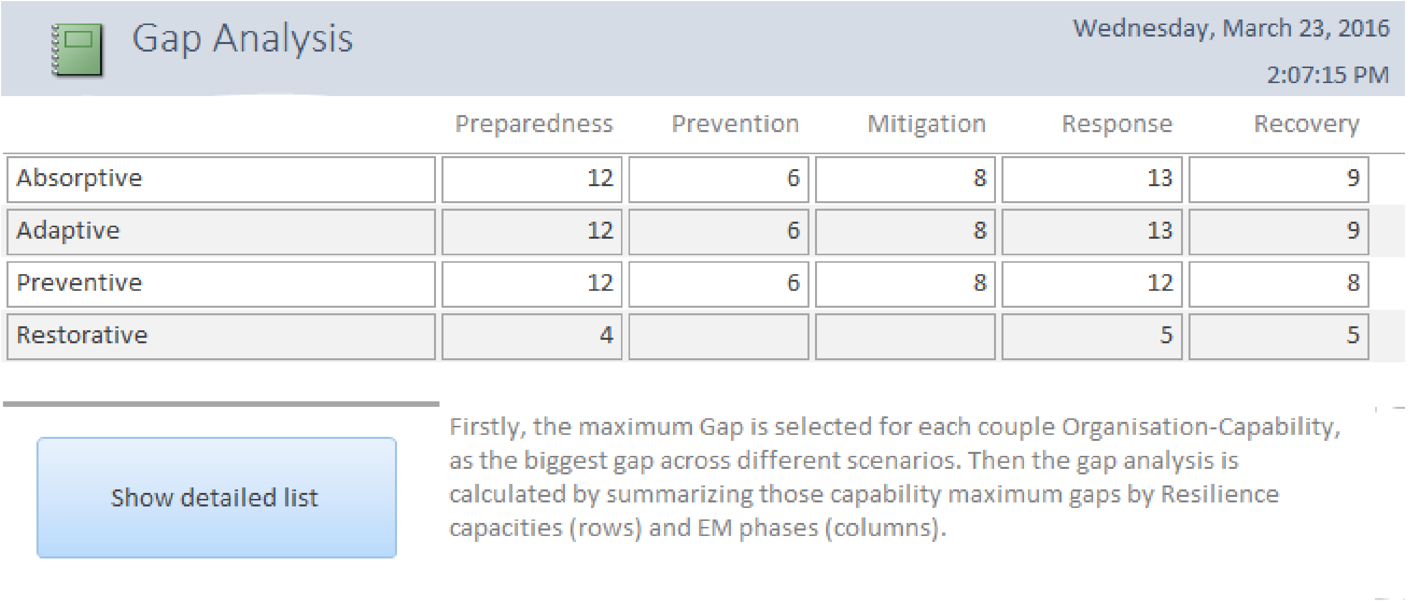
Record: 4 di 11

Current list of Capabilities for selected accident

Organisation Name	Capability Name	Current Level	Target Level
REGLOM	Communication and Information Sharing	Very Low	Low
SEA	Contingency Plan	Medium	Very High
SEA	Communication to public	Medium	High
SEA	Evacuation of passengers	High	Very High
ATM	Evacuation of passengers	Medium	High
ATM	Backup Electricity	Low	High
Autostrade per l'italia S	Communication to public	Medium	High
Ferrovie dello Stato	Backup Electricity	Medium	High
Ferrovie dello Stato	Communication to public	Low	High
Ferrovie dello Stato	Backup transport means	Low	High
Ferrovie dello Stato	Evacuation of passengers	Medium	Very High

Record: 12 di 12

A.2. Gap Analysis



Gap Analysis

Wednesday, March 23, 2016

2:07:15 PM

	Preparedness	Prevention	Mitigation	Response	Recovery
Absorptive	12	6	8	13	9
Adaptive	12	6	8	13	9
Preventive	12	6	8	12	8
Restorative	4			5	5

Firstly, the maximum Gap is selected for each couple Organisation-Capability, as the biggest gap across different scenarios. Then the gap analysis is calculated by summarizing those capability maximum gaps by Resilience capacities (rows) and EM phases (columns).