Integration of resilience capabilities for Critical Infrastructures into the Emergency Management set-up

Kozine, Igor; Andersen, Henning Boje

Published in:
Safety and Reliability of Complex Engineered Systems

Publication date:
2015

Document Version
Peer reviewed version

Integration of resilience capabilities for critical infrastructures into the emergency management set-up

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

ABSTRACT: We suggest an approach for maintaining and enhancing resilience that integrates the resilience capabilities of critical infrastructures (CIs) into the emergency management cycle (prevention, preparedness, response, and recovery). This allows emergency services to explicitly address resilience improvement measures while planning to cope with CI disruptions. To operationalise this approach we have developed a hierarchical taxonomy that classifies system resilience capabilities into intra- and inter-organisational categories. Capabilities are defined as a combination of assets, resources and processes specifically arranged to accomplish a critical task and assure a key objective. They are grouped into preventive, absorptive, adaptive and restorative sets. The capabilities are identified at both the technological and the organisational level in each organisation (CI operator or responder). 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.

1 INTRODUCTION

In current literature and discussion on Emergency Management (EM) of Critical Infrastructures (CIs) 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 and that there is a need to create more resilient CIs that can reduce chances of a shock, absorb it and quickly recover if it occurs. 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 (Vugrin, 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 approach described in this paper integrates the resilience capabilities of CIs 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.

To develop a consistent framework for maintaining and enhancing the resilience of CIs, we wished to establish sound, reasonably precise and practically useable definitions of key concepts on which our approach is based.

The definitions and concepts are given in section 2, while an overview of the developed framework is provided in section.

2 BASIC DEFINITIONS AND CONCEPTS

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

[1] MCEER refers to what was formerly the Multidisciplinary and National Center for Earthquake Engineering Research at University of Buffalo

an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions[2].

This definition is sufficiently precise for our purpose, though we are aware that there is indeed some variation in the ways in which different countries have characterized what infrastructures are "critical" for, which sectors are included and how broadly 'infrastructures' shall be interpreted.

Based on a literature review and the limited focus of major CI disruptions, we adopt the following definition of resilience:

The resilience of a CI system is its ability to

- *reduce the chances of a disruption of its performance and service to the public,*
- *absorb the consequences of any 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.*

This definition provides us guidance on how the resilience of CIs can be measured:

Measures of resilience:

1. *the probability that the CI suffers an interruption or reduction of performance given a shock,*
2. *the level of impact given a shock or a disruption,*
3. *the speed of recovery given a shock or disruption, and*
4. *the ability to adapt to novel conditions.*

Now we can introduce the definition of *objective for resilience that consists in minimising the three first measures of resilience to as low level as practicably possible and in maximising the fourth to as high a level as useful*.

In order to be prepared for an unexpected evolvement of an incident into an emergency situation, several countries have adopted a capabilities-based planning approach as part of their emergency preparedness work. (See, for example, Houdijk (2010) and the Swedish statutory instructions MSBFS (2010).) The strategy of capabilities-based planning is to prepare for a large variety of threats and risks instead of simply preparing for specific scenarios (Lindbom, 2015). We find this approach promising and apply this idea for the foundation of our framework to building the resilience of CIs. In this view, we need to define the concept of capability in a way that allows a clear separation and identification of all capabilities influencing the resilience of a CI.

On a general view (not related to CIs), we define a *capability of an entity (organization, person, system) as a feature, faculty or process that promotes the achievement of its objectives.* This definition is rooted in two others: one – given by Business Dictionary[3], and the other – given by Vincent (2008).

We further operationalise the definition of a capability to the definition of a resilience capability of a CI as follows.

We build the definition on the three concepts: *assets, resources* and *routines*. They 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 and assets. The distinction between assets and resources is context dependent – so what counts as a resource in once context may be an asset in another (say, ambulances, software programs). Finally, 'routines' refers both to 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 and incomplete definitions of these terms are the following:

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

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

---

[2] EU COM(2006) 786 EU Directive on European Programme for Critical Infrastructure Protection

[3] Business Dictionary: http://www.businessdictionary.com

Routine is defined as the way things are done, possibly codified as an explicit procedure, within a community or social group, a pattern of activities (Teece, 1997).

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

For the definition of *capacities* we follow the Sandia authors (Vugrin, et al. 2010) and distinguish the four groups with respect to supporting infrastructure resilience: (1) preventive, (2) absorptive, (3) adaptive, and (4) restorative capacity.

This division of the capacity groups is complete with regard to Emergency Management cycle, as it maps the capacities to the all phases of the EM cycle (see below Figure 1).

Each capacity is defined as follows.

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.

Following the MCEER framework (Bruneau, et al. 2003) we also distinguish among:

Types of CI dimensions (subsystems/components): (1) **T**echnical, (2) **O**rganisational, (3) **S**ocial, and (4) **E**conomic, (TOSE).

As one of the objectives of the developed framework was to couple resilience enhancement and maintenance measures to the EM cycle, we need to explicitly state where the borders of the different phases start and end and what activities are included in each phase.

The EM cycle is usually divided into four phases: *mitigation*, *preparedness*, *response, and recovery*. Though, the adjacent phases overlap meaning that critical activities usually cover more than one phase, and the boundaries between phases are seldom precise. In fact, there are multiple examples of using from three to eight phases of the EM cycle. Recent changes in labelling the phases involve additional words for a better coverage of the critical activities within the phases. For instance, “mitigation” is changed to “mitigation and prevention” to align with the disciplines and practices of risk management, security and loss prevention. The “preparedness” phase can be extended to “preparedness/planning”, to stress the planning activity within the phase (Malcolm, 2010).

We adopt the definition of the EM phases given in FEMA (2006).

*Preventio*n: 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.

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.

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 unfavourable 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.

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.

3 AN OVERVIEW OF THE FRAMEWORK FOR BUILDING RESILIENCE AGAINST CI DISRUPTIONS

The space in which resilience capabilities of CIs are defined is restricted to two dimensions: (1) types of the CI subsystems or components (TOSE) and (2) capacity groups (preventive, absorptive, adaptive, and restorative). Specific solutions or mechanisms that will be identified within this space are resilience capabilities that contribute in making the system resilient, i.e., enhancing at least one of its resilience capacity groups. The resilience capacity groups can be mapped in turn to the phases of the EM cycle. Nevertheless, we need to distinguish between the stages when the capabilities are built and sustained and when they are exercised and manifest their efficiency. These are the pre-incident stage and post-incident stage. For example, while organi-

sational-absorptive capabilities are built and maintained during the prevention/mitigation and preparedness phases, their efficiency is manifested during the response phase (see Figure 1).

The concepts defined in the previous section allow us now to shape an approach to building and maintaining the resilience of a CI system. The approach is diagrammed in Figure 2. As it is explicitly seen from Figure 2, the capabilities are aggregates of some or all of the three components: assets, resources, and processes.

Let us consider some simple examples to illustrate the approach.

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

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

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

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

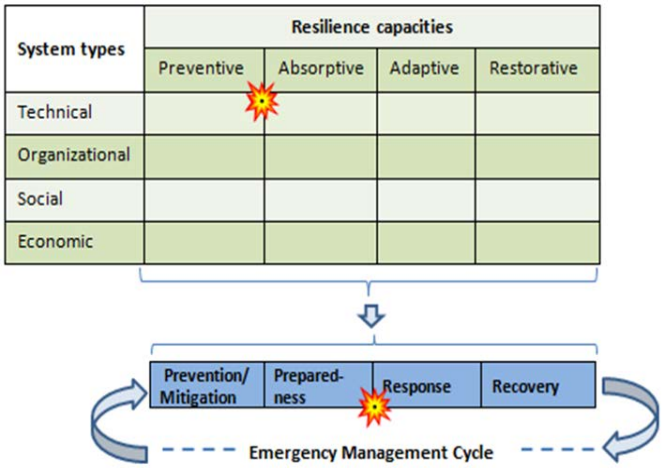

Figure 1. Resilience capabilities' space coupled to the

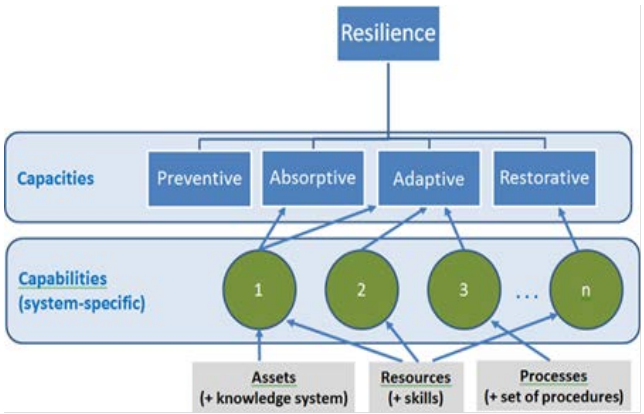

Figure 2. Building system resilience

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

In a tabular form the space is shown in Figure 3.

System types	Intra-/inter-organisational dimension	Resilience capacities			
		Preventive	Absorptive	Adaptive	Restorative
Technical	Intra				
	Inter				
Organizational	Intra				
	Inter				
Social	Intra				
	Inter				
Economic	Intra				
	Inter				

Figure 3. Resilience capabilities' space extended by the intra-/inter-organisational dimension

The inter-organisational model of capability building consists in the following. To enable inter-organisational relations and activities, there must be intra-organisational 'enablers' in place. That is to say, among many intra-capabilities contributing to the system resilience there are some enablers (capabilities) that allow establishing inter-organisational relations and conducting activities. The inter-organisational relations can have different gradations that are displayed in Figure 4.

This model facilitates the identification of inter-organisational resilience capabilities and their intra-enablers. Taking into account that CIs are complex socio-technical systems with a great deal of interconnections with other institutions and services, identification of the capabilities is a wide-ranging and laborious activity that - if performed in the full scale – must be done for each cell of the resilience capability space (Figure 3).

As a whole, the above sketched approach suggests that the starting point for resilience capability building is to work out an inventory of required capabilities that will populate the capability space (Figure 3). This exercise will result then in mapping the capabilities on the phases of the EM cycle, which is a step towards making the current framework workable in practice.

The identification of the capabilities is the key activity to make the framework operational, and splitting capabilities into assets, resources and routines will help assessing their efficiency for each specific application. To be able to work out an exhaustive set of resilience capabilities, additional aids should be provided to guide a purposeful search. These aids can emerge opportunistically and should become subject to scrutiny with regard to their value for our purpose. For example, the following sources of structured knowledge are seen as a potentially useful help in working out a set of the resilience capabilities of CI:

- Resilience capabilities and components identified to assess the Resilience Measurement Index of CI[4],
- Core functions of operational resilience (Birkie, et al., 2014),
- "Resilience properties" (robustness, redundancy, resourcefulness, and rapidity) (Bruneau, et al. 2003),
- Main barriers and capabilities in crisis information sharing and collaboration (Petrenj, et al., 2013).

The inventory of the resilience capabilities serves as a generic repository to be consulted to find resilience solutions for specific CI systems and the environments. To identify system-specific solutions, *system vulnerabilities* have to be identified as the next step of the framework. This exercise is rooted in risk analysis of

1. [4] Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. *Argonne National Laboratory Report*, ANL/DIS-13-01, April 2013

specific CIs, based on which, the mapping of the capabilities against the vulnerabilities provides an overview of what capabilities are in place for the system and what gaps may exist to enhance the resilience (Figure 5).

	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 4. Inter-organisational model

4 CONCLUDING NOTES

The development of the framework briefly described in this paper is still in progress. It is being developed to identify, build and assess specific resilience capabilities required to prepare, cope and recover from cross-border CI disruptions. The framework will be tested and validated through the practical tools built upon it and aiming at supporting the stakeholders involved in emergency management activities, including the CI operators. The preparedness and recovery tool is planned to be tested on real civil protection exercise scenarios (in 2016) involving the Øresund bridge-tunnel fixed link between Denmark and Sweden.

The recovery tool, built upon the framework, will be tested during a table-top exercise involving some selected EU stakeholders (emergency managers, civil protection authorities, first responders and CI operators).

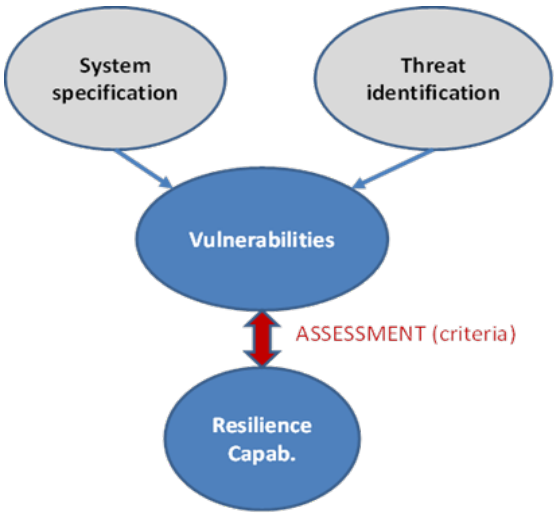

Figure 5. Coupling resilience capability solutions to specific CIs

5 ACKNOWLEDGEMENT

The approach 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 is co-funded by the Prevention, Preparedness

and Consequence Management of Terrorism and other Security-related Risks Programme, European Commission – Directorate-General Home Affairs.

We also gratefully acknowledge involvement in this work of professor P. Trucco and B. Petrenj from Fondazione Politecnico di Milano.

6 REFERENCES

Birkie S.E., Trucco P., Kaulio M. 2014. Disentangling core functions of operational resilience: a critical review of extant literature. *Int. J. Supply Chain and Operations Resilience*, Vol. 1, No. 1.

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

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

Houdijk, R. 2010. Regional risk assessment in The Netherlands – an introduction. The Hague

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

Malcolm, E.B. 2010. The "Phases" of Emergency Management. Background Paper prepared for for the Intermodal Freight Transportation Institute (ITFI) of University of Memphis

MSBFS 2010:7. "The Swedish Civil Contingencies Agency's instructions on governmental authorities' risk and vulnerability analyses", Sweden.

MSBFS 2010:6. "The Swedish Civil Contingencies Agency's instructions on municipalities' and county councils' risk and vulnerability analyses", Sweden.

Petrenj B., Lettieri E. and Trucco P. 2013. Information sharing and collaboration for critical infrastructure resilience – a comprehensive review on barriers and emerging capabilities. *Int. J. Critical Infrastructures*, Vol. 9, No. 4, pp. 304-329.

Teece, D.J., Pisano, G. and Shuen, A. 1997. Dynamic capabilities and strategic management, Strategic Management Journal, Vol. 18, No. 7, pp.509–533.

Vincent, L. 2008. Differentiating Competence, Capability and Capacity. Newsletter Vol. 16, No. 3. Vincent & Associates, Ltd.

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.