CRITICAL INFRASTRUCTURES RESILIENCE EVALUATION - RESILIENCE APPROACH, RESILIENCE MODEL AND RESILIENCE INDICATORS

ОЦЕНКА НА УСТОЙЧИВОСТТА НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ – ПОДХОД, МОДЕЛ И ПОКАЗАТЕЛИ ЗА ОЦЕНКА.

Associate professor Dimitrov D.L., Ph.D.
Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre “Acad. A Balevski” - Bulgarian Academy of Sciences, Sofia, Bulgaria
E-mail: ddimitrov@ims.bas.bg

Abstract: Aim of this report is to provide practical hints on how to evaluate the concept of Resilience in the domain of Critical Infrastructures (CI). The common understanding is that today best practices address cyber / physical protection of CI at the best they can, with traditional static and iterative solutions, trying to stop all possible known threats at the border of the single CI’s assets or CI’s full perimeter, ready to start with procedures of disaster recovery and business continuity in case of failure stopping external threats.

KEYWORDS: *RESILIENCE; RESILIENCE APPROACH; RESILIENCE MODEL; RESILIENCE INDICATORS; SECURITY; SECURITY MANAGEMENT SYSTEM (SMS); INTEGRATED MANAGEMENT SYSTEMS FOR BUSINESS SECURITY.*

1. Introduction

Nowadays, unfortunately, Infrastructure Operators have to deal with a landscape characterized by constantly evolving threats and vulnerabilities, in response to which we need dynamic and continuously adapted solutions. In addition to all the measures already in place for protection, resilience is intended to put in operation at physical and logical levels all possible status of the art measures, along with redundancy and fault tolerant mechanisms able to adapt the system to evolving threat landscape, to reduce the reaction time and increase the reconfiguration capabilities.

While at personal, organizational and cooperation levels is intended to put in operation the best practices for continuous training (aimed at reduce internal threats, environmental inertia and social engineering issues), communication within the same organization, among different organizations and with the external world, able to foster the solution of the crisis after a successful attack or natural disaster.

2. The resilience approach

Past and recent experiences have shown how likely is that protection policies, sooner or later, may fail.

For this reason, and being aware of the fact that the efforts put in place for protection of CIs can be easily bypassed, all of the stakeholders involved in the protection of such delicate and vital infrastructure have reached a level of awareness that strongly suggests putting more emphasis on critical infrastructure resilience **[1].**

What does resilience mean?

Though infrastructure protection and infrastructure resilience represent complementary elements of a comprehensive risk management strategy, the two concepts are distinct. Infrastructure protection is the ability to prevent or reduce the effect of an adverse event. Infrastructure resilience is the ability to reduce the magnitude, impact, or duration of a disruption. The spread in the continuous discovery of new threats that target CIs, stress the importance of a whole rethinking around the concept of protection. That’s where resilience emerges from and becomes an important part of the playing field. A resilient approach is a holistic set of procedures and measures that encompasses the entire structure of an institution/business/infrastructure, from the physical parts to the management, to ensure the ability to prevent, absorb, adapt, and recover to an attack, either physical or cyber.

Very often there is the tendency to confuse the concepts of: resilience, security, business continuity, risk assessment/management, crisis and emergency management.

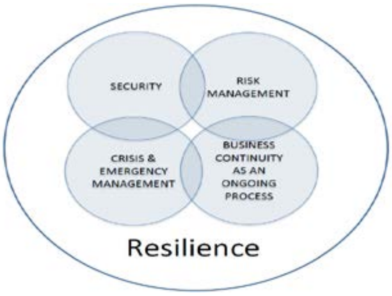
SECURITY
RISK MANAGEMENT
CRISIS & EMERGENCY MANAGEMENT
BUSINESS CONTINUITY AS AN ONGOING PROCESS
Resilience

Figure 1 *Resilience: A Multifaceted Problem*

Difference between Business Continuity and Resilience

Some authors argue: “Business continuity has been focused upon a defensive resilience posture, consisting of three basic building blocks - recovery, hardening and redundancy – that are widely recognized as vital ingredients for successful business continuity plans. A defensive posture is useful in protecting the organization and its revenue streams but it does not help the bottom line. It is an insurance or bomb-shelter mentality; a static initiative that makes you feel more secure or protected, but rarely gets updated” **[2].**

The concept of the “static initiative that make you feel more protected” is exactly what makes the difference with Resilience that is a step ahead to Business Continuity. According to other authors, Resilience provide “a mixture of continuity, availability, security, recovery and scalability” enabling a dynamic, proactive and holistic dimension to the protection approach. Resilience enable organizations to rapidly “self” adapt to abnormal events, faults or disruption ensuring a seamless service **[3].**

Resilience Evaluation is the overall activities of modelling, and analysis of critical infrastructure system aimed to evaluate the ability to prevent, absorb, adapt, and recover from a disruptive event, either natural or man-made.

Resilience Engineering is the overall activities of design, construction, operation, and maintenance of critical infrastructure system aimed to ensure the ability to prevent, absorb, adapt, and recover from a disruptive event, either natural or man-made.

As said, this aspect is not included in this report and should be, whether applicable, the focus of a future investigation.

A Critical Infrastructure is not only made of technologies but especially of people, processes and organizations. Any Resilience Evaluation and Engineering activity must take in consideration all these components, including cultural background, in view to be complete and successful.

To be univocally applicable, infrastructure resilience evaluation and engineering require a precise definition of resilience that is applicable to all infrastructure systems. The model consists of a hierarchy of four system resilience dimensions that concur to realize the four system resilience capacities taken from the definition. Resilience features occupy the engineering level of the hierarchy and represent the current infrastructure design implementations that contribute to one or more of the system capacities, while resilience indicators are quantified properties of the dimensions, capacities and features characterizing the system subject to assessment **[2].**

2. Overall basic assumptions of the model

The following statements sum up the proposed model features and point out some relations among model entities:

• Resilience is a quality of the system. Being a system composed of several subsystems, the overall system's resilience will be achieved through assuring resilience to single subsystem, considering higher risk priorities, as well as dependencies from other systems. The primary difficulty often involves how to represent infrastructure dependencies.

•The model addresses resilience evaluation but is also applicable to resilience engineering.

• Resilience has four dimensions: technical (logical & physical), personal, organizational, cooperative.

• Resilience relies on four capacities: preventive, absorptive, adaptive, restorative.

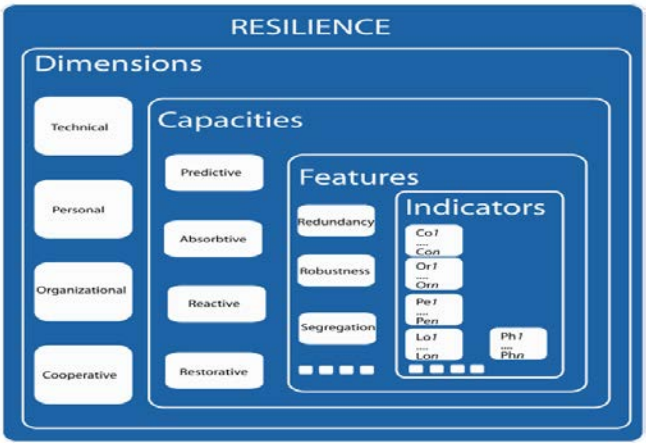

Figure 2 *Hierarchical Representations of the Infrastructure Resilience Model and Indicators*

• Each capacity is related to specific features (e. g. robustness, redundancy, segregation).

• Resilience indicators will be different for different application sectors (energy, transport, communications, and urban systems)

• Resilience indicators are physical and logical techniques, procedures, training activities, organizational solutions, etc. able to foster system capacities.

• Evaluating the system resilience may be downsized to evaluate the existence of resilience indicators, in the different features, capacities and dimensions of the system under evaluation.

• A software application based on the Resilience Model may be spun off the methodology **[3].**

Four system resilience dimensions:

The resilience dimensions derive from the assumption that a Critical Infrastructure is not only made of technologies but especially of people and organizations, and is dependent (or interdependent) from others infrastructures.

These dimensions may be stacked in an abstraction degree order from the highest abstraction level (Cooperative) to lowest abstraction degree level (Logical and Physical). Any Resilience Evaluation (and even Engineering) activity must take in consideration all these dimensions.

• *Logical & Physical dimension:* Individuate the most advisable technologies today available for the cyber and physical protection. Considering the best technologies to be used for sector specific applications. How to address the ever evolving threat and vulnerability landscape, with dynamic and continuously adapted technological solutions.

• *Personal dimension:* How to define the Profile of the people in charge for CI's resilience. How possibly certify the Resilience Skills of experts. Which should be the Training Program to prepare CI's resilient experts? In which way motivate the CI personnel not security specific to take part to the overall challenge of security.

• *Organizational dimension*: accordingly, with a proposed general logical model, how to define at organizational level a Resilience Management System and how to implement it. How to individuate the people to be involved. How to define the responsibilities and at which level.

• *Cooperative dimension:* How to promote the cooperation among different CI operators, both private and public. Who should have the responsibility of the initiative? Which is the state of the art and the best practices.

In building and evaluating resilience the contribution made by each of these four dimensions needs to be considered.

Four type of system resilience capacities

The resilience capacities are the intrinsic properties of the system infrastructure implemented into each one of the resilience dimensions, to make the system resilient.

• Preventive capacity: ability of a system to anticipate disruptive events.

• Absorptive capacity: degree to which a system can automatically absorb the impact of system perturbations and minimize consequences.

• Adaptive capacity: degree to which the system is capable of self-organization for recovery of system performance levels.

• Restorative capacity: the ability of a system to be quickly and easily repaired.

These capacities are represented in Figure 3. This figure has to be interpreted as that in case of disruptive event the four capacities will be activated from Preventive to Restorative, based on the real need

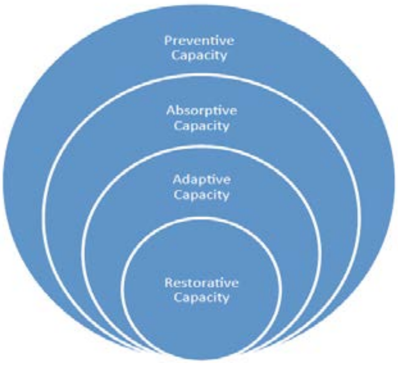

Figure 3 *System Resilience Capacities*

3. Resilience indicators

Resilience Indicators are quantified properties of the dimensions, capacities and features characterizing the system subject to assessment. Evaluating the resilience indicators means to evaluate the adoption of resilience solutions at the bottom level of the implementation used to implement features, enhancing capacities, acting in the four dimensions, with the goal to build a more resilient system. Resilience indicators are the basic tools for the evaluation process **[4].**

Resilience Indicator Name	**Related code (Dimension related)**
A - Description	Description of the specific Resilience Indicator of the sub-system/system subject to evaluation
B – Pertinent dimension(s)	To which dimension, sub-system / system, capacity it applies
C - CI Sector relevance	Relevance for the specific application sector (energy, transport, telecommunication, health care, etc.);
D - Evaluation method(s)	Method used to quantify this specific indicator while applying it to the sub-system / system subject to evaluation
E - Sources / References	References, if any, to authoritative sources from which card content is derived, totally or in part.

Figure 3 – Template *for Resilience Indicator Cards*

Validation Process for the Resilience Indicators

Resilience Indicators need to be validated for each specific sector or system of application by working together with Sector or System Experts. To this purpose, customization is essential to make the proposed methodology for engineering and evaluating resilience usable for CI operators and owners **[5].**

Today large organizations, such as most of the CI operators and owners, have a so called "silos" structures affected by the functions/roles assigned by the organization charts. This makes the process of resilience indicators validation still more difficult because of the necessity to interact with different key figures into the organization.

Here below is a suggestion about a potential approach towards the CI operators and owners: a matrix defining what to ask to the possible different key figures inside the organization. The rationale is to ask to quantify the magnitude of each resilience indicators to the key role in charge, respectively, of the logical, physical, personal, organizational and cooperative aspects.

4. Best practices to deploy a resilience management system

Tracking the knowledge path to resilience: how to take effectively the "as is" picture of the Organization Designing the organizational change posture for resilience.

It's important to gather good quality picture of all relevant assets of the organization and to estimate the overall exposure to business risk.

Let's say that organizations are required to perform a complex and knowledge intensive task that largely influences the "to be" project in terms of quality of results and effectiveness of the overall change effort. Specific knowledge management approach and techniques within organizations are available to face such a complex task.

From an operational point of view specific roles and responsibilities are a preliminary step along this path to use general or sector specific techniques. Strongly recommended here all the instruments and techniques referred to the "learning organization" approach and related collaborative tools and techniques.

How to create and communicate a Resilience Intent Statement?

The presence of an "intent statement" is helpful to clearly make people aware of the targeted objective and direct their emotional, physical and intellectual resources to the objective.

Intent should be composed by at least by three statement: the indication of the purpose, the description the overall approach intended to be adopted (the "doing how") and the desired end state.

An intent statement in "enacted" from the highest level of the organization and his function is to make clear and to commit all people of the organizations on the targeted objectives and the related expected behavior to be adopted.

The statement strongly upheld by top and diffused to all the organization must became the "motto" of every internal and external initiative to strengthen organizational resilience.

This approach has the twofold objective to make aware all the organization about the importance of the resilience and to definitely anchor the decision-making centers to the objective.

Creating a sound Resilience Policy

We suggest drafting a General Resilience Policy in which the organization recalls and details from the intent statement the main objectives, the methodology adopted by the organization to set up the resilience management system, the organization levels committed, the resources to be allocated, the expected results, and the envisaged control process.

Issue-specific policies will follow to grant details on the above mentioned topics or, if requested by the characteristics of the organization, or by sector-specific requirements, to provide a fine grain description of specific processes or sub-processes.

Building up an organization for Resilience and the "backpack of competences"

A definition of general and specific responsibilities for resilience needs to be allocated within the organization. This is not an "a priori" task but it's the results of the process flow design as provided by the resilience management system.

The responsibilities identified in the activity and process description need to be allocated to specific individuals and organizational units that take the commitment to carry out the envisaged assignments.

The ability to perform the related specific task needs a twofold set of competences: the knowledge of the process in which the subject is involved and the task-specific competence.

According to this requirement organization must provide an accurate "competence model" identifying a detailed competence/role matrix in order to set out the right competence "backpack" for individuals and providing specific programs for the related ongoing training.

5. Conclusion

Specific experience is needed to put in place a Resilience Management System. The design and the implementation approach although is strongly advisable to follow in any case the main steps of the overall model here introduced, largely depends on the characteristics of the organization such as the sector of operations, the size, the criticality of the business process and objectives; moreover internal factors (i.e. culture, characteristics of work processes, etc.) such as external factors (environmental, socio-political context, etc.) **[6].**

It follows that who has the burden to design and implement the system should pay particular attention to fit the system to the specific organization. Here we provide some tips and advice in order to achieve the goal of placing the system under control, whatever the level of specify and/or complexity to deal with.

The operation of the system is the moment of truth: the intent statement must be accomplished, the general and specific policies need to be properly enforced end the targeted results must be achieved.

Since treating resilience everything goes well until organizations experiment a real the problem, it’s really important never let your guard down and keep the focus on resilience always alive. Probably this is one of the toughest issue to manage to ensure resilience. Some basic practices will be here provided to set and maintain adequate levels of performance on this issue.

Measuring results and setting up a continuous improvement process for organization resilience - performance measurement is possible only if organization is capable to know and “read” what really happens inside itself. Several approaches are largely available on performance measurement and here we try to outline a specific one for resilience management.

Whatever the model adopted since the improvement is a step-by-step process, surveys on progress of the “maturity level” on resilience is recommended. Moreover, since resilience relates to mission critical objectives a “knowledge based” approach to performance analysis is also strongly recommended.

Literature:

[1] A. Boin and A. McConnell, “Preparing for critical infrastructure break- downs: the limits of crisis management and the need for resilience,” Journal of Contingencies and Crisis Management, vol. 15, no. 1, pp. 50–59, 2007;

[2] P. H. Longstaff, “Security, resilience, and communication in unpredictable environments such as terrorism, natural disasters, and complex technology,” Center for Information Policy Research, Harvard University, 2005;

[3] U. Rosenthal and B. Pijnenburg, Crisis management and decision making: simulation oriented scenarios. Springer, 1991, no. 1;

[4] Tim Prior, “Measuring Critical Infrastructure Resilience: Possible Indicators”, Risk and Resilience Research Group, Center for Security Studies (CSS), ETH, Zurich, 2015

[5] Birkmann J. “Risk and vulnerability indicators at different scales. Applicability, usefulness and policy implications” Environmental Hazards, 2007; 7(1): 20 – 31.

[6] George H. Baker III, Ph.D., “A Vulnerability Assessment Methodology for Critical Infrastructure Facilities”, 05, 2007;