EUROPEAN RESILIENCE MANAGEMENT GUIDELINES

Project Title	RESOLUTE
Project number	653460
Deliverable number	D3.5
Version	
State	FINAL
Confidentially Level	PU
WP contributing to the Deliverable	WP3
Contractual Date of Delivery	M12 (30/04/2015)
Finally approved by coordinator	
Actual Date of Delivery	
Authors	E. Gaitanidou, E. Bellini, Pedro Ferreira
Email	lgait@certh.gr , emanuele.bellini@unifi.it , pedro.ferreira@ulusofona.pt
Affiliation	CERTH, UNIFI, COFAC
Contributors	M. Tsami, K.Kalogirou, A.Touliou, I. Symeonidis, A. Zamihos, A. Adamopoulou (CERTH), E. Bellini, C. Martelli, P. Nesi, S. Morelli, , R. Fanti (UNIFI), A. Grifoni (THALES), L. Coconea (SWARCO), G. Vannuccini. M. Viani (CDF), A. Deloukas (ATTIKO), A. Candelieri (CMR),P. Ferreira, A. Simoes (COFAC),J.P. Leuteritz (FhG)

funded by the Horizon 2020
Framework Programme of the European Union

WWW: www.resolute-eu.org
Email: infores@resolute-eu.org

EXECUTIVE SUMMARY

The aim of the European Resilience Management Guidelines (ERMG) is to support decision makers and Critical Infrastructure (CI) managers in a self-evaluated multilevel gap analysis for resilience improvement in respect to the state of affairs of the CI considered. To this end, the ERMG development has adopted a system perspective applying the Functional Resonance Analysis Method (FRAM) to model a generic CI and to identify which are desired functions and the related interdependencies that should be implemented in a CI to be resilient. Then for each function identified, the present document provides a number of recommendations on how to dampen function performance variability to continue to deliver the desired outcome under unexpected condition/event. The objective is to sustain the adaptive capacity of the system to continuously changing operational conditions (flexibility) and the continued and coherent pursuit of goals within their own timescales (rigidity/robustness). Please note that the guidelines have been designed taking into account that they will be accessed and used by multiple experts addressing each of them a single part of the guidelines according to their responsibility and role in the CI management, So that some of the redundancy which is present in the document is intentional to facile the direct reading of the sections.

The result is a corpus of guidelines grounded on sustained adaptability principle and applicable across the various types of CIs.

The document is composed of 4 Chapters and 2 Annexes.

In the Chapter 1, which is the introductory chapter the scope of the document is explained along with the main items constructing its content; the EU perspective of Critical Infrastructure, the need for creating these guidelines and the collaborative approach needed to achieve it.

Then, in Chapter 2 the theoretical background and framework of ERMG is analysed, presenting the methods and methodology used. This section is an advancement of the project Deliverable D3.4 Guidelines methodology already released. However, the final release of the ERMG due by the end of the project, will include only the content related to the guidelines.

In Chapter 3, the guidelines are presented in detail, covering all four resilience cornerstones: anticipate, monitor, respond, learn that are at the base of the sustained adaptability concept adopted in the RESOLUTE project. The guidelines are organised in functions and for each function a number of recommendation to dampen variability are provided. Such recommendations should be considered valuable for different kind of CIs

In Chapter 4, finally, discussion is included and conclusions are drawn.

The three Annexes contain (respectively): a) the functions' description on which the development of the guidelines has been based and, b) a first version of the glossary of relevant terms.

PROJECT CONTEXT

Workpackage	WP3: European Resilience Management Guidelines
Task	T3.3: ERMG Development
Dependencies	These guidelines influence the whole project work.

Contributors and Reviewers

Contributors	Reviewers
M. Tsami, K.Kalogirou, A.Touliou, I. Symeonidis, A. Zamihos, A. Adamopoulou (CERTH)	COFAC
E. Bellini, C. Martelli, P. Nesi, S. Morelli, , R. Fanti (UNIFI)	SWARCO
A. Grifoni (THALES)	
L. Coconea (SWARCO)	
G. Vannuccini. M. Viani (CDF)	
A. Deloukas (ATTIKO)	
A. Candelieri (CMR)	
P. Ferreira, A. Simoes (COFAC)	
J.P. Leuteritz (FhG)	

Version History

Version	Date	Authors	Sections Affected
01	15/3/2016	E. Gaitanidou	All
02- 15	20/3/2016 – 20/4/2016	Several iterations collecting and revising partners' input	All
16	08/05/2016	E. Bellini	All
17	11/05/2016	E. Bellini	All
18	13/05/2016	E. Gaitanidou	All
19	14/05/2016	E.Bellini	All
20	14/05/2016	E.Gaitanidou	All
30	16/05/2016	P. nesi	All

Copyright Statement – Restricted Content

This document does not represent the opinion of the European Community, and the European Community is not responsible for any use that might be made of its content.

This is a restricted deliverable that is provided to the RESOLUTE community ONLY. The distribution of this document to people outside the RESOLUTE consortium has to be authorized by the Coordinator ONLY.

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 Scope

The concept of critical infrastructure has been evolving during the past few decades. In the 1980s, concerns about aging public works led the governments to focus on infrastructures in the public sector, such as highways, roads, bridges, airports, public transport, water supply facilities, wastewater treatment facilities, and solid-waste and hazardous-waste services. In the 1990s, as a result of increased international terrorism, the concept of infrastructure was redefined in terms of national security. After 9/11, the number of “critical” infrastructure sectors and key assets, particularly in the USA, as listed in the National Infrastructure Protection Plan, was expanded to 17 (DHS, 2006).

These infrastructure sectors range from agriculture and food systems, health care facilities, national monuments and commercial facilities, to energy and water supply systems, chemical facilities, road infrastructures, emergency services, nuclear power plants, telecommunications and information technology systems, transportation systems, and a wide variety of other public facilities. The proliferation of critical-infrastructure sectors has added complexity to an already complex field. In order to simplify and effectively focus in a critical range of such systems, the concept of a “lifeline system” was developed. This concept aims to evaluate the performance of large, geographically distributed networks during earthquakes, hurricanes, and other hazardous natural events. Lifelines are grouped into six principal systems: electric power, gas and liquid fuels, telecommunications, transportation, waste disposal and water supply. What all of these systems have in common is that they are intimately linked with the economic well-being, security and social fabric of the communities they serve. Thinking about critical infrastructure through the subset of lifelines helps clarify features that are common to essential support systems and provides insights into the engineering challenges to improving the performance of large networks (O’Rourke, 2007).

The aim of RESOLUTE project Deliverable D3.5 is to produce a first version of the European Resilience Management Guidelines (ERMG), as a product of work performed within project Task T3.3. Following the project structure, these guidelines will be operationalized for the Urban Transport System (Deliverable D3.7) and tested in the pilots of WP5, in order to be finalized (taking into account the consequent findings of the project work) in Deliverable D3.6 and Deliverable D3.8, respectively.

The methodology for the production of ERMG has been primarily defined in Deliverable D3.4 and is further specified and elaborated here (see Chapter 2) following the findings of WP2 (Deliverables D2.1 and D2.2). The guidelines aim to provide an overview of the actions and tools necessary to provide effective resilience management for critical infrastructures. The guidelines are based on a system’s approach. Rather than focusing on the description and analysis of organisational structures, human and technology features, RESOLUTE project addresses operational dynamic factors, mainly by modelling the operation of critical infrastructures as a system of interdependent functions. This provides the means for the development of guidelines grounded on principles applicable across the various types of critical infrastructures. In this sense, the guidelines proposed can be considered as generic, but nevertheless, taking into account the existing national and international sectorial approaches and the specific trends in terms of interdependencies, which may result in different degrees of “system openness” or exposure to changes within operational context.

1.2 Critical Infrastructures - the EU perspective

According to the definition given by the EC, Critical Infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have significant negative impacts for the security of the EU and the well-being of its citizens.

From the above definition, it is made clear that the EC considers Critical Infrastructures, CI, as an area of major interest for the safety and security of the citizens of the EU territory and, as such, it deserves a special focus to what regards its optimal function, protection and risk avoidance/prevention. To this end, a series of official documents have been produced, mainly within the last decade, aiming to set the framework and define the rules for the safety and security management of European CI.

A first important step has been the adoption of the 2006 European Programme for Critical Infrastructure Protection (EPCIP) Communication, followed by the Directive 2008/114/EC on the identification and designation of European Critical Infrastructures.

The European Programme for Critical Infrastructure Protection (EPCIP) (EC, 2006) sets the overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU States and in all relevant sectors of economic activity. The programme addresses a variety of threats, from terrorism to criminal activities, natural disasters and other causes of accidents. In short, it seeks to provide an all-hazards cross-sectorial approach. The EPCIP is supported by regular exchanges of information between EU States in the frame of the CIP Contact Points meetings.

A key pillar of this programme is the 2008 Directive on European Critical Infrastructures (2008/114/EC). It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. This Directive follows a sectorial approach, applying only to the energy and transport sectors. It also requires from owners/operators of designated ECI to prepare Operator Security Plans (advanced business continuity plans) and nominate Security Liaison Officers (linking the owner/operator with the national authority responsible for critical infrastructure protection).

A comprehensive review of this Directive has been conducted in close cooperation with the Member States and stakeholders during 2012. The preliminary results of this review have been summarised in a Commission Staff Working Document (EC, 2012). Based on the results of this review and considering other elements of the current programme, the Commission adopted a 2013 Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection (EC, 2013). This sets out a revised and more practical implementation of activities under the three main work streams – prevention, preparedness and response. The new approach aims at building common tools and a common approach in the EU to critical infrastructure protection and resilience, taking better account of interdependencies.

To facilitate the above described approach, the Commission has also developed a Critical Infrastructure Warning Information Network (CIWIN) (EC, 2008), providing an internet-based multi-level system for exchanging critical infrastructure protection ideas, studies and good practices. The CIWIN portal, which has been up and running since mid-January 2013, also serves as a repository for CIP related information. Its overall scope is to raise awareness and contribute to the protection of critical infrastructure in Europe.

Last but not least, a European Reference Network for Critical Infrastructure Protection (ERN-CIP) has also been created by the Commission to foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities. Its role focuses in linking together existing European laboratories and facilities, in order to carry out critical infrastructure-related security experiments and test new technology, such as detection equipment.

1.3 The need for ERMG: European Resilience Management Guidelines

Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of disruptions on the society and citizens must be limited as far as possible, whilst increasing the ability to cope with growing operational pressures emanating from factors such as the scarcity and variability of resources.

The risk environment affecting critical infrastructure is complex and uncertain; threats, vulnerabilities, and consequences have all evolved over the last decade. For example, critical infrastructure that has long been subject to risks associated with physical threats and natural disasters is now increasingly exposed to cyber risks. This stems from growing integration of information and communications technologies with critical infrastructure operations and an adversary focus on exploiting potential cyber vulnerabilities. Figure 1 illustrates the evolving threats to critical infrastructure (NIPP, 2013).

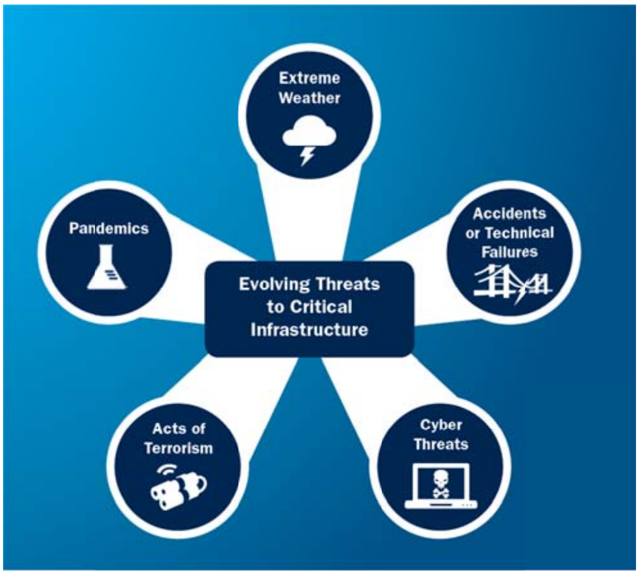
Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

Figure 1 Evolving threats to critical infrastructures

Knowledge about risks is currently quite extensive. As the OECD document on Resilience Systems Analysis (OECD, 2014) suggests, there are numerous risk analysis tools, indicating where and when conflict is likely, which areas are exposed to natural disasters, modelling how economic shocks and pandemics might spread, or how climate change will affect different communities and regions. What is actually missing is a vision of what to do about those risks; how to boost the resilience of individuals, households, communities and states to the risks they face every day. Where should time, skills and funds be invested to empower at-risk people, helping them to better absorb shocks, or adapt so that they become less exposed to shocks, or transform so that shocks no longer occur? (OECD, 2014)

The importance of Critical Infrastructure Resilience management is highlighted also by the fact that it is not only an EU but also a global priority. In many countries around the world, like the US, Australia, New Zealand, relevant initiatives are ongoing, for setting out the framework for the protection and enhancement of the resilience level of their National CIs.

Taking as an example the USA, the 5 National Priority Areas for NCISR R&D have been defined in the relevant plan issued in 2015 (NCISR R&D, 2015) as follows:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics.
- Develop integrated and scalable risk assessment and management approaches.
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure.

- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action.
- Build a crosscutting culture of CISR R&D collaboration.

As indicated in the Plan, Priority Areas A, B, C and D are intended to follow a logical progression from the creation of a usable system-of-systems perspective across the critical infrastructure sectors and the subsequent identification of complementary analytical approaches to risk assessment and risk management (Priority Area B). Risk management strategies can then be translated into capabilities (Priority Area C) that can be integrated (Priority Area D) in support of the foundational systems understanding described in Priority Area A. Priority Area E represents a core enabling activity to promote the partnerships necessary for the successful advancement of the other Priority Areas. The numbering convention within each Priority Area is provided as a means to organize and reference the specific examples of priorities and potential supporting activities. It does not represent a rank ordering of the items listed. (NCISR R&D, 2015)

From all the above, it is made clear that there is a gap in providing the Critical Infrastructure owners/managers with the necessary guidance that would allow them to organize and strengthen their facilities, personnel and any other kind of assets in an effective and standardized manner, in order to confront the continuously raising needs for resilience against any kind of risks.

This is the gap that the ERMG is striving to fill in, by suggesting guidelines for resilience management, focusing in the actual functions necessary for the effective operation of a critical infrastructure and given in a generic manner, so as to be applicable to and adaptable by any kind of critical infrastructure. For the needs of RESOLUTE, the ERMG is being adapted and operationalized for the Urban Transport System (in Deliverable D3.7 and through the tools of WP4) and tested in real life environments in the two RESOLUTE test sites (City of Florence and Athens Metro).

1.4 Recommendations at EU level

The approach of issuing resilience management guidelines in the present document is focused on how to manage resilience for a critical infrastructure as explained in Chapter 2.

However, the analysis has highlighted several issues that can be effectively tackled only at governmental and EU level, stemming from existing best practices worldwide. In fact in view of a coordinated resilience management throughout Critical Infrastructure at EU level and, most notably for the ones that have been recognised as European CIs, there should be an overall guidance from the EU for processes, response attitudes and progress in the area to be uniformly adapted and adequately adopted from the CI owners/operators.

Thus from the ERMG development experience emerges an opportunity of action at least in the following directions:

- Develop and promote a shared body of knowledge and a common understanding of resilience

Resilience is a complex and multifaceted concept that up to know, has been addressed from different perspective and disciplines generating a number of definitions, approaches and legal framework at any level of the society, from local up to EU and international level. Such fragmentation, along with the lack of a common understanding, prevents the development effective resilience strategies among all the interested actors. Moreover, due to the current cross-border interdependencies of the critical infrastructure at the EU level (see the Italian general blackout event of the 23 September 2003), a common definition of what resilience is and how it should be implemented and measured, becomes mandatory. The present document aims at supporting this political as well as methodological process of harmonization.

- Develop and continuously improve guidance materials and tools according to real needs, success/failure cases and technology advancement

This has mostly to do with compiling guidance material on resilience to assist critical infrastructure owners and operators and enhance their understanding of the resilience approach. This material shall contain practical information, tools, guides and references to other publications, as well as best/bad practices connected to event tracking and last scientific findings useful for resilience implementation. This Deliverable follows this direction, by involving public and private stakeholders in ERMG development and adopting an evidence-driven perspective supported by the latest developments in the fields of big data mining, network science, decision-support science, etc. Such an approach is now enabled by pervasive, ubiquitous and personalized technologies such as Internet of Things (IoT), smart devices (Bring Your Own Device –BYOD concept), mobile large band (LTE/4G), public free WiFi, etc.

- Raise awareness and preparedness for different stakeholders through resilience based training program

Apart from any training the Critical Infrastructure related stakeholders (employees, operators, local authorities, etc.) may undergo, there should be some common initiatives across EU able to involve and train citizens, which would set the minimum skill and awareness levels necessary for system resilience, while also providing relevant training tools. Such training material and tools, adaptable for operators as well as the general public and aiming to raise their preparedness and awareness, are among the products of RESOLUTE (e.g., Game base training app).

- Promote a socio- economical “value” perspective of resilience

While the concept and practice of resilience shall be promoted through the development of guidance materials, tools and training programs, a series of other initiatives need to be developed and implemented, in order to further promote resilience at different levels such as ethics, moral, economic, political, and so forth. For example, development and promotion of case studies that illustrate real life examples of the ‘*value proposition’* of resilience, or events shaped to explain resilience in terms of “*common good*”, whose advantages are beneficial for the EU society at large.

- Undertake specific research on resilience

The EU has already recognised the needs for deepening the understanding of organizational resilience as it specifically relates to the owners and operators of critical infrastructure. This is reflected in the European Commission’s research priorities within the first calls of Horizon 2020 such as DRS, DS and CIP. Such research should continue being encouraged by the EC, as the area of resilience and CI security in large is a critical one in the European territory.

2 RESILIENCE MANAGEMENT FRAMEWORK

The RESOLUTE ERMGs are built around the sustained adaptability concept and FRAM (Functional Resonance Analysis Method) approach. In this chapter, such a framework is introduced in order to familiarise the reader with the main drivers of the document.

2.1 Sustained Adaptability in Critical Infrastructure

The concept of sustained adaptability, specifically to what concerns Critical Infrastructure, is thoroughly discussed in Deliverable D2.2 (Conceptual Framework). Here, some basic features are mentioned for the better understanding of the context of the ERMG development.

System operation aspects become relevant, as by definition, resilience may only be perceived through system performance. Resilience is a system property that may or may not emerge from system operation (Deliverable D2.1). It relates to what a system "does", as opposed to what a system "has" or "is". This implies the identification of system performance characteristics, aiming to produce a set of requirements for indicators and monitoring tools as a fundamental support for management and decision making. Inline with the resilience engineering approach, the potential for resilience to emerge from system performance may be assessed based on the "four resilience cornerstones":

1. **Knowing what to do** corresponds to the ability to address the "**actual**" and respond to regular or irregular disruptions by adjusting functioning to existing conditions.
2. **Knowing what to look for** corresponds to the ability to address the "**critical**" by monitoring both the system and the environment for what could become a threat in the immediate time frame.
3. **Knowing what to expect** corresponds to the ability to address the "**potential**" longer term threats, anticipate opportunities for changes in the system and identify sources of disruption and pressure and their consequences for system operation.
4. **Knowing what has happened** corresponds to the ability to address the "**factual**" by learning from experiences of both successes and failures.

From this perspective, operational evidence (indicators and monitoring tools) should demonstrate that these four cornerstones are suitably embedded at all relevant system levels and contexts. Relating resources and adaptive capacities with the development of these four cornerstones will then support the production of the Resilience Analysis Grid (RAG). Thus, ***resilience focuses on sustaining the capacity for a system to adapt in the presence of continuous change***. Adaptive capacities are related to the level of resources that a system can allocate and its ability to manage these resources in view of specific adaptive cycles, described based on the four stages of event management cycle that a system needs to maintain, in order to be resilient (Deliverable D2.1 State of Art Review, 2015):

- **Plan/Prepare:** Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack)
- **Absorb:** Maintain most critical asset function and service availability while repelling or isolating the disruption.
- **Recover:** Restore all asset function and service availability to their pre-event functionality
- **Adapt:** Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient.

Like resources, also capacities for adaptability are inherently scarce. Thus, the variability that a system can cope with is bounded by consequent limitations. System resilience then, expresses the ability to understand and monitor resources and the capacities that they provide, towards coping with both expected and unexpected amplitudes of performance variability.

2.2 Functional Resonance Analysis Method

The Functional Resonance Analysis Method (FRAM; Hollnagel, 2004) describes system failures (adverse events) as the outcome of a functional resonance arising from the variability of normal performance. The method refers to a model or a representation of individual and/or organisational functions, where the characteristics of each function provide the basis for describing its potential variability. The emphasis is mostly on dynamic dependencies rather than on failure probabilities. The couplings among functions are described in terms of six dependency relations (input, output, time, control, pre-conditions, and resources) and are potential rather than actual, i.e., there are no pre-defined cause-effect relations. The dependency relations can be used to determine whether it is possible for two functions to become coupled, depending on the performance conditions. In this way, it is possible to identify both intended and unintended couplings. In case of risk assessment, this approach can be used to explain how coincidences may arise from performance variability, hence to identify the potential risks in a given situation. FRAM is originally ruled by four basic principles:

- **First principle**: The equivalence of success and failures
- **Second principle**: The inevitability of approximate adjustments
- **Third principle**: Consequences are emergent
- **Fourth principle**: Functional resonance

In its implementation, the method comprises the following five steps.

1. The first step is the **definition of the purpose** of the analysis since FRAM has been developed to be used for both accident investigation (past events) and safety assessment (future events).
2. The second step is the **identification and description of system functions**. A function, in FRAM terms, constitutes an activity which has important or necessary consequences for the state or properties of another action.
3. The third step is the **assessment and evaluation of the potential variability** for each function. The proposed methodology uses an a priori assessment of a set of Common Conditions (CCs) that have an influence on the function's performance variability, as described by (Hollnagel, 1998).
4. Step four is the **identification of functional resonance**. The aim of this step is to determine the possible ways in which the variability from one function could spread in the system and how it may combine with the variability of other functions.
5. The fifth and last step in a FRAM analysis is the **identification of effective countermeasures** to be introduced in the system. Such measures include those that keep the system in a safe state, as well as measures that can sustain or amplify functional resonance that leads to desired or improved outcomes.

RESOLUTE focuses on the definition of guidelines for critical infrastructure as whole, which requires a broad scope system analysis. FRAM was mainly developed around the modelling of specific (and "real work") system's operation. Despite this, FRAM was considered useful to RESOLUTE purposes, mainly for its approach to the identification and understanding of functional interdependencies. Hence, FRAM was here applied to develop a generic and "high level" system modelling. Within this scope, the six aspects of each identified function were described based on the expected operational requirements of each function, as opposed to aspects observed in "real" system operation.

2.2.1 Functions

The definition of functions is one of the most important aspects in FRAM modelling. Once the focus and level of the analysis have been determined, the system functions have to be identified. The overall rule is to try to achieve a description of the normal activities performed by the socio-technical system in focus. For the identification of the functions it is often useful to start from a task analysis, along with the contribution of the involved stakeholders. The process of function identification is essential to assure the quality of the resulting system modelling.

Following the function identification the safety assessment proceeds by characterising each function in terms of six aspects or parameters (Input, Output, Preconditions, Control, Time and Resources) (see Figure 2). Hollnagel (2004) defines the six parameters in the following terms:

1. Input (I): that which the function processes or transforms or that which starts the function,
2. Output (O): that which is the result of the function, either a specific output or product, or a state change,
3. Preconditions (P): conditions that must be exist before a function can be executed,
4. Resources (R): that which the function needs or consumes to produce the output,
5. Time (T): temporal constraints affecting the function (with regard to starting time, finishing time, or duration), and
6. Control (C): how the function is monitored or controlled.

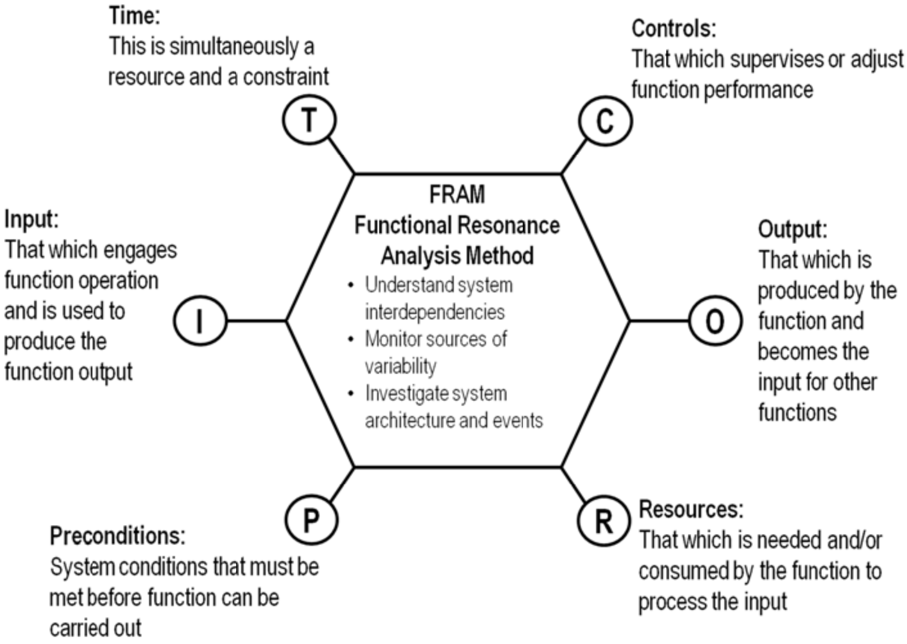
Time:
This is simultaneously a resource and a constraint
T
Controls:
That which supervises or adjust function performance
C
FRAM
Functional Resonance Analysis Method
• Understand system interdependencies
• Monitor sources of variability
• Investigate system architecture and events
Input:
That which engages function operation and is used to produce the function output
I
Output:
That which is produced by the function and becomes the input for other functions
O
P
Preconditions:
System conditions that must be met before function can be carried out
R
Resources:
That which is needed and/or consumed by the function to process the input

Figure 2: FRAM Function representation

The description of each function is made by using a simple table format, which then becomes the basis for the further analysis. It is also this description, rather than the graphical representation, that constitutes the FRAM model. It is indeed very important not to confuse the FRAM model with the graphical representation of FRAM. The representation is typically in the form of a diagram showing functions as hexagons and the connections between them as lines. The characterisation of the functions, in terms of the six aspects, contains the potential couplings among functions (see Annex I).

2.2.2 Performance Variability

The performance variability, i.e. the range of result in a function’s or an overall system’s performance, is highly dependent on the variability of the conditions under which the system/function is performing. This is also depicted in FRAM. Performance variability is on the whole considered as a strength rather than a liability and is the primary reason why sociotechnical systems work as well as they do – or work at all. The human ability to find effective ways of overcoming problems at work is therefore crucial for safety.

According to the same source, the six main sources of human and organisational performance variability are:

1. Fundamental human physiological and/or psychological characteristics. Examples are fatigue, circadian rhythm, vigilance and attention, refractory periods, forgetting, associations, etc.
2. Pervasive higher level psychological phenomena such as ingenuity, creativity, and adaptability, for instance in overcoming temporal constraints and under-specification.
3. Organisational conditions and requirements, as the need to meet external demands (quality, quantity), stretching resources, substituting goals, etc.
4. Social or team psychological factors, such as meeting expectations of oneself or of colleagues, complying with group working standards, etc.
5. Context variability (ambient working conditions), for instance if the working conditions are too hot, too noisy, too humid, etc.
6. Work environment variability induced by the unpredictability of the domain, e.g., weather conditions, number of flights, pilot variability, technical problems, etc.

2.2.3 Common Conditions

In order to evaluate the overall human performance variability, it is necessary first to consider each function in order to understand how likely it is to vary, and then to consider the interdependence of the functions. The effect of the context on performance is expressed by the Common Conditions. The set of proposed CCs is presented below.

- Availability of resources. Adequate resources are necessary for stable performance, and a lack of resources increases variability. The resources primarily comprise *personnel*, *equipment*, and *material*. Time is in principle also a resource, but since it has a very special nature, it is treated separately.
- Training and experience (competence). The *level* and *quality of training* together with the *operational experience*, determines how well prepared people are for various situations, hence how variable their performance will be.
- Quality of communication, both in terms of *timeliness* and *accuracy*. This refers both to the *technological aspects* (equipment, bandwidth) and the *human or social aspects*.
- HMI (human/machine interaction) and operational support. This refers to the human/machine interaction in general, including *interface design* and *various forms of operational support*.).
- Availability of procedures and plans. The *availability of procedures and plans* (operating and emergency procedures), and *routine patterns of response* affect the variability of performance. Operators use procedures and plans as the reference point for their routine activity. In case of an emergency, procedures are needed to support the response behaviour to degraded situations. In both cases the availability, quality and precision of procedures result in a different level of expected performance by operators.
- Conditions of work. The features of the working environment have an influence on the performance. An appropriate working environment may positively impact performance; on the other hand, inadequate working conditions may create constraints for work that result in a decrease of performance.
- Number of goals and conflict resolution. The *number of tasks* a person must normally attend to and the rules or principles (criteria) for conflict resolution.
- Available time and time pressure. The *time available to carry out a task* may depend on the synchronisation between task execution and process dynamics. Lack of time, even if subjective, is likely to decrease performance standard.
- Circadian rhythm and stress, i.e., whether or not a *person is adjusted to the current time*. Lack of sleep or asynchronism can seriously disrupt performance. The biological rhythm of human beings follows a cycle organised on the base of 24 hours. This cycle is maintained autonomously by the

human nervous system but can be affected by external factors such as the environment or socio-professional factors.

- Team collaboration quality. The *quality of the collaboration* among team members, including the overlap between the official and unofficial structure, *level of trust* and *general social climate*.
- Quality and support of the organisation. This comprises the quality of the *roles and responsibilities of team members, safety culture, safety management systems, instructions*, of *guidelines for externally oriented activities*, and the *role of external agencies*.

2.3 Measuring resilience

According to the OECD Guidelines for Resilience Systems Analysis (OECD, 2014) different types of indicators can be used to deepen the understanding of system resilience, and thereby help refine and modify plans, policies and programmes to boost resilience. Within the same guideline, these indicators are categorized as follows:

- System resilience indicators (outcome indicators) look at the resilience of the main components of the system over time, including how the overall well-being of people and the system is affected when shocks actually occur, for example how political capital is affected by an actual earthquake, or how social capital is affected by new or escalating conflict. These indicators should be complemented by negative resilience indicators.
- Negative resilience indicators look at whether people are using strategies to boost resilience that may have negative impacts on other areas of the system, for example turning to crime to deal with unemployment; or negative impacts on certain vulnerable people, for example by reducing the number of meals eaten a day, or taking children out of school.
- Process indicators ensure that the resilience roadmap is being used in policy making and programming.
- Output indicators show the results of implementing different parts of the resilience roadmap.
- Proxy impact indicators help show the results of resilience programming. These must be used with caution, but can be necessary when other more nuanced measures (such as system resilience indicators) are difficult to create, or difficult to communicate to a specific target audience.

2.3.1 Resilience Analysis Grid

The present guidelines are focused on the Resilience Analysis Grid (RAG). The RAG is mainly intended as a resilience measurement and monitoring tool. It focuses on determining the range and levels of adaptation of a system to its environment, and the adaptive capacities that it is capable of generating in view of both known and unknown operational pressures.

The RAG is foremost driven from the principle that no system is ever fully tuned or adapted to its environment. The reality is that, to a certain extent, any complex sociotechnical system is always out of tune with its environment and therefore, in addition to the need to be adapted to current operating conditions, the system must develop adaptive capacities. These adaptive capacities are essentially structured around the ability to “monitor” what is known to be a potential need for a change and to “anticipate” any possible unknown need for such a change. The recognition of the need for change requires the “ability to learn” from operational experience and feedback, and effectively place such learning into action at all system levels, thus supporting adaptive capacities. (Deliverable D2.2)

This is directly linked to the four cornerstones of resilience and allows assessing them in terms of human, technical or organisational aspects. This is highlighted in Table 1.

Table 1: Resilience Cornerstones correspondence to adaptive capacities

The four cornerstones	The adaptive capacities
Knowing what to expect	ANTICIPATE - look ahead for the potential
Knowing what to look for	MONITOR - pay attention
Knowing what to do	RESPOND - be effective
Knowing what has happened	LEARN - build an organisational memory

Within the scope of RESOLUTE, the use of this tool aims to produce an overview of a broad range of human, technical and organisational aspects regarding their contribution for system resilience. As clarified also in the RESOLUTE Conceptual Framework ?????ref?????, this does not aim to produce a measurement of resilience in itself, but rather depict the level at which a system may be prepared to adapt within various time scales (from current operation and short-term to long-term) to changes deemed possible in the operational environment, either as a threat or an opportunity for performance enhancement. This may be defined as assessing the potential for resilience. The RAG can be proposed as a monitoring tool to be integrated in the ERMG. **Errore. L'origine riferimento non è stata trovata.**3 shows an illustration for the potential system guidance that could be offered through the use of the RAG.

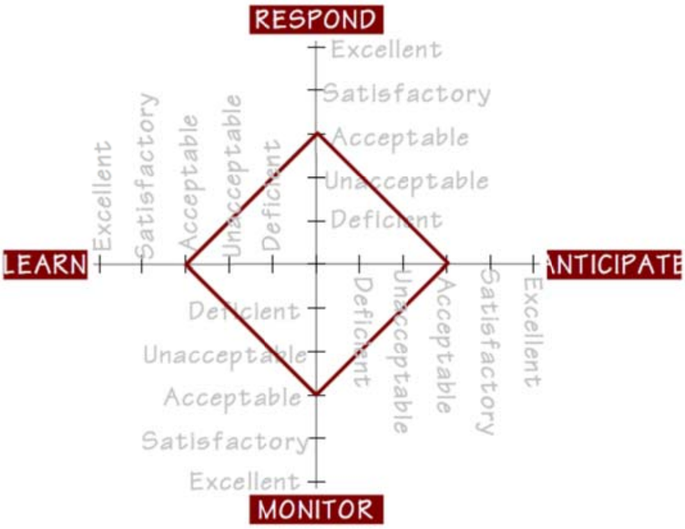

Figure 3: Illustration of the Resilience Analysis Grid (Hollnagel, 2009)

Regardless of this option, the fundamental contribution of this approach resides in the set of questions emerging from the assessment of the four resilience cornerstones in terms of the adaptive capacities, as defined in the RAG, as they set the ground for the work undertaken within WP3, regarding resilience at generic critical infrastructure level (Deliverable D3.5), as well as in the case of the Urban Transport System (Deliverable D3.7). In Deliverable D3.5, these questions have been cross-referenced to each of the defined functions, and are included in each function's emerging guideline template in Chapter 3.

2.4 Guidelines definition methodology

The methodology of guidelines definition has originally been described in Deliverable D3.4. However, having also in the meantime defined the RESOLUTE Framework in Deliverable D2.2, the methodology had to be refined, still following the same principles and step, but also including the tools and methods that are linked to and optimally used in the case of resilience management. These methods, theories and tools have been briefly described in the previous sections of this chapter and their application in terms of the work performed in Deliverable D3.5 is presented here.

2.4.1 Consensus driven approach

The development of European Resilience Management Guidelines constitutes a complex and multi-functional procedure, involving several different parties and stages of research, work, consultation, approval, operationalization, etc. Aiming to develop an operational, effective and applicable set of guidelines and, for the needs of the project, also specified and exemplified in the case of UTS, there is the need for a clear and concise methodology to be followed.

Within the methodology followed in RESOLUTE, as defined in Deliverable D3.4 Guidelines Methodology, and refined here, the overall strategy is to follow consensus-driven approach. This is achieved through the consensus-driven semantic harmonization of concepts, terminologies, metrics and indicators for risk identification, analysis and evaluation, hazards and impacts assessment, recovery performance, etc. through collecting risk scenarios from stakeholders (Government, NGOs, public, Critical Resilience Management Framework Infrastructure Providers, Civil protection, etc.) and establishing a reliable Open Process for ERMG review and acceptance.

Within this concept, a Stakeholders' Engagement Strategy has been adopted. This strategy is composed by 3 phases. The first two phases are addressed in the WP3 (T3.1) since the focus of the project is to develop the ERMG through a consensus driven process and while the third phase is addressed in the WP7:

Phase 1 ERMG Advisory Stakeholders Board: The first phase of the Stakeholders Engagement Strategy involves the formation of an high level ASB to be composed of senior stakeholder representatives, not just to monitor the compliance of the project to policies and standards, but to actively assess the ERMG definition and their evaluation though the pilots. The structure and function of the Board is designed to reflect and represent the diversity of the resilience constellations, legal frameworks and technological infrastructures underpinning different critical infrastructures, government regulations, which enable RESOLUTE to operate also towards market success.

Phase 2 User Forum: This phase involves mainly virtual or face-to-face periodical consultations with users/stakeholders representative of organizations that deal with resilience such as civil protections, first responders, volunteering associations, and the like. The purpose of this phase is to allow the project and its users to develop complimentary and mutually supportive perspectives on the core challenges facing the design and implementation of RESOLUTE user-centred services. Moreover, members of the User Forum will be involved in the RESOLUTE pilots. In particular will be engaged in the RESOLUTE Game based Training program.

Phase 3 High Visibility Events with the Stakeholder Community: The third phase of the strategy involves a series of high visibility workshops around the EU in order to enable stakeholders including EU members and Associated Countries' decision makers to participate and explain the strategic orientation and challenges of their respective organizations and exchange experiences with their counterparts from other organizations, as well as the wider scientific and research community involved in the domain; all under the project's guidance as to priorities and recommendations coming from RESOLUTE research in accordance with stakeholders' opinions.

2.4.2 Critical Infrastructure Functions definition: from Work-As-Done to Work-As Desired

The guidelines have been produced following the FRAM approach. The generic (sector-independent) FRAM diagram is illustrated in Figure 4. Please note that the model reported in Figure 4 representing the guidelines is also accessible as formal model, that can be edited by some FRAM editor.

According to the FRAM and Safety II (Hollnagel et al. 2013) approaches, the identification of the generic system functions originally followed the "Work as Done" rather than the "Work-As-Imagined" perspective. In fact, "Work-

As-Imagined" is an idealistic view of the formal task that disregards how task performance must be adjusted to match the constantly changing conditions of work and of the world. "Work-As-Imagined" describes what should happen under nominal working conditions. "Work-As-Done", on the other hand, describes what actually happens, how work unfolds over time in a concrete situation. Moreover, since "Work-As-Done", by definition, reflects the reality that people have to deal with, the unavoidable conclusion is that perceptions about Work-As-Imagined are inadequate, if not directly wrong. Today's work environments require looking at Work-As-Done rather than Work-As-Imagined, hence at systems that are real rather than ideal. When such systems perform reliably, it is because people are flexible and adaptive, rather than because the systems are perfectly thought out and designed. Humans are therefore no longer a liability and performance variability is not a threat. On the contrary, the variability of everyday performance is necessary for the system to function, and is the source of successes as well as of failures. Because successes and failures both depend on performance variability, failures cannot be prevented by eliminating it; in other words, safety cannot be managed by imposing constraints on normal work.

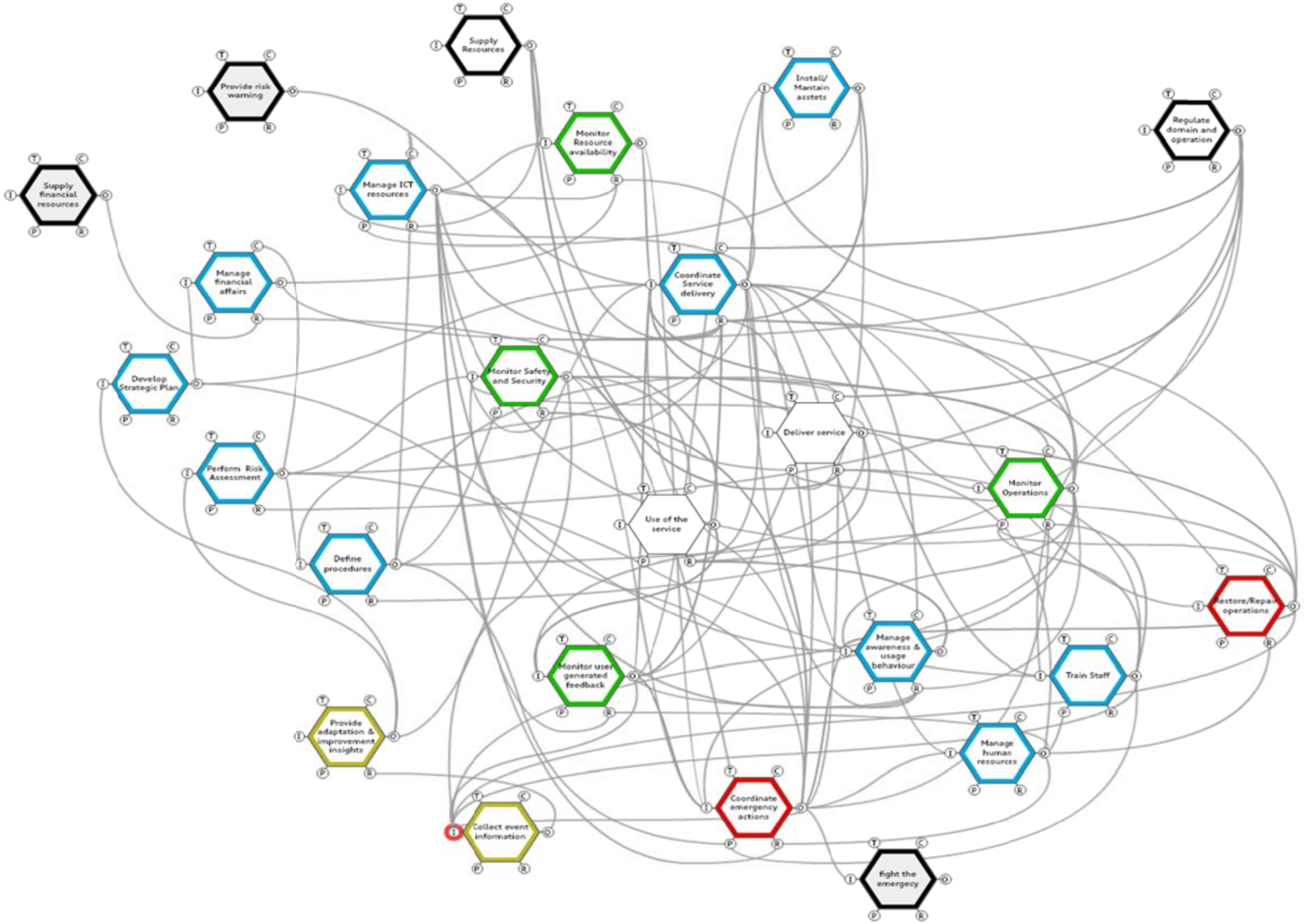
Supply Resources
Provide risk warning
Install/ Mantain asstets
Monitor Resource availability
Regulate domain and operation
Supply financial resources
Manage ICT resources
Manage financial affairs
Coordinate Service delivery
Develop Strategic Plan
Monitor Safety and Security
Deliver service
Perform Risk Assessment
Monitor Operations
Use of the service
Define procedures
Restore/Repair operations
Manage awareness & usage behaviour
Monitor user generated feedback
Train Staff
Provide adaptation & improvement insights
Manage human resources
Coordinate emergency actions
Collect event information
fight the emergecy

Figure 4: FRAM visualisation

However, the interesting thing from the guidelines perspective is to identify which functions are needed and how their interdependencies and variability should be managed to enhance resilience; and this requires going beyond the "Work-As-Done" level. Thus, the adopted perspective adopted is on focuses on functions and interdependencies that are **desired/recommendable** to enhance CI resilience, i.e. "Work-As-Desired". The following steps (see Figure 5) compose the "Work-As-Desired" system analysis:

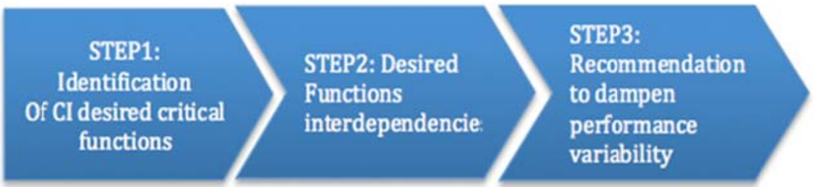
STEP1: Identification Of CI desired critical functions
STEP2: Desired Functions interdependencie
STEP3: Recommendation to dampen performance variability

Figure 5: "Work-As-Desired" steps

In order to accomplish the steps two main decisions should take to frame the system analysis:

a. definition of the system boundaries, and
b. definition of the level of granularity for the function identification and description.

In particular, the level of detail adopted and at which the variability of a function has an impact are critical decisions that may affect both the complexity and the value of the outcome. In the present document, the description of the functions remains at a high level in order to provide a better overview of the sector-independent system as a whole, since the main target audience are CI managers and decision makers that need to improve their system thinking.

2.4.2.1 Functions description

The functions description has been driven by a number of triggering questions. An example of such questions derived by (Clay-Williams et al, 2015) is reported in Table 2. The questions are mainly devoted to identify external relationship of the aspects with other functions.

Table 2: Questions guiding to Functions' Descriptions (source: Clay-Williams et al., 2015, adapted by RESOLUTE)

	Condition Guided question
Input	• What should start the function? • What should the function act on or change?
Output	• What should be the output or results of the function? • Do you should to inform anyone? • Do you have to collect or record/report anything? If so, where? • Who needs the output? Who will use what is produced?
Precondition	• What should be in place so that you can complete the function normally?
Resource	• What resources do you need to perform the function, such as people, equipment, IT, power, buildings, etc.?
Control	• Should be any formal procedures or instructions controlling the function? • Should be people, such as supervisors, controlling the function? • Should be there any priorities? • Should be there specific constraints?
Time	• Should be there any time related to the function? • Should be a certain time where you have to perform the function?

The iterative process of data collection and FRAM modelling resulted in the identification and description of 25 functions. The first sub-step has been addressed working with CI managers and experts, leveraging their local knowledge on how the activities "should be done". The second sub-step has been the definition and application of selection criteria on the identified functions. Since the ERMG should be applicable to any kind of CI, the focus was on selecting functions that different CIs have in common. For instance, a function like Monitoring Operation should be present in every type of CIs. As mentioned above, for the ERMG definition purposes the level of detail in the functions description is rather generic. The third sub-step has been the classification of each function according to each of the 4 adaptive capacities (Respond, Anticipate, Monitor, and Learn) according to its main contribution, supporting RAG-based analysis.

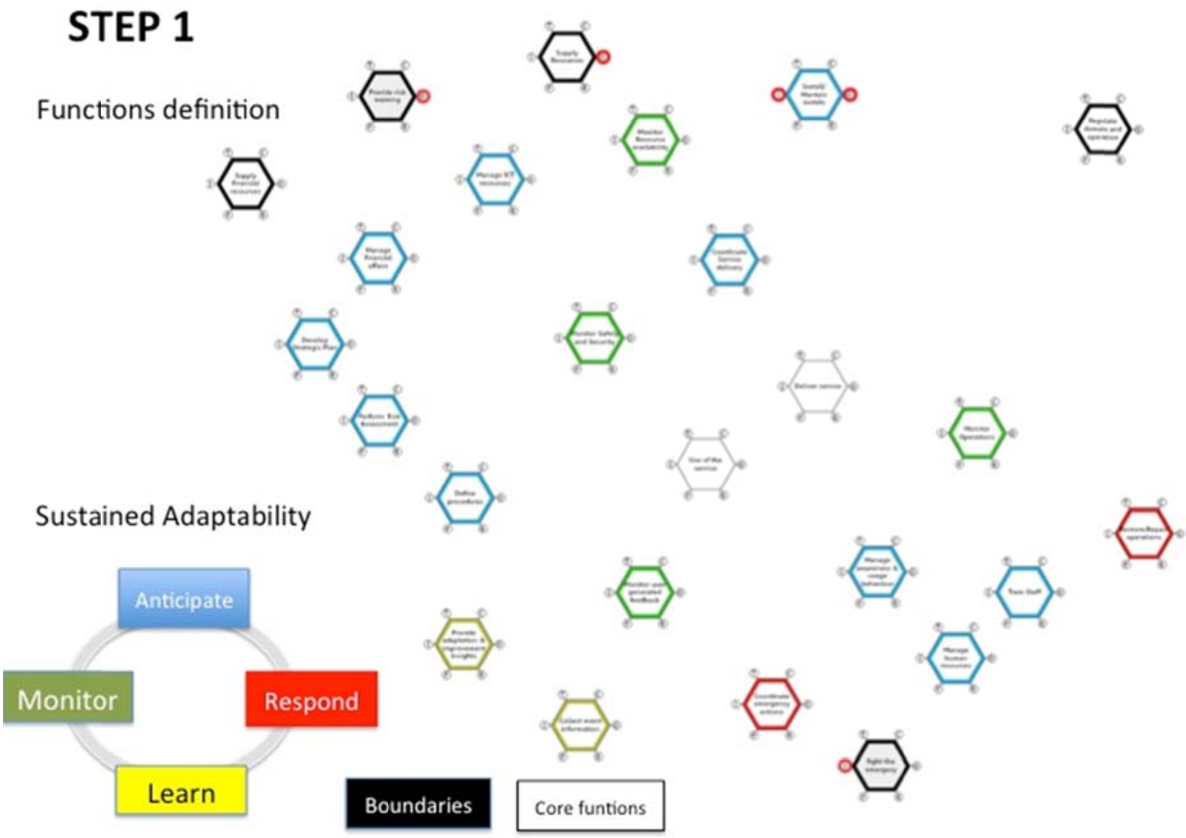

Figure 6: Functions representation in the FRAM diagram

In Figure 6, the functions are represented in different colours, each representing a different type or classification of function:

- White: System Core functions.
- Blue: functions sustaining Anticipate Capacity
- Green: functions sustaining Monitor capacity
- Red: functions sustaining Respond Capacity
- Yellow: functions sustaining Learn Capacity
- Black: Background functions

2.4.2.2 Core Functions

The core functions are the “object” (Table 3) of the system and dumping the Deliver service and Use of the Service variably is the actual goal of the resilience management. The connection between these two functions represents the first touch point between a CI and its users. Keeping the quality and the performance of the interaction among these two actors during adverse events is the end of the resilience. … ???....

Table 3: CI core functions.

CI Core functions	
Deliver service	The actual delivery of the service by the system. It contemplates how all stakeholders operate to make the service provided by a critical infrastructure available to the end-user.
Use of the Service	The actual usage of the service (roads usage) by users (e.g. drivers, citizens, bikers, etc.)

2.4.2.3 Desired functions

The CI desired critical functions (Table 4) are those functions that CI managers, operators, stakeholders and experts recognise as necessary/desired for enhancing CI resilience. Moreover, since the audience of the present guidelines are the CI in wide sense, the functions identified below, are domain-independent. This means that all of them should be present and working independently by the kind of CI assessed.

Table 4: CI desired critical functions.

Anticipate	
Develop Strategic Plan	Define the long term objectives and identify critical resource needs and allocation strategy. It also involves the definition of policies, according to which all stakeholders should be strategically aligned. This is expected to take place by policy makers, regulators and with the participation of key stakeholders
Manage financial affairs	Develop financial control and plan financial assets in accordance to financial needs of the operation and financial obligations. Often maintenance or renewal investments required by critical infrastructures greatly exceed the scope of legal ownership or responsibility of a given stakeholder. Managing such large scale projects requires detailed coordination amongst stakeholders and frequently the oversight of regulators, in particular for the oversight of financial responsibilities.
Perform Risk Assessment	Organisations carry out multiple risk assessment activities. Such activities tend to be developed within relatively limited scopes (i.e., specific tasks or projects, specific equipment…) and limited to a given domain of risk (i.e., safety, security, financial, environmental…). Assessment tools also tend to undermine risk factors that are not formally recognised and described in particular those emanating from beyond the formal boundaries of an organisation. This function should recognise the added value of integrating risk factors of diverse nature and of coordinating with multiple stakeholders, in particular along the supply chain of the service supplied by the critical infrastructure.
Coordinate Service delivery	The delivery of critical infrastructure services requires a thorough coordination amongst multiple stakeholders. Coordination activities should be carried out at various planning and operational stages of service delivery. This function contemplates operations related to decision-making and activities that directly aim at keeping service delivery aligned with the strategic plan and the overall level of service in terms of quality and safety.
Manage awareness & user behaviour	As providers of fundamental public services, critical infrastructures tend to be significantly exposed to individual and collective behaviours, in many cases not just of the service end-users, but also of the wider public. Recent technological developments, in particular in relation to ICTs, offer a great potential for the enhancement of interactions with the public and the use of this potential towards an increased effectiveness in managing and deploying operational adjustments to various relevant events and circumstances.
Develop/update procedures	The complete set of procedures forms a body of formal knowledge regarding management and operation requirements. They tend to reflect the structure of decision-making and production processes of a given organisation, so as to ensure coordination and shared understanding of operations and their goals. While this may be relatively well achieved at organisational level, amongst stakeholders of complex sociotechnical systems such as critical infrastructures, this is often very challenging. Procedures are essentially tools internal to organisations within the scope of the function here described, to the extent possible and in addition to safety and efficiency requirements, procedures should also reflect the need for synchronisation and coordination amongst stakeholders at various CI process stages and supply chain levels. This should follow from the scope of a regulator's initiative, down to an active cooperation amongst stakeholders.
Manage human resources	Managing human resources within an organisation involves dealing with multiple relations between in-house and sub-contracting staff. The contractual boundaries may often be misaligned with real operational demands, where tight and dynamic cooperation amongst team members is required, regardless of the fact that various stakeholders are likely to be formally involved. Beyond the management of staff contractual relations, rosters and other human related operational needs, this function takes into account the need to manage the dynamics of close operational cooperation amongst multiple stakeholders and the need to align such dynamic relations with the formally

	established and recognised responsibilities and accountability.
Training staff	In line with the principles previously outlined in relation the management of human resources, in addition to employee training needs, and their quality control, this function must also account for the need to provide and control the quality of training of staff that while working under other stakeholders, may operate on a more or less continuous basis with the premises of a given organisation such an infrastructure owner or manager. This relates to initiatives such as cross training and shared expertise programmes.
Manage ICT resources	Provide/maintain/update/develop/repair information and communication services to support critical infrastructure operation and management. Information systems may be owned and managed by a given organisation and may be strongly reliant on the operation and input from multiple stakeholders. ICT often gives shape to many interdependencies and the management of such resources should recognise this critical system role, namely by providing an overall system understanding of how these resources and made available and used by stakeholders in view of the overall service delivery (system operational purposes).
Maintain physical/cyber infrastructure	Maintenance activities require increasingly skilled and specialised staff and technical resources. Because their nature, maintenance services are often subcontracted and providers become stakeholders with tight couplings with operational requirements. In addition to the planning, delivery and testing of maintenance activities, this function also incorporates the need to continuously assess the integration between in-house and sub-contracted maintenance resources, in view of process and technology changes, and overall operational environment demands.
Monitor	
Monitor Safety and Security	Integrated risk management has been recognised as a potentially valuable approach and it has been proven to present many managerial and operational challenges. As two of the fundamental risk domains for the operation of all critical infrastructures, safety and security should be managed in the scope of an integrating function, aiming to maximise efficiency and effectiveness of assessment and control measures and to integrate multiple interdependent risk factors that emanate from both within and beyond organisational boundaries.
Monitor Operations	The monitoring of service delivery performance is often singly based on lagging indicators and stakeholders tend to each assess their performance in reference to internal targets to be met, which may not necessarily reflect overall needs of the service delivered at critical infrastructure level. This function envisages the development of shared performance assessment practices amongst critical infrastructure stakeholders, mainly by integrating stakeholders targets with overall service delivery needs. This becomes fundamental to generate overall system performance understanding.
Monitor Resource availability	Complex sociotechnical systems such as critical infrastructures rely on increasingly diversified and dynamic supply chains. This function focuses on generating an overall coordination of resource planning and deployment, taking into account the need to align multiple stakeholder needs with CI service delivery. This requires an understanding of resource flows and their main variability trends.
Monitor user generated feedback	Current technology provides the means to monitor service usage on a wide range of parameters and produce in real time fundamental support to the deployment of operational adjustments. This function deals with the need for an integrated approach to the assessment of user generated feedback, mainly by placing this data and information in the context of operational monitoring. This requires the coordinated action amongst multiple stakeholders under a shared framework.
Respond	
Coordinate emergency actions	The operation of critical infrastructures relies on the close cooperation amongst multiple stakeholders. Emergency response scenarios pose additional challenges, mainly by adding significant time pressure and high uncertainty (and therefore heightened risk) to this already complex operational environment. Coping with such challenges places even greater emphasis on the coordination needs and increased pressure on already limited resources. This function deals mainly with the requirements of an efficient distributed decision making process under emergency response scenarios, namely the availability of accurate and timely information and data, and coordinated action of multiple and diverse stakeholders, often under unplanned and unforeseen circumstances.
Restore/Repair operations	Restoring operational capacities after significant damages requires much more than the re-allocation of system resources, namely those foreseen under maintenance and renewals projects. Dedicated teams are normally put in place to design, plan and execute specific projects, which in the case of critical infrastructures, in addition to the need to maintain minimum operation capabilities, is also likely to require the containment of impacts on other interdependent infrastructures.
Learn	
Provide adaptation & improvement insights	With the scope of resilience, the operation of complex sociotechnical systems is challenged by two opposing needs: sustaining adaptive capacities to continuously changing operational conditions (flexibility) and the continued and coherent pursuit of goals within their own timescales (rigidity/robustness). For instance, Operation and production goals may be reassessed on an annual

	basis, while strategic goals may be addressed on a five year basis. Without compromising the consistency and feasibility of planned operations within each of those timescales, a given degree of flexibility must be ensured, in order to sustain the ability to respond to unforeseeable operational changes. This relates to aspects such as learning from ex-post event analysis, de-briefing, daily operations and providing insights for system capacities adaptation, Keeping operations record, Examining good practices, performing impact analysis of suggested actions, among others.
Collect event information	Collecting in house and external event data as good practices and/or historical data (archiving). From the perspective of resilience, this should not only address the occurrence of undesired events but most of all the understanding of factors that under highly variable circumstances become critical for achieving successful performance.

2.4.2.4 Background functions

The background functions (Table 5) identify the boundaries or the context of the system. In particular, the system boundaries have been identified with the functions that are out of a direct or indirect organization responsibilities and controls but that their variability can directly affect the success of the CI operations and service delivery. In FRAM, background functions provide support and means for the performance of the set of foreground functions. Therefore, the systemic approach adopted by the FRAM requires that both foreground and background functions are modelled with the same approach. The identification of the background functions is based on the consistency check of the model and starts from the descriptions of the foreground functions. In this manner it is ensured that all the relevant context-related aspects are considered, while unnecessary efforts in considering negligible factors are reduced (Oedewald et al., 2012).

Table 5: CI background functions.

Background Functions	
Supply Resources	This function provides all the resources need for organization and operations functioning (expect money) like energy. It is the input channel through with other critical infrastructures supply their services and goods but also through cascade effects are propagated from once CI to other.
Supply financial resources	It includes resources from bank, finance, investment funds etc.
Regulate domain and operation	It includes EU, national and local laws, safety regulation, standards, ordinance
Provide risk warning	This function basically covered by official authorities, provide messages regarding weather conditions, manifestations, security agencies, etc.

2.4.3 Desired Interdependencies definition

The Desired Interdependencies should be defined taking into account the Work-As-Done and the CI managers' and operators' knowledge and expectations. The interdependencies represent a source of functions' variability on one hand, and they also can be seen as an information exchange opportunity, able to enhance the sustained adaptability. According to this perspective, desired interdependencies are designed considering the risk-benefit trade-off and their actual capability to enhance the sustained adaptability of the system.

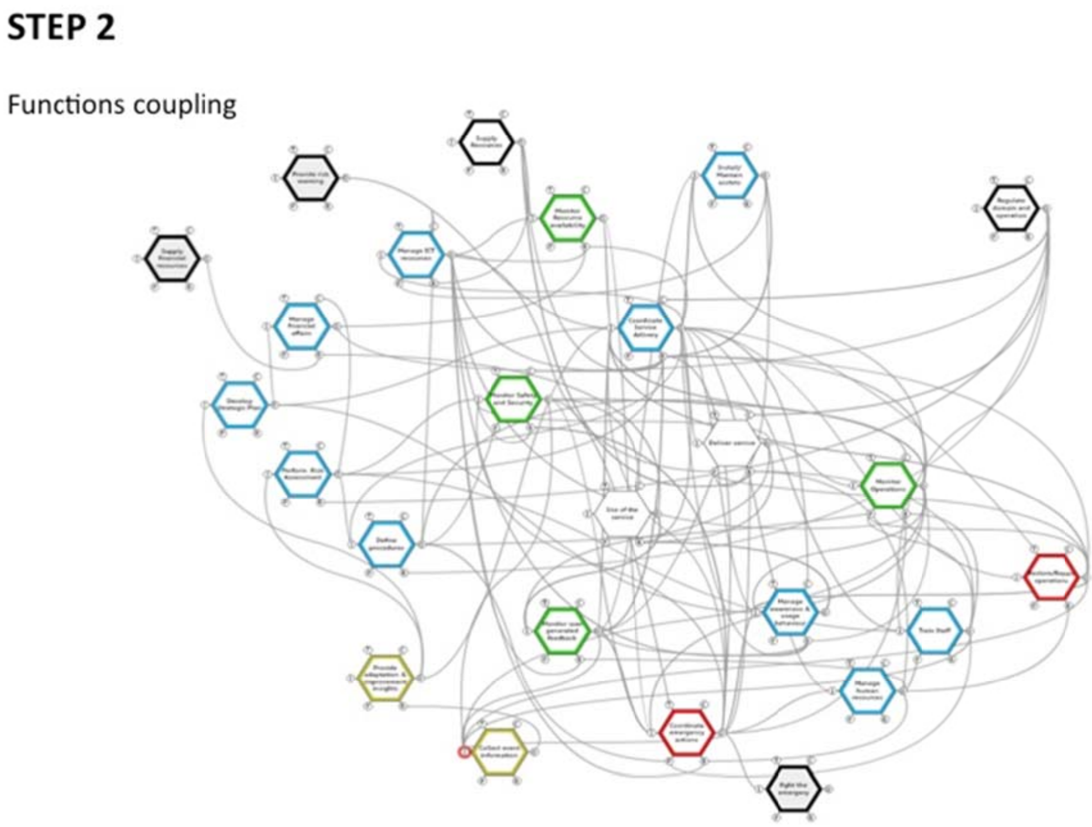

Figure 7: Functions coupling

2.4.4 Building ERMG: How to dampen functions variability and resonance

According to (Hollnagel et al, 2013) in order to evaluate the system performance variability, it is necessary first to consider each function in order to understand how likely it is to vary, and then consider the interdependencies of the functions. The methodology chosen to represent the effect of the context on performance makes use of the 11 common conditions (CC) (see Figure 8 and Table 6), as defined in (Hollnagel et al, 2013):

Thus the ERMG guidelines definition approach is aiming:

a) to provide a number of expert recommendations for each CC of each function to dampen the variability identified, taking into account:

- the "Work-As-Done" limits identified with the CI managers, operators and experts
- the possible failures mode of the function (Timing, Duration, Sequence, Object, Force, Direction, Speed, and Distance)

b) to provide a number of expert recommendations to dampen the variability considering the function interdependency.

The result is a corpus of precise guidelines related to each function's CC and interdependencies that can be easily translated into the field.

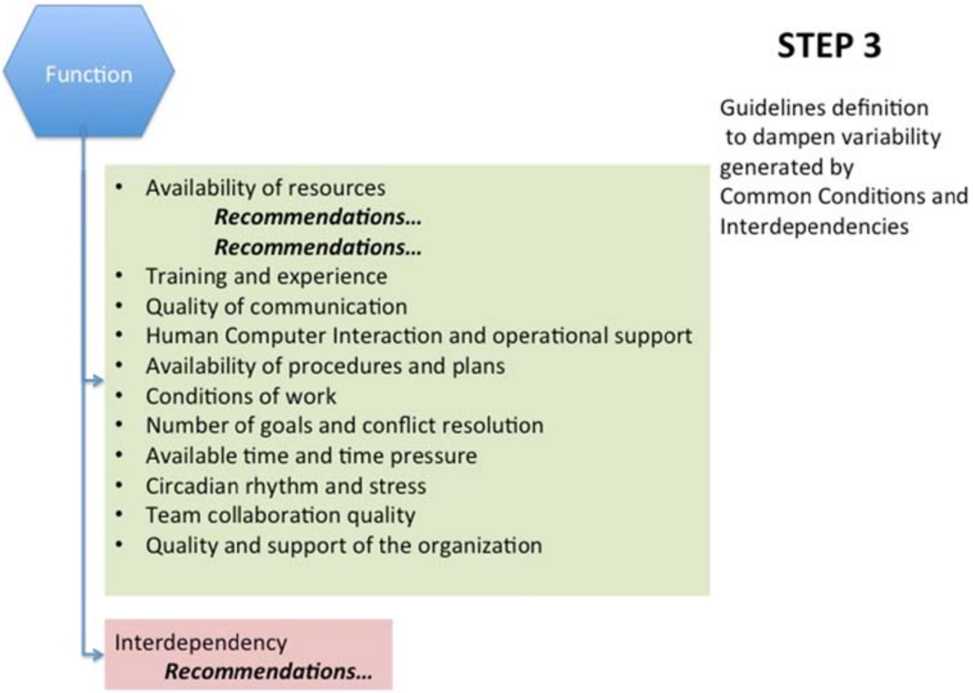
Function
STEP 3
Guidelines definition to dampen variability generated by Common Conditions and Interdependencies
Availability of resources
Recommendations…
Recommendations…
Training and experience
Quality of communication
Human Computer Interaction and operational support
Availability of procedures and plans
Conditions of work
Number of goals and conflict resolution
Available time and time pressure
Circadian rhythm and stress
Team collaboration quality
Quality and support of the organization
Interdependency
Recommendations…

Figure 8: Managing functions' variability

In the end, the CI managers, decision makers and all actors that need to assess the resilience of their own CI, can use the ERMG to evaluate the gap between their current practices, executing the 'Work-As-Done analysis (and then comparing the result with the Work-As-Desired defined in the present document. Such assessment is done through the RAG tool.

2.5 Cross-sector variability

The functional description was used to identify critical operational aspects; in particular interdependencies that support resource needs, and operational control and synchronisation requirements that ensure the capacities needed to continuously pursue operational goals. In order to facilitate the relation between the functional system description and the human, technical and organisational features that may give shape to critical infrastructures, the following matrix relates each of the CI sectors to the set of eleven performance conditions. These performance conditions are here described in terms of their variability and potential impacts in terms of uncertainty. The guidelines built around the functional system perspective are then related to this through the performance conditions. In this way, the intent is for the guidelines to provide support in coping with the identified variability and potential uncertainty. The matrix can be summarised as follows:

- Each raw represents the critical sectors as identified in the EU Directive (2008/114/EC) in order ground the guideline approach on concrete human, technical and organisational aspects;
- the columns represent the 11 common performance conditions (Hollnagel, 2005) linking each of the contexts to the contents of each function, thus relating to the system functional perspective on which the guidelines were produced.

Table 6: CI sectors - performance conditions analysis in terms of variability and uncertainty.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Energy	This sector tends to be reliant on international economic and political scenarios. It is significantly variable and unpredictable.	Strongly reliant on highly qualified professionals and expertise. Longlife training is required to update & improve expertise according to technological development.	Communications are critical but operations may withstand some variability in quality and availability. Timing is an important element for in the system operation.	Enhancement of automation flexibility facilitates operation but often intensifies interdependencies and complexity. Automation has prompt a considerable development in terms of centralised control, which renders these aspects evermore critical.	International standards and best practices are common. Political scrutiny and legal obligations tend to impose strong compliance regimes.	Shift work is frequent and in many cases under severe weather conditions. Risk of being exposed to dangerous goods and substances is frequent.	Product/service specifications tend to be relatively stable but operation tends to involve numerous stakeholders and different (often subcontracted) organisation, which may potentiate conflicting goals and needs.	Production pressures tend to be strong and highly variable according to market changes. While operation may be considerably tolerant to degraded modes, production failures are unacceptable and may rapidly produce serious impacts on other sectors.	This is a safety critical sector, with high potential for industrial and environmental disasters. Compliance with fundamental principles of safety such as the maximum limit of working hours and the abidance to safety procedures tends to be higher than in most sectors.	Team cohesion and coordination assumes a critical operational and safety role, namely when dealing with operational complexity and degraded modes.	Large scale organisations with diversified and international operations predominate. The scale and complexity of organisational hierarchical structures and of the decision-making processes they support tend to erode support to local needs.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Information, Communication & Technology	The required & updated communication technology, as well as its relevant contents & the timing for diffusion, display or broadcasting, are critical aspects to reach the targets. The availability of communication channels at any time is a major resource. All resources are variable requiring the identification of the variability sources to be managed. Hardware availability may not be critical but software is likely to generate much higher uncertainty and may become unavailable unexpectedly. Resources may be considerably dispersed geographically and organisationally.	Technological skills & communication qualities are required for operators. Social & Human science expertise is also required for the definition of information contents according to the target users and any other agents. Communication & information tools are important resources to create public awareness. High competences and skilss are required to reduce variability and manage uncertainty.	The quality of communication in terms of wording, clarity, accuracy and timing, is a major resource, particularly in emergency situations. Cooperation skills and leadership qualities are also required for the communication quality. High quality of communication reduces variability and uncertainty.	Human-centred design (HCD) of ICT will ensure appropriate conditions for safe, easy, comfortable & secure interactions towards successful human-computer dialogues. International standards & usability requests direct HCD in each context of use as a way to reduce variability and uncertainty.	international standards are regulating ICT procedures, including security access & management. More specific plans are defined by organisations from each context of use. The wide variability of plans & procedures is a reality to cope with.	In some sectors, conditions of work involve 24h schedules imposing night & shift work. Working in control rooms impose high attentional and visual demands, which require information sharing & frequent breaks to avoid fatigue and consequent errors. In this sector there is a wide variability of working conditions that should be reduced by following international standards and usability requests.	Being also a tool to be used in every sector or company, ICT use is internally regulated according to the defined goals. Thus, any conflicts can be managed internally based on communication qualities, regulations & leadership. The wide variability of procedures and plans requires leadership and specific skills for conflict resolution.	Timing is a critical aspect in ICT use, particularly in business competition & emergency situations. These conditions give rise to time pressure, which requires from operators, technicians & decision makers, high skills in stress management in order to avoid errors or other negative impact on production or service provision. Great variability and uncertainty are common features of the sector.	Circadian rhythm desynchrony is very critical for human performance as it leads to decrements in vigilance. Stress results from the negative balance of task demands, the perceived ability to cope with, and the importance of being successful. It is often related to time pressure. High workload results in an increase in subjective stress level. These three frequent features of working conditions lead to low performance conditions with short, medium and long-term effects giving rise to an unnecessary variability.	Team cohesion and coordination assumes a critical operational and safety role, namely when dealing with time pressure. This requires a judicious selection of personnel and high qualities of communication and leadership. The variability in team collaboration can have a negative impact on any system performance.	A variety of companies from every sector use and depend on ICT. Together with gains in time, accuracy and quality of production, the easiness of ICT can be reflected in the perception of a better support from the organisation although the complexity of organisational hierarchical structures and decision making processes.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Water	This is a vital sector reliant on national and often international natural resources together w/ human, technological and organisational support towards the production of high quality water and distribution. The high patterns of water quality impose high supervision and frequent quality control as a way to manage variability, whici is also influence by seasons and atmospheric conditions.	Strongly reliant on highly qualified personnel for the service production and distribution, together with emergency intervention on the urban infrastructure. Long-life training is also recommended to update and improve competences and skills.	Being the service supported by ICT, this is critical for both routine and emergency operations. This reflects the system variability, particularly the risk of disruption following extreme weather conditions, accidents or planned interventions on the urban infrastructure.	Work management, planning and water distribution impose high technology based work in many cases requiring some level of automation. This aspect increases complexity imposing continuous work in control room. This requires appropriate conditions for easy, comfortable and secure human-computer interactions.	International standards and best practices are followed in this sector together with legal obligations due to its criticality.	Shift work is frequent in some professional groups: those ensuring 24h supervision in critical areas, as well as those involved in emergency interventions. In many cases, these interventions are carried out at open air & under severe weather conditions, which increase the variability and uncertainty of the system.	Service specifications tend to be relatively stable but the participation of different municipalities from a region managing a natural resource may potentiate some conflicts. A good leadership and high competencies are required to avoid or manage some potential conflicts.	Production is continuous and relatively stable unless when a disruption occurs. Then, there is a time pressure for the required intervention to restore the service within the shortest delay. This creates a wide variability to the system and some uncertainty.	Due to the importance of this sector for life, different services are available 24h, imposing night & shift work to some operators. Thus, it is required compliance with fundamental safety principles regarding work schedules & shift work and respecting resting & sleeping times in order to avoid circadian rhythm desynchrony. Besides the variability of the system, human variability in terms of functional abilities and stress management require high concerns for work scheduling	Team cohesion and coordination assumes a critical operational and safety role, particularly when dealing with emergency interventions under time pressure & operational complexity. This requires a good leadership to promote cooperation and manage variability.	Organisations providing the water service depend on each municipality, which reduces the scale & complexity of the organisational hierarchical structure and the decision-making processes, thus easing the perception of support from the hierarchy.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Food	This is a vital sector involving production & distribution at different levels together with safety procedures regarding food quality & preservation. Hygiene, health & quality patterns imposed by national regulations require a wide variety of resources allocated to the production, distribution, commerce & consumption.	This sector involves different professions to ensure the whole process from production to consumption. Thus, training professionals involved in the different phases of the process and each specific domain (agriculture, livestock, food industry, inspection, transport, commerce, cooking & consumption) is a main request to ensure safety, hygiene & food quality.	The quality of communication in this sector in terms of specific vocabulary, clarity, accuracy & timing is a major resource. The lack of quality in communication can lead to errors or misses with negative impacts on safety/security.	The use of ICT in this sector is very diversified. Anyway, human-centred design principles allowing for easy, efficient and safe human-computer interactions should be followed.	International standards and best practices are followed in this sector together with safety & quality regulations regarding the final product and each phase of the process. Due to the number of stakeholders involved in each process, there is a huge variability a procedures and plans.	The food sector involves a diversity of working conditions, which are specific of each phase & specific domain. Most working conditions in the food sector involve night and shift work with the purpose of providing consumers with good quality & required quantity of food in due time. The variability of working conditions in the sector is huge.	The complexity and diversity of the food process involving so many stakeholders, has a potential for conflicts that can result from supplying delays or lower quality than expected. Within the same organisation, any potential conflict is easily managed but conflicts between different stakeholders are more difficult to be managed, which increases variability and uncertainty.	Timing is a very critical aspect in this sector due to its complexity and involvement of different stakeholders. Furthermore, as the distribution requires transport, delays are frequent and their effects on food preservation are critical. Thus, time pressure is very frequent in this sector and extremely variable in terms of process and distribution.	The process complexity resulting from the different phases & stakeholders impose 24h working and so, night & shift work to some actors. Thus, it is required compliance with fundamental safety principles regarding work schedules & shift work in order to avoid circadian rhythm desynchrony. This is particularly critical for the transport phase of the process increasing variability and uncertainty.	The process coordination & the cohesion of each team involved in the process assume a critical operational role, particularly in what concerns the right time from the first phase to the last one, thus ensuring the food quality & preservation.	The diversity of the organisations providing the final goods for consumption might have a small or medium size, which means a reduced scale & complexity of the organisational hierarchical structure & the decision-making processes. This aspect can ease the perception of support from the hierarchy within each organisation. However, in the whole process, this is not applicable due to the amount of organisations involved in the process.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Health	Health sector involves different subsectors (Medical & hospital care; Medicines, serums, vaccines & pharmaceuticals; Bio-laboratories & bio-agents), giving rise to a wide variability & requiring different resources (human, technological and organisational).	Strongly reliant on highly qualified professionals & expertise. The access to each profession and career is regulated imposing defined education & training requests. All services are directed to users' health and life, which imposes high competences and skills and leads to a wide variability & uncertainty depending on each case & contextual conditions.	The communication in this sector is a major issue in what concerns the communication between pairs, from a professional to a patient, or asking for assistance in an emergency. Thus, the communication quality in terms of specific vocabulary, clarity, accuracy & timing is a major request. Variability is high and the related uncertainty must be controlled with competence and commitment.	ICT is a very important resource in this sector. A wide variety of equipment is used in a daily basis and multiple situations. These new technologies are an important support to diagnosis, surgery, reanimation, etc. International standards & regulations direct HCD and each technology must be approved by health authority.	Being a very critical sector where human life is currently on stake, every act must comply with defined procedures. Planning is also in practice but the frequency of emergencies requires a strong organisation & cooperation together with the ability to manage the strong variability & uncertainty.	The Health sector imposes 24h work, which requires night & shift work. These schedules must take into account hours of continuous service and needs for breaks and rest in order to favour the best operational conditions of all actors. The risks of a non compliance with human factors related requests are very high and must be prevented.	The variety of goals, the required expertise to perform the tasks and useful time for it are factors of variability, uncertainty & complexity. There is a potential for conflicts but they are usually overcome by each actor's professional awareness of related risks.	Routine actions are carried out under a planned schedule. They are not supposed to generate time pressure but they do as a consequence of special needs of some patients & related procedures. Emergency situations involve time pressure and require the ability to decide and act in due time. The variability is huge and increase health related uncertainty.	The existence of 24h work with night and shift work creates conditions for sleep debt and gives rise to circadian rhythm desynchrony. As every actor in this sector must be in good conditions for the tasks performance, working schedules must be planned on the basis of human factors requests for the best performance. Human variability and the individual adaptation abiity to night and shift increase variability and uncertainty.	Team cohesion and coordination assumes a critical operational and safety role, particularly when dealing with high risk routine actions or emergency interventions, both under time pressure & operational complexity. This requires a good leadership to promote cooperation and manage variability and uncertainty.	The number of organisations from every sub-sector providing the defined service or product, as well as their size, is varied. Thus, the scale and complexity of each organisational hierarchical structure and decision-making processes can be different. So, the perception of support from the hierarchy will also be different and thus, variable.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Financial	This sector manages and generates economic resources (it relies itself on financial resources but in the same measure that any other sector does so). To that purpose, it relies most critically on information. Informational resources tend to be very diverse and highly variable. Sources and channels of communication also tend to be highly variable. The principle of the “black swan” is here very present: what one does not know tends to be more critical than what one does know.	Experience tends to assume a fundamental role, as this is a sector that greatly relies on contacts and decision-making. A continuous update, renewal and focus on such contacts tends to be critical.	Given the criticality of information to this sector, the quality of communication also tends to assume a fundamental role. Communication is in many cases driven by numerical data and assumes a relatively well standardised nature (structure and contents).	The use of computer systems is intensive, mainly for the analysis of data and frequently based on complex forecasting algorithms. Substantial resources tend to be devoted to the stability and updating of these computer systems. International standards and usability request must be followed in hardware and software design.	Procedurisation has been intensified, particularly in recent years. However, the high system complexity and dynamics, and the great number and diversity of stakeholders appears to raise considerable challenges for the development of suitable procedures and to planning.	Work tends to impose high variability in terms of pressure, working hours and objectives, among others.	High number and diversity of goals, amongst which, multiple and dynamic conflicts may emerge.	Time pressure tends to be significant and highly variable, with potential impacts on decision-making.	Irregular work hours tend to be frequent and under high levels of stress.	High levels of stress and pressure may erode team collaboration. Also, high performance and goal achievement tends to be highly rewarded, which may potentiate competitiveness amongst team members. Regardless, team collaboration and distributed decision-making tend to be valued.	Highly variable, as it tends to be exposed to multiple stakeholders and dynamic shifts in organisational strategies and goals.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Public & Legal Order & Safety	Extensive levels and diversity of resources to be managed. Despite this, the forecasting of resource needs and planning their allocation poses significant challenges and is normally considerably uncertain.	Highly skilled and specialised staff that must meet different levels of certified training. Refreshment training is also a requirement, which tends to control “excessive” variability of qualifications.	The coordination of multiple stakeholders and many different types of resources, particularly under emergency response scenarios, is strongly reliant on the availability of high quality communications. Communications must meet the needs of demanding and uncertain environments and the potential need to make decisions under significant time pressure.	Increased use of computer systems and automation, which may intensify interdependencies but also provides significant additional resources for coordination and synchronisation. Complex simulation software and decision support systems are well embedded into operations.	Strong presence of procedures at all levels of this sector. Abidance tends to be particularly critical for both operational and legal reasons and therefore, also strongly enforced.	Employment conditions tend to be stable. On-the-job conditions may be highly variable and unpredictable, and often may require exposure to significant hazards.	This tends to be minimised by clarity of roles and strong hierarchical engagement.	Frequent working under time pressure conditions, in particular in emergency response scenarios, where, in addition to time pressure, uncertainty also tends to increase.	Occupational stress is often a problem that requires psychological or even psychiatric follow-up. Working in a roster regime is also frequent	Role clarity is fundamental to ensure quality of synchronisation, both amongst team members and between stakeholders. Often collaboration under strict synchronisation may assume a life critical importance.	Strong public and political scrutiny, both on the organisations and their members. Cohesion and support amongst team members tends to be solid and with different characteristics, this may extend throughout the hierarchy of the organisation.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Civil Administration	Political & administrative services require a diversity of resources to develop the assigned civil service & enable organisations with the permanent ability to identify, anticipate, recognise and adapt to every crisis scenario coping with complexity, variability, uncertainty & system Vulnerabilities.	A variety of staff requests makes the sector more dynamic & complex than supposed to be. Thus, skilled & specialised staff with certified training enabling them to perceive, identify and manage risks & threats, are required to keep the system under normal operation. Life-long training is required for every staff to maintain awareness & risk perception and manage variability & uncertainty.	The variety of services regulated by the political power at national, regional or local level require coordination & communication meeting the service needs and requirements. The communication contents & quality are particularly important when dealing with critical situations & related variability, uncertainty & the potential need to make decisions under significant time pressure.	Increased use of computer based systems may increase interdependencies but also provides significant additional resources for communication & coordination. This requires human centred design & human factors concerns to ensure safe & efficient human computer interactions, particularly in critical situations & related variability, uncertainty & the potential need to make decisions under significant time pressure.	Being services in this sector very formal, they are strongly supported by procedures at all levels.	Conditions are likely to be very stable and supported by robust contractual relations.	Goals are likely to be numerous. They can be difficult to determine and with complex relations amongst themselves. Conflicts tend to be amongst many different goals and involving multiple stakeholders, which renders decision-making highly complex and potentially uncertain. Conflicts may emerge amongst team members, as views on issues may differ significantly.	Problems can often become complex and conflicts difficult to resolve. Issues are likely to linger as the search for viable or acceptable solutions may take unexpected periods of time. Issues may be deprioritised and placed on hold indefinitely.	Some services can be available around the clock, imposing night & shift work to operators. Most services follow regular schedules (9 to 5) sometimes imposing time pressure to accomplish tasks under the deadline. In any case, it is required compliance with fundamental safety principles regarding work schedules & shift work, respecting resting & sleeping times in order to avoid circadian rhythm desynchrony.	Team cohesion may be eroded by strong pressures. The more conflicts emerge amongst team members, the more team collaboration can be devalued and replaced by individual initiative, defensive behaviours or even self-promotion ones.	Public work contracts tend to offer stable and robust organisational support. Depending on the hierarchical level of public service administration, the effects of a higher state interest over public servants may be perceived and generate uncertainty. The perception of support from the organisational hierarchy is variable with the scale & complexity of each hierarchical structure & the decision-making processes.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Transport	Great importance for national & international economies. Requires different types of resources, which are significantly variable and sometimes unpredictable. New technological developments towards the autonomy of vehicles require significant improvement on technology together with appropriate regulations. Resources variability & transport dynamics increase complexity & uncertainty. Resource needs are significantly diverse and they also tend to be geographically dispersed and reliant on many different stakeholders, rendering their management and availability considerably more uncertain.	Strongly reliant on highly qualified personnel and expertise for all tasks performance within the transport domain. The quality of training, as well as its update & adaptation to a new reality towards automation is required. Long-life training for all professionals in the sector & users is also required.	Communications are very critical in this sector. Transport involves regulation & control, safety & security actions, private or shared ways, drivers, pilots, controllers or common users. All these elements of the transport system rely on communication & information. Autonomous vehicles tend to be more dependent on real time communication. ITSs provide the technology for all communication requests with the aim of improving safety & efficiency and increasing complexity & variability.	Nowadays driving or piloting, as well as most tasks in the Transport sector, involve human computer interactions. Safety and efficiency of these interactions require compliance of design, contents & conditions of use with international standards, usability requests & transport regulations. Human computer interactions in the transport sector are varied & subject to a wide variability related to each technology and its context of use.	Being a very critical sector where safety and security are major concerns, international standards & best practices are usually followed. Transport operators plan their activities and define procedures complying with safety, efficiency & security requests. As incidents, accidents or simply breakdowns occur, the transport sector requires a strong organisation & cooperation with other sectors to respond to sudden or emergency situations. These aspects give rise to a wide variability & uncertainty.	Night & shift work are frequent in the transport sector. Schedules and trip planning must comply with human factors related requests for the tasks performance in safe conditions. Driving or piloting vehicles or controlling traffic require continuous work focusing attention for long periods, which create conditions for drowsiness & loss of control. Breaks and the required sleep hours are the main request for operational conditions of every actor in this sector. The wide variability is also an issue to be considered.	Being a very complex and broad sector involving different stakeholders, the variety of goals is specific for each one but there are common purposes (safety, security & efficiency) although the existence of competition, particularly in the professional transport. Thus, there is some potential for conflicts in the frame of business competition. In the private transport (road) some conflicts occur that rely on unsafe attitudes & behaviour. Great variability of goals & conflict resolution.	The dynamics of transport and the business competition in the professional area have a potential for creating time pressure. Frequently, traffic jams give rise to time pressure leading to unsafe decisions. Transport operators are used to impose performance times thus creating time pressure and compromising safety. The variability is huge and its factors compromising safety must be identified to be controlled.	The transport sector involves activities around the clock. The existence of night and shift work creates conditions for sleep debt and gives rise to circadian rhythm desynchrony. As every actor in this sector must be in good conditions for the tasks performance, working schedules and trip planning must comply with regulations and human factors requests for the best performance.	Due to the features of the sector, it is desirable to establish cooperation and coordination of activities among stakeholders. At the level of each transport operator, team cohesion, cooperation and coordination of actions exist being important for operations goals. Concerning private transport (road), cooperation is required but not always practiced. All this reflects the great variability that is typical of the sector.	The sector involves companies of different size & transport modes. Thus, the scale & complexity of each organisational hierarchical structure and decision-making processes can be different. So, the perception of support from the hierarchy will also be different.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Chemical & Nuclear Industry	Resources tend to be secured through long-term contracts and relying on international economic/political commitments.	Most operations rely on highly skilled and competent staff. Enhanced process automation tends to promote some reduction of staffing, which in return may impose additional pressures on issues such the transfer of skills and expertise.	Informal communication tends to fulfil fundamental operational roles, often due to the specific nature and complexity of its contents. The attempt to formalise and standardise these communication practices may cause them to erode and reduce their effectiveness.	In view of the continuously growing presence of automation and the increased complexity of operation and safety control systems, these aspects assume an increasingly critical role. Interactions are rapidly becoming more diverse, dynamic and variable.	International standards and best practices are common. Political scrutiny and legal obligations tend to impose strong compliance regimes. This is particularly relevant for the nuclear industry, where public scrutiny also plays an important role.	Shift work is frequent and in many cases under severe weather conditions. Risk of being exposed to dangerous goods and substances is frequent.	Product/service specifications tend to vary according to market trends, namely variations in oil prices. Operation tends to involve numerous stakeholders and different (often subcontracted) organisations, which may potentiate conflicting goals and needs.	These sectors experience strong pressures during major maintenance halts (normally would take place every 5 to 8 years). Production pressures tend to be strong and highly variable according to market changes. This may not be so much on competitiveness issues but mostly on potential losses that may result from breaching delivery contracts. While operation may be considerably tolerant to degraded modes, production failures are unacceptable and may rapidly produce serious impacts.	These are safety critical sectors, with high potential for industrial and environmental disasters. Compliance with fundamental principles of safety such as the maximum limit of working hours and the abidance to safety procedures tend to be higher than in most sectors. Despite this, regarding maintenance staff, work pressures may be higher, also because they are normally subcontracted crews.	Team cohesion and coordination assumes a critical operational and safety role, namely when dealing with operational complexity of start-ups or halts of equipment and degraded modes.	Large scale organisations with diversified and international operations predominate. The scale and complexity of organisational hierarchical structures and of the decision-making processes they support tend to erode support to local needs.

	Resources availability	Training & Experience	Quality of Communication	Human Computer Interaction and operational support	Availability of procedures and plans	Conditions of work	Number of goals and conflict resolution	Available time and time pressure	Circadian rhythm and stress	Team collaboration quality	Quality and support of the organisation
Space & Research	The features & risks of the sector require enormous, highly specific resources and great expertise to ensure the continuous research & development, missions and related safety/security. The main feature of space research and missions is uncertainty, which together with the resources variability increase complexity.	Strongly reliant on highly qualified professionals & expertise. The access to each profession and career is regulated imposing defined education and training requests. All services are directed to projects and related missions, which lead to a wide variability & uncertainty depending on each case and contextual conditions.	Communications are very critical in this sector at all levels: research, including design, missions and control tasks, as well as analysis and reporting. All elements of this sector rely on communication and information following strict and formal procedures. The variability of communications in terms of nature and contents is huge.	High technology involved in Space Research and its continuous development require main concerns about human computer interactions. Safety & efficiency of these interactions require compliance of design, contents and conditions of use with human factors requests and expected and unexpected external conditions. Due to the uncertainty in this context, human-computer interactions are subject to a wide variability.	Very critical sector where safety and security are major concerns. The innovative features of this sector, sometimes out of previous experience, require long time research with experiments towards the required construction of knowledge to support plans, define procedures, direct training and make decisions. The wide variability is also an issue to be managed.	Working around the clock, sometimes orbiting the Earth in weightless environment, including times in the dark or light and various time zones, are hard working conditions that are common to astronauts. The remaining people work for the planned missions also on an around the clock basis. The wide variability is also an issue to be managed.	Very complex sector but centralised and subject to a strong leadership, rigorous discipline and regulated teamwork. Every work is directed to politically defined goals. Thus, there is no room for conflicts of goals or even conflicts among actors that could impact the work. In case of any identified potential for conflict, the excellent expertise and leadership are the keys for conflict resolution. Some variability occurs but, being a very closed and controlled system, there is no room for a great variability.	Time is critical in this sector. At a macroscopic level, projects and missions are developed along extended time, but, at a microscopic level, actions must be performed in due time or they will fail the objective. In these cases requiring the right action at the right time, time pressure is present at any time. Depending on the circumstances & the project evolution, time can be more or less critical. There is some variability but there are defined procedures for its control.	The referred working conditions give rise to circadian rhythm desynchrony. As every actor in this sector must be in excellent conditions for every task performance, working schedules must comply with human factors requests for the best performance. There is a wide variability in this sector in terms the diversity of projects and tasks, performance conditions and human resources.	Due to the features of the sector, cooperation and coordination of projects, as well as team cohesion, cooperation and coordination of actions, assume a critical operational and safety role, namely when dealing with operational complexity. Although the existing control, discipline and leadership, there is some variability.	The features of the sector and its inherent risks, the scale of the organisations, as well as their complexity, organisational hierarchical structure and the decision making processes, require permanent & high quality support to projects & their actors.

3 RESILIENCE MANAGEMENT GUIDELINES

3.1 Introduction

The section that follows provides a series of guidelines for Critical Infrastructures in order to enhance their level of resilience, according to the detailed methodology described in Chapter 2. Here, the main ERMG outcomes:

- Raise awareness on CI resilience
- Drive modifications in organisation and functions implementation
- Focus on resource availability and allocation as key factor for resilience
- Understanding the importance of (open/big) data generated by the system and "how-to" manage them to support the planning, preparing, absorbing, recovering and adapting resilience phases.
- Develop a culture of safety and of expecting unexpected
- Build an organizational knowledge of the past events and establish a cyclical learning process
- Inform and get informed all the stakeholders continuously
- Being Open to society
- Being Open to science and technologies

All these issues are tackled in the following sections, each within the framework of the corresponding function.

3.2 How to use the guidelines

The ERMG aims to support a **self-evaluated multilevel gap analysis** in respect to the state of affairs of CIs considered. The ERMG are structured to support the reader in the assessment as well as improvement of the CI of interest. In particular, three levels of analysis are identified and supported by the ERMG:

Level I: The first level of analysis can be carried out by the comparison between the "desired functions" defined in ERMG against the functions identified through a FRAM analysis of the CI under assessment. The absence of one or more functions immediately orients decision makers towards its implementation as applicable. This preliminary assessment is able to highlight relevant issues in the organization.

Level II: The second level of analysis is carried out by the assessment about how the functions implemented in the assessed CI are actually aligned with the ERMG recommendations. The readers should be able to understand if general as well as common conditions and recommendations are applied and at which level of detail. Moreover, indications and insights on how to improve the existing ones to manage the variability of functions' output can be retrieved by the document.

Level III: The third level of analysis is oriented to the function interdependencies assessment. The ERMG provides a number of desired interdependencies that are able to increase the system resilience. The missing connections between functions in the CI assessed may suggest that information or resources are not properly supplied or shared, creating vulnerability in the system. Moreover, a function that is coupled with another may be prevented from providing the expected outcome if the variability of the upstream function exceeds the capacity of the downstream function to manage it. Thus, in order to manage such functional resonance, the ERMG provides to readers recommendations about how to manage variability at function level coming from the upstream functions.

The synthesis of the gap analysis is obtained adopting the Resilience Analyses Grid tool.

At the end of the assessment, the reader will be more aware about the importance of the resilience thinking in CI domain, which is the status of the CIs analysed and what to do at operational, tactical and strategic level to increase the resilience of the system.

3.3 Guidelines structure

The guidelines are organised as follow:

- Section: Anticipate, Respond, Monitor, Learn: These are the 4 resilience cornerstones. The functions are grouped under the characteristic to which they mainly contribute.
- <<Name of the Function>>: The name of the system function identified during the FRAM based system analysis. The description of the function is reported in 2.4.2.3 section and in Annex 1.
- Background facts: The main rational behind the guidelines, the current issues and roles associated to the function are reported.
- General recommendations section includes recommendations related to the function's "should do" in terms of activities to sustain the system adaptive capacity.
- Common Conditions recommendations section provides recommendations about "how to dampen function performance variability" to continue to deliver the desired outcome under unexpected conditions/event. This part represents the real added value of the present document.
- Interdependencies recommendations section describes how the reported recommendations address a function to manage possible input variability generated by upstream functions within the system.

The boxes include:

- Abstract: a distilled summary of the guidelines is provided in order to quickly orient the reader.
- Questions: The questions provided aim at supporting the reader in assessing its own function. In fact they are questions that CI managers or decision makers should pose to themselves in order to verify the level of implementation of the guidelines in their own organization.
- Examples: A number of best practices related to each function are reported to improve understandability of the guidelines
- Resources: In this box relevant articles, standards, directives, etc. are listed, which have been used to justify the provided recommendations and for further technical and scientific investigations of the reader.

3.4 Anticipate

3.4.1 Develop Strategic Plan

Abstract

This guideline provides recommendation on how to integrate operational uncertainty into planning, mainly through the identification of potential adaptive capacity needs. The strategic planning is about resource allocation

Questions

- Are the roles and responsibilities clearly defined?
- How the strategic planning processes are defined, established and communicated?
- When a strategic plan is revised?
- How much effort is allocated on organizational strategic planning improvement?
- Are the stakeholders involved or consulted during the strategic plan definition?
- How the organization guarantees redundancy in decision making?
- How conflicting goals are managed in the strategy?
- Does planning take into account all resource needs and availability?
- Does the planning take into account past events and risk assessment results?
- How should the organization model, simulate and analyze the interactions within its Critical Infrastructure (CI) and other interconnected CIs
- Do you have a roadmap for actions and targets of your organization? What is the timeframe?

Background facts

Within this risk environment, our critical infrastructures are inherently interdependent — domestically and internationally — and vulnerable both within and across sectors due to the nature of their physical attributes, operational environments, international supply chains, and logical interconnections. From the perspective of system resilience, planning should establish and describe, according to various levels of detail (i.e. strategic, tactical and operational), what is considered successful performance. Strategic planning (at its different organisational levels) supports the definition and understanding of desired achievements, which should be aligned with system purposes (what the system is meant to produce and achieve). The understanding of resilience as sustained adaptability towards successful performance places considerable emphasis on planning and in particular the production of a strategic plan that supports a suitable allocation of resources at subsequent levels of planning and operation.

Strategic planning assumes a critical role in aligning technology and other operational assets with institutional mission and priorities.

Strategic planning involves a structure or framework, a set of procedures (both formal and informal), and of course content. Beyond these basic elements, the underlying assumptions about strategic planning are that the future can be anticipated, forecasted, managed or even controlled, and that the best way to do so is to have a formal and integrated plan about it in place. The process of planning itself may turn out to be more important than the results, and that process requires both analysis and synthesis. Planning simply introduces a formal “discipline” for conducting long-term thinking about an institution, and for recognizing opportunities in and for minimizing risks from the external and internal environments. The importance of risk analysis in association with planning relates to the need to understand and identify critical uncertainties regarding performance outcome. This may be referred to as a deliverability risk assessment and can be critical for establishing fundamental resilience related aspects such as buffer capacities.

General Recommendations

Align the organizations internal operations with achieving resilience through:

- *Attempting to gather board members and key employees together for planning.*
- *Establishing the overall goal for the alignment.*
- *Analysing which internal operations are most directly aligned with achieving that goal, and which are not.*
- *Establishing adaptive capacities goals to more effectively align operations to achieving the overall goal. Methods might include organizational performance management models, for example, Business Process Re-engineering or models of quality management, such as the TQM or ISO models.*
- *Incorporating a "flexible" decision making process that does not lock the company's future development into a rigid path, and rather constantly evolves to reflect updated knowledge to make the best possible decisions.*
- *Producing quantitative indicators in order to manage and check the strategic plan performance.*
- *Establish an effective business-government partnership with public administrations and critical infrastructure owners and operators.*
- *Establish a suitable alignment and sharing of strategic goals (adoption of the principles of collaborative planning) amongst stakeholders within critical infrastructure supply chain.*
- *Acknowledging existing legal acquis*
- *Developing strategies considering:*
  - *various contingency plans,*
  - *risk management program,*
  - *completion of a formal business impact analysis,*
  - *backup data centre establishment costs,*
  - *disaster activation costs,*
  - *support of the major equipment vendors,*
  - *insurance program.*
- *Adopting the Strategic Environment Assessment (SEA) as an effective tool for introducing climate change considerations into development and planning processes. The SEA provides a framework for assessing and managing a broad range of environmental risks which may contribute to the integration (or "mainstreaming") of climate change considerations into plans and programmes (P/Ps) that fall into the scope of the SEA Directive. The integration of climate*

Examples

Communication Company case study

In January 1997, water contaminated with rust was accidentally discharged from a gas suppression system into a $350m^2$ computer data centre (CDC). This affected $120 million worth of computing equipment spread across 180 computer cabinets housing 70 different computer systems running approximately 83 different applications. The water had been left in the heat exchanger and some associated piping after a hydrostatic test that was undertaken during the commissioning process in 1994.

This resulted in the formation of rust which was discharged into the room by the gaseous fire suppressant when the system was manually activated. The result was rusty water sprayed over and underneath all of the operating computer equipment in the CDC.

The equipment was still operational but required decontamination. This created significant risks of malfunction and breakdown, which would have had serious consequences for the company. The recovery was ultimately successful, taking 18 months to complete and costing in the order of $27 million. Despite this, the incident was not declared a disaster in terms of the Business Recovery Plan, and it was managed well enough so that it didn't cause any serious business disruption or revenue loss to the company. At the time of the incident the company only had the one CDC and the Business Recovery Plan was in draft form only Resilience)

For years the company had been working towards detailed recovery plans, the establishment of dual processing equipment for some computer applications, and the establishment of a disaster recovery site. The issue of data centres, the number of them, their size and location had been subject to frequent reviews since 1992, and in December 1995 a strategy of developing split data centres was established.

In deciding on the business recovery strategies the company considered factors such as the amount of money that would need to be expended initially, the amount of money that would need to be expended

> *change into strategic planning through the application of SEA should lead to better informed, evidence-based P/Ps that are more sustainable in the context of a changing climate, and more capable of delivering progress on human development(Intergovernmental Panel on Climate Change-IPCC).*

Decisions made during the early stages of an investment can have the greatest impact on the ultimate business outcome and the *success of the project. The strategic decisions are taken when a project is least well-defined but little information may be available as a basis for assessments. Despite this, it is essential for CI resilience that risks and uncertainties are considered in the analyses and decisions made at these stages.*

Given the information availability at this stage, high level vulnerability analysis and risk assessment as well as a **flexible attitude** *towards strategy adaptation to changed condition are* necessary.

Common Conditions Recommendation

1. Availability of resources

- Humans– skills/competence

- *All member of the organization should be involved in the process of policy and vision definition.*
- *Consult with the relevant stakeholders,*

in the event of a disaster, the availability of insurance, the availability of contingency plans, the testing of crisis management capability, and competency of management. (source Organizational Resilience)
This case is a good example of how resilience does not need to have an 'all bells and whistles' protectionist approach. Instead it illustrates how many different complementary strategies can come together within an enabling management culture to support the organisation through a period of disruption or loss. The company is still operating very successfully today using a similar mix of strategies.(source: www.organisationalresilience.gov.au)

Limitations

The guidelines do not seek to catalogue each available strategy, system or standard, whose adoption is a matter of choice of the strategy managers.

2. Training and experience

- *Consider all the content domains affected by the CI (all): subject matter experts,*
- *Project management skills and cooperation skills,*
- *Strategic planning, CSFs, and scenario planning all require expertise in the particular method. Expertise in the domain where the techniques will be applied (e.g. organizational strategy, information technology [IT] strategy, security management) is also advised,*

3. Quality of communication

- *Support efficient coordination and cooperation of both shareholders and (internal and external) experts,*
- *Guarantee the accuracy and understandability of the communication through standardized and accessible communication tools, protocols and languages.*

4. Human Computer Interaction and operational support

NA

5. Availability of procedures and plans

- *Planning business and organizational process that recognizes distributed decision making requirements*
- *Creating and communicating the strategic planning process within the organization*

- *Defining a strategic plan, coupled with review and maintenance of the strategy to ensure that they stay relevant over time*

6. Conditions of work

NA

7. Number of goals and conflict resolution

Planning teams should be built taking into account the scale and timeline of the plan and the dynamic of the issues aimed to be addressed (e.g. impact of changes in regulatory or business condition)

8. Available time and time pressure

Planning milestones and deadlines should integrate degrees of flexibility to cope with planning quality requirements

9. Circadian rhythm and stress

NA

10. Team collaboration quality

Adherence to the principles of collaborative planning through the development of mutual benefit relations

11. Quality and support of the organization

- *Clear decision making process and alignment of responsibility with accountability*
- *Establish a Public-Private Sector Partnership Framework to provide an excellent collaborative mechanism for improving infrastructure resilience*
- *Ensure senior sponsorship*
- *Financial capacity of each stakeholder and emergency unit should be included in the Strategic Plan including the level of financial involvement of each stakeholder*
- *Service delivery cost, replacement service (e.g. buses in case of subway unavailability) should be evaluated and included in Strategic Plan. In order to make this evaluation, time for full repair of system and full recovery should be known from involved stakeholders*

Sources

- SEI Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework Linda Parker Gates November 2010, TECHNICAL REPORT CMU/SEI-2010-TR-037 ESC-TR-2010-102
- National Infrastructure Advisory Council (NIAC) Critical Infrastructure Resilience Final Report and Recommendations 2009
- http://managementhelp.org/strategicplanning/models.htm#one
- BS65000 (2014) Guidance on organisational Resilience BSI Group
- ISO 22301:2012 Societal Security - Business Continuity Management Systems - Requirements. Geneva: ISO
- Organizational Resilience – Australian Government position paper
- ORGANISATIONAL RESILIENCE: The relationship with Risk related corporate strategies – Ernst &Young
- http://www.organisationalresilience.gov.au/resources/Pages/default.aspx

Interdependencies recommendations

In many sectors, planning often adopts a prescriptive approach and disregards many degrees of uncertainty and variability that affect operations. This is frequently compensated at various operational levels through local adjustments, which may jeopardise coordination needs. Interdependencies with various operation and management related functions should be maintained in order to both develop and integrate adaptive capacities into planning, and identify needs for the deployment of such capacities, including the need for planning revision.

In particular, according to the function analysis (Annex I) this function receives input from the adaptation and improvement function. If the related variability exceeds threshold of acceptance (e.g. the expected advice for improvement do not arrive in due time), the strategic planning should overcome such issues establishing and promoting an enabling management culture on self-protecting, so that appropriate adaptation action is undertaken.

3.4.2 Manage financial affairs

Abstract

The function aims at financially sustaining operational, maintenance and emergency and recovery requirements. It assumes a critical role for all stages of system life cycle (design, operation and decommissioning).

Background facts

Financial resources assume a critical role, not only for system operation, but also for the provision of any other resources and assets. States, regions and cities are largely responsible for arranging public services funding and management together with private companies. It is important to know in advance which are the state, regional, cities, and private resources available to fund the operation, its maintenance needs, and any recovery effort that may emerge from occurrences, and understand any eligibility or documentation requirements for obtaining such funding.

Financial affairs function is one of the prerequisites for any system current functioning and/or recovery as funds will be needed for managing full system recovery.

This function interacts with all involved shareholders (new income, market extension, protect from financial loss, etc.) as well as with market and socioeconomic trends (user needs, new products/services, economic situations) and financial adaptation.

The financing of the operation and up-keeping of critical infrastructures resorts to many different financial market mechanisms and products. The increasing uncertainty and variability of the financial sector (itself designated as a critical one) must be taken into account, in particular when forecasting fundamental operational capital needs.

This function is activated during normal operation as well as for emergency cases. In the latter case, it must be activated from the very beginning of the emergency, receiving requests from emergency teams and analysing priorities. It would be appropriate not to end this function before critical emergency is finished and full recovery is attained.

During current operation, financial data should always be available for analysis in order to improve current functioning. In the case of an emergency, after the end of operations and full system recovery, all financial data should be made available in order to allow for analysis and possible improvement for the future. Centralisation is particularly relevant for financial control monitoring and coordination. However, strong centralisation of financial management may lead to many operational obstacles and inefficiencies. Hence centralised control should be balanced with local decision making and coordination mechanisms.

Questions

– How often is the match between resources available and resource needs assessed?
– Does planning take into account all resource needs?
– Is there an appropriate insurance plan?
– How can measures that benefit other organizations / the society and that are not directly linked to everyday efficacy be (co-)financed?
– Is the match between resources available and resource needs assessed?
– Have you a priority rule to decide on the allocation of financial resources during the emergency?
– How do you measure performance? What kinds of indicators are used and how are they defined/classified/planned for revision?
– How are the “measurements” made? (qualitative, quantitative)
– When are the measurements made (continuously, regularly)?
– What are the delays between measurement and interpretation?

General recommendations

The aspects that should be targeted in managing financial affairs in order to increase resilience of a critical infrastructure can be summarised in the following:

- *Assess potential disaster impacts and negotiate insurance and re-insurance plans accordingly.*
- *Assess private disaster risk financing markets and financial sector resilience.*
- *Know and be able to use Governmental disaster risk financing tools.*
- *Identify disaster risk financing markets and institutional arrangements.*
- *Investigate government compensation and financial assistance arrangements.*
- *Ensure a fair and efficient deployment of funds.*
- *Develop financial control and plan financial assets in accordance to financial needs of the operation and financial obligations.*
- *Evaluate financial needs for emergency.*
- *Evaluate financial needs for complete system recovery.*
- *Analyse financial capacity of each involved stakeholder.*
- *Analyse capacity and financial resources possibly (at institutional level e.g. county, city, state…).*
- *Identify and analyse ways to obtain necessary funds in case of emergency.*
- *Plan budget reserve in case of emergency needs.*
- *Plan cost-sharing procedures between involved stakeholders.*
- *Manage over-payment situations if any.*
- *Revise financial needs regularly in accordance with system and operational environment changes.*
- *Staff with knowledge of financial resources should be involved at all resilience stages: Plan, Absorb, Recovery and Adapt to ensure that disaster assistance is effectively provided.*

OECD Methodological framework can be used to assess and finance risk, as shown in figure 9:

Examples

Infrastructure Australia: Urban Transport Strategy from Federal government of Australia

This report discusses the development of a strategy for a national framework for planning, financing and managing urban transport infrastructure. The strategy would target city planning, transport services and investment in road and rail infrastructure. It would complement national strategies for ports, airports and freight. The report raises issues relating to the development of a national urban transport infrastructure strategy and suggests key principles to guide its development, considered with reference to systems, economic, social, environmental and governance criteria.

A Pre-Event Recovery Planning Guide for Transportation, TRB report

NCHRP Report 753: A Pre-Event Recovery Planning Guide for Transportation (The Guide) provides an overview of what can be done to prepare for the recovery of transportation critical infrastructure. Principles and processes based on federal guidance, effective practices and lessons from case studies are provided to guide transportation owners and operators in their efforts to plan for recovery prior to the occurrence of an event that impacts transportation systems. Tools and resources are included to assist in both pre-planning for recovery and implementing recovery after an event. The Guide is intended to provide a single resource for understanding the principles and processes to be used for pre-event recovery planning for transportation infrastructure. In addition to the principles and processes, the Guide contains checklists, decision support tools, and resources to support pre-event recovery planning. The Guide will be of interest to transportation infrastructure owners/operators, transportation planners, and practitioners at the state and local levels.

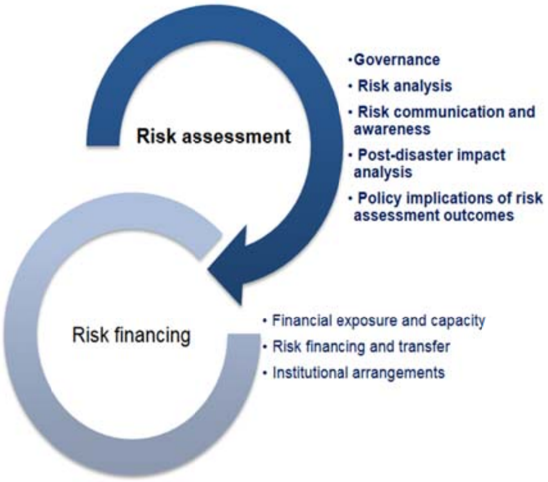
Risk assessment
•Governance
• Risk analysis
• Risk communication and awareness
• Post-disaster impact analysis
• Policy implications of risk assessment outcomes
Risk financing
• Financial exposure and capacity
• Risk financing and transfer
• Institutional arrangements

Figure 9: OECD Methodological framework

Queensland Government (2013). Queensland 2013 Flood Recovery Plan for the events of January– February 2013

This Queensland 2013 Flood Recovery Plan (for the events of January – February 2013) provides the framework to lead the recovery, encouraging all levels of government to work with industry and the community to rebuild stronger infrastructure than before and leave a permanent legacy of safety and resilience for the future.

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence

  - *Persons in charge of financial affairs for each department of the organization should be assigned.*
  - *One person to be named and able to decide for the entire operation and a secondment able to immediately overtake the operations in case of deficiency from the first one. Both not in the same place and reasonably far from crisis point in order to be kept safe for ruling operations.*

Limitations

- Possible limited financial resources of involved parties
- Possible resistance of involved parties to plan a budget reserve in advance

- Budget:

  - *Secure the availability of budget reserves for emergency cases reserving a proper amount of financial assets that be easily and quickly mobilised with a minimum loss.*
  - *Awareness of structures from which funds are available and how to recover them.*
  - *Budget allocation should be revised at least once a year in order to take into account all possible evolutions for each of the involved stakeholders. However establishing a mechanism for a dynamic and close to real time monitoring of the money flow during the emergency is necessary to support a proper resources allocation.*
  - *Financial Planning should allow an optimum matching between available and necessary resources requested to address the strategy plan. The matching between the two has to be taken into account during planning phase so that resources may be efficiently and readily deployed.*
  - *Each involved party has to calculate the necessary budget for recovery (emergency costs, repair costs etc.), communicate these costs to the monitoring party who will compile the information. Matching between necessary costs and available resources should be calculated in the strategic plan, taking into account resources available from each stakeholder but also from cities, regions, states, etc.*

- *Reserve funds control during and after the crisis management, in order to avoid overpayments needs. In any case funds should be ready to finance full recovery even if this means more payments than planned reserved.*
- *The allocation of supporting funds should be budgeted in relation to urban structure and relative risks. The portfolio should also have a wide margin of use because of the variability of each possible event in terms of typology, level of criticalities and extension.*

- Data & Algorithm:

  - *Use of project management concept and models to collect and monitor financial data.*
  - *Use data coming from all the systems collected to monitor and control the critical infrastructure during normal operation.*
  - *Reliability, Availability, Maintainability and Safety (RAMS) practices and algorithms for calculating the target thresholds according to the maintenance objectives.*
  - *Collection and close monitor of financial data during & after emergency operation.*
  - *Analyse data after operation in order to obtain re-usable data for the future.*

2. *Training and experience*

- *Training in terms of financial affairs, should be focused in the following areas:*

  - *Financial management skills.*
  - *Project management skills.*
  - *Cooperation skills.*
  - *Public security, operational head skills.*
  - *Crisis management (well trained and experienced personnel in this field should head the operations).*
  - *Current operation skills.*
  - *Adaptability & capacity to adapt current functioning to possible emergency needs.*

3. Quality of communication

- *Communicate available resources to involved stakeholders.*
- *Submit detailed information about the financial*

Sources

100 Resilience City http://www.100resilientcities.org

Action Plan on Urban Mobility – State of Play http://ec.europa.eu/transport/themes/urban/urban_mobility/doc/apum_state_of_play.pdf

A Pre-Event Recovery Planning Guide for Transportation, TRB report https://www.massport.com/media/266266/Report_A-Pre-Event-Recovery-Planning-Guide-for-Transportation-2013.pdf

Financial Protection Against Natural Disasters – World Bank report https://olc.worldbank.org/sites/default/files/Financial%20Protection%20Against%20Natural%20Disasters.pdf
Disaster Risk Financing in APEC Economieshttps://www.oecd.org/daf/fin/insurance/OECD_APEC_DisasterRiskFinancing.pdf

FEMA. (2011). *National disaster recovery framework: Strengthening disaster recovery for the nation.* https://www.fema.gov/pdf/recoveryframework/ndrf.pdf (Mar. 24, 2016)

Queensland Government (2013). Queensland 2013 Flood Recovery Plan for the events of January– February 2013. http://www.statedevelopment.qld.gov.au/resources/plan/local-government/lg-flood-recovery-plan.pdf

United States Department of Homeland Security. (2008). *National Response Framework*. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (Mar. 24, 2016)

Organizational resilience: the relation with risk related corporate strategies – Ernst&Yang report – Australian Government

Emergency Financial First Aid Kit (EFFAK) https://www.ready.gov/financial-preparedness *status and recovery plan to stakeholders in order to establish transparent relationships and get funds quickly.*

- *Establish quick and reliable communication with operational teams in order to manage funds availability and fair distribution until full recovery.*

4. Human Computer Interaction and operational support

- *Utilization of software tools to analyse financial data.*
- *Utilization of software tools to plan and monitor budget and resources availability.*
- *Utilisation of software tools to communicate with all function and allocate funds according to the plan and the emergency needs.*
- *Utilization of software tools to simulate and analyse the costs of business continuity interruption due to disrupted system and evaluate economic impact on the society.*

5. Availability of procedures and plans

- *Strategic financial plan in case or emergency ready.*
- *Operational plan ready.*
- *Fast availability of necessary resources.*

6. Conditions of work

- *Emergency work during crisis.*
- *Ability to know priorities for recovery after crisis in order to disseminate funds properly.*
- *Work in teams, able to immediately take over the current operations, in case of long recovery.*

7. Number of goals and conflict resolution

- *Conflicting objectives should be managed during the strategic plan phase, in order to define priorities order and allocate funds accordingly. This strategic plan should be agreed by all involved parties in order to avoid conflicts during the crisis management.*
- *Necessary to define priorities in order to stop possible conflict in advance.*
- *Define strategic plan and communicate it to involved parties so that they know where funds will go first and avoid conflict.*
- *Give decision power to experienced people in order to avoid conflicts.*

8. Available time and time pressure

- *During current operation, work is made under normal time pressure.*
- *In case of emergency, immediate response is needed in order to call for necessary funds as quickly as possible and be able to give appropriate answer to operational teams.*

9. Circadian rhythm and stress

NA

10. Team collaboration quality

- *Adherence to the principles of collaborative financial planning through the development of mutual benefit relations.*
- *Preliminary analysis of capacity in team working in order to avoid conflicts and conflicting payment orders.*

11. Quality and support of the organization

- *Clear decision making process and alignment of responsibility with accountability.*
- *Alignment of decisions with available resources.*
- *Alignment of decisions with defined priorities.*
- *Measurement of performance will be made after the emergency situation, in an early phase, in order to analyse used resources and remaining ones. Comparison should be made with what was planned in order to assess the validity of planning that was made and allow necessary adjustments to be made for future strategic plans. Second phase of analysis should be made after full recovery together with final used budget accounting. Financial reports have to be provided to each involved party and necessary adjustments have to be made in future plans based on final financial results. Deviations from initial planning should be analysed (why, how, how much) in order to better take them into account in future planning.*
- *Interpretation of financial results should be made immediately after full recovery in order to allow improving the strategic plan quickly and be ready in case of a new emergency situation*
- *Coordination between all stakeholders should be ensured by knowing in advance the financial capacity of each one of them and producing a financial plan accounting the level of financial involvement of each entity in case of emergency and recovery procedures.*
- *Cost of emergency action and cost of CI full recovery should be evaluated in advance and financial planning should take this evaluation into account.*
- *Constant monitoring of financial resources (incomes, expenses, financial involvement of each involved party) should be conducted during and after the emergency, during the recovery phase, until full CI recovery.*
- *Monitoring of the use of financial resources should be centralized to only one point in order to allow better resources allocation depending on the urgent needs. Monitoring should respect what is planned in strategic plan but should also be able to adapt to urgency and reallocate resources quickly enough in case of urgent need that was originally not planned. Should also be able to adapt financial plan in case of re-allocation needs.*
- *The supply of resources should come from involved parties and stakeholders: service providers, cities, region, etc. Monitoring entity should be able to request funds quickly enough in order to be able to allocate resources in due time. It is needed to know in advance the way to obtain funds in order not to lose time during normal or emergency operation.*

Interdependencies recommendations

In order to manage the potential issues generated by the strategy planning function, an organization should consider applying the Corporate Social Responsibility (CSR); this is a corporate self-regulation, to align the business model to goals that emphasise accountability for the impact of actions taken on stakeholders and the broader community in which business operate. CSR encourages efforts to achieve a sustainable, positive impact through corporate activities. It provides opportunities to enhance the perception of a company's integrity and reputation, and can help increase brand recognition.

This function must provide the highest possible feedback to Coordinate Service delivery, Coordinate emergency actions, *Monitor Resources availability, Use of services and Supply financial resources functions so that it can coordinate the financial management. This can be performed by direct communication or by continuously monitoring the operations.*

3.4.3 Perform Risk Assessment

Abstract

Risk assessment is inherently related to an estimation of uncertainty at different levels. Often, the single most important feature of risk assessment is considered to be the forecasting of possible future outcomes and the estimation of their likelihood. Current practices for risk assessment are strongly based on the understanding of causality relations of known past events. It is widely recognised that this leaves out a great amount of critical factors, mainly related to high system dynamics and complexity. Risk assessment must foremost encompass the fact that certain levels and factors of uncertainty are inescapable and that hindsight operational knowledge does not take into account the potential impacts of continuously changing operations. Therefore, in addition to minimising uncertainty, risk management must also take into account, on the one hand, the estimation of types and levels of resources that may be required to adapt to unforeseeable events, and on the other hand, the need for continuous and timely update in view of emerging factors or perceived operational changes.

Background facts

Risk assessment serves the fundamental purpose of supporting both the definition of priorities for action and the determination of the nature and course of such action. Since its origins, risk management has evolved very differently depending mainly on the domain (i.e. industry, health care, services, etc.) and the nature (i.e. industrial safety, occupational safety and health, security, economic and financial risk, etc.) of risk. This has resulted in a highly fragmented approach to risk assessment, which is reflected at normative and legislation levels. Currently, at EU level, not only legislation and standards for risk management and assessment remain aligned with industry sector needs and risk nature specificities, but also they emanate from different institutional organisms. While the benefits and needs for enhanced coordination amongst different risk management practices are becoming increasingly apparent, many obstacles remain at political, organisational and operational levels. Operational and environmental changes that may impose additional stresses on available resources must be assessed, even if not compromising planned operational goals. Resources are always finite and therefore, when estimating the likelihood of things not happening as planned and within the planned resources, the potential need for additional capacities and resources must be considered and aligned with actual potential operational needs at different levels. Beyond the identification of hazards and the estimation of the risk levels that these may generate, this requires the ability to map risk onto actual operational scenarios and conditions.

General recommendations

Risk assessment should take into account the following:

- *Introducing the Integrated Risk Assessment practice, the approach that combines the process of Risk estimation for humans, biota and natural resources in one assessment.*
- *Need for periodic update of risk models (the identification and characterisation of hazards and safety objectives and requirements) in view of operation and context changes.*
- *Increased need for integrated risk assessment in order to facilitate coordinated risk management actions and measures.*
- *Shifting from single "all purpose" tools to a set of integrated tools that respond to different risk assessment needs (i.e. local specific operations, global and interdependent overview of risks) and that are able to exploit heterogeneous data generated within (operation) and outside (environment, usage) the system.*

- *Adopting tools that provide the ability to continuously update risk assessment needs in view of changes in safety models.*
- *Prospective and anticipation needs through the assessment of potential changes (both in terms likelihood and magnitude) in operations and their environment.*

Common Conditions recommendations

1. *Availability of resources*

Risk assessment may require measurement or detection equipment but often sufficiently precise assessment methods may be used.

- Humans (labour) – skills/competence
  - *Risk assessment activities should be carried out by qualified dedicated teams but always in coordination and relation with local operational staff.*
  - *To the possible extent, assessment activities should be carried out within teams that gather various relevant expertise, ranging from engineering (i.e. mechanical, chemical, etc.), and human factors, among others. An in-depth knowledge of processes and operations is fundamental.*
- Budget
  - *Risk assessment budget should account for the possibility of instrumentation and external expertise needs.*
- Data & Algorithm:

Historic and statistical data provide essential support for risk assessment procedures:

- *Data sets should be reviewed periodically, in order to integrate new potentially relevant risk variables. This provides the means to integrate changes in risk models.*
- *Data sets should include relevant variables of operational environment, namely economic and social outsets and forecasts.*
- *Exploit Big Data generated by the personal smart devices and sensors as well as Open Data generated by organizations and public institutions to support risk assessment.*

2. Training and experience

- *Subject matter experts should be consulted in order to validate hazard identification.*

Questions

- What are the dangers/risks that might be encountered?
- How do you identify them?
- For which events is there a response ready?
- How was the list of events created?
- When and why is the list of events revised?
- What is the threshold of response? (Rate of change)
- How soon can a response been given?
- How long can it be sustained? (Size of buffers)
- How was the type of response determined?
- How many resources are allocated to response readiness?
- How is the readiness verified or maintained?
- What are the elements of the infrastructure that are more critical? How can they be identified and classified?
- Is the match between resources available and resource needs assessed?
- Is there a systematic list of cascading effects to be considered in case of incidents?
- Are you aware of the vulnerabilities of your infrastructure?
- How do you measure performance? What kinds of indicators are used and how are they defined/classified/planned for revision?
- How are the “measurements” made? (qualitative, quantitative)
- When are the measurements made (continuously, regularly)?
- What are the delays between measurement and interpretation?
- How can the organization infer the time needed to its customers to return to the normal level of service usage after a disruptive event (e.g. a terrorist threat)?

- *Local staff may also provide useful input in terms of risk perceptions and operational processes insight.*

3. Quality of communication

Ensure the accuracy of data and risk assessment outcome communication to all interested actors in the organization (e.g. decision makers, operators, etc.) avoiding allegations and manipulations.

4. Human Computer Interaction and operational support

N/A

5. Availability of procedures and plans

- *Risk Assessment activities must be contemplated and integrated in business and organizational process description, as opposed to independent or "stand-alone" activities.*
- *In addition to periodical needs, operation and process change control processes must call on risk assessment and determine when such activities are required.*

6. Conditions of work

A suitable level of independency and autonomy should be formally ensured to risk assessment teams

7. Number of goals and conflict resolution

- *It is necessary to adopt tools that respond to assessment needs of different process stages: planning, operation, maintenance, decommissioning, etc.*
- *Precision (quantitative and qualitative) of risk assessment must match process stage requirements and objectives.*

Examples

- Risk forums that bring together teams involved in managing different risk domains, addressing in particular, the potential need to review risk models and assessment tools.
- Team reviews of risk analysis activities, mainly focusing on the interpretation of risk factors and their mapping onto real operational context and specific scenarios.

Limitations

Resources are inherently finite. For risk assessment, this means that, on the one hand, assessment must be built and adapted to the inevitable limitations of available information, both quantitatively (the amount and volume of information) and qualitatively (the accuracy and reliability of information). On the other hand, assessment activities must always adjust to time limitations in terms of, both the different time scales at which assessments are needed (different stages and levels of decision making processes and operations), and the timeframe within which an estimation must be produced to support decision making.

8. Available time and time pressure

While time requirements for risk assessment may not vary significantly, time pressure should be kept to a minimum, so as to not compromise thoroughness and validity of risk reporting.

9. Circadian rhythm and stress

NA

10. Team collaboration quality

- *Team work may be particularly relevant when assessing more complex operations and when producing risk reports.*
- *To be effective in risk assessment, It is necessary to establish a collaborative environment among the different sectors and departments of the organization and the team dedicated to risk assessment.*

11 Quality and support of the organization

- *Since the risk assessment may require interviews to operators as well as workplace inspection, it is necessary that the senior management, to overcome possible ostracism, officially endorse evaluators.*
- *The clear and explicit organisational recognition of the critical role of risk assessment is a fundamental contribution for the robustness of risk assessment activities and their outcome*
- *Some interaction with stakeholders may be relevant in view of estimating supply chain related risks, which may require some formal pre-established organisational setting.*

Sources

- Commission Staff Working Paper 1626-2010. Risk Assessment and Mapping Guidelines for Disaster Management. The European Commission
- Gustin, J. (2007) Safety Management: A guide for facility managers. CRC Press
- Hollnagel, E. (2014) Safety-I and Safety-II: the past and future of safety management. Ashgate
- ISO 31000: Risk management – Principles and guidelines
- Sodhi, M., Tang, C. (2012) Managing Supply Chain Risk. Springer
- OHSAS 180001
- WHO Integrated Risk Assessment
- http://www.who.int/ipcs/publications/new_issues/ira/en/

Interdependencies recommendations

Hindsight on events constitutes a fundamental input to risk assessment. This requires reliable relations both within the organisation and often amongst stakeholders. Beyond the description of linear relations of causality, this should support the identification of interdependencies and their impacts in terms of performance variability. This requires more than conventional accident and incident investigations. Team reviews and discussions based on a thorough description of events (as opposed to an identification of failures) can produce valuable learning experiences and support the development of adaptive capacities. Risk assessment activities should be developed based on multi-disciplinary teams and integrate stakeholders as relevant. It should also feed into all management and operation practices namely through the identification of the need for procedure reviews, or the redesign of operation or technology, among others.

3.4.4 Training staff

Background facts

Training is defined as all activities deliberately performed to enhance knowledge, skills, and abilities of members of the organization with the aim of enabling them to better perform their specific job and to contribute to the resilience of the system.

A training *objective* is characterized as the measurement method and the cut off-criterion used to evaluate if a person has acquired the desired enhanced knowledge, skills, and abilities while participating.

A training *curriculum* is a description of how the training is done and includes a specification of when, where, how, using which materials and based on which scenarios the participant is expected to acquire the desired knowledge, skills, and abilities.

All named sources support the assumption that training is a key element to ensure resilience. Suitable local adaptive capacities, understanding and awareness of operational conditions strongly rely on staff knowledge and skills. In emergency situations, different actors from different organizations need to collaborate efficiently in order to maintain or restore the operations of a critical infrastructure. However, a specific organization can in most cases only take an influence on the training of their own staff, with the exception of collective exercises, such as emergency simulations. Therefore, this guideline is focused on providing guidance on how to organize the training of an organization's own personnel.

To which extent certain trainings are available or even obligatory to certain members of an organization differs between European countries. Therefore, the application of this guideline requires gathering information on the availability and legal requirements of certain trainings.

General recommendations

Plans cannot be considered reliable until they are exercised and have proved to be workable. Exercising should involve: validating plans; rehearsing key staff; and testing systems which are relied upon to deliver resilience (e.g. uninterrupted power supply). The frequency of exercises and training depends on the organisation, but should take into account the rate of change (to the organisation or risk profile) and outcomes of previous

Abstract

This guideline defines how to properly coordinate and evaluate training activities in order to ensure the resilience of a critical infrastructure.

Questions

– How does the organization decide which training measures it should provide, when, how and to whom?
– For which target groups / persons / stakeholders should training be provided?
– When does learning take place (continuously or event-driven)?
– Which method is used to determining the objective(s) of a certain training?
– What is the learning based on (successes – failures)?
– What is the target of learning (individuals, organisation)?
– Which method or measurements (operationalizations) are used to determine the effectiveness of a certain training?
– How to decide on the allocation of resources (money, effort, ...) to a certain training?
– How to determine how often a training has to be repeated / refreshed?
– How are the effects of learning verified and maintained?
– Which training methods can be used for which training purposes/objectives/target groups?
– Are there any emergency training and procedures?
– What is the learning based on (successes – failures)?
– What is the nature of learning (qualitative, quantitative)?
– What is the target of learning (individuals, organisation)?
– How are the effects of learning verified and maintained?

exercises (if particular weaknesses have been identified and changes performed).

To contribute to the resilience of the system, training activities need to be organized in a manner that fulfils the following criteria, ensuring that:

- *the allocation of resources to training is coherent with the overall strategic planning,*
- *undesired variability in the training's outcomes is reduced, and*
- *training activities are revised to take newly discovered requirements into account.*

Achieving this requires following some generic guidelines:

- *The organization's HR responsible for training should document the training or competence requirements for each role or job within the system. The documentation should follow a standardized schema. This identifies the minimum criteria to be achieved in training, which do not allow for variance among different members of staff. This should nevertheless, undermine the management of specific expertise needs that may be required, for instance, by staff performing highly complex tasks.*
- *The documentation should include precise information on official or legal success criteria, for instance naming a specific type of driving license required. Success criteria may be qualitative or quantitative. The training should include requirements related to the general service delivery as well as requirements related to the known vulnerabilities and respective mitigation strategies. It should particularly address the individual's role in detecting emergencies and subsequent mitigation actions.*
- *"Informal" knowledge and expertise should be fostered and steered in such a way that it remains aligned with safety and operation requirements, whilst fulfilling its fundamental role in terms of local adaptive capacity to operational variability (inherent to complex operations).*
- *The documentation should specify the time by which training needs to be refreshed and how tolerate delays in refreshment to maintaining the service operation in general or including the individual staff member into service operations.*

Examples

- Driver training in driving simulators and in vehicles without passengers for beginner drivers of trains.
- Joint simulacrum exercises involving not only supply chain stakeholders, but also neighbouring and even competing businesses as needed.
- Training programs on crisis management for the executives of a critical infrastructure.

Training method selection

Based on ISO 22301:2012, the guideline defines training "*as all activities deliberately performed to enhance knowledge, skills, and abilities of members of the organization with the aim of enabling them to better perform their specific job and to contribute to the resilience of the system*."

Training methods should be selected based on the following aspects:

1. What is the objective of the training an in which context does the training need to be done?
2. Which resources are available?

RESOLUTE D2.1 describes 3 main types of training criteria in the context of resilient systems:

- *Knowledge*
- *Analytical and social skills*
- *Personal skills*

RESOLUTE D2.1 also describes five training methods:

- *Classroom training / frontal instruction*
- *Simulator training*
- *On-the-job-training*

- *Training activities should be evaluated by measuring training success by criteria assessing to which extent the trainees acquired the necessary skills and contents. This refers to tests, such as theoretical and practical exams.*
- *Training effectiveness and knowledge transfer should be evaluated by measuring staff performance on the job, as far as this is compatible with data privacy regulations. This requires data from the monitoring of the service delivery. This should also include feedback from the trainers, if available.*
- *The results of both evaluation processes should be fed back to the HR responsible developing the training requirements. Staff should be consulted in the process of reviewing or updating training needs.*
- *Additionally, training requirements need to be updated if safety regulations change, if new technologies are introduced and if internal emergency mitigation strategies are modified. Updates should also take into account changes in overall operational context, shifts in market trends, among others.*
- *Based on the training requirements, training resources are allocated. In order to meet budget restrictions specified in the strategic plan, training requirements (or minimum variability criteria) may be reduced as long as legal requirements are not violated.*
- *Partnering with other organizations may reduce training costs and increase training effectiveness due to an improved basis of lessons learned as a foundation or additional input to training. Training and education programs should promote a common cross-organizational understanding of risk and interdependencies in the system.*

Common Conditions Recommendation

1. *Availability of resources*
   - *Humans (labour) – skills/competence*
     - *The collection of training requirements should be linked to feedback processes available to all members of the organisation.*
   - *Budget:*
     - *Budget planning should account for the working hours spent on training by both trainers and trainees, including external trainers, training materials, training locations or infrastructure, working hours of HR specialists updating training procedures, and auditing or certification costs.*

The influence of training objectives

When trainees are meant to acquire new knowledge, classroom training would be the method of choice. This does not only need to involve frontal instruction; it can be enhanced by group work and other cooperative learning practices. It provides a cost-effective option of communicating contents to the trainees, allowing for questions about the content and to use written or oral exercises for supporting the intake of the contents into long-term memory. Classroom-training can also be done in telepresence-classes with trainees accessing the class remotely. Depending on which personal skills need to be trained, any training method could be best. Whenever practicing the skills in real-life would involve enormous costs or risks, simulator training or drills are recommended. Examples are driving skills trained in a driving simulator or fire-extinguishing skills that are trained with controlled fires during drills. Additionally, simulations can be used to induce stress before training certain skills, which may be useful to test and train people for situations of extreme stress, such as crisis management. On-the-job-training is also eligible for training personal skills, as long as risks and costs can be controlled. For example, a new employee could perform the job while a senior colleague is watching and intervening when necessary. Analytical and social skills will mainly require interaction between trainees or trainer and trainee and thus all methods except for simulator training are principally eligible.

Context factors that may influence the choice of a training method may be time pressure, leading to the exclusion of preparation-intense methods such as simulator-based training or e-learning. Some trainings require the use of a realistic setting, e.g. night-time or bad lighting conditions, certain weather, the presence of stressing factors such as loud noise, etc. This can be particularly important when training skills.

- *Data & Algorithm:*
  - *Use official and standardized formats to describe training requirements and test procedures where applicable.*
  - *Store documentation of trainings and tests according to legal regulations.*

2. Training and experience

- *Collect feedback from trainers for improving the process.*
- *Scenario-based training can be used to validate contingency plans.*

3. Quality of communication

- *Support efficient shareholders and (internal and external) stakeholders/experts coordination and cooperation.*
- *Guarantee the accuracy and understandability of the communication through standardized communication tools, protocols and languages.*

4. Human Computer Interaction and operational support

- *When choosing the method for delivering the training, the following recommendations should be taken into account:*
  - *Classroom training should be chosen if basic knowledge needs to be learned and if individual differences between trainees do not seem to influence training efficiency.*
  - *Simulator training should be used for practical skill acquisition if training with real-world objects is related to high risks concerning the health of persons or the destruction of costly equipment.*
  - *On-the-job-training or drills and exercises should be used for practical skill acquisition if training with real-world objects is not related to high risks concerning the health of persons or the destruction of costly equipment.*
  - *E-learning may be used if the contents of training are assumed to be relatively stable over longer periods of time.*

5. Availability of procedures and plans

The influence of resources

Usually, simulator-training, e-learning and drills will be the more expensive solutions. Simulator-training requires a well-maintained simulator and well-programmed scenarios, plus personnel to run the simulator. E-learning requires learning applications to be programmed. Drills and exercises require a location, such as a fire brigade training centre, and the involvement of a greater amount of people, also for preparation and aftermath. Disposable materials may be expensive, too.

Some E-learning solutions may be applied with comparably limited effort, e.g. when content management systems are used to create or adapt web-based learning solutions, such as hypertext information systems (for instance: wikis) or for testing knowledge acquisition or retention (e.g. using online-questionnaire tools). Nevertheless, it is generally advised to rather use e-learning solutions when contents are not expected to change over longer periods of time, thus justifying the effort and budget required. E-learning and web-based testing is, for example, used for assuring that all employees are correctly informed about legally required procedures, such as corruption-prevention or workplace-safety regulations

The guideline summarizes:

When choosing the method for delivering the training, the following recommendations should be taken into account [7]:

1. Classroom training should be chosen if basic knowledge needs to be learned and if individual differences between trainees do not seem to influence training efficiency.
2. Simulator training should be used for practical skill acquisition if training with real-world objects is related to high risks concerning the health of persons or the destruction of costly equipment.
3. On-the-job-training or drills and exercises should be used for practical skill acquisition if training with real-world objects is not related to high risks concerning the health of persons or the destruction of costly equipment.
4. E-learning may be used if the contents of training are assumed to be relatively

The definition of training objectives and curricula, as recommended in the general recommendations, should be formalized as a recurring organizational process and be embedded within the organization's HR procedures, such as personnel acquisition, promotions, and support for Management by Objectives (MbO) approaches.

6. Conditions of work

It is recommended to appoint the head of HR as a responsible to ensure that the conditions necessary to perform the trainings are created. This includes the provision of space, materials such as media and consumables, budget and buffer personnel to account for the temporal unavailability of trainers and trainees to standard operations.

7. Number of goals and conflict resolution

- *Often, restrictions in time and budget will make it impossible for certain employees to achieve all possibly defined training goals, at least within the desired timeframe. To resolve such conflicts, training objectives and subsequently training curricula need to be prioritised. It is recommended to prioritise trainings following this scheme:*
  - *Is the training legally required for standard operations?*
  - *Is the training legally required for relevant emergency situations?*
  - *Is the training directly relevant for life-saving in emergency situations?*
  - *Is the training relevant to create buffer capacities for emergency situations?*
  - *Is the training relevant for improving the efficiency of standard operations?*

Limitations

The usefulness of training as a measure to increase system resilience should not be limited to the training for specifically known and anticipated risks and to the training of meta-competences (such as team-work, participative leadership, team-based problem solving, etc.). Training on aspects such as the overall knowledge and understanding of operations or the flow of products and information, can be useful towards enhanced resilience. However, the management, implementation and assessment of such training initiatives may be challenging. In some cases, implementing cross-sector/department exchange of knowledge and expertise can benefit this purpose.

The use of a guideline-based training approach has its limitations with respect to the training of target groups that are not identified as a finite number of known individuals, such as users, clients or other stakeholders.

The guideline does not serve to plan organizational learning as such. Although the training of individuals contributes to organizational learning, it is not a sufficient yet alone a necessary requirement for it. Organizational learning, for example, may require changing or adding job descriptions instead of just providing different training methods to account for new environmental conditions.

8. Available time and time pressure

- *Planning milestones and deadlines should integrate degrees of flexibility to cope with planning quality requirements.*
- *Schedule trainings according to predicted demands: Perform trainings outside of demand peaks, such as high touristic season.*

9. Circadian rhythm and stress

- *Perform trainings during regular working hours unless the training requires a specific setting, such as night time.*
- *As long as specific purposes do not justify a distinct approach, trainings should always avoid an excess of workload for both trainers and trainees. This implies the definition of realistic objectives and timeframes. Exceptions may occur when employees have to be drilled for dangerous situations, such as in military contexts.*

10. Team collaboration quality

- *Provide training on the principles of collaborative planning to all strategic management teams.*
- *Provide training on collaborative crisis management to all crisis management teams.*
- *Provide team development interventions to recently formed teams.*
- *Provide trainings that increase awareness and understanding of vulnerabilities and respective mitigation strategies (Homeland Security, 2013)*
- *When on-the-job training is applied and experienced colleagues are supposed to act as trainers, the training effectiveness should be evaluated by another, independent person.*

11. Quality and support of the organization

- *Work objectives of team and department leaders should include objectives on the training that the respective employees need to receive. Leaders need to be responsible for enabling their co-workers to conclude the required training.*
- *"Training should go beyond procedures and address generic competencies related to unexpected and escalating situations" (DARWIN, 2015)*
- *Techniques:*
  - *Role-playing;*
  - *Scenario-based training;*
  - *Training for role improvisation.*

Sources

- Eurocontrol (2014). System thinking for safety.
- Homeland Security (2013) NIPP (2013. Partnering for critical infrastructure security and resilience. USA:
- National Infrastructure Advisory Council (2014) Critical Infrastructure Security and Resilience National Research and Development Plan.
- Homeland Security (2015). National Critical Infrastructure Security and Resilience Research and Development Plan.
- DARWIN Project (2015). D1.1 Version 0.6: Consolidation of resilience concepts and practices for crisis management.
- D2.1 State of the Art Review (2015) RESOLUTE project

Interdependencies recommendations

The management and implementation of raining needs should be grounded on a close cooperation and coordination between HR staff leading training, and the remaining organisational and operational areas. This becomes fundamental for issues such as the need to align the overall minimum training requirements for all members of the organisation with local specific training needs. To this end, training staff as a system function may develop strong interdependencies with most other system functions.

3.4.5 Coordinate Service delivery

Abstract

This guideline aims to provide recommendation for the effective resilience management of the coordination of service delivery in a CI. An overall supervising authority responsible for the function should be established. All organizations involved (both supervising authority and specific service providers) should be adequately staffed and funded. Best practice and European standards should be followed as available per critical infrastructure. category.

Background facts

Across all industry sectors, service and product supply chains are becoming increasingly complex, mainly due to the growing diversity of stakeholders, the tighter couplings between them, and a significant geographical expansion. This renders management and planning of service delivery equally complex and demands additional coordination efforts. The limits of ownership and accountability for certain service delivery aspects often become unclear or misaligned with formal institutional and contractual relations.

The function relates to all planning and oversight activities needed to ensure that service is delivered according to established levels of performance and quality. It aims at coordinating service delivery during ordinary /normal operation, as well as during and after incidents/disruptions of normal service.

Coordination of service delivery before a disruption, concerns business as usual where standard operation and safety procedures should be used. From a resilience perspective, it is fundamental to integrate in such practices a continuous assessment of overall operational conditions and the matching of such conditions to the planned service level and the allocation of resources.

Coordination of service delivery during or after an incident/event requires the implementation of emergency rules and procedures as well as wider communication and coordination with first responders.

Post –event coordination of service delivery should focus on selecting and implementing alternative recovery scenarios according to emergency plans and procedures and pre-event risk assessment based on the strategic plan.

Decision makers need to understand the consequences of policy and investment options before they enact solutions, particularly for the highly complex alternatives available for protecting critical infrastructures in today's threat environment.

Questions

- Which are the stakeholders that should be involved and how?
- How the roles and responsibilities are clearly defined?
- How the processes are defined, established and communicated?
- When a process or a procedure is revised?
- How conflicting goals are managed?
- How should the organization model, simulate and analyse the interactions within its Critical Infrastructure (CI) and other interconnected Cis
- How can the organization - additionally to maintaining its service - contribute to the resilience of other key services / society in general?
- How can measures that benefit other organizations / the society and that are not directly linked to everyday efficacy be (co-)financed?
- Do you have access to every communication channel?
- How should the organization manage sources of information, e.g. sensors, cameras, staff, etc. in order to get a realistic picture
- How can the organization infer the time needed to its customers to return to the normal level of service usage after a disruptive event (e.g. a terrorist threat)?
- Which are the media (in particular social media) the organization should monitor to estimate the "mood" of its customers after an adverse event

General recommendations

- *Specific service providers should follow compatible* *operation, maintenance and emergency procedures.*

- *Safekeeping and cross-labelling of incident inventories should be given priority. Immediate communication and information of management staff for all potentially severe incidents subject to immediate risk or other system weaknesses relevant to health and safety needs.*
- *Access links to critical infrastructure for service provision should be planned, defined and communicated by overall supervising authority to service providers.*
- *Alternative access routes should be planned and communicated to service providers in cases of service disruptions.*
- *Consider the availability of resources for the management of operational degraded modes. This becomes particularly relevant when aiming to ensure a minimum level of operation under certain emergency scenarios. In many cases this minimum level of service may constitute in itself a fundamental emergency response resource.*
- *Implementing tools to support decision makers in taking internal and external risk-informed decisions.*
- *24x7 support for customer should be documented in a manual for processes and technical resolution of problems. There should be clear guidelines for assigning the priorities and taking actions. Assignment of priorities depends upon the criticality and impact of the problem.*
- *The escalation procedures should be clearly defined with Primary and Secondary backup persons and their contact numbers. The support personnel should be provided with whatever is needed to service the calls from out of the office.*

- How the organization guarantees flexibility?
- Do you have a resilient Internet network, with many different infrastructure (cabled, G4, SAT, micro-wave), overlapping the territory, able to backup each other in case?
- How can the organization involve its customers/citizens to design adaptation strategies aimed at improving the overall perceived level of safety and security

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence

  - ***Communication****: timely, contextualised, prioritised, based on the value addition for the listener*
  - ***Relationship****: the Delivery Manager is the organization front end*
  - ***Problem solving****: in depth understanding of user/client problems and demands and attitude to support user/client with a long lasting solution to run their business effectively and efficiently.*
  - ***Managerial and Planning****: Identification of resources. Capacity to keep a mid-long term perspective.*
  - ***Technology****: a skill set related to cutting edge technologies is necessary. Technology plays a vital part in the client's business, e.g. systems like business process management, ERP, supply chain, production planning, content management, business intelligence, enterprise application integration, CRM etc. To put in place a technology that works for the client, and which can deliver a high ROI is a mission of task.*
  - ***Trade-off****: Capacity to address business need and service demand while respecting the safety and security requirements.*

- Budget:

Being aware on which is the adequate budget to carry out operation and maintenance activities according to Service Level Agreement/KPI and safety and security requirements. If the budget allocated does not consent to address business and safety properly, an immediate alert should be forwarded to the organization management (Strategic Planning and Financial Affair functions).

- Data& Algorithm:

Consult with the relevant stakeholders (e.g. general public). Use surveys to adjust and coordinate service delivery

- ICT resources:
  - *State of the art technical equipment and ICT infrastructure should be used, including a resilient internet network covering all areas of service delivery.*
  - *Examine trade-offs between the benefits of risk reduction and the costs of protective action utilizing a Decision Support System that incorporates threat information, vulnerability assessments and disruption consequences, operational data in quantitative analyses through advanced modelling and simulation.*

2. Training and experience

Staff should be adequately trained to implement relevant rules and procedures (e.g. operating, communications procedures, safety procedures). Staff should be periodically tested for adequate training and knowledge of routine and emergency rules and procedures to catch up updated operating, safety and emergency procedures. Staff should also be trained for ICT infrastructure. Safety-critical personnel should be licenced.

Examples

Coordination of metro service delivery is the responsibility of the Operations Control Centre (OCC). All signalling and train control functions can be controlled from the OCC. The staff include network controllers in overall charge of the OCC, power controllers, traffic regulators (positions manned continuously on a 24 hour basis), as well as security controllers and information controllers. Public address systems and mimic panels are components of the OCC.

Limitations

Possible budget constraints or inadequate legal framework may impose limitations to coordination of service delivery.

3. Quality of communication

- *Clearly define all potential communication channels among service providers.*
- *Use standardized communication tools (templates) and protocols.*
- *Establish an effective communication between the actors involved in the operations and in the contingency.*
- *Establish a single point of contact for service delivery coordination.*

4. Human Computer Interaction and operational support

Provide operational support for use of ICT infrastructure.

5. Availability of procedures and plans

Ensure that clear operation plans and emergency procedures and plans are available.

6. Conditions of work

NA

7. Number of goals and conflict resolution

- *Establish conflict resolution procedures in case of different orders by ordinary upper level staff and emergency staff.*

- *The decision to increment the service delivery performance to address unexpected increment of demand should take into account the safety and security requirements. In case such decision conflict with goals of other organizations, because of the interdependencies of the infrastructures, a prompt communication to each stakeholders affected by the decision is required in order to allow a synchronised systemic response to an unexpected event.*

8. Available time and time pressure

Ensure a degree of flexibility when planning milestones and deadlines to cope with quality requirements.

9. Circadian rhythm and stress

Ensure compatible nightshifts for staff of various service operators.

10. Team collaboration quality

- *Take into account team collaboration competences when recruiting personnel.*
- *Establish mutual performance monitoring procedures.*

11. Quality and support of the organization

- *Establish clear decision making process and alignment of responsibility with accountability.*
- *Perform regular audits to check the need to update operating procedures following specified time periods.*
- *Perform audits to check the need to update operating procedures following disruptions of service.*

Sources

- Rulebook on Operations System Management of the Public Power Corporation (DEH) http://www.rae.gr/old/SUB2/2_3.htm#%CE%A5.%CE%91.6296/01
- Decision on Adoption of Rules of Operation of Sewage Network (EYDAP SA) available in Greek https://www.eydap.gr/userfiles/c3c4382d-a658-4d79-b9e2-ecff7ddd9b76/kanonismos-diktuou-apoxeteusis.pdf
- STASY Rulebook
- STASY Fire Drill Aghia Marina Station
- STASY Fire Drill Final Plan Aghia Marina Station
- STASY Lavyrinthos Program (Communication Plan)
- Information from Athens Metro Operating
- Plan for Lines 2 and 3 has also been taken into account for the implementation example.
- Bush et al, Critical Infrastructure Protection Decision Support System – Intentional System Dynamics Conference 2005

Interdependencies recommendations

The function is closely interrelated with the condition of both physical and cyber infrastructure. Physical infrastructure should be both regularly maintained and monitored for unusual circumstances to perform the function. This is one of the aspects for which thorough and continuous coordination with stakeholders becomes critical.

Maintenance procedures for physical/cyber infrastructure should take into account service delivery peaks, to adjust to greater maintenance needs.

Efficient coordination of service delivery should also take into account user behaviour and awareness of service characteristics through both adequate information supply to users and surveys. User generated feedback should be monitored to adjust the coordination of service delivery to changes of service peaks. The monitoring of operational context factors such as weather and social events is fundamental, in particular for sectors such as transport, for which the adjustment or re-planning of service delivery may be required in view of foreseeable significant changes in such factors.

Implement a prev*entive maintenance program: proper care and regular maintenance provided by a comprehensive service plan gives you peace of mind in knowing that you are protected against unnecessary downtime.*

3.4.6 Manage awareness & user behaviour

Abstract

This guideline defines how to increase the resilience of a critical infrastructure by taking directed influence on the perceptions and behaviours of non-staff users in the system. Such users are in many cases the general public or customers of the service provided.

Questions

- Do you have access to every communication channel?
- Which (social) media should be used by the organization to provide information/communication in order to support a quick return to the normality?
- Have the user the right risk perception and awareness?
- Do you have multimedia communication expert in your team?
- Have you considered message accessing and understanding differences for culture, language, disabilities, positions, skill, etc.?
- Have you design your communication strategy around the addressability concept namely 4R (Right people at the Right time in the Right place, through the Right channel)?
- Are you able to measure/quantify communication effectiveness?
- Have you established a people-cantered early warnings system?
- Have the local communities been involved?

Background facts

“Human beings do not have the time or the ability to be concerned about every problem in the world. They devote their time and energy to problems that involve them and for which they can make a difference” - J E Grunig quoted in Leffler (1998)

The shift from a public awareness approach to one of community-individual safety alters the traditional top-down, 'command and control' relationship with the population. In this new approach, the person is seen as an **active participant** in his/her own safety, rather than a passive recipient of services. This requires flexibility, new skills and new approaches.
Managing awareness and user behaviour needs to understand the main determining factors of intention, in order to undertake behavioural change such as:

- Attitude of a person
- Community norms
- Social settings
- Degree of self-efficiency of a person

This function considers CI clients/users such as passengers or drivers (for transport system), citizen at large (for energy), etc. as key actors to build system resilience.

In order to anticipate, detect, or recover from an adverse event, such as a service disruption, the active and experienced collaboration of the end users may liberate important resources. Therefore, an ex-ante designed strategy for managing user awareness and user behaviour towards desired actions, can lead to a higher organizational efficiency in terms of how resilience is achieved.

Managing user awareness and user behaviour may include short-term and long-term actions. Ad-hoc-communication is the tactical information immediately given to the users, such as information about delays or evacuation routes via signs and P.A. system. Long-term actions may include the provision of general information through **personal smart device**, posters, organized events, trainings for children organized at schools, and similar means of communication that are not meant to produce immediate effects.

General recommendations

- *Communication plan: All communications to the users or the targeted community should be based on a plan that contains a justification and the objective of a message, the media and channels to use, the expected results and a timeline for delivering the message.*
- *Collaboration: The support of private or public organizations should be sought to implement real time (during the emergency) as well as long-term actions such as campaigns or educational programs for raising community awareness about risks, safety behaviours and the needs of being prepared.*
- *Public and private educational institutions should be involved in the awareness campaign.*
- *Establish a cooperation of privately owned infrastructure operators and public bodies across sectors and borders, as well as with local communities as citizens organisations, business, academy, NGO, local and regional government, in order to enable a multi-dimensional response to problems and needs*
- *Events: Anniversaries of past disastrous events are recommended for the implementation of campaigns, along with events to raise awareness.*
- *Awareness: the community awareness campaigns are recommended, if:*
    - *A new type of adverse event has been added to the risk analysis and the cooperation of the community is required to reduce the risk or increase buffer capacities.*
    - *It has become clear that the community is unaware of the risks related to a certain type of event and/or the safety behaviours has not been adopted.*
- *Training: The awareness can be raised also through dedicated training activities for the population. To have an effective emergency management program, facility managers need to conduct training and drills to ensure that people understand the emergency management program's elements and how they are to respond in the event of an emergency. Three tiers of training can be identified. Tier 1 is classroom training; it is easy to organize but only provides an overview of the emergency management program and the basic response protocols. Tier 2 is scenario training and involves creating a mock scenario in a*

Examples

Greater use of social marketing methods.

Mass persuasion methods originally developed in the commercial marketing field are now widely used to foster positive behaviours. These are being applied to improve community resilience to natural hazards, e.g. FloodSafe (NSW SES). The National Flood Warning Centre (UK) ran a social marketing and health promotion campaign that is credited with raising flood awareness from 48% to 79% over the past five years (Proudley and Handmer, 2003).

ATTIKO Metro Athens

- Partnering between a local metro company and the local government to promote alternative routes in case of flooding.
- Planning of evacuation routes from a metro station for different user groups, including vulnerable users such as wheelchair users or persons with diminished eyesight.

Limitations

Both campaigns and ad-hoc communications may be valuable additions to the overall strategies of an organization that manages a critical infrastructure. However, the effects of such communications are not guaranteed. The organization should always be prepared for undesired user behaviour, independently of the efforts undertaken in user awareness management.

controlled environment to test the attendees' ability to coordinate a response to a given event. Ideally, Tier 2 training offers a real-life feel to a response, but unless planned carefully and moderated properly, some attendees may be disinterested and not understand the value of the training. Moreover both Tier 1 and Tier 2 are expensive and time consuming. In order to engage an higher number of people, reducing the costs and increase the effectiveness, innovative solutions as ***Game Based approach to train people on emergency management delivered through smart mobile should be considered.***

- *Tier 3 training — conducting live drills by first responders and civil protection — is the most effective method, but if the drill time and date are announced ahead of time, citizens may cheat and prepare themselves to respond at the appropriate time. Even if it may not indicate their actual ability to cope with the emergency, it may represent a strong tool for awareness rising.*
- ***Early warnings:*** *Communication and early warnings systems should be people-centred rather than agency-centred, thus tailored to meet the needs of every group in every vulnerable community*
- ***Personalized context aware communication:*** *The communication strategy should be even more designed around the* ***addressability concept namely the 4R - Right person at the Right time in the Right place through the Right channel.*** *Real time context aware and personalized communication aims at empowering individuals and communities threatened by hazards to act in sufficient time and in an appropriate manner to reduce the possibility of personal injury, loss of life and damage to property and the Environment. Such type of communication should exploit current smart technologies such as mobile and wearable smart devices as well as every kind of communication infrastructures (Wi-Fi, LTE/4G, Bluetooth, capillary network, Delay Tolerant network, etc.).*
- ***Personalized or community-based communications should support each phases of the resilience****: preparation, absorption, recovery and adaptation. Thus plans and procedures for delivery pre-scripted messages prepared during the risk assessment or just in time context aware and profiled built messages need to be aligned with the mitigation strategies or emergency respond activities.*
- *At individual user request, provide 1:1 advice on “how to”; (e.g. contacting local authorities and other bodies as well as provide advice on how to protect themselves and their property against future events*

Sources

- UNISDR & GFDRR (2015). How to make cities more resilient. A handbook for local government leaders.
- International Federation of Red Cross and Red Crescent Societies (2011) Public awareness and public education for disaster risk reduction: a guide
- The Associated Press-NORC Center for Public Affairs Research (2013) Communication during disaster response and recovery.
- Pan American Health Organization (2009). Information management and communication in emergencies and disasters: manual for disaster response teams. PAHO: Washington, D.C.
- Scottish Flood Forum Business plan 2015-2018
- Developing Early Warning Systems: A Checklist – International Strategy for Disaster Reduction – ISDR 2006
- AEMC (Australian Emergency Management Committee), 2002 National Good Practice Review of Public Awareness, Education and Warnings in Emergency Management - High Level Group of the COAG Review of Natural Disaster Relief and Mitigation Arrangements, unpublished draft
- Institute of Medicine, (2002), Speaking of Health, Washington D.C., The National
- Academies Press.
- Macdonald, J, (1998), Primary Health Care, Medicine in its place. London:
- Earthscan Publications Ltd
- Peter O'Neill Developing A Risk Communication Model to Encourage Community Safety from Natural Hazards –State Emergency Service
- JUNE 2004
- IETF RFC 4838 Delay-Tolerant Networking Architecture
- Capillary network http://www.ericsson.com/news/140908-capillary-networks_244099436_c

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence
  - *The task of managing long-term campaigns on awareness and user behaviour should be leaded by experts in communication and social innovation.*
  - *The task of managing and orient user behaviour during the emergency should be performed by operators with skill in emergency management and evacuation behaviour of large groups of people.*
  - *Psychological and empathic skills are also needed to be effective in 1:1 communication*
- Budget:

Budget planning should account for the required communication infrastructure, as well as for the planning of the procedure itself. Certain channels, such as social media, need constant attention to be maintained functional and thus require adequate budget availability.

- Data & Algorithm:

Awareness and Communication strategy effectiveness can be assessed through classical tools such as interviews of with innovative systems capable to reduce the bias introduced by the questionnaire tool such as social media analysis or Game based training score.

- ICT infrastructure:

***Computer Aided Dispatch**: CAD systems are an essential component of public safety operations. The CAD user's operating environment is characterized by real-time information processing**.** CAD systems provide deployment and tracking of resources for efficient responses to events. CAD should be designed to process standardised messages as Common Alerting Protocol (CAP).CAD should include an escalation strategy. It's not enough to simply send alerts: needed to ensure that someone acknowledges the alert and handles the recovery. Since people have "real lives," and aren't always on call, it should be possible to send alert to someone on the front lines, and if they cannot respond, pass that alert onto someone else. Moreover, it's possible to turn on alerts for many different metrics, but this has the effect of "spamming" administrators, and decreasing the relative (perceived) importance of any given alert. Finally messaging system should be compatible with multiple contact methods (mails, mobile, signalling panels, etc.*

2. Training and experience

- *Evaluate the entire communication process by researching if communication has the desired effects.*
- *Collect feedback from employees and users for improving the communication.*
- *Specific expertise in Risk management and communication*
- *Operators devoted to manage communication during the emergency needs to be trained to be fully operative also in stressful condition.*

3. Quality of communication

- *To ensure the content quality of the ad-hoc messages, predefined messages or message types should be used in anticipated situations, such as different types of emergencies*
- *Test the different communication channels and tools before using them in emergencies in order to ensure they have the desired effects and to ensure that each channel is used in an appropriate manner.*
- *General principles for qualitative information to users / public are:*
  - *Accessibility (e.g., through the use of different channels)*

- *Inclusiveness (represent all necessary stakeholders)*
- *Inter-operability*

4. Human Computer Interaction and operational support

- *Applications provided to the users should undergo usability testing to ensure their helpfulness during emergency situations.*
- *Select communication methods by their scalability and sustainability.*

5. Availability of procedures and plans

- *A strategy for long-term communications, such as campaigns, should be created.*
- *The procedure for delivering ad-hoc messages should be defined, including general standards for the communication and specific messages / communication actions for predefined situations. This includes the use of channels and precise phrasing.*

6. Conditions of work

Responsible for ad-hoc communications need to be continuously provided with status information or orders from the coordinators of service delivery.

7. Number of goals and conflict resolution

- *Individual communication on evacuation procedures should provide specific information for users with special needs.*
- *Disasters often affect vulnerable groups most. Therefore, where applicable, communication should specifically aid vulnerable groups, for example by naming accessible exit routes in the case of fire.*

8. Available time and time pressure

- *In emergency situations, communications related to safety issues should always be prioritized.*
- *Campaigns that encounter time pressure, e.g. due to a critical event approaching, should rely on social media strategies and news agencies to deliver relevant key messages.*

9. Circadian rhythm and stress

Defining turns among operators is mandatory for the call centre activities (e.g. 118 or 911). Smooth transition among turns should be managed in order to avoid any loss of knowledge or situation awareness.

10. Team collaboration quality

Communication team should be composed by experts in different field, thus it is necessary to clearly match the competencies with the duties avoiding overlaps or mismatching.

11. Quality and support of the organization

Planning an awareness rising campaign as well as the communication in emergency are very specialized and critical activities that require a specific commitment of the organization. In fact, the dynamics (timing, language, content, etc.) of such communications are very different respect to the classical institutional communication or marketing or advertising. To this end the creation of a dedicated unit devoted to manage communication under critical events within the organization is recommended.

Interdependencies Recommendations

In both standard operations and critical situations, the end user communication serves the following functions, in the given priority:

1. *Enable the end users to preserve their own well-being.*
2. *Steer the use of the service to dampen variability in demand, such as peeks, or make users return to a full usage of the service after a disruption has been dealt with and service delivery has been restored.*
3. *Create/restore public trust in the service provided by the CI.*
4. *Provide information to the users to increase service quality (e.g. real-time information on the reliability of transport services).*

In the case of disruptive events, the responsible for the ad-hoc communication to users should be in direct contact with the person or team responsible for the Service Delivery, Operation Monitoring and Emergency Management. In case of standard operations, the responsible for the communication to users should be in direct contact with the person or team responsible for the coordination of service delivery. Additionally, it is highly recommended to provide the communication responsible staff with direct access to monitoring data, such as movement of users through the infrastructure.

In case the connection between functions that provide inputs for the Manage Awareness & User behaviour is temporarily lost, and the uncertainty about the nature of the event is high, the last status detected or the default safety recommendations as redundancy and recall should be forward through the channels. Such practice avoids triggering wrong behaviours that it could make things worse.

3.4.7 Develop/update procedures

Background facts

Procedures are developed at many different organisational levels but from a system perspective they respond to a fundamental need for a formal steering and support of different operational requisites and conditions.

The complete set of procedures forms a body of formal knowledge regarding management and operation requirements. The structure and organisation of this knowledge should be cohesive and logical, in such a way that it reflects the structure of decision-making and production processes. While this may be relatively well achieved at organisational level, amongst stakeholders of complex sociotechnical systems such as critical infrastructures, this is often very challenging. Procedures are essentially tools internal to organisations but to the extent possible and in addition to safety and efficiency requirements, they should also reflect the need for synchronisation amongst stakeholders at various process stages and supply chain levels.

From the perspective of resilience, procedures should be developed and managed so as to support an alignment between the need for a centralised and standardised operational control (supports overall operational coordination), and the need for a local flexibility and autonomy (generates adaptive capacities).

Procedures are essentially a formal coordination mechanism. They should produce a shared understanding of system operation. Both safety and operation procedures should establish the boundaries and conditions within which local adjustment should be undertaken to ensure that overall system operation remains coordinated (fundamental for monitoring and control) and within system capacities (avoid unacceptable variability).

The purpose of operating procedures is to strengthen organizations support in preparing and responding to crises, as well as to strengthen the effectiveness in international humanitarian action in response to urgent needs. This is usually being achieved by the consistent use, by a critical mass of organizations personnel trained in the defined procedures, of a minimum number of key procedures at critical moments in emergency preparedness and response, resulting in increased

Abstract

This guideline is dealing with the development and management of safety and operation procedures, as a set of instructions designed by an organization in order to cover those features of operations which lend themselves to a definite sequence of carrying out tasks without loss of effectiveness, according to risk assessment and ex-post event analysis (learning) in a way to also provide re-usable data and be re-applicable.

Questions

- Who is entitled in SOP production?
- How frequently a valid SOP should be periodically revised?
- Who decides on the date of the implementation?
- Who should be informed?
- How the processes are defined, established and communicated?
- When a new procedure is added?
- How much effort is allocated on organizational process improvement?
- Is there a systematic list of routine safety rules and procedures for prevention and avoidance?
- How the communication inter organization is assured?
- How the communication intra organization is assured?
- How the organization guarantees flexibility?
- For which events is there a response ready?
- How was the list of events created?
- How is the readiness verified or maintained?

predictability, timeliness and accountability of the interventions in crisis contexts. This applies to both regular and emergency personnel.

General recommendations

To contribute to the resilience of the system, some general considerations should be taken into account when developing/ updating procedures:

1. *Identify the goals and objectives for the procedure by defining the exact operational conditions and stings it applies to (standard, degraded mode, emergency…) and by clearly stating to whom and by who the procedure should be applied (job, area of operation…).*
2. *Review critical operational procedures, in particular those relying on multiple stakeholders and for which it is fundamental to determine principles for the coordination of activities, communications and resources (avoid unacceptable operational variability).*
3. *Periodically Review of SOPs according to threat scenarios identified during the risk assessment.*
4. *Assess the availability and capabilities of resources for incident stabilization including people, systems and equipment available within the addressed organisation and from external sources.*
5. *They should provide the means for the identification of degraded operational modes (beyond standard or normal operation) and of the circumstances that require the engagement of emergency response mechanisms.*
6. *Confront with public emergency services (e.g., fire, police and emergency medical services) to determine their response time to the addressed facility, knowledge of the addressed facility and its hazards and their capabilities to stabilize an emergency at the addressed facility.*
7. *Align the design, scope and objectives of procedures with national and international regulations, and with stakeholders needs.*
8. *Define protective actions for life safety (evacuation, shelter, shelter-in-place, lockdown).*
9. *Develop hazard and threat-specific emergency procedures using guidance from existing material.*
10. *Coordinate emergency planning with public emergency services to stabilize incidents involving the hazards at the addressed facility.*

Examples

For example Florida law established the Comprehensive Emergency Management Plan as the master operations document for the State of Florida and is the framework through which the state handles emergencies and disasters. It defines responsibilities of the government, private, volunteer and non-governmental organizations that comprise the State Emergency Response Team (SERT). The document, public, consists of a Basic Plan, which describes the process for preparedness, response, recovery and mitigation activities of the SERT. It is the plan to which the State of Florida's other disaster response plans are aligned.

http://floridadisaster.org/documents/CEMP/Emergency%20Operations%20Plan.pdf

The recommendations of the 9/11 Commission share a common attribute — the assumption that the adoption of standard procedures and guidelines will improve the capabilities of individuals, businesses, and public agencies to respond to catastrophes and enhance the safety of individuals and communities after a disaster occurs.

11. *Train personnel so they can fulfil their roles and responsibilities.*
12. *Facilitate exercises to practice the operational procedures, both under standard and degraded or emergency conditions.*
13. *Set up a filing system for all documents right at the outset. This will spare much inconvenience, confusion and embarrassment, not only in internal use but also with respect to the institute's management, authorities, clients and, if applicable, inspectors of the accreditation body.*

Common conditions recommendations

1. Availability of resources
   - Humans (labour) – skills/competence
     - *The operational procedures should be defined by specialized personnel.*
     - *The procedures should also identify staff or team responsible for its application, if not identified elsewhere.*
   - Budget:*Budget planning should account for the required time in order to permit the knowledge and testing of the operational procedures.*
   - Data & Algorithm:
     - *Use official and standardized formats and test them where applicable.*
     - *The operational procedures should be defined in compliance to existing regulations.*
2. Training and experience

The operational procedures should be the subject of training and feedback should be collected during training phase.

3. Quality of communication
   - *Effective and cohesive organisational communication is fundamental for the suitable dissemination, implementation and enforcement of procedures.*
   - *There must always be a mechanism for informing potential users that a new SOP has been written or that an existing SOP has been revised or withdrawn.*
4. Human Computer Interaction and operational support

The development and review of procedures should be as much as possible based on local knowledge of operations and on operators initiative.

5. Availability of procedures and plans

Sources

- http://floridadisaster.org/documents/CEMP/Emergency%20Operations%20Plan.pdf
- http://www.odpm.gov.tt/sites/default/files/NEMA%20Disaster%20SOPs%20and%20Contingency%20Plans%202000.pdf
- https://www.gatwickairport.com/globalassets/publicationfiles/business_and_community/regulation/economic_regulation/14-10-01-operational-resilience-report-and-monitoring-report-final-for-publication.pdf
- http://sydney.edu.au/whs/emergency/emergency2.shtml
- ISO 22320:2011, Societal security – Emergency management – Requirements for incident response
- https://www.fas.org/sgp/crs/homesecRL32520.pdf
- http://emergency.cdc.gov/planning/

Limitations

Limitations in relation to operational procedures might be related to their complexity and non-applicability

The existence of regulatory bodies or certified management systems (i.e. ISO) that determine the need for safety and operation procedures should be used as guidance. In most cases, management processes establish the need for procedural initiatives and the periodicity of their review.

6. Conditions of work

   N/A

7. Number of goals and conflict resolution

   - *The operational procedures should have a well-defined target in relation to the addressed facility and personnel. They serve as a goal conflict avoidance and/or regulating mechanism.*
   - *The operational procedures should provide specific information for special categories of users.*

8. Available time and time pressure

The operational procedures should be specific, clear and succinct.

9. Circadian rhythm and stress

N/A

10. Team collaboration quality

Roles should be clearly identified when developing or reviewing procedures, in order to ensure that all relevant competencies and operational levels/areas are included in the process. Procedures should emerge from multi-competency team collaboration processes.

11. Quality and support of the organization

The organization should support the financial aspects in relation to operational procedures definition, training and testing.

Interdependencies recommendations

Risk assessment

- *Risk assessment provides the factual basis for activities proposed in the strategy portion of a hazard mitigation plan. An effective risk assessment informs proposed actions by focusing attention and resources on the greatest risks. The four basic components of a risk assessment are: 1) hazard identification, 2) profiling of hazard events, 3) inventory of assets, and 4) estimation of potential human and economic losses based on the exposure and vulnerability of people, buildings, and infrastructure.*
- *The risk assessment should provide the basis for procedures development and should follow a standard (e.g. OSHAS); nevertheless in case of missing or incomplete risk-assessment the process of developing procedures should overcome to this in Step 2. The process should be also continuously updated and learned.*

Operation plan

- *The Operational Plan does present highly detailed information specifically to direct people to perform the day-to-day tasks required in the running the organisation. Organisation management and staff should frequently refer to the operational plan in carrying out their everyday work.*
- *Procedural documents, the SOP, describe how to accomplish specific activities needed to finish a task or achieve a goal or objective. Put simply, Operational Plans describe the “what” and SOP describe the*

> *"how." The SOP should grow naturally out of the responsibilities identified and described in the Operational plans.*

Safety regulation

All defined procedures should follow standard guidelines in relation to existing safety and health regulations (e.g. OSHAS 18001).

3.4.8 Manage human resources

Background facts

Strategic workforce planning should address two critical needs:

(1) aligning an organization's human capital program with its current and emerging mission and programmatic goals and

(2) adopting long-term strategies for acquiring, developing, and retaining competencies and expertise to achieve programmatic goals.

HR function develops effective human capital management strategies to ensure the organization is able to recruit, select, develop, train, and manage a high-quality, productive workforce in accordance with merit system principles. This sub-function includes:

- developing human resources and human capital strategies and plans;
- establishing human resources policy and practices;
- managing current and future workforce competencies;
- developing workforce and succession plans;
- managing the human resources budget;
- providing human resources and human capital consultative support;
- measuring and improving human resources performance;
- determining, implementing, monitoring, reviewing and evaluating human resource management strategies, policies and plans to meet business needs;
- advising and assisting other managers in applying sound recruitment and selection practices, as well as appropriate induction, training and development programs;
- developing and implementing performance management systems to plan, appraise and improve individual and team performance;
- representing the organisation in negotiations with unions and employees to determine remuneration and other conditions of employment;
- developing and implementing occupational health and safety programs and equal employment; opportunity programs, and ensuring compliance with related statutory requirements;
- overseeing the application of redundancy and other

Abstract

The guideline is devoted to provide advice for dampen the Human resource management function variability. Human resources management is devoted to hire experienced human resources, develop human capital and to manage human reliability in task execution. To this end, skilled HR manager should be employed, and a person centric approach considering not only the skill at work but also parameters as family conditions, attitude, belief, etc. should be applied. Such a complex way to manage human resource require advanced software application

Questions

– What is the effectiveness of personnel selection?
– Are selection processes aligned with cooperate policies and strategic goals?
– Are selection processes responding to skill and competence needs?
– How often are selection processes and HR policies reviewed?
– How are HR needs assessed and how often are they reviewed?
– How is employee performance assessed?
– Are performance assessment criteria aligned with corporate policies and strategic goals?
– What mechanisms are in place to ensure the sharing and integration of corporate values? How is organisational culture promoted?
– How much effort is allocated to support communication?
– How much effort is allocated to support team collaboration?
– How the organization guarantees redundancy in decision making?
– How conflicting goals are managed?
– Are employees encouraged to develop new skills and use initiative?
– Can the task be redesigned?

employee retrenchment policies;
- monitoring employment costs and productivity levels;
- training and advising other managers in personnel and workplace relations matters.

Anyhow there are several drawbacks that may increase the function variability up to an undesired level, such as:

- Personnel
  - Different ranks
  - Different experience levels
  - Different skill and competencies
- No standard approaches for HRM systems
- The lack of data
- Non-harmonized processes
- Classification problems
- Insufficient synchronization
- Skill mismatch
- Lack of common language based on occupational areas
- An organization that supports HCM provides employees with clearly defined and consistently communicated performance expectations. Managers are responsible for rating, rewarding and holding employees accountable for achieving specific business goals, creating innovation and supporting continuous improvement

General recommendation

- *Human resource availability needs to be secured for both daily activities and during emergency. A dedicated buffer capacity (e.g. stand-by staff) should be defined in advance and tailored according to emergency scenarios.*
- *Implement a Human Resource Management system/Human Capital Management System.*
- *The skills and expertise that staff develops over years in performing highly complex processes, constitutes a critical operational asset. The retirement, dismissal or leave of absence of specialised staff should be anticipated and accounted for, namely by provided a sufficient overlap period with replacement staff to support suitable on-job training.*
- *The 10 human capital components that a CI should develop are:*
  1. *Organizational design*
  2. *Leadership*
  3. *Culture*
  4. *Engagement & awareness*
  5. *Learning & adapting*
  6. *System thinking*
  7. *Safety and Security behaviour*
  8. *People analytics*

Examples

US. Department of Energy Office of the Chief Information Office – (OCIO)

The OCIO Human Capital Management Plan is designed to support the mission of the OCIO. The OCIO continues its focus on the full range of human capital initiatives, and we continue to align our human capital management to support the mission of the organization

Training needs assessments of the current workforce are conducted and key competencies for development are identified to accomplish the OCIO Focus Points and DOE Strategic Plan through appropriate training, mentoring, and developmental assignments. Given a high number of eligible retirees in the near term, succession planning is underway through the utilization of National Defence University Development Programs, appointment to task/working groups, and detail/developmental assignments to ensure employees are better positioned to transition into leadership positions and through initiatives that maximize the use of corporate knowledge management. From an enterprise perspective, qualification of IT Project Managers identified in the Capital Planning and Investment Control process on Exhibit 300s is an ongoing initiative to ensure that employees managing multi-million dollar IT projects have the necessary skills to manage within cost, on schedule, and within performance targets.

9. *Workforce management*
10. *HR Manager skill*

- *HR should manage employee stress and burnout threats caused by internal (e.g. work conditions, task assignments, human relationship (e.g. mobbing)) and external factors (e.g. family status, mourning) taking into account both psychological and physiological health. Every stress and burnout threat detected by medical controls should be communicated to the HR in due time in order to allow for the application of specific countermeasures (e.g. shifts rescheduling, vacations, different tasks assignment) to mitigate the risk of errors/failures or of self-harm actions (e.g. Germanwings Flight 9525 crash). To this end a strong connection (e.g. procedure) between medical services and CI HR management should be established, balancing the privacy and security issues.*

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence
  - *Compensation and Benefits management skill: Being able to keep compensation and benefit packages attractive over time is essential to retaining top talent.*
  - *Recruitment and Hiring skill: A complementary set of decision-making skills, avoid biases skill and strong interpersonal skills are necessary skills for an effective hiring manager.*
  - *Performance/Employee Evaluation skill: Developing a successful and meaningful performance evaluation process takes time and innovation. Human resource managers who actively develop programs that engage the employee in an on-going professional development process help build a dynamic workforce. In order to frame performance evaluations positively, human resource managers need to develop versatile communication skills.*
  - *Training and Staff Development skill: In the role of a training and staff development leader, human resource managers have an opportunity to develop a wide range of important skills such as leadership, team building, teaching, tutoring, etc.*
  - *Adaptation and flexibility skill; HR managers must be well prepared to respond to rapidly changing workforce dynamics. With three generations in the*

Performance plans for Senior Executive Service (SES) members and managers are linked to the DOE Strategic Plan and cascade to non-SES supervisory and employee performance plans/ expectations.

Outstanding performance is recognized through the use of monetary awards for performance, special act awards, quality step increases, and other innovative awards, including time-off awards and certificates of appreciation. The OCIO continues to support the Departmental initiatives for a flexible workforce

The OCIO is committed to build on the foundation already established to make workforce recruitment and retention decisions based on mission needs and customer expectations to close skill gaps in the short-term and long-term in its current and anticipated workforce; to employ a diverse workforce; provide for continuity of leadership through succession planning and professional/career development; continue to develop and foster knowledge management programs to share and transfer institutional knowledge; build a direct line between employee performance expectations and mission accomplishment; and utilize the current administrative tools and flexibilities in combination with innovative strategies to maximize return on investment.

Limitations

Limitations in relation to operational procedures might be related to their complexity and non-applicability.
The present guidelines do not recommend specific methodology or tools. Each tool or method can be considered suitable if is able to address the organizational goals in HR management.

modern workplace, managers need to be equipped with sound knowledge as well as a wide repertoire of skills to address the four top competency areas in human resources environments across all industries. Building effective communication skills, organizing complex corporate policies, preparing employee programs, and demonstrating creative problem-solving and conflict resolution ability, are among the top skills needed to be successful in a human resource management position.

- *Data & Algorithm*

Historic and updated performance data and its analysis in view of current operational conditions and the demands these may impose. Human Resources Management System/Human Capital Management ICT system (HRMS/HCM)

- *Use an auditable real-time HRMS/HCM system to maintain employee status, role information and system for collecting and analysing hiring data. In the back office, HCM is either a component of an enterprise resource planning (ERP) system or a separate suite that is typically integrated with the ERP. HCM is a software tool for both employee records and talent management processes. The records component provides managers with the information they need to make decisions that are based on data. Talent management can include dedicated modules for recruitment, performance management, learning, and compensation management, and other applications related to attracting, developing and retaining employees.*
- *HRMS/HCM software streamlines and automates many of the day-to-day record-keeping processes and provides a framework for HR staff to manage benefits administration and payroll, map out succession planning and document such things as personnel actions and compliance with industry and/or government regulations. While now nearly synonymous with HRMS, HCM systems usually go beyond*
- *HRMS/HCM should contain information about knowledge, skills and abilities (KSAs), interests General Work Activities, (GWAs) and work context*

- *Financial plan*

Sources

- EUROCONTROL - System Thinking for Safety: Ten Principles – Moving towards Safety –II
- EUROCONTROL (2013). From Safety-I to Safety-II: A White Paper. EUROCONTROL.
- Hollnagel, E. (2014a). Safety-I and Safety-II. The past and future of safety management. Ashgate.
- HSE publication HS(G)65 Successful Health and Safety Management - Health and Safety Executive (1997).
- US. Department of Energy - FY 2013 HUMAN CAPITAL MANAGEMENT PLAN - http://energy.gov/sites/prod/files/2013/05/f0/OCIOWorkforcePlan.pdf.
- Fiat Group Human Capital Management Guidelines
- University of Florida Essential Skills for the Human Resource Manager http://essentialsofbusiness.ufexec.ufl.edu/resources/human-resources/essential-skills-for-the-human-resource-manager/#.VvADa3BycQQ
- 220.0 - ANZSCO - Australian and New Zealand Standard Classification of Occupations, First Edition, Revision 1 - UNIT Group 1323 Human Resource Managers http://www.abs.gov.au/ausstats/abs@.nsf/0/7624A042D303B867CA2575DF002DA6CB?opendocument
- ISO/TC 260 Human resource management
- ISO/NP 30414 Guidelines -- Human Capital Reporting for Internal and External Stakeholders
- CANADA Information and Comunication Technology Council - CYBER SECURITY - Critical
- ICT Human Resource in the Digital Economy - http://www.ictc-ctic.ca/wp-content/uploads/2012/10/ICTCCyberSecurityReport1.pdf
- Forbes http://www.forbes.com/sites/jacobmorg

Recruitment activities should be in driven by the financial plan. According to this it is recommended to gather labour market intelligence coherently and consistently in order to quantify the skill requirements and its market value.

2. Training and experience

As the development of employees and the continuous improvement in corporate performance are strictly interrelated, the organization's main objective is to increase the value of internal human resources through targeted programs. Training and knowledge management, in fact, guarantee continuous improvement by developing cultural competencies, reinforcing the organization identity and spreading its values.

3. Quality of communication

Encouraging internal communication: To keep employees constantly informed of the organization activities and business development, a wide range of corporate communication means are in place (intranet, internal corporate magazines, etc.). Moreover, in order to promote an open and transparent organisational culture, the organisation should encourage continuous dialogue between managers and employees both informally, using an approach of listening, and through structured feedback meetings, primarily focussing on individual performance and professional growth.

4. Human Computer Interaction and operational support

Integrate HRM System with IT Physical Security Access control system to ensure real time employees' access management (e.g. terminated employees are consistently denied access, throughout the organisation).

5. Availability of procedures and plans

- *Adopt a Consistent Skill and Competencies Categorisation and Experience Levels -The aim is to develop a table-based structure on occupational areas, such as Administration, Intelligence, Operations, Logistics, etc. that categorise the manpower skills and associated competencies required. The Technical Team must use standardized Occupational Area Codes as the starting point to develop this catalogue.*
- *Catalogue of Current HRM Models, Methods, and Methodologies: The technical team should develop a catalogue that delineates the various models with*

– Kasthurirangan Gopalakrishnan Srinivas Peeta - Sustainable and Resilinect Critical Infrastrucutre System A framework for Manifestation of Tacit Critical Infrastructure Knowledge: Simulation, Modelling and Intelligent Engineering - Springer 2010
– Simon, H.A. Rational decision Making in business organization. American Economic Review 69 (4), 493-513 (1979)
– US DOE - SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Behavioural Interview Guidelines by Job Roles
– US Government Accountability Office - GAO http://www.gao.gov/assets/250/240817.html
– Electronic Communications Privacy Act (ECPA)
– NATO RTO Technical Report TR-SAS-059 Human Resources (Manpower) Management
– Pollack, L.J., Simons, C., Romero, H. and Hausser, D., "A Common Language for Classifying and Describing Occupations: The Development, Structure, and Application of the Standard Occupational Classification", Human Resource Management, Vol. 41, No. 3, pp. 297-307, Fall 2002.
– Occupational classification: ESCO – European Classification of Skills/Competences,
– ILO- International Standard Classification of Occupations (ISCO),
– US. Standard Occupational Classification (SOC),
– Holland, Hexegow, The world of work map (MM),
– The North American Industry Classifications Systems (NAICS),
– Occupational Information Network (O*Net),
– Skills and framework for the Information age (SFIA),
– NATO Occupational Code (NC),
– UNESCO International Standard Classification of Education (ISCED) 1997,
– Skills for the Information Age (SFIA) v3 2005.

their associated methods and methodologies that are currently used in their HRM. The group shall be responsible for categorising models, methods and methodologies.

- *Minimize downside to employees for participation, such as demotion, loss of employment or privacy.*
- *Include coordinated policy to appropriately scale employee access during high-risk periods, minimizing risk of sabotage.*
- *Use (available/CERT) research findings to develop a process and a set of policies focused to protect assets and operations while dealing with a potential hostile insider.*

– Fields of Education and Training Supplementary Manual 1999 (Statistical office of the European Communities-EUROSTAT)
– http://hrdailyadvisor.blr.com/2012/06/07/emergency-management-preparedness-what-is-hr-s-role/#sthash.kngr3C7W.dpuf
– University College London http://www.ucl.ac.uk/hr/occ_health/health_advice/managing_pressure

6. Conditions of work

- *Shift from a fully controllable resource to a new dimension that treats personnel issues such as working environment, warfare of personnel their feelings, creative personnel as high priority.*
- *Establish an all-party-consent statute to track information exchange (e.g. emails) and work behaviours for security and knowledge protection purposes.*

7. Number of goals and conflict resolution

- ***Motivational approach*** *– involvement of human resources through inducements and contribution strategy. Inducements are desired aspects of participation. For instance, inducements of working for a company are a suitable salary along with insurance options. Contribution on the other hand has a negative utility form the HR perspective, but is the requirements for participation. Inducements and contributions of a position in a system, should be contracted each other since human resource may not adhere to contribution.*
- *Ensuring equal opportunities Career opportunity and career progression are managed without discrimination while respecting and enhancing diversity. Considering skills as an asset to be developed and shared, organizations should be committed in helping people adapt in real time to change in an increasingly complex world.*
- *Attention to the* ***Work/Life Balance*** *- In order to promote respect for all employees as individuals, organization should promote care and attention to employees by supporting them in achieving a sustainable work/life balance.*

8 Available time and time pressure

HRs are the most effective means of coping with operational variability and the time pressure that often results from such variability. This should be taken into account, both in the management and the training of HR. Nevertheless working conditions should be designed in such a way that impacts of variability and time pressure are minimised and do not compromise inherent human adaptive capacities.

9 Circadian rhythm and stress

Human Resource management is a stressful activity that requires dedicated resources and specific organizations. The impact of stressed HR manager can be reflected on a wrong candidate evaluation, an under/over workload estimation, a task assignments to not skilled employee rising the risk of injuries or the failure or the task execution in due time, etc. The use of the software together with a proper rotation of the HR officers *among the HR management activities contributes to reduce the stress generated by specific situations (e.g. firings) or activities (e.g. high number of interviews).*

10. Team collaboration quality

- *HRM polices to be integrated with business strategies.*
- *Develop HRM policies in coordination with internal legal, security and human resources team managers and, where applicable, with the resource manager for job specific policies.*
- *Build a cross-departmental insider threat approach and response team, to include: IT, Physical Security, Legal, and Human Resources.*
- *Coordinate employee hiring, screening, and termination policies with legal team and asset owners/ risk managers to ensure legal team understanding of the potential costs of insider threats.*
- *Coordinate legal perspective with asset owners and risk managers to develop clear understanding of insider threat consequences and costs.*
- *Assign all employees with an active role in contributing to their own development and the success. In order to minimise the risk of work-related stress, staff must:*
  - *ensure good communication with colleagues and their manager;*
  - *support colleagues by providing appropriate information and by sharing knowledge and resources where appropriate;*
  - *engage in discussion about their performance and act on feedback;*
  - *raise issues of concern at an early stage and seek constructive solutions;*
  - *make use of the support and training resources available;*
  - *ensure that bullying and harassment is not tolerated;*
  - *comply with organization employment policies and policies on health, safety and security;*
  - *seek appropriate advice and support at an early stage if difficulties arise.*

11. Quality and support of the organization

- ***Establish** a strong Employee Assistance Program to help employees identify themselves and peers for assistance during high-risk periods of difficulty.*
- *Develop documents to establish accountability, e.g., employee's annual ethics certification, confidentiality agreements, supplier security requirements for contracts.*
- *Focus on Talent Management and Succession Planning: Talent Management is a key lever in achieving the organisation's talent development goals and releasing the potential of people. Therefore attracting, retaining and developing leaders which can face future challenges, thus giving priority to the development of internal resources, is crucial to solid succession planning. A consistent, global approach that encourages cross-functional and cross-sector mobility (even across geographies) allows capitalisation of the talent management process which constitutes an essential competitive advantage. This process ensures that the leadership pipeline is continuously fed at all levels of the organization.*

Interdependencies recommendations

- Emergency HR request
  - *Preparing for emergencies involves evaluating your risks, determining the legal and regulatory players, and determining the role of (and how to manage) unions, vendors, and contractors, especially on a multi-employer site. Moreover the cooperation with safety, engineering, risk management and operations to both address contributing factors and to implement best practices is recommended.*
  - *Establishing an institutionalised connection with emergency responders in order to create reliable communication channels. Such collaboration includes the participation in the investigation and root cause analysis, the contribution to define training requirements, etc.*

- *Managing pay and benefits for employees engaged in emergency respond and extra time work requested by the emergency.*
- *Create and maintain up to date an emergency plan for mobilizing right human resources in due time. In particular, it is necessary to establish a reliable engagement process with different level of employee readiness.*

- Operation HR plan
  - *Involve top management employees and other stakeholders in developing, communicating, and implementing the strategic workforce plan.*
  - *Determine the critical skills and competencies that will be needed to achieve current and future programmatic results;*
  - *Develop strategies that are tailored to address gaps in number, deployment, and alignment of human capital approaches, for enabling and sustaining the contributions of all critical skills and competencies.*

3.4.9 Manage ICT resources

Abstract

This guideline provides advice towards managing ICT resources in order to support critical infrastructure operation and management. The management of the ICT resources for a critical infrastructure includes the provision, maintenance, update and development of information and communication equipment and services. The guideline goes beyond common practices incorporating the concept of resilience. Recommended actions stress the importance of supply resources availability, operators' and citizens' training and experience, the need for communication quality and alternative communication channels, the required aspects of human-computer interaction and operational support, as well as the need for establishing and updating suitable ICT procedures and plans. Furthermore, principles are provided concerning the proposed conditions of work, the number of goals assigned to each worker, conflict resolution, timetable definition, time and stress management, the assurance of team work quality, the means for ensuring the safety/adequacy of ICT resources, and organization support. Finally, this guideline addresses interdependencies with other functions and imposed limitations, and gives some examples of existing implementations for managing ICT resources.

Background facts

Information and communication technologies (ICT) are at the core of many sociotechnical systems interdependencies. Across all industry sectors ICTs have introduced many new layers of complexity, mainly through the integration of operations and their centralised control at unprecedented geographical and organisational scales. The tight relations between an increasing number and diversity of stakeholders have made operations much more flexible and potentially more efficient. However, this has also generated new risk natures, which are yet to be suitably managed. In many cases, rather than the access or availability of information, the challenge has become the ability to process a growing volume and diversity of information, in order to produce meaningful support for operational and managerial decision-making.

ICTs are also important tools for lessening the risks brought on by disasters through early warning, coordinating and tracking relief activities and resources, recording and disseminating knowledge and experiences, and raising awareness. The challenge is gaining commitment to incorporate ICT tools effectively in disaster risk reduction (DRR), and providing favourable political, social and economic conditions for identifying and applying an appropriate mix of ICTs to address vulnerabilities in the different contexts.

Several case studies existing in literature examine the important role ICTs play in disaster preparedness, response and mitigation, and share the lessons learned by those disaster management practitioners who have deployed ICT in response to disasters in countries like Bangladesh, China, Sri Lanka, and Haiti.

Organizations need to act swiftly and decisively to ensure that they provide an enabling environment for the use of ICTs in creative ways towards disaster risk reduction. Unfortunately, many policymakers, including disaster management authorities, have yet to acquire the knowledge and skills needed to leverage opportunities provided by ICT and integrate ICT applications in their daily work.

General recommendation

- *ICT tools should be widely used to build* knowledge warehouses *using Internet and data warehousing techniques. These knowledge warehouses can facilitate planning & policy decisions for preparedness, response, recovery and mitigation at all levels.*

- *ICT tools should include **GIS-based systems** to improve the quality of analysis of hazard vulnerability and capacity assessments, guide development planning and assist planners in the selection of mitigation measures.* In particular, *Geographic Information Systems (GIS) provide a multilayer geo-referenced information which includes hazard zoning, incident mapping, natural resources and critical infrastructure at risk, available resources for response, real time satellite imagery etc. GIS-based information tools allow disaster managers to quickly assess the impact of the disaster/emergency on geographic platform and plan adequate resource mobilization in most efficient way. Thus, a reliable GIS-based database will ensure the mobilization of right resources to right locations within least response time. Such database would also play a fundamental role in planning and implementation of large scale preparedness and mitigation initiatives.*
- *Communication systems have also become indispensable for providing emergency communication and timely relief and response measures GIS-based technology solutions and **remote sensing** should be extensively used in disaster management activities.*
- *During any emergency situation, the role of a reliable **Decision Support System** is very crucial for effective response and recovery.*
- *In the emergencies field, social media (blogs, messaging, sites such as Facebook, wikis and so on) should be also used in seven different ways: listening to public debate, monitoring situations, extending emergency response and management, crowd-sourcing and collaborative development, creating social cohesion, furthering causes (including charitable donation) and enhancing research*
- *The following are some of the media – both traditional and new – that can be effectively used for disaster warning purposes:*
    - *Telephone (Fixed and Mobile)*
    - *Short Message Service*
    - *Cell Broadcasting*
    - *Satellite Radio*
- *The International Telecommunication Union (ITU) has identified various radio communication media that can be used in disaster-related situations:*
    - *Internet/Email*
    - *Amateur and Community Radio*

Questions

- When and why is the list of events revised?
- Which are the stakeholders that should be involved and how?
- How the roles and responsibilities are clearly defined?
- How the processes are defined, established and communicated?
- When a process or a procedure is revised?
- When a new procedure is added?
- How often is the match between resources available and resource needs assessed?
- Does planning take into account all resource needs?
- Is the match between resources available and resource needs assessed?
- How should the organization manage sources of information, e.g. sensors, cameras, staff, etc. in order to get a realistic picture

Examples

UbAlert
UbAlert is a global social network that operates to save lives by sharing the knowledge of the world's citizens with those in danger.

IDRN
IDRN is a nation-wide electronic inventory of resources that enlists equipment and human resources, collated from districts, states and national level line departments and agencies.

Tsunami Early Warning System (TEWS)
The Tsunami Early Warning Systems (TEWS) is a set of common protocols and procedures used to ensure that tsunami advisories or warning messages are sent from a national focal point to all relevant government officials and the public quickly and accurately.

- *Sirens*

The role of the ICTs in emergencies is of vital significance, especially in the first days of the emergency. Due to this the management of the ICT should be based on a well-established plan, regarding all the possible difficulties and taking into account all ICT resources needs. The management plan should reference in detail the procedures that have to be followed in crisis and have to be easily adaptive to new conditions.

Technical experts have to be trained properly to manage, update and repair the ICT resources, in order to guarantee the quality and the reliability of the ICT services

ICT infrastructure should support the escalation strategy coping with the increased demand of computation and connectivity during the emergency. To this end a cloud based approach and virtualization are solutions to be taken in to account.

ICT should be considered a critical infrastructure for the organization existence. To this end it requires to be protected against cyber and physical threats. The application standards to manage the data centres as well as the redundancy and backup strategy of hardware, data and services should be considered.

A specific attention should be dedicated to the long term preservation of organization memory/knowledge*. It is necessary to define, apply and support a digital preservation strategy to maintain accessible documents, archives, and data in long run while preserving their integrity, renderability, authenticity, discoverability, reuse. It is also necessary to nominate a reference of the digital preservation strategy (the digital curator) to continuously monitor the status of the preservation and to improve the strategy cording to the organizational needs. . Such strategy should be communicated to the stakeholders.*

Common Alerting Protocol (CAP)

The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

Reuters AlertNet

Reuters AlertNet is a good example of an ICT/media initiative set by the Reuters Foundation that contributes towards early disaster warning and management at an international level. AlertNet covers natural disasters, conflicts, refugees, hunger, diseases and the human impacts of climate change.

Limitations

- ICT cannot eliminate possible economic loss and damage to property in case of a disastrous event but it can mitigate its negative impacts
- Lack of adequate financial support.
- Limitations set by energy, technology, communication channels
- Limitations set by governments, legislation, cyber security regulations and international standards.

Common Conditions recommendations

1. Availability of resources

- Supply resources:
  - *Information stored in Databases referring to :*
    - *System operation performance, resources and capacities*
    - *Disaster history for trend & pattern analysis*
    - *Disaster management plan*
    - *Human & material response resources*
    - *Trained human resources*
    - *Satellites (whereabouts, size etc.)*

  - o *Demographic information*
  - o *Hazard mapping & vulnerability Assessment*
- *Easy access to GIS (Geographical Information System) based information system.*
- *System for analysing data retrieved from social media in order to provide a detailed, real-time map of displaced people, fatalities and damages to properties.*
- *Technical Equipment: Computers, Servers*, *Cameras, Wi-Fi, Sensors (Touch/Proximity, fire/flood/tsunami/earthquake detection sensors), Sensor Networks, GPS, Wearables, Bluetooth*
- *Alternative communications (e.g. ad-hoc networks, satellite radio, sat-phones etc.) to cope with emergency cases.*
- *Electrical energy for supplying the ICT resources.*

2. Training and experience

- *Training of technical experts in order to be able to manage, update, and repair in time the ICT resources during an emergency.*
- *Regular test exercises for the technical experts.*
- *Education and creating awareness in the population so that they may respond with the appropriate action.*

3. Quality of communication

- *Guarantee the quality and reliability of the communications (referring to the technological aspects).*
- *Provide alternative (emergency) communication types employing both terrestrial and satellite-based technologies to establish a network for emergency communications.*

4. Human Computer Interaction and operational support.

- *User-friendly platform for the technical experts and the citizens.*
- *Easily manageable by people with special needs.*
- *Operational platform which will ensure the communication of citizens and rescuers in emergencies.*

5. Availability of procedures and plans

- *An ICT management plan should be established in an early stage and updated regularly.*
- *Several plans for acting in emergency situations, regarding all the possible difficulties, have to be developed.*
- *Plans should take into account all ICT resources needs.*
- *Detailed reference to the procedures that have to be followed.*

6. Conditions of work

Sources

- Communication Technology for Development (APCICT), ICTD Case Study 2, May 2010
- ICT for Disaster Risk Reduction - The Indian Experience, Ministry of Home Affairs, National Disaster Management Division Government of India
- Alexander, David E. "Social media in disaster risk reduction and crisis management." *Science and engineering ethics* 20.3 (2014): 717-733.
- Country Case Studies in ICT for Disaster Management of India, Ms. Renu Bhudhiraja
- The role of ICT during the disaster – A story of how Internet and other information and communication services could or could not help relief operations at the Great East Japan Earthquake, Izumi Aizu
- *Doran, G. T. (1981). "There's an S.M.A.R.T. way to write management's goals and objectives". Management Review (AMA FORUM) 70 (11): 35–36*
- ICT for disaster risk reduction, Asian and Pacific Training Centre for Information and
- Gander, Philippa, et al. "Fatigue risk management: Organizational factors at the regulatory and industry/company level." *Accident Analysis & Prevention* 43.2 (2011): 573-590.
- Hoegl, Martin, and Hans Georg Gemuenden. "Teamwork quality and the success of innovative projects: A theoretical concept and empirical evidence." *Organization science* 12.4 (2001): 435-449.
- ICT for Disaster Risk Reduction - The Indian Experience, Ministry of Home Affairs, National Disaster Management Division Government of India
- http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html
  - http://nctr.pmel.noaa.gov/
  - https://en.wikipedia.org
  - https://www.ubalert.com/U4gc
  - http://idrn.gov.in/default.asp

- *Friendly working environment*
- *ICT infrastructure should be accessible for all.*

7. Number of goals and conflict resolution

- *The ICT management plan should set goals and objectives that are S.M.A.R.T (Specific, Measureable, Actionable, Relevant, Time-framed).*
- *The roles and responsibilities of each team member should be clearly define d and not overlapped in order to avoid conflicts.*
- *The number and scale of tasks/responsibilities assigned to each person should be reasonable (and not excessive) based on the ICT management plan and the corresponding timetable.*
- *Specific rules/principles should be defined in conjunction with a hierarchical working structure in order to address possible conflicts.*

8. Available time and time pressure

- *Planning milestones and deadlines should integrate degrees of flexibility to cope with planning quality requirements.*
- *Timely disaster warning to mitigate negative impacts. Such warnings must be unambiguous, communicate the risks succinctly and provide necessary guidance.*
- *The potential of most advanced technologies is required to be harnessed in early warning, preparedness and response systems along with adequate emphasis on building human capacities to use these tools and technologies.*
- *In emergencies the importance of the ICT support is of vital significance especially in the first 72 hours referred as "Golden 72 Hours". Moreover, during this period any damages in the communication infrastructure have to be repaired.*

9. Circadian rhythm and stress

- *A plan should be defined for managing the risk of employee fatigue and the disruption of the circadian rhythm in safety-sensitive businesses (e.g. a Fatigue Risk Management System (FRMS) in order to reduce the possibility of critical human errors.*
- *The management of ICT resources should be such that it reduces sources of stress for ICT operators.*
- *In case of critical operations carried out by only one person a second person should be in stand-by.*

10. Team collaboration quality

- *Adherence to the principles of collaborative planning through the development of mutual benefit relations.*
- *Adherence to the facets of teamwork quality (communication, coordination, balance of member contributions, mutual support, effort, and cohesion).*
- *Utilize suitable team collaboration tools to ensure effectiveness.*
- *Establish tools/methods for evaluating often team collaboration quality (e.g. Col-MM)*
- *Continuous training of the team to retain the quality of the team's collaboration in high level.*

11 Quality and support of the organization

- *Perform external and internal audits to ensure the safety/adequacy of ICT resources.*
- *Ensure that ICT resources are managed based on the predefined plan.*
- *Quality assurance plans for information and communication services.*
- *Support from the local bodies (fire department, police, government, rescue teams etc.)*

- *In emergency response and management, it is extremely important to have the communication links operational between decision makers at various levels and operational response teams/personnel on the site.*

<u>Interdependencies recommendations</u>

- In order to monitor the operation of the critical infrastructure the ICT equipment and services have to be set/installed.
- The definition of the procedures has to be performed considering the requirements of the ICT infrastructure.
- The coordination of emergency actions is based on the quality and the readiness of the ICT resources.
- Supply resources availability should be monitored in order to ensure ICT proper operation. In case a problem is detected immediate action should be taken based on the backup plan in order to reduce any negative consequences.
- User generated feedback should be considered in a timely manner in order to ensure proper and efficient ICT operation.

3.4.10 Maintain physical/cyber infrastructure

Background facts

Maintenance, and hence maintenance engineering, is increasing in importance for modern critical infrastructures due to rising amounts of equipment, systems, software applications and where machinery and structures have grown increasingly complex, requiring a host of personnel, vocations and related systems needed to maintain them.

Maintenance mainly responds to operational safety requirements. It remains one of the most significant costs for infrastructure managers. As attempts are made to maximise the operational use of infrastructures, ware out levels of assets also tend to increase, and thus, maintenance needs are likely to be intensified. Not only often assets must be redrawn from operation to carry out maintenance, but also increasingly skilled and specialised staff and equipment are needed to perform maintenance operations.

It is virtually impossible to formulate a classification of types of maintenance but it can, in general, be possible to divide it in ordinary and extraordinary. It is called ordinary or preventive maintenance when performed periodically, at predetermined intervals of time or after a given period of operation (e.g., substitution at fixed intervals of certain parts of the technology and parts); it is called extraordinary or corrective maintenance when performed as a result of unforeseen or exceptional events (floods, disruption of defective parts, etc.).

The ordinary maintenance of an apparatus must be limited to that component or those components, whose average life is significantly less than the life of the CI itself, and this because the cost of maintenance is less than the damage caused by the failure of the component and the subsequent repair. During the operation of a CI, it can happen that technical progress makes the plant or the machinery itself economically surpassed for their excessive cost of maintenance; for that reason, there rises the need to proceed with infrastructure renovation and purchase of new machines even when the old ones are still technically valid.

For what regards cyber infrastructures (e.g. ICT equipment), maintenance includes a set of activities that have to be performed on software or hardware to allow them to work to the best of their potential. While the case of hardware assets maintenance can be traced back to normal industrial

Abstract

This guideline aims at providing best practices and references for coordinating the maintenance service to keep systems, equipment, hardware assets, ICT and other infrastructure facilities (e.g. smart city assets for mobility, energy, telecommunication) in operation, and operating efficiently and safely.

It includes many tasks including repairing, replacing, servicing, inspecting and testing. The maintenance is also related to the importance of keeping staff safe, fit and healthy.

To reduce the risks and make the system more resilient, the deployment of maintenance actions is of prime importance both in the design phase and in the operating phase.

Besides, it helps to eliminate infrastructure hazards. Lack of maintenance or inadequate maintenance can lead to dangerous situations, accidents and health problems. It is requested that a planned maintenance program is in place and that all maintenance work is risk assessed before beginning the task.

There are normally two main types of maintenance work. Routine/Preventative Maintenance is mandatory to prevent critical situations in the infrastructure and it is usually planned by defining scheduled inspections, repairs and replacement to make sure everything continues to work. Instead, Corrective Maintenance is needed when failures happen on Physical, Hardware or Software Infrastructures, and critical scenarios occur demanding reactive action to be taken to get systems up and running again.

maintenance activities of the machinery, in the case of software managing complex information systems, the maintenance processes are more complex, having to consider also backwards compatibility and several integrations with other IT systems.

The maintenance activities require an active monitoring of physical components since aging and degradation poses significant safety concerns, especially in light of increased use of these structures or climate changes. The economic downturn further exacerbates such concerns, especially for critical structures such as bridges, where replacement is infeasible and maintenance and repair are expensive. The US Federal Highway Administration has classified over 25% of the bridges in the United States as either structurally deficient or functionally obsolete, underscoring the importance of structural health monitoring to ensure public safety.

Depending on importance, ownership, use, risk and hazard, such structures have inspection, monitoring and maintenance programmes that may even be mandated by law. The effectiveness of maintenance and inspection programs is only as good as their timely ability to reveal problematic performance, hence the move to supplement limited and intermittent inspection procedures by continuous, online, real-time and automated systems.

Questions

- For which equipment is there a test ready?
- What is the threshold of the result of the test? (Rate of change)
- How was the test determined?
- How many resources are allocated to maintenance?
- Which are the stakeholders that should be involved and how?
- How the roles and responsibilities are clearly defined?
- How the processes are defined, established and communicated?
- When a test or a procedure is revised?
- When a new test is added?
- Do you have a diary of events
- How do you monitor the current status of physical equipment?
- What happens when a test is failed?
- How maintenance is managed during day-by-day operations?
- How the communication between validators and operative is managed?
- How the quality of communication is measured (e.g. response time)?

Major drivers in this area have been the oil industry, operators of large dams and highways agencies, whose installations have received the greatest attention and research effort. Residential and commercial structures have received relatively little attention due to potential obligations and consequences of owners knowing about poor structural health. In these cases, structural health monitoring (SHM) can only be implemented after efforts have been made to educate owners or to coerce them via building control protocols (legislation) or insurance premiums.

A significant challenge in developing an SHM strategy for civil infrastructure is that except for certain types of public and private housing, every structure is unique. This means that there is no baseline derived from type-testing or the expensive qualification procedures applicable for aerospace structures. Hence, a unique feature of SHM for civil infrastructure is that a major part of the system has to be geared towards a long-term evaluation of what is ‘normal’ structural performance or ‘health’, the two terms being synonymous.

Historically, the monitoring of structures has involved many ingredients of the modern SHM paradigm, such as data collection and processing followed by diagnosis. At the simplest level, recurrent visual observation and assessment of structural condition (cracking, spalling and deformations) could be viewed as SHM, yet the aim of present-day discipline is to develop effective and reliable means of acquiring, managing, integrating and interpreting structural performance data for maximum useful information at a minimum cost, while either removing or supplementing the qualitative, subjective and unreliable human element. Historical developments in SHM have generally focused on subsets of the SHM paradigm, but in recent years, a few studies have begun to focus on, or at least recognize, the need for a holistic approach to optimization of SHM.

General Recommendations

- *Maintenance should adopt an "asset management" approach in order to: a) evaluate an monitor the resource lifecycle b) evaluate and monitor financial sustainability c) maximise the life of the asset while reducing the costs. Thus maintenance can be considered as factor of cost reduction, competitiveness and safety increment.*

  Within asset management the Condition Based Maintenance (CBM), an application of the Reliability Centred Maintenance approach (RCM) should be taken into account. In fact maintenance needs should be tailored to specific asset performance data, whilst having to continuously minimise its disruption in favour of operational efficiency. Hence, intelligent maintenance is required to significantly enhance its flexibility and ability to adapt to continuously changing operational conditions. To this end CBM implements a method based on real time infrastructure status monitoring, so that the maintenance is triggered only when necessary.

  According to the Prognostic and Health Management (the most advanced CBM application) three main actions are necessary in maintenance:

  a) *Advanced fault detection (remote control, thermography, IoT, etc.)*
  b) *Data driven fault diagnosis (data mining)*
  c) *Prognostic (predictive modelling)*

- *Infrastructures should be continuously monitored against environmental threat (such as nuclear, biological, chemical, and explosives), infrastructure condition (e.g. integrity), through object sensors, video and audio surveillance equipment, multispectral analysis, etc. Data from such sensors and surveillance equipment may be processed in the field or sent to a centre for processing.*
- *Supervisory Control and Data Acquisition, or SCADA systems are specialized computer networks and devices widely installed in power, industrial and transportation networks that work in concert to monitor and control key processes involved in the management of machinery, equipment and facilities.*
- *Measurements taken from a variety of sensors (temperature, pressure, flow etc.) are used to make decisions, for example to open a valve and release*

Examples

1. The maintenance of a telecommunication network is an implementation example of both a cyber and physical infrastructure:
   - A proper multi-organization GIS is needed to ensure that under-pavement pipes containing optical fibers are well-known by all actors doing street works.
   - A failure at the physical optical fibre pipe may lead to a failure of thousands of cyber infrastructures, even critical.
   - People working on the telecommunication network need to be well trained and not under stress in order to perform the complex task of posing, configuring and settling down the fiber optical network in the streets.
   - A proper communication needs to be set-up among people working on the physical and cyber infrastructure, because workers configuring routers need also to know specific constraints given by the physical network topology.
   - Very detailed written procedures are required in order to perform proper maintenance upon the network, even if the complexity of the system often requires the full skill of the worker in order to adopt un-documented and unexpected actions.
2. The maintenance of the Tree Eco-system of a city is another interesting example where a proper maintenance of both a physical and cyber infrastructure are addressed.
   - A proper GIS is needed to map all the trees, to keep track of all the past maintenance activities on each tree, and to assess all the vulnerabilities given a specific species of the tree
   - A very careful vulnerability analysis need to be performed continuously, in order to avoid

water from a tank when it fills up, or to initiate an emergency shutdown of an electrical substation.

branches falling down with possible serious risks for people.

- A very reactive alert sensor-based system can be associated to the Tree eco-system and maintained, in order to rapidly alert population to avoid parks or dangerous sites when strong wind storms are forecasted

Common Conditions recommendations

1 - Availability of resources

- Humans (labour) – skills/competence
- *A significant challenge for maintenance management professionals of critical infrastructures is related to the need for them to possess a truly multi-disciplinary set of competencies. The competences requested today to maintenance engineers span a wide range and go from specific technical knowledge of the systems and components of the infrastructure to expertise relevant to standardized international processes and local practices.*
- *In Europe, maintenance competence requirements are usually based on standardisation bodies' recommendations, or requirements defined by National bodies, such as the Institute of Asset Management (IAM) in the UK, or the European Federation of National Maintenance Societies (EFNMS). Demand for certification in specialised maintenance has also lead to standardisation. Different training methodologies are applicable to support competencies development in a practice-oriented discipline, such as Maintenance Management.*
- *An innovative approach to the predictive maintenance thread is asking today for new ICT competences and skills to be able to understand and manage tools implementing new information technology paradigms, such as big data and machine learning.*
- *A continuous exchange of information between maintenance personnel and the other infrastructure's stakeholders, including the management, should be put in place in order to increase the level of awareness on the real status of the infrastructure.*
- Budget:
- *Adequate financial resources have to be reserved for acquiring new ICT systems and tools, as well as to update those currently used, with the aim to improve awareness on the real level of the system health and safety.*
- Data & Algorithm:
- *Historic and fabric data on characteristics and features of constructions, systems and all technological devices being part of the infrastructure.*
- *Use of standardized project management concept, models and protocols.*
- *Data coming from all the systems and information technology tools collected to monitor and control the critical infrastructure during normal operation.*
- *Reliability, Availability, Maintainability and Safety (RAMS) practices and algorithms for calculating the target thresholds according to the maintenance objectives.*
- *Data/information collected by on field operators and citizens during standard infrastructure operation.*
- *Integration of new IoT data*

2. Training and experience

- *The increasing importance given by modern Infrastructure Management authorities to quality and safety, while meeting sustainability targets, has upgraded the attention paid to effective maintenance and asset management, which is considered critical by all stakeholders. However, maintenance management training is rarely included in formal education. It requires multi-disciplinary skills, which in most cases are not readily targeted by higher education or postgraduate courses. Efficient maintenance management* *training enhances the capacity of human capital to contribute towards the enterprise strategic goal of rationalizing asset usage and increase the safety.*

- *More efficient training can be achieved through on-the-job training (OJT). However, real-life OJT can incur significant costs. Imitation of OJT can be achieved by augmented reality (AR) for problem-based maintenance training, avoiding the cost of setting up a real case. Yet, AR is still rather expensive and mostly applicable to special training. E-learning can support asynchronous training in a cost-efficient way. With personalized virtual environments, trainees can choose the training pace, the course subjects and self-assessment that fit their needs.*

3. Quality of communication

- *Guarantee a structured and validated flow of information among maintenance personnel, decision makers and citizens (the final users of the infrastructure) aiming at increasing the awareness level of the real status of the infrastructure.*
- *Guarantee the accuracy and understandability of the communication through standardized communication tools, protocols and languages.*

4. Human Computer Interaction and operational support

- *Utilization of maintenance software tools for real time and offline data analysis and maintenance focused intervention plans.*
- *Utilization of software tools implementing standardized and local maintenance procedures and practices permitting operative personnel and infrastructure managers to take right decisions.*

Limitations

Complexity of the Physical/Cyber Infrastructure leads to parts or subsystems not properly maintained, which becomes then a vulnerability in case of failure or emergency.

Many of the current technologies (e.g. Internet of Things) are lacking consolidated standards and reference maintenance procedures; this can lead to vulnerabilities.

Strength of environmental disasters may overcome the limits of tolerance to system failure of the asset, even if maintained.

Communication failures among the many and heterogeneous actors of the physical and cyber infrastructure maintenance may lead to cases where the single part or subsystem is well-maintained, but the system as a whole is not.

Lack of dedicated human resources often forces the same person maintaining multiple systems, thus causing stress and error-prone activities. Difficulty to scale the monitoring system to city level

Difficulty to share diagnostic information between heterogeneous systems

Difficulty to share information between systems managed by different entities

5. Availability of procedures and plans

- *Decide on the best practices based on standards to be adopted for infrastructure maintenance management in order to increase resilience level.*
- *Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation's change management procedure. Include periodic reviews against business needs, patch management, upgrading strategies, risks, vulnerabilities assessment and security requirements.*
- *Strategic financial plan aiming to assure a stable and accurate maintenance of the critical infrastructure.*

6. Conditions of work

Guarantee an efficient flow of information through infrastructure's stakeholders increasing in this way the awareness on the status of the systems and facilitating the decision making process.

7. Number of goals and conflict resolution

- *Roles and duties of the different actors maintaining a complex physical or cyber infrastructure need to be defined and documented in order to reduce conflicts during intervention upon failure or regular ordinary maintenance operations.*
- *The efforts and the timing during the emergency should be reduced by being able to early detect the anomaly generating the crisis.*
- *The amount of data collected during standard operation to be used during the emergency should increase.*

8. Available time and time pressure

- *Maintenance personnel shall be able to help people dedicated to emergency management in a very short-time.*
- *Standard maintenance activity shall be carried out during normal infrastructure's operation.*
- *Workers need to be trained to perform rapidly during normal maintenance operation, in order to be able to solve rapidly failures during emergencies.*

9. Circadian rhythm and stress

To ensure that physical and cyber infrastructures are properly managed and well-maintained, it is important also to allow workers proper time shifts. As a matter of fact, the stress and the excess of working hours can lead to human errors in following written procedures for the infrastructure maintenance.

10. Team collaboration quality

High quality of human relations is required, in particular among technical personnel of critical infrastructure, infrastructure managers and emergency stakeholders.

Sources

- ISO/TC 71/SC 7 - Maintenance and repair of concrete structures (ISO 16311-x, ISO/TR 16475, ISO 16711, ISO 16774-x)
- NEMA ICS 1.3-1986 (R2015) Preventive Maintenance of Industrial Control and Systems Equipment
- ANSI/NEMA KS 3-2010 Guidelines for Inspection and Preventive Maintenance of Switches Used in Commercial and Industrial Applications
- AGA X01084 LNG Preventive Maintenance Guide
- NFPA 70B-2013 Recommended Practice for Electrical Equipment Maintenance, 2013 Edition
- Information Technology Infrastructure Library (ITIL) practices for IT Service Management
- ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems
- https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf
- https://standards.ieee.org/findstds/standard/C37.1-2007.html
- ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries
- Vestrucci, La Rovere - Quando come e perche' innovare la manutenzione – Manutenzione & Innovazione 2013

11. Quality and support of the organization

- *Clear decision making process and alignment of responsibility with accountability.*
- *Maintenance organization shall be characterized by task assignments, workflow, reporting relationships, and communication channels that link together the work of diverse individuals and groups.*
- *Any structure of the organization must allocate tasks through a division of labour and facilitate the*

> *coordination of the performance results. There is not one optimal structure that meets the needs of all circumstances. Organization structures dedicated to maintenance should be viewed as dynamic entities that continuously evolve to respond to changes in technology, processes and environment.*

Interdependencies recommendations

The current guidelines are related to several functions. In particular, specific attention should be paid to the relation with service delivery, because a proper maintenance of the physical and cyber infrastructure is a very important prerequisite for a successful service delivery. The Monitoring functions are also very strategic and relevant for Infrastructure maintenance function in order to trigger extra-ordinary maintenance operations upon the detection of a failure. The ICT management and maintenance are strongly linked, because the fast evolution of technologies requires a strong capability to manage the evolution of the IT infrastructure as a whole, in order to provide sustainable costs and efforts for the maintenance of the cyber infrastructure itself.

3.5 Monitor

3.5.1 Monitor Safety and Security

Background facts

Organisations deal with risk of many different natures and origins. Despite this diversity, risk is a single overall phenomenon that inherently relates to uncertainty. From the perspective of operation continuity, critical risk relates to both unintended and undesired human, technological or process/organisational failure (safety related), and human intentional disruptive action (security related). The distinct nature of risk factors that must be managed within each of these two domains is at the origin of equally different approaches, practices and assessment tools. The evolution of safety domain has benefitted from several decades of industrial development, whilst the security domain only in recent years acquired more significant relevancy for the wider civil society and industry in general.

Despite their fundamental differences, safety and security can develop multiple overlaps within the operation of most industry sectors, both in terms of risk exposure areas, and control or mitigation measures. The path towards integrated risk management is complex and challenging but opens a wide range of potential benefits, namely in terms of overall efficiency in the allocation of risk management resources through the development of coordinated control measures. One of the fundamental challenges for such approaches relates to the management of information. While in general safety benefits from wide and open sharing of information, such an open access to information tends to pose a threat in terms of security.

Monitoring provides the information that the organization needs to determine whether adjustment in current course of action are needed in view of new emerging factors or shifts in already identified ones. Monitoring provides valuable information about operating conditions that could indicate a need for active organizational involvement and embodies fundamental management feedback loops.

Abstract

This Guideline refers to the issues of monitoring safety and security of the both the operations and the service delivery of a Critical Infrastructure.

This Function is highly depending and triggering a series of other functions in the CI, thus many interdependencies exist that affect the performance of this Function.

Questions

- For which events is there a response ready?
- How was the list of events created?
- How is the readiness verified or maintained?
- Is there a systematic list of routine safety rules and procedures for prevention and avoidance?
- Is there a classification scheme for threat types? (large scale intentional attacks, natural and environmental disasters, (near)-accidents, unexpected disruption (e.g. blackout), harmful intentional actions (e.g. hacking, graffiti)
- Is there a classification system for emergency incidents? (e.g. bomb attack, firefighting, train evacuation, gas attack)
- How do you measure performance? What kind of indicators are used and how are they defined/classified/planned for revision?

General Recommendations

Effective monitoring of safety and security requires continuous and dedicated efforts at all managerial and operational levels. Within highly complex and dynamic environments, the adoption of "self-monitoring" principles, as opposed to the implementation of monitoring activities that are external to operational processes and their agents, has proven to be more effective. This must *be grounded on coordination and information flow mechanisms, so as to produce context based and timely sense-making of operation conditions and performance.*

Common Conditions recommendations

1. Availability of resources

The relevant resources refer mainly to:

- *personnel,*
- *equipment,*
- *budget*
- *processes and procedures*
- *material.*

In order to specify the required resources, a determinant factor is to identify the related stakeholders and define the requirements of the monitoring (see also "Number of goals and conflict resolution").

- ***Personnel**: In the case of safety and security, relevant resources in terms of personnel refer to a wide range of people, from the higher administration that should set the fundamentals of risk management systems, to security guards and every single employee who should address safety and security regulations in everyday work. A very important role is the one of monitoring equipment operators, who should assure the proper functioning of the monitoring equipment.*

  Suitable levels of operation staffing are a fundamental requisite for the development and implementation of self-monitoring principles. When production pressures become too significant, such monitoring mechanisms tend to rapidly erode.
- ***Equipment**: Technical equipment such as CCTV cameras, data collection, storage and management systems, etc. In any case, the nature and specifications of the equipment are depended on the requirements of the monitoring. Originally, the existing infrastructure and capabilities should be identified and then decide on the need for additional needed equipment to satisfy the requirements. Regardless of available equipment, the undertaking and continuity of monitoring activities often rely on staff collective or individual initiative.*
- ***Budget:** It is the prerequisite for the organisation to be able to acquire all necessary equipment and material, as well as secure personnel costs for the optimal function of required safety and security monitoring processes. Adequate budget should be reserved for these key activities.*
- ***Processes:** These should clearly be defined and carefully followed. Depending on the type of the CI and the requirements of the monitoring, such processes can involve the ingress/egress control, the data collection, storage and management, etc. The definition of monitoring processes is also part of the monitoring program*

Examples

- Critical infrastructure safety monitoring

  http://www.nec.com/en/global/solutions/safety/critical_infra/index.html
- Example safety and security plan
  http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security-plan-example.pdf
- Airport safety plan
  https://www.zurich-airport.com/business-and-partners/safety-and-security/safety-principles
- Transportation safety surveillance
  http://www.swri.org/4org/d10/isd/surveil/

Limitations

In case the organisation does not have the resources or competencies to perform safety and security monitoring, this task may be assigned to an external entity. In this case additional provisions for data security should be made and possible a MoU between the organisation and the external operator should define the details of how the collected data should be managed and exploited. This would require developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions including process tasks in measuring performance of external entities against contractual instruments *and plan. Beyond these formal process requirements, many relevant monitoring activities are produced informally and are strongly based on expertise and overall understanding of operations.*

- ***Material*** *Data is the cornerstone of monitoring, thus the contents of data to be collected should clearly be defined (e.g. the secure and accurate functioning of systems and networks, key performance indicators that demonstrate achievement of safety and security objectives, the actions of persons, objects, and entities when they access and use organizational assets, vulnerabilities, threats and risks to organizational assets, events and incidents that can disrupt organizational assets and services, the physical movement of persons and objects through organizational facilities and physical plant, the status of compliance with regulations, laws, and guidelines, changes in the organization's risk environment that would warrant changes in operational risk etc.) as well as the data types (log files, video, paper, etc.). Data management is also a crucial issue, in terms of collection, storage, analysis and distribution, where the appropriate tools should be available and they should be guaranteeing the timeliness, accuracy and secure handling of data.*

Sources

- Richard A. Caralli, Julia H. Allen, David W. White., "The CERT resilience management model : a maturity model for managing operational resilience", ISBN 978-0-321-71243-1, Pearson Education, 2011
- CGI group Inc., "Developing a Framework to Improve Critical Infrastructure Cybersecurity", 2013
- https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- UK National Occupational Standards, "SS03 Promote, monitor and maintain health, safety and security in the workplace"
- Van Brabant, K.,"Mainstreaming the Organisational Management of Safety and Security", HPG Report 9,March 2001
- Kyriakides, E., Polycarpou, M., (Eds), "Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems", Springer 2015, ISBN 978-3-662-44159-6
- Gander, Philippa., et al. "Fatigue risk management: Organizational factors at the regulatory and industry/company level." Accident Analysis & Prevention 43.2 (2011): 573-590.
- http://ec.europa.eu/justice/data-protection/
- http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

2. Training and experience

- *The main activities that the stuff would be required to perform regarding the monitoring process are:*
  - *operating, monitoring, and configuring monitoring systems components*
  - *supporting stakeholders in understanding and interpreting monitoring data*
  - *securing data collected from monitoring system components*
  - *apply safety and security regulations in everyday practice*
- *In order to assure that the employees are capable to perform the required activities, the following are needed:*

a) Identify process skill needs.

- *Knowledge of tools, techniques, and methods used to collect, record, distribute, and ensure the confidentiality, integrity, and availability of monitoring data, including those necessary to perform the process using the selected methods, techniques, and tools.*
- *Knowledge unique to each type of service, asset, and operational resilience management process area that is required to effectively perform process activities.*
- *Knowledge necessary to elicit and prioritize safety and security requirements and needs and interpret them to develop effective process requirements, plans, and programs.*
- *Knowledge necessary to analyse and prioritize process requirements.*

- *Knowledge necessary to interpret monitoring data and represent it in ways being meaningful and appropriate for managers and stakeholders.*
- *Knowledge of safety and security regulations applied in the CI and what they imply to the everyday routine of employees.*
- *Knowledge of how to act in a case of emergency.*

b) Identify process skill gaps based on available resources and their current skill levels.

c) Identify training opportunities to address skill gaps. These are examples of training topics:

- *operating, monitoring, and configuring monitoring system components.*
- *supporting stakeholders in understanding and interpreting monitoring data.*
- *data collection, recording, distribution, and storage techniques and tools.*
- *securing data collected from monitoring system components to ensure data confidentiality, integrity, and availability.*
- *using process methods, tools, and techniques that are in application for monitoring safety and security in the CI.*
- *Safety and security regulations and instructions for everyday practice and in the case of emergency.*

d) Provide training and review the training needs as necessary.

3. Quality of communication

- *Monitoring safety and security, as mentioned above, is mainly a data collection and management process. Thus communication issues lie mostly in the communication of monitoring data. The main aspects of data quality are* ***accuracy***, ***validity***, ***security*** *and* ***timeliness*** *of data.*
- *Important considerations for an appropriate supporting infrastructure include the* ***protection and timeliness of data*** *collected and distributed. Monitoring data can expose the organization's weaknesses and therefore must be protected from unauthorized, inappropriate access where it is stored or collected, and in transmission to users and stakeholders. In addition, the timeliness of the collected data is paramount to providing an appropriate response to events, incidents, and threats and other actions the organization may take for improving its safety and security operations. Moreover, as this process includes also monitoring of people, personal data should be carefully treated, according to existing standards and regulations. Moreover, issues of cyber security should also be treated in cooperation with F19 and according to existing recommendations.*
- *Regarding* ***data accuracy and validity***, *the selection of appropriate tools and the handling of data by skilled personnel are the parameters that should carefully be dealt with.*

4. Human Computer Interaction and operational support.

This part has mostly to do with the personnel responsible for handling the monitoring equipment. As detailed above, only specialised personnel should be responsible for this task, or personnel that have gone through adequate training.

5. Availability of procedures and plans

The procedures and plans for safety and security monitoring should be clearly defined in the Safety and Security Monitoring plan and should comply with the monitoring requirements as defined by the needs of the addressed stakeholders. Each involved party should be aware of their responsibilities and recommended actions in normal routine or in case of an emergency. The goal of establishing specific procedures is that the performance of the task is realised in a well-organised and effective manner, so as to provide timely and accurate information of the safety and security status of the CI. Such processes may involve the collection, storage and generally the management of data, as well as monitoring operation procedures (controls, reports, etc.). Moreover, these *procedures address also the overall operation of the CI and are closely linked with the guideline 3.3.7 and the emergency operation.*

6 Conditions of work

- *Safe working environment*
- *Shared and standard procedures*
- *Clearly specified responsibilities and alignment with accountability*

7 Number of goals and conflict resolution

The goals set are also defined by the requirements of the monitoring plan. In general, some indicative ones are:

- *correctly identify people entering the environment and establish their right to enter;*
- *ensure practice in relation to health, safety and security is consistent with legislation and organisational requirements;*
- *identify the risks involved prior to starting work activities and ensure they are undertaken in a way which minimises the risks;*
- *maintain work areas as safe and as free from hazards as possible during work activities;*
- *ensure equipment and materials are used in a correct, safe manner which is consistent with current legal and organisational requirements;*
- *store equipment and materials safely and securely when not in use;*
- *dispose of waste and spillage without delay in a safe manner and place;*
- *take the appropriate action to minimise safety and security risks which arise during work;*
- *put into effect, without delay, the appropriate safety procedures in an emergency;*
- *ensure safety and security records are accurate, legible and complete;*
- *identify the risks when carrying out work activities and take appropriate actions to minimise risk;*
- *use approved safe methods and systems when undertaking potentially hazardous work activities;*
- *stop the work activity immediately if there is the likelihood of an accident or injury, and take the appropriate action to remedy the problem.*

8. Available time and time pressure

- *The required tasks should be executed in an automatic manner so that they would not require additional time from the employees (part of working routine).*
- *The data collected should be managed in a timely manner so that it serves its scope of effectively identifying safety and security threats in time to react and take adequate action to confront them.*
- *It should however, be taken into account that sense-making of data may require an unplanned amount of time, in particular when cross-referencing multiples sources.*

9. Circadian rhythm and stress

- *A plan should be defined for managing the risk of employee fatigue and the disruption of the circadian rhythm in safety-sensitive businesses (e.g. a Fatigue Risk Management System (FRMS)) in order to reduce the possibility of critical human errors.*
- *The safety and security monitoring should be as unobtrusive as possible in order not to cause additional stress to the employees and allow them perform their work without feeling being watched.*
- *Safety and Security monitoring tasks should be executed in an automatic manner so that it would not cause stress to the employees to deliver e.g. reports in time.*

10. Team collaboration quality

- *The quality of team collaboration in terms of safety and security (and any other kind) of monitoring can be established with the specification of the involved stakeholders and their responsibilities. Within the monitoring plan, responsibilities and authorities should be assigned for the performance of the whole* *process and its specific tasks. Moreover several other recommendations are provided:*

- *defining roles and responsibilities in the process plan, including roles responsible for collecting, recording, distributing, and ensuring the confidentiality, integrity and availability of monitoring data*
- *including process tasks and responsibility for these tasks in specific job description*
- *The stakeholders involved usually are:*
- *boards of directors and governors,*
- *higher-level managers,*
- *information technology staff,*
- *external entities, such as business partners and vendors,*
- *security guards, police, or other public agencies,*
- *external agencies, such as regulatory bodies,*
- *internal and external auditors.*

11. Quality and support of the organization

The role of the organisation in this case is to provide the safety and security program/plan and effectively apply it. This is usually decomposed in the following:

- *Establish and Maintain a Monitoring Program*
  - *Establish a Monitoring Program.*
  - *Identify Stakeholders.*
  - *Establish Monitoring Requirements.*
  - *Analyse and Prioritize Monitoring requirements.*
- *Perform Monitoring*
  - *Establish and Maintain Monitoring Infrastructure.*
  - *Establish Collection Standards and Guidelines.*
  - *Collect and Record Information.*
  - *Distribute Information.*

Interdependencies

- *Guidance of Training Staff in terms of training personnel for safety and security monitoring tasks.*
- *The procedures definition function of Defining procedures in combination with the Risk Assessment would define the procedures that should be of special focus for safety and security monitoring, as the ones of higher risk and thus needing closer attention and preventive measures.*
- *Emergency actions coordination should be in close cooperation with Monitoring Safety and Security, as they should consulted in defining the monitoring plan.*
- *The requirements of Service delivery should be taken into account when defining the requirements of safety and security monitoring.*
- *Operations monitoring should be in close cooperation with Monitoring Safety and Security as the overall monitoring actions within the organisation should be coordinated and not overlapping in order to avoid confusion and excess workload by the employees.*
- *Emergency actions coordination should be in close cooperation with Monitoring Safety and Security, as they are of the main recipients of safety and security monitoring data in order to take adequate action.*
- *The collection of event information is closely related with Monitoring Safety and Security as they are the of the major recipients of data collected within the framework of safety and security monitoring.*

3.5.2 Monitor Operations

Background facts

Critical infrastructure companies from utilities and energy to rail transportation require real-time operations monitoring and control capability. Responsibility for monitoring, i.e. the collection of the figures and for comparison of output with target, lies at different levels of oversight. It is important that even junior supervisory staff is aware of the targets and can take corrective action if there is under-achievement, without having to wait for more senior staff to react. Reporting and summarising is done at different hierarchical levels too, but detailed analysis is the responsibility of more senior levels. Monitoring of operational progress should be given the same emphasis, or priority, as applied to other operational activities.

General Recommendations

Beyond mismatches between performance and service level targets, monitoring must also take into account the growing need to follow up on any overall operational context changes and events, as it may present fundamental opportunities for preventive and proactive operational adaptations to such changes. This normally requires in-depth understanding and knowledge of overall system operation and expertise. The use of multi-disciplinary teams to analyse such operational changes tends to provide useful operational sense-making.

Monitoring operational performance can be executed with different timeframe according to purpose:

- *Periodic Monitoring: Periodic monitoring involves making comparisons between achievements and strategic targets at the end of specified time periods, for example, monthly, three-monthly or longer intervals.*
- *Continuous Monitoring: Useful at Tactical level, Continuous monitoring is applied frequently to specified key indicators which enables information on plan implementation to be collected often, such as at weekly intervals. Continuous monitoring provides a CI manager with the means of applying close control over operations enabling frequent comparisons to be*

Abstract

The guideline is devoted to reduce function variability while enhancing system and situational awareness.

Monitoring refers to the practice of collecting data regarding the infrastructure and operation in order to provide alerts both of unplanned downtime, network intrusion, and resource saturation. Monitoring also makes operational practices auditable, which is useful in forensic investigations. Monitoring provides the basis for the objective analysis of systems performance in view of the potential need for adaptive behaviours.

Questions

- What kinds of issues and errors will the solution detect, and what kinds of situations is the solution unable to detect?
- How soon can a response been given?
- How long can it be sustained? (Size of buffers)
- How the roles and responsibilities are clearly defined?
- How the processes are defined, established and communicated?
- When a process or a procedure is revised?
- When a new procedure is added?
- How much effort is allocated on organizational process improvement?
- How much effort is allocated to support communication?
- How much effort is allocated to support team collaboration?
- How the organization guarantees redundancy indecision making

- How many systems can the solution monitor and what kinds of resources does the tool require to support this level of service?
- How much logical, physical, and/or network separation can the monitoring application get from the monitored application?
- Can the platform provide alerts and notifications or must it integrate with another solution?
- What monitors the monitoring system?
- How conflicting goals are managed?
- Does planning take into account all resource needs?
- How should the organization model, simulate and analyse the interactions within its Critical Infrastructure (CI) and other interconnected CIs ?
- Do you have a roadmap for actions and targets of your organization? What is the timeframe?
- How does the platform collect data and what impact does this collection method have on the performance of the monitored system?

made between planned programmes and inputs of resources with actual achievements and inputs.

- *Real time Monitoring: Needed at operational level, real time monitoring is needed for system components whose working dynamics can evolve suddenly and the cascade effects can be propagated with unpredictable effects.*

As information gathering and control demands increase, the reliability, capacity and protocol limitations of existing communications infrastructure is constraining organizations' ability to meet performance, cost and security objectives. One of the primary means by which organizations have chosen to improve their capabilities is to begin migrating applications from proprietary protocols to IP because it is more economical and scales better.

Common Conditions Recommendations

1.-Availability of resources

- Humans (labour) – skills/competence
  - *Human resource availability needs to be secured for both daily activities and during emergency. A dedicated buffer capacity (e.g., stand-by staff) should be defined in advance and tailored according to degraded operational modes and emergency scenarios.*
  - *Monitor capability can tightly depend to specific technical and not technical skills (e.g. leadership, problem solving), knowledge, competencies. In order to control the possible function variability it is necessary to mitigate such dependencies defining a* Human Resource Replacement Plan *where missing human resources are immediately replaced with others (properly trained in advance) that are currently assigned to different tasks/activities/roles.*
- ICT infrastructure:

Monitoring infrastructure should:

- *Run as distinctly as possible from production services.*
- *Have high performance.*
- *Be redundant.*
- *Be reliable.*
- *Have a graceful degradation.*
- *Not create a significant impact on the system under monitoring.*

Failure of the monitored system should not cause a failure in the monitoring system. Simple redundancy and automatic fail-over is particularly important for monitoring systems, as it is important to "monitor the monitoring," or ensure that an inoperative monitoring system doesn't generate false positives.

In order to guarantee the operation monitoring and event detection is necessary to set up a proper ICT infrastructure able to collect information for the CI. Both ***structured*** *(e.g. legacy database) and* ***unstructured*** *(e.g. sensor data) data generated by operations should be considered.*

Collecting these data presents its own set of technological problems and general purpose monitoring tools require a great deal of customization and configuration for most uses. At the same time, most specialized monitoring tools only collect certain types of data and must integrate into general purpose systems. In order to support the monitoring function properly is necessary to go towards a Unified System Approach composed by the following decoupled conceptual layers:

- ***Knowledge Management Layer (KML):*** *operators use these systems to query the knowledge base in an easy-to-use and familiar format. KMS automate the capture of structured and unstructured information generated by the operations, the users and the environment (context) to manage high volume stream of data (Big Data) generated by heterogeneous resources as required.*
- ***Application Layer*** *encompasses state-of-the-art, integrated algorithms and models that automate CI resilience assessment quantification, cascade effect calculation, event dynamic prediction, etc.*
- ***Resilience Management Support System*** *extracts knowledge from the data and translates such knowledge into a meaningful dashboard for supporting critical decisions. Such layer allows modelling, analysis and visual monitoring of the status of the system.*
- ***Field network sensors:*** *a network of fixed or mobile sensors present on the field and able to deliver information about the many aspects such as: level of the river, traffic flows, people concentrations, pollution, position of buses, etc.*
    - ***Personal Mobile Device:*** *Mobile data applications are used for the on-scene aspect of public safety operations. They are designed to crowd-sensing and crowdsourcing data of the user on the ground to support operation and emergency respond.*

Examples

In Km4City Ecosystem www.disit.org a unified model and services based on aggregated data and services, data hub, is the first instrument to control city evolution, provide services to city stakeholders, accelerate commercial activities, create a common environment on which new data and services can be easily added to the ecosystem for all. For a city, to cover the role of data aggregator is strategic decision that put the control back in the hands of the city and not in those of the multinational commercial operators.

Km4City models and simplify the production of semantically integrated data from different domains, takes advantage of inferential deductions, enables a set of solutions for setting up Control Rooms, perform data business intelligence, data analytics, decision support, risk analysis, user behavior analysis, suggestion and stimulus towards city users, etc.

Limitations

Improving the effectiveness monitoring and early warning systems does not, in itself, lead to reduced risk for disaster-prone communities — early warning does little good unless it is followed by (early) action.

- Data management and privacy
    - *Define where and how the data collected and examined will be stored and maintained.*

  - *Define who will have access to the data and which actions are allowed.*
  - *Define how the confidentiality and privacy of the data will be maintained. The level of*
  - *Define how personally identifiable data will be handled. The*
  - *Use of standard to document data sources.*
  - *Define a data quality profile for each data source and a method for quality assessment addressing the following dimensions: Relevance (Fitness), completeness, consistency, accuracy, timeliness, integrity, accessibility and clarity, comparability, and coherence.*
  - o *Integrate and fuse data through an holistic driven semantic approach*

- *Monitoring method*
  - ***Active monitoring**: Monitoring systems that collect data by directly interacting with the monitored systems. Administrators must consider the impact (i.e. cost) of the monitoring and weigh this with the value of the test itself.*
  - ***Passive monitoring**: Monitoring systems that collect data by reading data already generated by the monitored system. The system collects this data from logs/"traps" or from messages sent by the monitored system to a passive data collection agent. The log data is an example of passive monitoring. Passive monitoring is significantly less resource intensive for the monitored system than other methods.*

2. Training and experience

- ***Increase Risk perception:** Dedicated training activates should be organized for the staff in order to gain the desired risk perception level. Risk perception of the staff directly affects the capacity of recognising potential issues, classifying them according to the internal risk procedures and forwarding the information to the right functions at the right time.*
- ***Manage internal Knowledge transfer:** This involves managing the internal transfer of knowledge and experience among employees involved in the monitoring activities. Managers, safety specialists, designers, engineers often have inadequate access and exposure to operational filed experts and operational*

<u>Sources</u>

- SO/DIS 9241 http://www.iso.org/iso/cataloguedetail.htm?csnumber=63500
- Ergonomic requirements for office work with visual dis play terminals (VDTs) (1998) is a multi-part standard that provides requirements and recommendations impacting the usability and ergonomics of hardware, software and context of use.
- ISO 13407: Human-centred design processes for interactive systems (1999) provide guidance on user-centred design methods for software applications.
- ISO 11064 part 1: Ergonomic Design Principle for Design Control Room
- ISO/IEC 10741-1 Dialogue interaction - Cursor control for text editing
- ISO/IEC 11581 Icon symbols and functions
- ISO 9241: Ergonomics requirements for office work with visual display terminals:
- Part 10, 12-17: dialogue design
- Process plant control desks utilising human-computer interface: a guide to design, operational and human interface issues. Engineering Equipment & Materials Users Association (EEMUA) Publication 201: 2002 available via EEMUA on 020 7628 7878
- EUROCONTROL - System Thinking for Safety: Ten Principles – Moving towards Safety –II
- EUROCONTROL (2013). From Safety-I to Safety-II: A White Paper. EUROCONTROL.
- Hollnagel, E. (2014a). Safety-I and Safety-II. The past and future of safety management. Ashgate.

environment. To understand and improve work, mutual access and interaction at vertical and horizontal level should be ensured.

- ***Train employees in view of system thinking, problem solving and naturalistic decision making.*** *In fact, a critical characteristic of a complex system is its under-specification. This means that existing procedures might not be applicable to an unexpected scenario. Thus the skill of problem solving and situation contextualisation needs to be acquired through adequate training, for the employees to be able to cope with unexpected issues.*

3. Quality of communication

- *Support efficient shareholders and (internal and external) stakeholders/experts coordination and cooperation.*
- *Guarantee the accuracy and understandability of the communication through standardized communication tools, protocols and languages.*
- *Secure data understandability.*
- *Provide early warnings.*
- *Report operational performance for infrastructure maintenance.*

4. Human Computer Interaction and operational support

- *Equipment should be designed in accordance with key ergonomics standards including EN614 Parts 1 and 2.*
- *Control rooms should be designed in accordance with key ergonomics standards and best practices (e.g. EN11064, EEMUA 191 and EEMUA 201, High Velocity Human Factor)*
- *Staff should be involved in the design process. This should include different types of users including operatives, maintenance and systems support personnel.*
- *Monitoring interfaces should be usable in both normal and emergency situation. The CHI design and evaluation needs to be conflict free, independent and stakeholder and situation oriented.*

5. Availability of procedures and plans

- *Defining clear processes that recognize distributed decision making requirements.*
- *Enabling procedure and plans accessibility and wide dissemination within the organization. All kinds of communication channels should be used like email,*

- High Velocity Human Factor (HVHF) – Moin Rahman - High Velocity Human Factors: Human Factors of Mission Critical Domains in Nonequilibrium Proceedings of the Human Factors and Ergonomics Society Annual Meeting October 2007 51: 273-277, doi:10.1177/154193120705100427.
  The High Velocity Human Factor (HVHF) paradigm concerns human capability and limitations when working in safety-critical domains. It is included in User-centred design principle with a focus on mission critical communication technology.
- The HVHF approach supports the design of intuitive, robust and reliable user interfaces from to device to dispatch and back office control room.
- Ergonomic principles in the design of work systems BS EN ISO 6385:2004. A work system is defined as "a combination of people and equipment, within a given space and environment, and the interactions between these components with a work organisation" (p10)
- COUNCIL Ergonomic design of control centres, Parts 1-7, ISO 11064. Covers design principles, control room arrangements and layout, workstations, displays, controls, interactions, temperature, lighting, acoustics, ventilation, and evaluation. Designers should be following this standard for new control rooms, and it can usefully be referred to for upgrades and modifications to existing ones especially where there are known problems.
- 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

intranet, leaflets, etc.

6. Conditions of work

- ***Establish a "Safety culture"** means the value and priority replaced on safety across all levels within an organisation. It refers to the extent to which individuals commit to their personal safety (independence) and to safeguarding others (interdependence). It is necessary to go beyond the classical approach based of the fear of repercussion and consequences (or reward conformity) towards the true commitment to safety and adaptation as an internal organization value.*
- ***Leverage the role of context and culture** in order to socially influence the right behaviours. In fact social influences have the propensity to change an employee's thoughts, beliefs and values, which in turn, can shape their behaviour. An example of social influence is the organisational culture of a workplace and the style of leadership that governs it.*
- ***Just culture** signifies the growing recognition of the need to establish clear mutual understanding between staff, management, regulators, law enforcement and the judiciary. This helps to avoid unnecessary interference, while building trust, cooperation and understanding in the relevance of the respective activities and responsibilities.*

- Ontologies: INSPIRE, OECD, EUROVOC, GEMET, AGROVOC, MONITOR
- ISO 25000, ISO 8000,
- ISO31010, PAS200, BS65000, UNISDR2009, PROVIA
- EUROSTAT Quality Assurance Framework of the European Statistical System)ESS QAF) http://ec.europa.eu/eurostat/documents/64157/4392716/ESS-QAF-V1-2final.pdf/bbf5970c-1adf-46c8-afc3-58ce177a0646
- INSPIRE ISO19131
- http://cyborginstitute.org/projects/administration/monitoring-tactics/
- HSE publication HS (G) 65 Successful Health and Safety Management - Health and Safety Executive (1997).
- COST Action ICO806: Intelligent Monitoring, Control and Security of Critical Infrastructure Systems (IntelliCIS)
- Common Alert Protocol-CAP format
- http://www.scidev.net/global/communication/feature/early-warning-of-disasters-facts-and-figures-1.html

7. Number of goals and conflict resolution

- ***Adopt a mind-set of openness, trust and fairness.** Understand actions in context, and adopt systems' language that is non-judgmental and non-blaming*
- ***Basic goal conflicts drive most safety-critical and time-critical work**. As a result, work involves dynamic trade-offs or sacrificing decisions: safety might be sacrificed for efficiency, capacity or quality of life (noise). Reliability might be sacrificed for cost reduction. The primary demand of an organisation is very often for efficiency, until something goes wrong.*
- ***Reflect on mind-set and assumptions.** Reflecting on how to think about people and systems, especially when an unwanted event occurs and work-as-done is not as imagined. A mindset of openness, trust and fairness will help understanding how the system behaved.*
- ***Consider independence and any additional competence required.** Managers should consider whether they are independent enough to be fair and impartial, and to be seen as such by others. Also they should consider what additional competence is needed from others to understand or assess a situation.*

8. Available time and time pressure

- ***Understand demand over time**. It is important to understand the types and frequency of demand over time, whether one is looking at ordinary routine work, or a particular event. Identify the various sources of demand and consider the stability and predictability of each.*

- *Separate value and failure demand. Where there is failure demand in a system, this should be addressed as a priority as it often involves reworking and runs counter to the system's purpose.*
- *Look at how the system responds. When the system does not allow demand to be met properly, this will result in more pressure. It should be considered how the system adjusts and adapts to demand, for understanding the trade-offs used to cope. Field experts should be consulted and signals that may indicate trouble should be seeked.*

9. Circadian rhythm and stress

- *Managing fatigue and workload as hazard: Fatigue refers to the issues that arise from excessive working time or poorly designed shift patterns. It is generally considered to be a decline in mental and/or physical performance that results from prolonged exertion, sleep loss and/or disruption of the internal clock. It is also related to workload, as workers are more easily fatigued if their work is machine-paced, complex or monotonous. Compliance with the Working Time Regulations alone is insufficient to manage the risks of fatigue. Measures to manage fatigue are:*
  - *Ensure that workload assessment considers visual inputs (e.g. scanning display screens, looking out of windscreens, CCTV), auditory inputs (telephones, radios, alarms), cognitive activities (analysis of inputs, decision making) and psychomotor skills (physical actions, such as controlling a process using a mouse, keyboard, or buttons and levers).*
  - *Consider not just the number of personnel, but how they are being utilised.*
  - *Set clear roles and responsibilities, ensuing that staff are clear on their priorities. This will help to ensure that even when workload is high, staff is able to focus on key activities.*
  - *Some tasks may be re-allocated from humans to machines/computers, or vice-versa; considering human performance, safety, maintainability, personnel requirements, etc.*
  - *Develop a policy that specifically addresses and sets limits on working hours, overtime and shift-swapping, and which guards against fatigue.*

10. Team collaboration quality

- *Consider the information flow: Field experts of all kinds, (including system actors, designers, influencers and decision makers) need effective ways to raise issues of concern, including problems and opportunities for improvement and need feedback on these issues.*
- *Field experts as co-designer and co-decision maker:. Field experts need to be empowered as co-designers and co-decision-makers to help the organization improve.*

11. Quality and support of the organization

- *Active monitoring - By "active monitoring" we are referring to all those checking activities, formal and informal, carried out by line managers which lie at the heart of effective management. Active monitoring involves checking that all these components, people, equipment and systems, continue to work as intended. What distinguishes it is the recognition that the topics which are actively monitored must include those barriers or controls needed to prevent a major accident. This needs to include preventive barriers as well as those barriers which are intended to mitigate the consequences of the event if it materialises. In particular an effective active monitoring program will ensure that the staff are:*
  - *doing what they should be doing and checking what they should be checking;*
  - *reporting what should be reported and to the right people;*
  - *taking appropriate action on the information provided particularly to remedy*
  - *identified deficiencies in risk control systems.*

Interdependencies recommendations

Monitoring function is strictly connected with the ICT infrastructure. A failure in ICT infrastructure affects the capacity of the monitoring function to achieve its objective properly. In order to manage such potential variability it is necessary to define a contingency plan including at least the following 4 strategies: monitoring system redundancy and replace degraded monitoring operation, indirect monitoring, visual inspection of the operator on the field.

3.5.3 Monitor Resource availability

Abstract

As every resource (human, technological or organizational) should be available for the system functioning and prompt for any emergency request, the related guidelines should comply with the control of:

- Expertise and functional abilities of human resources in relation to the system functioning, as well as anticipation of disturbances and recovery capacities;
- Technology required for the system functioning, including internal and external communications;
- Organisational conditions favouring the system functioning and the mobilisation of resources in emergency situations.

Background facts

In the face of inevitable resource limitations, every organisation strives to maximise operational efficiency. Across all industry sectors, access to diverse and variable resource needs relies on increasingly tight system couplings that must be developed and sustained amongst supply chain stakeholders. The high complexity and dynamics that emerges from such system interdependencies require a continuous ability to monitor the flow of multiple critical resources, aiming to develop updated and thorough support to the planning of operations and the subsequent allocation of resources. This may be particularly relevant when faced with the need to adjust (planning and resource allocation) to changes in the operational environment.

Understanding that a sociotechnical system and its functioning goes much beyond the description of human, technological and organisational resources and their interdependencies, it is essential to consider:

- The way in which such interdependencies support the provision of critical resources;
- The types and degrees of variability to which these are submitted in the face of pressures emanating from a system’s operational environment.

Therefore, monitoring resources availability implies that operational variability of the system must be considered and managed in order to ensure the system functioning.

The sources of operational variability, as well as the mechanisms that may potentially propagate it and impact on system performance must be identified.

The resources and system capacities required to manage and cope with operational variability must also be taken into account.

General recommendations

Following these research statements, some general recommendations for practice are stated in the following (to be used if relevant):

- Work organisation and task allocation ensuring acceptable workload and work schedules.
- Manage working times and shifts, in order to ensure the individual’s arousal and prompt reaction in critical situations.
- Providing training in accordance to job needs with the appropriate frequency.
- Favouring the development of competences and expertise with experience in order to ease the formation of compensation behaviour with increasing age.
- Selection of trainers according to their status, expertise and communication qualities.
- The contents and quality of communication must be clear and easily understood by all users.

- The design of Human Computer Interaction must comply with usability requests.
- Public infrastructure must be totally accessible without any physical barrier to the access and use of the facility by any individual.
- The displayed information within and outside any public infrastructure must be totally accessible to users providing alternative sensorial channels for the information display.
- The implementation of a Safety Culture project in the organisation should start by the creation of a mental model of Safety allowing for risk and safety perception. This requires a good leadership, the involvement of all employees in the process, the identification of personal responsibility, the definition of risk management principles, the development of an activity-based safety system, the development of methods and tools for risk analysis, and the required training.
- As a team leader has an important role in the management of human resources, his/her selection must be based on defined and relevant criteria, particularly leadership and communication characteristics.
- As acting under time pressure is recognized to degrade human performance across a variety of cognitive domains, operators who must act in critical situations must be specially trained to improve their decision making ability towards the appropriate action to be performed in due time.
- Due to the risks of a circadian rhythm desynchrony, which lead to decrements in vigilance and has negative effects in performance, the definition of job schedules, as well as individual rest and sleeping times, must comply with related European or International standards and regulations.

Questions

- How soon can a response be given?
- How long can it be sustained? (Size of buffers)
- Is there a specific response for any particular situations?
- How the roles and responsibilities are clearly defined?
- How the processes are defined, established and communicated?
- When a process or a procedure is revised?
- When a new procedure is added?
- How much effort is allocated on organizational process improvement?
- How much effort is allocated to support communication?
- How much effort is allocated to support team collaboration?
- How the organization guarantees redundancy in decision making?
- How conflicting goals are managed?
- Does planning take into account all resource needs?
- How should the organization model, simulate and analyse the interactions within its Critical Infrastructure (CI) and other interconnected CIs?
- Do you have a roadmap for actions and targets of your organization? What is the timeframe?

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence
  - *Highly trained and skilled personnel.*
  - *Provision of conditions for the development of competencies with experience.*
  - *Technical and organisational conditions ensuring acceptable workload, managing fatigue and stress in order to anticipate negative effects on job performance, controlling workability across ageing, and promoting health, arousal and preparedness towards prompt reactions in emergency situations.*
- Budget:
  - *Ensure the required budget for the system functioning and emergency situations.*
  - *Preview the needs for external operations and the related budget.*

- *Preview specific budget for Training.*

- Data & Algorithm:
    - *Use of historic and updated data bases on human, technological and organisational resources and their isolated and combined influences on the system functioning.*
    - *Use of agreed concepts and definitions.*

2. Training and experience

- *Continuous and updated training over time in order to maintain and improve relevant skills and expertise of the staff.*
- *Ensure training for emergency situations in relation to the use of all resources.*
- *Selection of trainers according to their status, expertise and communication qualities.*

3 Quality of communication

- *Ensure the contents and quality of communication.*
- *Ensure the required communication assets.*
- *Adopt the use of communication tools, protocols and languages.*

4 Human Computer Interaction and operational support

- *Technological equipment and tools should comply with ergonomic standards and recommendations, such as:*
    - *They should allow for easy, comfortable and secure interactions and successful human-machine dialogues, thus requiring appropriate design of interfaces and the definition of contents according to the targeted mission.*
    - *They should be located in an adequate environment complying with ergonomics standards and recommendations regarding screen reflexions that lead to mental and visual fatigue.*
    - *The duration of exposure when working with technological equipment must be regulated following ergonomics standards and recommendations.*
    - *Working schedules and shifts should respect biological needs for rest and sleep in order to ensure the necessary performance of every operator.*

<u>Examples</u>

- Funding Resilient Infrastructure in New Jersey: Attitudes Following a Natural Disaster (Robert B. Noland, Ph.D., Marc D. Weiner, Ph.D., and Michael R. Greenberg, Ph.D., Mineta National Transit Research Consortium, College of Business, San José State University, San José, CA 95192-0219. Sponsored by U.S. Department of Transportation).
- Disaster Resilience: A National Imperative NRC 2012. TRB.
- Best practices in risk and crisis communication: Implications for natural hazards management (Toddi A. Steelman • Sarah McCaffrey (2013).)

<u>Limitations</u>

- Difficulty in updating the information on resources use.
- Difficulty in assessing the situation and mobilising the appropriate resources.
- Difficulties resulting from limited financial resources.
- Difficulties resulting from unavailability of technological assets resulting from breakdown or lack of energy.
- Difficulties resulting from low human performance due to fatigue, inappropriate workload or sleep deprivation.
- Difficulties resulting from insufficient personnel.

- *Usability requests on the design of Human Computer Interaction.*

5. Availability of procedures and plans

- *Planning of infrastructures previewing physical and informational accessibility needs and requirements within the infrastructure and surroundings.*
- *Planning process that recognizes distributed decision making requirements (as opposed to a centralised decision making).*
- *Planning previewing conditions for emergency response based on naturalistic decision making, which means the way people use their experience and knowledge to make decisions in real-world settings, including dynamic and continuously changing conditions, real-time reactions to these changes, ill-defined tasks, time pressure, and significant personal consequences for mistakes. This requires experienced decision makers.*

6. Conditions of work

- *A Safety Culture project in the organisation should be implemented as it is the basis for a perfect coupling of all system resources towards the system resilience.*
- *Working conditions (technical and organisational) should respect the mode of human functioning and the individual limits for a continuous job performance. Passive fatigue of operators working in control rooms leads to drowsiness and, in consequence, reduces the individual ability to monitor a system, anticipate any disturbance and react promptly in an emergency situation. The performance of a fatigued or drowsed operator is similar to a performance under the effect of alcohol.*
- *An understanding of human performance, and particularly the human error, should also be integrated in the Safety Culture project as a basis for safety management.*
- *Anticipation ability should be promoted by means of increasing competencies and using job-related experience and knowledge.*

7. Number of goals and conflict resolution

- *Planning teams should be built taking into account the scale and timeline of the plan.*
- *The choice of team leaders should be based on leadership profile, communication qualities, and the ability to create a healthy clime based on trust and*

Sources

- Karwowski, W. (2005). Handbook of Standards and Guidelines in Ergonomics and Human Factors. New Jersey: Lawrence Erlbaum Associates, Publishers.
- Staal, Mark A. (2004). Stress, Cognition, and Human Performance: A Literature Review and Conceptual Framework. NASA/TM—2004–212824. Ames Research Centre Moffett Field, California 94035. Website: http://human-factors.arc.nasa.gov/flightcognition/Publications/IH_054_Staal.pdf
- International Labour Standards on working time. Website: http://www.ilo.org/global/standards/subjects-covered-by-international-labour-standards/working-time/lang--en/index.htm
- The EU's Working Time Directive (2003/88/EC). The Directive also sets out special rules on working hours for workers in a limited number of sectors, including emergency services and transport sectors (passengers and goods).
- UK Working Time Regulations. HSE Website: http://www.hse.gov.uk/contact/faqs/workingtimedirective.htm
- Bevan, N. (1995). Human-Computer Interaction Standards. In Anzai & Ogawa (eds.). Proceedings of the 6th International Conference on Human Computer Interaction, Yokohama, July 1995, Elsevier.
- Hubbard, D. (2014) How to Measure Anything: Finding the Value of Intangibles in Business. Wiley.
- Shah, J. (2009) Supply chain management: text and cases. Pearson Education India.

respect.

- *A good team leadership is required to avoid and eventually manage conflicts without creating additional risks to the system.*

Merk, O. (2014), “Metropolitan Governance of Transport and Land Use in Chicago”, OECD Regional Development Working Papers, 2014/08, OECD Publishing. http://dx.doi.org/10.1787/5jxzjs6lp65k-en

8. Available time and time pressure

- *Planning milestones and deadlines should integrate degrees of flexibility to cope with planning quality requirements.*
- *Acting under time pressure is recognized to degrade human performance across a variety of cognitive domains (judgment and decision making; visual search behaviour, vigilance and attentional processes; memory recall strategies; concession making and integrative agreements; and subject’s self-ratings of performance).*
- *In emergency situations, time pressure is a common reality that operators must be trained to deal with in order to avoid negative interference on decision making.*
- *As time pressure increases workload, particularly in situations of concurrent tasks or task switching, operators must be trained for reducing the interference of those conditions on the tasks performance and ensuring the performance of the required actions in due time.*
- *It must be understood that time pressure could decrease human performance and lead to errors if operators are not prepared for acting under those circumstances.*
- *Time pressure is the underlying stressor that determines operator performance, error production, and judgments of workload.*

9. Circadian rhythm and stress

- *Circadian rhythm asynchrony has important effects in performance, which are related to decrements in vigilance. This statement has implications on job schedules, individual rest and sleeping times and sleep quality as contributing factors to the desired performance.*
- *Research has shown that the direct effects of various stressors (including fatigue) can be modulated by individual differences and psychological processes (i.e., motivation, effort, etc.).*
- *The "trinity of stress" is referred as consisting of input features (environmental stressors), adaptation features (cognitive appraisal), and output features (changes in bodily functions and ultimately performance efficiency).*
- *Stress has been defined as the interaction between three elements: perceived demand, perceived ability to cop e, and the perception of the importance of being able to cope with the demand. Unlike many previous definitions of stress, this formulation distinctly incorporates the transactional process believed to be central to current cognitive appraisal theories. These reciprocal influences have direct implications for personnel selection, choice of team leaders and training.*
- *Fatigue and stress effects on decision making and task performance are difficult to separate. After measuring levels of arousal and anxiety during different stages in a continuous and prolonged task, it has been found that the expectation of the end of the shift resulted in a release in tension (although no performance decrements were noted). These findings should be taken into consideration for training.*
- *High workload results in an increase in subjective stress level and, objectively, in gradual, not sudden, decrements in recognition memory accuracy and reaction time. Acceptable workload should be targeted.*

10. Team collaboration quality

- *Adherence to the principles of collaborative planning through the development of mutual benefit relations.*

- *Information flow and continuous update.*
- *Autonomy, flexibility and accurate control under a good leadership.*

11. Quality and support of the organization

- *Clear decision making process and alignment of responsibility with accountability.*
- *Check, report, decide and act.*

Interdependencies recommendations

Monitoring resources generates information on resource allocation and the understanding of their flows. This constitutes one of the fundamental tools for planning activities, both as a primary input and as indicators for the potential need of planning revision or reassessment.

ICT constitutes a fundamental resource for all operational and managerial activities. The failure of ICT services may critically compromise operation continuity. The monitoring of these services should provide the ability to anticipate potential disruptions and the deployment of contingency resources (adaptive capacities).

Keep updated information on the status and supply of critical resources constitutes a fundamental resource for the anticipation of potential needs for operational adjustments.

In case the ICT infrastructure needed to support the resource monitoring fails, a dedicated communication and periodic reporting channel should be established with the suppliers. Reporting data about the resource consumed should be provided "on demand" and on pre-determined period.

A specific protocol and procedures to promptly inform about resource delivery failure and the related causes should be defined in advance between the CI and its suppliers. Such procedures should be included in the emergency plan of the parties.

3.5.4 Monitor user generated feedback

Abstract

This guideline addresses the implementation of a human/social sensing approach to support a more effective and efficient resilience management of critical infrastructure.

Background facts

Most critical infrastructures are directly related to the provision of fundamental social and economic needs, which often places the managers and operators of such infrastructures under strong public and political scrutiny. Within this context, maintaining an updated and accurate flow of information between operation stakeholders and user/public becomes critical, not only for the efficiency of service usage as whole, but also for the promptness and effectiveness of any measures diploid as an adjustment to potential or verified changes in operation (i.e. service disruptions, among others).

Resorting to recent ICT such as social media can, on the one hand, considerably enhance the ability to tailor information contents to customer needs, and on the other hand, develop a timely and context related understanding of service usage.

Failures in customer information tend to significantly hinder user and overall public level of trust in the providers of the service. A disruptive event affecting a critical infrastructure can significantly impact the social opinion, at different levels, depending on the "effect" induced by the event (e.g. the impact on the opinion of citizens is different if a disruptive event generates a reduction in the quality of service rather than causalities).

The widespread of mobile technologies – in particular smartphones – and social networks (e.g. Twitter, Facebook, Instagram, etc.) has enabled an every-time and every-where collaborative and active participation of citizens who are free to generate and share information and opinions about any event occurring in their daily lives.

Questions

- Which are the media (in particular social media) the organization should monitor to estimate the "mood" of its customers after an adverse event?
- For which target groups / persons / stakeholders should training be provided?
- Which (social) media should be used by the organization to provide information/communication in order to support a quick return to the normality?
- What ways are optimal to be used to inform/alert about an imminent risk?
- How can the organization involve its customers/citizens to design adaptation strategies aimed at improving the overall perceived level of safety and security?

In case the communication network is not affected by the disruptive event, social/human sensing is crucial in order to infer useful information which cannot be otherwise acquired, for instance acquire information about the entity of the effect of the event in an area which is not monitored through ICT systems. In this case, the human/social sensor is crucial to support the emergency management.

On the other hand, after an event, the social/human sensing becomes crucial to analyse the social opinion and facilitate both recovery to the normal situation and system adaptation. For instance, human/sensing can be adopted to infer the perceived level of security and safety of the citizens after a terrorist attack, as well as to identify possible criticalities, reported by the users, which represent barriers to the acceptance/usage of a specific service.

General Recommendations

- *The consistency and accuracy of the information flows with service users and the wider public can only be achieved through a dedicated coordination unit that centralises and processes all communication contents. On the one hand, information to be disseminated to customers must be processed internally, namely to establish its meaningfulness to different types of users, among others. On the other hand, the gathering of feedback and data from the multiple sources available (i.e. "twitter" and other social media) requires a dedicated assessment in terms of meaning and reliability, in order to produce useful support to overall service operation and management.*
- *Foresee a technical escalation mechanism (e.g. leveraging the elastic management of the computational demand provided by the cloud technology), to increase the granularity of the feedback collections and processing on demand.*
- *User generated data crawled should be used as further source of information to improve effectiveness and efficiency of the service, to coordinate the emergency respond, and to support a quick recovery to the normality.*
- *Data generated by users/citizens has to be analysed and processed to extract, collect and monitor relevant information about an event.*
- *Communication mechanisms and channels can be refined and improved to infer, characterize an possibly predict usage behaviour as well as increase user awareness and implement demand side management strategies.*
- *User generated data should be managed according to the Privacy and Ethics constraints. To this end a Data Management plan and Ethics commitment documents should be defined by the organization and communicated by the users without ambiguity.*

Examples

The Federal Emergency Management Agency (FEMA) wrote in its 2013 National Preparedness report last week that during and immediately following Hurricane Sandy, "users sent more than 20 million Sandy-related Twitter posts, or "tweets," despite the loss of cell phone service during the peak of the storm." New Jersey's largest utility company, PSE&G, said at the subcommittee hearing that during Sandy they staffed up their Twitter feeds and used them to send word about the daily locations of their giant tents and generators. "At one point during the storm, we sent so many tweets to alert customers, we exceeded the [number] of tweets allowed per day," PSE&G'S Jorge Cardenas, vice president of asset management and centralized services, told the subcommittee.

Limitations

Trustworthiness of the sources: data generated by citizens contrary to official data sources (such as ICT based monitoring and control systems) cannot be completely considered "trustworthy". Data analysis can allow for the estimation of trustworthiness of the sources in order to minimize – but not exclude – misleading information

Common Conditions Recommendations

1. Availability of resources

- Humans (labor) – skills/competence
  - *Personnel in charge to monitor and manage communication channels have to be trained in order to use simple social media monitoring and social network data analysis tools. The aim is to detect and*

infer useful information, "hidden" in the user generated content, in order to define suitable communication material for supporting a more rapid recovery to the normality.

- *Stakeholders involved in the emergency management have to be able to access to social/human sensing data as any other data source, in order to have a more complete view of the scene and, in case, involve citizens to improve the effectiveness of operations/actions.*

- *Budget:*

Costs for accessing, implementation and update of social/human sensing data have to be considered.

- *Data & Algorithm:*
  - *Data which can be crawled from the web and the social networks.*
  - *Software tools for analysing – online and batch – the crawled data:*
    - *Time-series and trend analysis*
    - *Natural Language Processing and Text Mining*
    - *Sentiment and opinion mining*
    - *Statistics and Data Mining*

2. Training and experience

- *Training on social media monitoring and opinion/sentiment analysis tools*
- *(Social) communication skills*
- *Basic expertise in statistics and Data Mining*

3. Quality of communication

- *Communication material aimed at supporting a quick recovery to normality*
- *Diffusion of the communication material on the different channels, in particular social networks and media*

4. Human Computer Interaction and operational support

- *Access to social/human sensing data and analysis software supporting the operators during the emergency management.*
- *Access to social/human sensing data and analysis software supporting the personnel in charge for communication to achieve the recovery to normality quickly as well as to support the definition of adaptations.*

5. Availability of procedures and plans

Sources

Yondong, Z.: Social networks and reduction of risk in disasters: an example of Wenchuan earthquake. In: Yeung, W.J.J., Yap, M.T. (eds.) Economic Stress, Human Capital, and Families in Asia, vol. 4, pp. 171–182. Springer, Berlin (2013)

Brown, K.: Global environmental change I: a social turn for resilience? Prog. Hum. Geogr. 38, 107–117 (2014)

Jassbi, J., Camarinha-Matos, L.M., Barata, J., "A Framework for Evaluation of Resilience of Disaster Rescue Networks", in L.M. Camarinha-Matos et al. (Eds.): PRO-VE 2015, IFIP AICT 463, pp. 146–158, 2015.

Gao, J., Liu, X., Li, D., Havlin, S., "Recent Progress on the Resilience of Complex Networks", Eergies 2015, 8, 12187-12210.

Vos, M., & Sullivan, H. (2014). Community Resilience in Crises : Technology and Social Media Enablers. Human Technology, 10 (2), 61-67.

Fekete, A., Tzavella, K., Armas, I., Binner, J., Garschagen, M., Giupponi, C., Mojtahed, V., Pettita, M., Schneiderbauer, S., Serre, D., "Critical Data Source; Tool or Even Infrastructure? Challenges of Geographic Information Systems and Remote Sensing for Disaster Risk Governance", ISPRS Int. J. Geo-Inf. 2015, 4(4), 1848-1869.

Deliverable 3.1 "usage Patterns of Social Media in emergencies", EU-FP7-SEC project EmerGent (Emergency Management in Socia Media Generation), available at: http://www.fp7-emergent.eu/wp-content/uploads/2014/09/D3.1_UsagePatternsOfSocialMediaInEmergencies.pdf

Fiskel J., "Connecting with Broader Systems", Resilient by design, (2015), 191-208

Avvenuti, Marco, et al. "Pulling information from social media in the aftermath of unpredictable disasters." 2nd international conference on information and communication technologies for disaster management (ICT-DM). 2015.

Establish the operational circumstances or scenarios for which user based input becomes relevant and also on which service updates to the user should be provided.

6. Conditions of work

Guarantee privacy and security of the public data crawled from the web and social networks – according to the internal and local policies.

7. Number of goals and conflict resolution

- *Reducing efforts during the emergency management while increasing its effectiveness.*
- *Increasing the amount of data and information available during the management of the emergency*
- *Reducing time to recovery to the normal condition*

8. Available time and time pressure

- *Personnel must be trained and put under exercises*
- *Access and examine data in very short time through easy friendly visualization*
- *Prompt and quick action and timely monitoring for prevention*

9. Circadian rhythm and stress

N.A.

10. Team collaboration quality

Adherence to the principles of collaborative planning through the development of mutual benefit relations, during the management of the emergency and the recovery and adaptation

11. Quality and support of the organization

Alignment of responsibility for communication actions

Interdependencies recommendations

The analysis of user-generated information is strongly dependent from the ICT infrastructure since the added value of integrating heterogeneous data into a digital system is undoubted. However, the variability of the ICT infrastructure function in terms of computational capacity, system reliability and network connectivity should be managed. In particular two strategy should be applied: a) mitigation of the computational overload risk with appropriate SLA definition and, b) definition of a service degradation strategy.

In the second case, a monitoring channels mix of backup to collect user feedback should be take into account. In fact even if the data integration and analysis can be affected by the ICT infrastructure failure, information coming from web and social media, radio, mobile phone (background sensing or voice), sensors data can be continuously acquired and managed by operators exploiting their native channels.

To this end, experienced staff able to understand, manage and synthetises multichannel information in critical events in absence of the support of the system should be employed in the present function.

3.6 Respond

3.6.1 Coordinate emergency actions

Background facts

An efficient emergency coordination activity is necessarily linked with the environment and social context in which it is performed.

A social community eco-system, which is not weakened by chronic stresses, as overtaxed or inefficient public transportation system, poor air quality, junk food, water shortages, is also very keen to collaborate with the emergency coordination activity performed by the Responsible Body in charge of this task.

Typical emergency actions covered under this Function are:

- - *Response to an earthquake*
- - *Response to a flooding due to river overflow or water-bomb*
- - *Response to a fire*
- - *Response to a terrorist attack*
- - *Response* to a serious transportation accident (e.g. several cars with several people injured and important traffic jams caused)

General recommendations

- *National bodies responsible for developing a response capacity and for responding to critical situations resulting from attacks, weather-related disasters or accidents, should be prepared anytime to assess the situation and react accordingly as fast as possible. For this, besides the necessary budget, communications have a major importance, as well as the required technology, appropriate plans and procedures, and highly skilled and competent HR under the command of an excellent leadership.*
- *The different nature of threats and disasters gives rise to a wide variability of impacts, which require permanent monitoring, as well as fast and required decisions allowing for the appropriate actions in due time.*
- *The relevant organisations should promote public awareness in order to facilitate cooperation from citizens instead of panic and hasty behaviour. So, the general public must be aware of vision and policies definition.*

Common Conditions recommendations

Abstract

The coordination of actions during an emergency needs to have a unique Responsible capable and in charge to orchestrate the multiple actors involved in the crisis management. Coordinated emergency actions are usually managed by a specific trans-organization responsibility centre with a unique head of operations: an emergency centre, a civil protection authority, a situation room, a special emergency management agency. The function should have mandate and power enough to coordinate the emergency in according with laws, bylaws and the national and local emergency plans. As various groups of emergency response personnel arrive at the scene, this function assures that a clear chain of command might be maintained and written operational procedures are respected during the crisis.When communication, and namely communication with top management, top leadership, have become impossible upon dramatic events, this function might have autonomy and manoeuvre room, expressed in protocols and an appropriate budget.

Questions

- For which events is there a response ready?
- Do special case studies exist (i.e. bomb attack, firefighting, train evacuation, gas attack)?
- What is the threshold of response?
- Is there a comprehension of the possible event magnitudes?
- How is the type of response determined?
- Do you have strategic emergency centres, headquarters able to operate in emergency?
- Can the emergency centre count on backup power supplies, radio and internet?
- Is there a list of emergency rules and procedures for response and

1. Availability of resources

- Humans (labour) – skills/competence
  - *Members of the emergency coordination should be people who profoundly know the territory, the locals, the vernacular cultures, the infrastructures, able to move on the ground literally on their own foot, counting on their own personal experience as inhabitants, pedestrians, drivers, and commuters.*
  - *In addition to scientific, technical, legal and procedural education, Training exercises, simulations and case studies should be carried out. These must be conducted on a regular basis in order to improve the ability to cope with stress and extraordinary emergency awareness, with emphasis on human factors.*
  - *Emergency actors must know each other in person, having clear, fair communication, and having established a relevant human empathy among them, being prepared for responding to an emergency and acting as required.*
  - *All the relevant shareholders (authorities and citizens) must have voice in the function and all its connections.*
  - *It should be clearly defined how the emergency response team is composed, and the role of each participant.*
  - *The members of the emergency response team should be periodically collected and informed together, in order to facilitate their communication and relationship.*
  - *There must be consultation with all the relevant stakeholders. Operators and actors must be consulted.*
  - *There must be knowledge of existing legal "acquis".*
  - *In all the phases of a crisis response, a strong communication and information plan must be implemented, involving all the main actors of the neighbourhood. Community centres, parishes, volunteer associations and clubs must be kept aware of their pivotal role in disseminating information during a crisis, and leading people within their communities to react according to the existing approved procedures. Leaders of such communities need to be trained and informed continuously on the capabilities and operational procedures related to crisis management.*

- Which resources are allocated to response readiness, and in what measure?
- Which are the stakeholders that should be involved and how?
- Are roles and responsibilities clearly defined?
- Are processes and plans defined, and how are they communicated?
- When a process or a procedure is revised?
- Whom a new procedure is added by, and when?
- How much effort is allocated to support communication?
- How much effort is allocated to support team collaboration?
- How conflicting goals are managed?
- Are traditional and social media part of a strategy of public education and emergency information?
- Are there unattended, automatic sources of information (e.g. sensors, cameras)?
- Do you have basic cartography and essential GIS files?
- Do you listen and critically analyse on a regular, fair, diligent basis to people sending you alarms?
- How can the emergency units prepare?
- Do you have believable, honest clear communication channels towards the public?
- In emergency, do you have access to existing communication channels?
- How is inter-organization communication assured?
- How is infra-organization communication assured?
- Is there a checklist for first responders existing?
- Are you aware of emergency resources, capabilities dimension and location?
- How stress and burn-out are managed?
- Are effectiveness and timing of response measured, and critically analysed?
- Are emergency experiences channelled within strategic planning?
- Is there a due diligence of flaws, wastes, leanness and effectiveness of emergency responses history?

- Budget:
  - *Financial reserves to be accessed in case of emergency should exist. A proper financial planning devoted to resilience and crisis management must be included in the overall budget definition process. When dedicated funds for new resources required for crisis management are not available, a proper reuse procedure may be defined, where existing assets are borrowed from other departments during the crisis operation (e.g., laptops or tools necessary to the civil protection may be taken from other departments of the Municipality that are not using those assets during the crisis).*
  - *A proper insurance system should exist in parallel to the crisis management budget, to be used in order to cover the costs and risks, which the Organization is not able to cover with its own financial resources.*

- Data & Algorithm:
  - *Crisis Management team should have immediate access to executive summaries and dashboards of historical, environmental, technical, estate, industrial, infrastructural data and Standard Geographical Information System (GIS) files, possibly available and accessible even without networking and power supply infrastructures, through local copies, data backup, business-continuity and emergency recover solutions.*
  - *Data required during crisis operation should be planned in advance and properly kept updated by the different data providers.*

2. Training and experience

- *Crisis Management team should plan and regularly maintain a proper awareness and competence of people regarding response to the crisis.*
- *Simulations, game-based training, learning events, and continuous information procedures should keep population as well as the different actors well informed on the risks, the recommended procedures, and the existing answers to the different emergencies occurring in the specific territory.*
- *Due to the complexity of operations and variety of stakeholders to be engaged during the crisis,*

Examples

In the European experience, one could see the 1966 Florence flood, as a changing mind-set event. The dramatic flood provoked by Arno river in Tuscany may be considered, in many ways, a turning point in modern emergency awareness, in a complex territory, where enormous common goods were at stake. In the case of Tuscany it was the case of thousand lives, industries, farms, but also crucial communication infrastructures connecting the North of Italy to Rome. Last, but not certainly least, there was the immense artistic and historical heritage that was imperilled.

The relief inadequacy was patent. In the early days rescue arrived almost exclusively by citizens' self-help and by volunteers. The early “angels of mud” where young students already in Florence and Tuscany for study, holidays. Several military units stationed down town also immediately reacted to the disaster, as they could. People reacted literally moving on their foot and digging in the mud with their hands.

Metropolitan, regional authorities were then absent, and also the municipal machine was very weak, backward, and in shortness of expertise and funds. The war experience, the post-war reconstruction efforts were still relatively near, but they could not provide much expertise in front of a natural disaster, if not sense of sacrifice, and personal, collective endurance.

It took days before the national government was able to put in place organized rescue.

In the following decades, European public authorities have become gradually more aware of dramatic consequences of natural disasters occurring on densely inhabited and industrialized territories, and the increasing challenge of protecting a cultural and environmental heritage of world significance *specific project management, coordination and human relations skills are necessary in the Crisis Management team.*

- *When new tools (such as new digital communication channels) are introduced within the operational procedures (e.g., the usage of WhatsApp or Telegram to communicate with people), a specific training program must be put in practice within the crisis management team.*

In order to improve the capacity of individuals, communities, institutions, businesses, and systems within a community, city to survive, adapt, and grow no matter what kinds of chronic stresses and acute shocks they experience, civil protection authorities have been established.

3. Quality of communication

- *Given the complexity of the crisis scenario, where multiple actors react in the same time in the same territory, communication is a critical factor to be properly managed and addressed.*
- *Operational procedures need to specify who is in charge of communicating what to whom, when, and on which channels. Decisions must be rapidly delivered to the person/entity in charge of communication and multiple and redundant channels need to be activated, with a unique source of the information itself.*
- *Semantics of the communication is crucial to avoid misunderstanding and to activate the needed actors at the right moment. Time and effort must be dedicated during the planning phase in order to ensure that the same terms are well understood and agreed by the different actors of the crisis response process.*
- *Simulations should be implemented periodically also to tune and optimize communications and messages during crisis response.*

<u>Limitations</u>

- Poor security culture and awareness in population and workers.
- Limited resources and spare time for training of workers.
- Extremely dynamic processes to be managed during crisis.
- Communication gaps among the different actors.

4. Human Computer Interaction and operational support

- *The opportunities of new digital media and tools need to be leveraged in order to maximize the effectiveness of the emergency actions. Not only social media and common messaging tools, but also game-based training and augmented reality applications can be used to collect possible requirements from stakeholders, and to train on best practices of crisis management.*
- *Regarding the software adopted within the emergency coordination centre, user interfaces should be periodically revised and analysed, in order to ensure that information is provided instantly in a clear and simple way to the specific decision-maker. Multiple login should be avoided in order to save time to access information, promoting single sign-on across the different information systems.*

5 - Availability of procedures and plans

- *Preparedness implies planning and it must be carried at all the organizational levels. Coordination of emergency actions is responsible for setting up, maintaining and updating general, localized, specific plans for each kind of risk, based on risk identification, analysis, evaluation and reduction .*
- *Civil protection planning is carried out according to the "Augustus" method established in 1997 (see:* http://ec.europa.eu/echo/files/civil_protection/vademecum/it/2-it-2.html*) to face complex emergencies*

through a standardised and easy-to-implement approach. The Augustus method is a current guideline to set up emergency coordination centres at all (local, provincial, regional and national) civil protection levels. The method includes a checklist for the setting up of up to 14 operational lines, which can be considered as 14 potential sub-functions of the present:

SF 8.1: Planning techniques
SF 8.2: Health, social and veterinary assistance
SF 8.3: Media and information
SF 8.4: Volunteers
SF 8.5: Means and materials
SF 8.6: Transportation and viability
SF 8.7: TLC
SF 8.8: Essential services
SF 8.9: Damage assessment
SF 8.10: Operative structures
SF 8.11: Local authorities
SF 8.12: Dangerous materials
SF 8.13: Assistance to the population
SF 8.14: Coordination of operational centres.

- *Approved and updated procedures and plans need to be properly published and made accessible to the different actors. Meetings with the emergency coordination team need to be periodically (at least twice per year) organized, and be used to disseminate and promote knowledge of the approved procedures.*

6 - Conditions of work

- *Emergency response and management actors need to be endowed with proper tools, instruments, and skills to behave correctly and effectively, according to the approved procedures.*
- *A proper personnel shift and timetable scheduling need to be organized in the planning phase, by reducing as much as possible stressing conditions, and by rotating personnel as possible given the emergency conditions.*
- *The organization must provide workers with proper insurance guarantees covering the risks associated to their activity.*

7 - Number of goals and conflict resolution

- *Operational emergency procedures need to include*

Sources

- Example of a Civil Protection communication & dissemination website, where operation procedures and information to citizen are widespread: http://protezionecivile.comune.fi.it
- http://opendata.comune.fi.it/
- Example of a City Datastore, where information usefull for the emergency coordination centre can be collected: http://opendata.comune.fi.it

- Example of an hyperlocal community proposing Smart City initiatives and urban design: http://firenzesmartcity.org/

- The RESOLUTE website: http://www.resolute-eu.org

- An international initiative on Resilient Cities: http://www.100resilientcities.org

- High Velocity Human Factor (HVHF) – Moin Rahman - High Velocity Human Factors: Human Factors of Mission Critical Domains in Nonequilibrium Proceedings of the Human Factors and Ergonomics Society Annual Meeting October 2007 51: 273-277, doi:10.1177/154193120705100427. The High Velocity Human Factor (HVHF) paradigm concerns human capability and limitations when working in safety-critical domains. It is included in User-centred design principle with a focus on mission critical communication technology.
- The HVHF approach supports the design of intuitive, robust and reliable user interfaces from to device to dispatch and back office control room.
- Ergonomic principles in the design of work systems BS EN ISO 6385:2004. A work system is defined as "a combination of people and equipment, within a given space and environment, and the interactions between these components with a work organisation""(p10)

the expected goals of each emergency response process (e.g. to restore viability under a flooded road underpass)

- *After crisis solutions a proper assessment need to be implemented to check any occurred conflicts (e.g. actor X thought that actor Y would have solved issue Z, actor Y thought it was a duty of actor X).*
- *Occurred conflicts need to be addressed, solved and reported in the update of the following operational procedure.*

8 - Available time and time pressure

- *Simulation and training programs need to address the time pressure issue, as workers need to be trained to react with prompt actions, and decision makers need to be trained to solve issues in due time.*
- *Risk assessment and critical system functions need to take into account the time after which the damage and impact of an unavailable resource is going to worsen (e.g., after 6 hours of power supply downtime, hospital temporary power supply system are going down)*

9 - Circadian rhythm and stress

- *There must be specific psychological training of the personnel involved in the emergency response to cope with stress*
- *Working shifts may take into account wake/sleeping rhythm and manage shifts according to the severity of the event and the availability of human resources*

10 - Team collaboration quality

- *Training courses may include team working and group-working, thus improving relationship and group empathy among the emergency coordination team members.*
- *Specific training programs for work under very stressful situation need to be implemented at least once per year.*

11 - Quality and support of the organization

- *The organization needs to annually check human resources, technological tools and equipment requirements from the emergency coordination team.*
- *External human resources hiring for the emergency coordination team must be screened, carefully designed and administratively conceived during the planning phase, and must be agreed in such a way to provide the required resources with a near-to-zero time notification (e.g. during the night, or during festivities).*

- Ergonomic design of control centres, Parts 1-7, ISO 11064. Covers design principles, control room arrangements and layout, workstations, displays, controls, interactions, temperature, lighting, acoustics, ventilation, and evaluation. Designers should be following this standard for new control rooms, and it can usefully be referred to for upgrades and modifications to existing ones especially where there are known problems.
- Process plant control desks utilizing human-computer interface: a guide to design, operational and human interface issues. Engineering Equipment & Materials Users Association (EEMUA) Publication 201: 2002 available via EEMUA on 020 7628 7878
- The Civil Protection authority in the City of Florence
- http://protezionecivile.comune.fi.it/wp-content/uploads/2011/09/Il-Sistema-Comunale.swf
- Civil Protection Plan in the City of Florence – General guideline
- http://dominoweb.comune.fi.it/OdeProduzione/FIODEWeb2.nsf/AttiWEB/49E27A9AE74726B0C1257E0100025CDF/$File/2015_C_00008.pdfRESOLUTE_ERMG_v3.docx
- Flood Emergency Plan in the City of Florence
- http://dominoweb.comune.fi.it/OdeProduzione/FIODEWeb2.nsf/AttiWEB/F6D8CF80EB3EF0E7C1257E6800805F19/$File/2015_C_00030.pdf
- Snow and Ice Emergency Plan in the City of Florence
- http://dominoweb.comune.fi.it/OdeProduzione/FIODEWeb1.nsf/AttiWEB/87E222B64C78BA2CC125795A0032F4C8/$File/2011_G_00444.pdf

- *Periodical meeting occasions need to be scheduled by the organization in order to show the emergency coordination team to the rest of the organization, thus promoting communication flows across the vertical departments and the emergency coordination team.*

Interdependencies recommendations

This Function is strictly related to the human behaviour, to the reaction instinct that humans and workers activate during an emergency. Several human factors need to be considered, mainly related to stress management, training, functional abilities allowing reacting promptly and relationship with people being rescued. In this sense, awareness and user generated feedback are key aspects to take into account.

Moreover, monitoring operation, the physical infrastructure, and addressing the service delivery are also other important aspects to which this function is related.

3.6.2 Restore/Repair operations

Background facts

Disaster impacts comprise physical and social impacts. Physical impacts can be subdivided in infrastructural impacts and services and procedures. Literature and media diffusion about services/procedures impacts are not so diffuse as the ones about procedures. This is due partly to the different scale with which both problems are perceived or caused. A limited disaster could not have a significant impact on infrastructures but can block some services.

Damage to infrastructures can cause direct service and procedures related problems. However, restoring infrastructures is not always enough to repair correctly services and procedures linked to them. Furthermore, it is necessary to act quickly to restore services and procedures, in order to avoid more social impacts including psychosocial, economic, and political implications.

There are a lot of different cases that can block or damage urban services and directly influence community procedures. These can be catalogued in different scales:

- localized impacts (i.e. local traffic stop due big incidents, heavy machinery fall, etc.; water supply interruption due to a landslide on the pipeline)
- diffused impacts (i.e. traffic and public transport congestion due meteorological events; railway network block due to derailments);
- total impacts (i.e. dramatic events like 1966 Florence flood or 2009 L'Aquila earthquake);

Despite infrastructure are normally handled by public authorities, service and procedures are almost always outsourced to private or semi-private companies. They are responsible for the continuity of services, their implementation and of all communications to citizens and institutions. Institutions instead care infrastructures from which the services are dependent. Relations between the two entities are normally controlled by contracts signed previously. In these contracts normally are foreseen the procedures and recovery times in case of service problems or disruption.

General recommendations

Abstract

There shall be a function able to rebuilding and repairing services and procedures Goal of this function is involving the restoration of normal community activities that were disrupted by disaster impacts. It’s done by a plurality of persons and equipment and encompasses multiple activities, some implemented sequentially and others implemented simultaneously. To achieve it is necessary resources availability and planning in short-term recovery and long-term reconstruction.This Function is also highly depending and connected to the restoring of physical infrastructures.

Questions

- Which are the stakeholders that should be involved and how?
- How the roles and responsibilities are clearly defined?
- How the processes are defined, established and communicated?
- What are the dedicated available resources? Buffer capacities?
- Are you aware of the vulnerabilities of your infrastructure?
- How can the organization infer the time needed to its customers to return to the normal level of service usage after a disruptive event (e.g. a terrorist threat)?
- How the productivity/efficiency and precision of the work is assessed?
- How the organization guarantees flexibility?
- Are buffer capacities/resources assessed?
- Which (social) media should be used by the organization to provide information/communication in order to support a quick return to the normality
- Are good practices and existing gaps classified in a chronological order? (pre-incident, during-incident and post-incident)

- *National bodies and organisations involved in restore/repair operations should be prepared anytime to react promptly and efficiently on the basis of an accurate evaluation of the impacts so that the normal operations will be restored as fast as possible.*
- *The different nature of disasters and the variability of the system operation should be managed supported by the necessary technological, human and organisational resources, including the necessary budget.*

Common Conditions recommendations

1 - Availability of resources

- Humans (labour) – skills/competence

Members of Restore and Repair operations should be people who profoundly know the urban environment in relation to the essential functional priorities (technical and procedural) of the affected system for which they are in charge and its connection with different aspects of the urban framework (geographically, socially, and legally). Their working vision should be based on an integrated operational approach, which encompasses a set of actions useful to recover people's daily activities, public and sensitive data mobility and goods transport, but also to obtain a life-line system for rescuing people and economic values and for repairing and restoring all the related systems when they are disrupted. In relation to this dual aspect people involved in the function should maintain their skills and competences at a high level by means of recurrent trainings in the field of smart cities urban planning and urban resilience activities. Such acquired expertise must be shared with the territorial management authorities in order to maximize the effectiveness of the possible restore and repair activities, to optimize the intervention times within the local planning rules and to ensure continuity between the emergency phase and the ordinary management phase.

- Budget:

In case of critical situations that turn into emergencies financial reserves should budgeted for store and repair. The allocation of support funds should be budgeted in relation to urban structure and relative risks. The portfolio should also have a wide margin of use because of the variability of each possible event in terms of typology, level of criticalities and extension. In this perspective funds must be designated both by the involved privet companies and the public entities in relation to their responsibilities.

- Data & Algorithm:
  - *Use of standard documentation for data and algorithms*

Examples

- National Response Framework (NRF) - USA

This is a guide to how the U.S. Nation conducts all-hazards response. It is built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the Nation, linking all levels of government, nongovernmental organizations, and the private sector. It is intended to capture specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters. The term "response" as used in this framework includes immediate actions to save lives, protect property and the environment, and meet basic human needs. Response also includes the execution of emergency plans and actions to support short-term recovery. The Framework is always in effect, and elements can be implemented as needed on a flexible, scalable basis to improve response.

http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (Mar. 24, 2016)

- National Disaster Recovery Framework (NDRF) - USA

It describes the concepts and principles that promote effective Federal recovery assistance in U.S. It identifies scalable, flexible and adaptable coordinating structures to align key roles and responsibilities. It links local, State, Tribal and Federal governments, the private sector and nongovernmental and community organizations that play vital roles in recovery. The NDRF captures resources, capabilities and best practices for recovering from a disaster (localized or at large scale).

- *Use of recognized project management concepts*
- *Use of standardized models and protocols*
- *Production of quantitative measures in order to manage the required action plans*
- *Use of Historic data in relation to short- to long-term responses (natural and anthropic) of the urban context to possible and actual critical scenarios.*
- *Acknowledge existing legal acquis, local conditions and regulatory regimes*
- *To locate the exact relationship between infrastructures and services/procedures is a sensitive issue, but it can provide major advantages in terms of resilience. This relationship must be properly applied to simulation models. Models are used to prepare backup services and redundant procedures that can avoid problems due localized disaster impacts, mitigate and absorb problems due diffused disaster impacts. The same model can also identify stressful situations that must be avoided in order not to become fatal in case of disaster.*

2 - Training and experience

- *Social and territorial data analysis, network examination and software simulation by good practice experts*
- *Management and coordination skills to collect the contingent information and to project restoration activities*
- *Expertise in financial and environmental management, procurement and technical issues in design, construction and maintenance*
- *Periodic training sessions should be carried out in order to maintain, improve and update skills and competences*

3 - Quality of communication

- *Guarantee a complete and clear share of knowledge, data and aims among all the actors and from actors to the final users (active interaction) at all the main steps of the implemented actions*
- *Guarantee the accuracy and understandability of the communication through standardized communication tools, protocols and languages*

Moreover it is a companion document to the NRF and is supported by the ongoing development of detailed operational, management, field guidance and training tools. The focus of the NRF is the response actions as well as the short-term recovery activities that immediately follow or overlap those actions. The NDRF does not speak to these short-term activities. However, they influence recovery activities, necessitating the need for a structure to consider and advice on recovery implications during the early phases of incident management. The NDRF provides the tools to encourage early integration of recovery considerations into the response phase operations. The NRF fully transitions to the NDRF when the disaster-specific mission objectives of the Emergency Support Functions (ESFs) are met and all ESFs demobilize.

https://www.fema.gov/pdf/recoveryframework/ndrf.pdf

- Queensland 2013 Flood Recovery Plan - Australia

This Recovery Plan provides strategic guidance for the coordination and management of recovery, reconstruction and community resilience activities undertaken by the Queensland State government, local governments, non-government partners, industry and not-for-profit organisations after the flood and damage impacts of Tropical Cyclone Oswald (TCO) in 2013. Its purpose is to assist disaster-affected communities get back on their feet as quickly as possible while ensuring the effective and efficient employment of limited resources. In particular, it sets the context for improved enhancement of resilience across the functional areas of recovery. The scope of this Plan is restricted to those local government areas impacted by TCO and it associated rainfall and flooding. The Recovery Plan recognises the complex and dynamic nature of the disaster recovery environment and has been also

4 - Human Computer Interaction and operational support

- *Utilization of software tools to analyse data and project focused intervention plans.*
- *Utilization of social networks to collect data and information about the opinion of citizens with respect to the recovery actions*
- *Utilization of software tools to analyse the impact of the operational strategies which could be applied to the disrupted system, also supporting the evaluation socio-economic cost-benefit.*
- *In normal situation or in case of emergency, the monitoring of services/procedures is directly connected to the monitoring of infrastructures, with all the temporal, qualitative and quantitative connected considerations. However, services and procedures also have a great social impact. To monitor and to be able to interpret feedbacks from media and social network becomes important. Evaluate the psychological impact that the lack of a service has on the population is difficult and not temporally immediate. But being able to understand what services and how quality is perceived as belonging to a normal situation is a key point to focus energies.*
- *Human Factors concerns on human-computer interfaces, contents and dialogues should be set up in order to ensure easy, safe, comfortable and efficient interactions avoiding errors or any type of fatigue or distraction*

5 - Availability of procedures and plans

- *Open Planning process to effectively outline the structural and not-structural list of actions*
- *Strategic financial and operational plans according to possible scenarios to be repaired*
- *Procedure for fast availability of all the necessary resources*

6 - Conditions of work

- *Take into account (in advance) specific legislation to ensure that personnel may bear responsibility, also under an effective insurance system*
- *knowledge and awareness about priorities for recovery after the emergency in order to*

developed to incorporate strategies necessary to recover from subsequent similar natural disasters.

http://www.dsdip.qld.gov.au/resources/plan/local-government/lg-flood-recovery-plan.pdf

- Dudley Recovery Plan (DRP) - UK

This plan is an integral part of the emergency management process and it has been produced by the Metropolitan Borough Council to detail the arrangements for multi-agency recovery coordination in Dudley (UK). This document is intended for strategic representatives of all agencies who would have a role to play in multi-agency management (i.e., rebuilding, restoring and rehabilitating the community) after an incident. This practice is distinct from, but sometimes overlaps with, the response phase, which can be defined as the actions taken to deal with the immediate effects of an emergency. The principle, guidance and annexes contained in this plan may also provide options and structure to recovery management in smaller scale incidents that would not trigger multi-agency coordination.

Dudley Metropolitan Borough Council (2010). *Recovery Plan*. Contingency and disaster management.

<u>Limitations</u>

- Possible limited financial resources
- Possible contracts limitations between institutions and private companies
- Possible resistance to allocate more money to avoid hazard vulnerability in future
- Possible lack of infrastructures where to place alternative services and procedures

disseminate properly funds, material and human resources

- *Capacity to facilitate the cooperation among the different stakeholders during the debriefing activities and all the steps of the field operations*
- *Manage physical, temporal and organisation conditions of work in order to enable actors with the best conditions for acting and taking risks for the required actions towards the best efficiency of operations*

7 - Number of goals and conflict resolution

- *Tangible structural and not structural measures to restore the ordinary and fully operational condition that were disrupted by disaster impacts.*
- *the operating units should be organized taking into account the scale of the problem and timeline of the plan*
- *Quantitative and qualitative measures about the expected impact of the applied working methodologies*
- *Definition of the activities that must be planned before and in prevision of a disaster impact and those that must be improvised only after disaster impact.*

8 - Available time and time pressure

- *Immediate response needed in order to restore basic services as soon as possible*
- *Function must be planned to act in short-term recovery and long-term reconstruction based on the importance of the service/procedure*

9 - Circadian rhythm and stress

- *Restore quickly service/procedures the lack of which can stress ordinary life*
- *Identify what services and how quality are perceived as belonging to a normal situation*
- *Take into account minimum rest and sleep times for operators in order to avoid circadian rhythms asynchrony and consequent errors or mishaps*

10 - Team collaboration quality

- *Adherence to the principles of collaborative planning*
- *It's very important collaboration and cooperation between institutions and private companies that operates*

Sources

- Baroudi, B., & Rapp, R. (2013). Disaster Restoration Projects: A Conceptual Project Management Perspective. In Australasian Journal of Construction Economics and Building-Conference Series (Vol. 1, No. 2, 72-79).
- Crawford, L., Langston, C., & Bajracharya, B. (2013). Participatory project management for improved disaster resilience. International Journal of Disaster Resilience in the Built Environment, 4(3), 317-333.
- Dudley Metropolitan Borough Council (2010). Recovery Plan. Contingency and disaster management.
- Duque, P. A. M., Dolinskaya, I. S., & Sörensen, K. (2016). Network repair crew scheduling and routing for emergency relief distribution problem. European Journal of Operational Research, 248(1), 272-285.
- FEMA (2011). National disaster recovery framework: Strengthening disaster recovery for the nation. https://www.fema.gov/pdf/recoveryframework/ndrf.pdf (Mar. 24, 2016)
- Karen Miranda (2013). Adaptive self-deployment algorithms for mobile wireless substitution networks. Networking and Internet Architecture [cs.NI]. Université des Sciences et Technologie de Lille - Lille I
- Kochs, A., & Marx, A. (2009). Innovatives Instandhaltungsmanagement mit IDMVU, Leitfaden Teil 1 Überblick Gesamtprozess. Forschungsvorhaben Infrastruktur-Daten-Management für Verkehrsunternehmen (IDVMU).
- Lindell, M. K. (2013). Recovery and reconstruction after disaster. In Encyclopedia of natural hazards (pp. 812-824). Springer Netherlands.
- United States Department of Homeland Security (2008). National Response Framework. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (Mar. 24, 2016)

on services/procedures

11 - Quality and support of the organization

- *Clear decision making process and alignment of responsibility*
- *Alignment of decisions with defined priorities*
- *Having clear what type of services and procedure must be repaired before others*

Interdependencies recommendations

This function must be activated by and with the supervision of the Coordinate Service delivery function, receiving by it plans and coordination with other procedures. It would be appropriate to not start this function before critical emergency is finished.

This function must provide the highest possible feedback to Coordinate Service delivery function so that it can coordinate the activities. This can be performed by direct communication or by monitoring continuously the repair operations. This function must also communicate with Manage awareness & usage behaviour function so it can be awareness about status of services and procedures.

- Queensland Government (2013). Queensland 2013 Flood Recovery Plan for the events of January–February 2013. http://www.dsdip.qld.gov.au/resources/plan/local-government/lg-flood-recovery-plan.pdf (Mar. 24, 2016).

- Ramachandran, V., Long, S., Shoberg, T., Corns, S., & Carlo, H. (2016). Post-disaster supply chain interdependent critical infrastructure system restoration: A review of data necessary and available for modelling. Data Science Journal, 15.
- http://www.sadc.int/themes/infrastructure/transport/roads-road-transport/
- http://ec.europa.eu/transport/themes/urban/studies/doc/2007_urban_transport_europe.pdf

It's strongly recommended that this function should coordinate itself with Restore/repair physical infrastructure function. In particular it is necessary to share operation plans and carefully coordinate restore timing plans. Also human resources can be optimized to repair/restore both infrastructures and services/procedures. Obviously, it is necessary that a service must be restored after the infrastructures it depends are restored and checked.

To increase resilience it is also important, after the activities, that all data regarding the restoring operation became available to those who deal to collect information about the disaster event.

Degraded operations must observe at all times legal requirements and standards.

3.7 Learn

3.7.1 Collect event information

Abstract

This function aims at collecting relevant data and information about the event and its impact. It is important that data coming from in-house and external sources should be considered in order to have a complete and comprehensive overview of the event and the response of the affected critical infrastructure/system.

Then, data and information collected have to be stored, in order to establish an updated and holistic historical knowledge-base, to be used for defining new good practices and more effective resilience guidelines.

To achieve this goal, and taking into account the different sources of data and information which could become available over time, suitable data storage and data integration/fusion has to be used, in order to collect both structured (from ICT systems) and unstructured data (i.e. user generated contents).

Finally, it is important, in the data collection and integration process, to access to data coming from other interconnected critical infrastructures as well as similar events in different geographical areas, in order to better define and model relationship between features of the overall setting and impact of the event.

Background facts

When a disruptive event affects a critical infrastructure, it generates “effects” at different layers which could be monitored – and hopefully controlled during the emergency management – through ICT systems or information reported by operators and citizens.

The collection of information and data related to disruptive events are therefore crucial in order to enable the definition of good practices, the contribution to the definition and update of guidelines, the identification and evaluation of actions supporting a quick recovery to normality as well as adaptations to increase the overall resilience of the system.

An organization works with three classes of knowledge: *tacit knowledge*, rule-based knowledge, and background knowledge. Tacit knowledge consists of the hands-on skills, special know-how, heuristics, intuitions, and the way people develop as they immerse in the flow of their work activities; *rule-based knowledge* is explicit knowledge that is used to match actions to situations by invoking appropriate rules; *background knowledge* is part of the organizational culture and is communicated through oral and verbal texts such as stories, metaphors, analogies, visions, and mission statements. Thus a dedicated information/knowledge management is necessary.

The basic goal of information management is to harness the information resources and information capabilities of the organization in order to enable the organization to learn and adapt to its changing environment.

Different ICT systems and platforms are generally used to constantly monitor the current condition of the critical infrastructure and support the evaluation of possible risks. Other ICT solutions are then employed during the emergency management, often requiring a high level of integration and interoperability with monitoring systems. In many cases, the solutions adopted during the emergency management also requires integration and interoperability with monitoring and control systems of other critical infrastructures – interconnected to the affected one – as well as across the different stakeholders involved in the operations.

All these ICT based systems, platforms and solutions usually allow to collect and store in-home data (usually structured) which can be stored in order to be analysed – ex-post – to better understand the features of the event, its impact and the effectiveness of the current guidelines and good practices.

However, a huge amount of external information is usually lost, even if it could be extremely relevant to deeply understand, model and analyse the event and evaluate the current resilience capabilities of the system. In effect, any event is characterized by a multi-domain and multi-level nature, involving not only ICT systems and operators but also citizens. People involved in the event can for sure provide a lot of information which can complete the data and information collected through ICT systems and reported by the operators, respectively. It is important to highlight that in some cases the " human/social sensing" could be the only solution to collected information (e.g. about a specific area not covered by monitoring systems and not yet reached by the emergency management operators).

The critical issue associated to this function is related to the modifications that may occur over time and affecting ICT systems used at every level: to monitor and control the critical infrastructure, to coordinate, monitor and support the operations during the emergency management, to collect and store relevant information reported by the users of the critical infrastructure – or citizens in general – usually defined as "user generated contents".

<u>Questions</u>

– For which events the data are collected?
– How should the organization manage sources of information, e.g. sensors, cameras, staff, etc. in order to get a realistic picture
– How are the "measurements" made? (qualitative, quantitative)
– When are the measurements made (continuously, regularly)?
– How the quality of communication is measured (e.g. response time)?
– Do you have strategic centres (potential headquarters able to operate in emergency, with evidence of power supplies, antennas, satellite links, radio centres)?
– Which (social) media should be used by the organization to provide information/ communication in order to support a quick return to normality.

General Recommendations

- *Establish an organisational knowledge base to record ongoing operation data*
- *Identify organisational information needs. The identification of information needs should be sufficiently rich and complete in representing and elaborating users' real needs. Since information use usually takes place in the context of a task or problem situation, particular information needs will have to be elicited from individuals. Unveiling information needs is a complex, fuzzy communication process. Most people find it difficult to express their information needs to their own satisfaction. Personal information needs have to be understood by placing them in the real-world context in which the person experiences the need, and to the ways in which the person will use the information to make sense of the environment and so take action.*
- *Information acquisition seeks to balance two opposing demands. On the one hand, the information needs of the organisation are wide-ranging, reflecting the breadth and diversity of its concerns about changes*

<u>Example</u>

B. Hardjono, A. Wibisono, A. Nurhadiyatna, I.Sina and W. Jatmiko "Virtual Detection Zone in smart phone, with CCTV, and Twitter as part of an Integrated ITS", INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS VOL. 6, NO. 5, 2013

<u>Limitations</u>

Post-event stress could make difficult to collect reliable and consistent information about the event from involved citizens/users *and events in the external environment. On the other hand, human attention and cognitive capacity is limited so that the organisation is necessarily selective about the messages it examines. The first corollary is therefore that the range of sources used to monitor the environment should be sufficiently numerous and varied as to reflect the span and sweep of the organization's interests. While this suggests that the organization would activate the available human, textual and online sources; in order to avoid information saturation, this information variety must be controlled and managed. A powerful way of managing information variety is to involve as many persons as possible in the organization in the gathering of information, effectively creating an organisation wide information collection network.*

- *Human sources of information are among the most valued by people at all levels of the organisation: human sources filter and summarize information, highlight the most salient elements, interpret ambiguous aspects, and in general provide richer, more satisfying communication about an issue. Information acquisition planning should therefore include the creation and coordination of a distributed network for information collection.*
- *The adaptive organization needs to be able to find the specific information that best answer a query, and to collate information that describes the current state and recent history of the organization. Well integrated archival policies and records management systems will enable the organization to create and preserve its corporate memory and learn from its history.*
- *The system should capture hard and soft information, support multiple user views of the data, link together items that are functionally or logically related, permit users to harvest the knowledge that is buried in these resources, and so on. Because the same information can be relevant to a range of different problem situations, it becomes necessary to represent and index the unstructured information by several methods. The development of automated indexing systems makes it increasingly feasible to adopt a user-centred approach to indexing, over and above document-oriented indexing that represents the document's content*

Sources

- White, K.J.S., Pezaros, D.P., Johnson, C.W., "Using Programmable Data Networks to Detect Critical Infrastructure Challenges", In: 9th International Conference on Critical Information Infrastructures Security (CRITIS'14), 13-15 Oct 2014, Limassol, Cyprus.
- Labaka, L., Hernantes, J., Sarriegi J.M., "A holistic framework for building critical infrastructure resilience", Technological Forecasting & Social Change, 103, (2016), 21-33.
- Vos, M., & Sullivan, H., "Community Resilience in Crises: Technology and Social Media Enablers", Human Technology, 10 (2), (2014), 61-67.
- Caschilli, S., Medda, F.R., Wilson, A., "An Interdependent Multi-Layer Model: Resilience of International Networks", Netw Spat Econ (2015), 15, 313-335.
- Asprone, D., Cavallaro, M., Latora, V., Manfredi, G., Nicosia, V., "Assessment of urban ecosystem resilience using the efficiency of hybrid social-physical complex networks", in Computer-aided Civil and Infrastructure Engineering 29, February 2013
- Jassbi, J., Camarinha-Matos, L.M., Barata, J., "A Framework for Evaluation of Resilience of Disaster Rescue Networks", in L.M. Camarinha-Matos et al. (Eds.): PRO-VE 2015, IFIP AICT 463, pp. 146–158, 2015.

Common Conditions recommendations

1. Availability of resources

- *Humans (labour) – skills/competence*

  - *At the heart of the organization are four groups of experts who need to work together as teams of knowledge partners: the domain experts; the information experts; and the information technology experts:*
    - ***The Domain experts** are individuals in the organization who are personally engaged in the act of creating and using knowledge;*
    - ***The Information experts** are the individuals in the organization who have the skills, training and know-how to organize knowledge into systems and structures that facilitate the productive use of information and knowledge resources;*
    - *The **information technology experts** are the individuals in the organization who have the specialized expertise to fashion the information infrastructure of the organization. The information technology experts include the system analysts, system designers, software engineers, programmers, data administrators, network managers, and other specialists who develop computer-based information systems and networks.*

  - *Skill and competences involved in this function are really different and multi-domain. Personnel of the critical infrastructure, who is in charge to internally cooperate to the emergency management, has to be trained in order to effectively support emergency management operators and guarantee cooperation and information sharing even beyond the current integration/interoperability of the ICT systems and solutions.*
  - *Furthermore, human factors and social science experts should cooperate to support users and citizens involved in the event in reporting information that could be useful in order to comprehensively understand the nature and characteristics of the event and the effectiveness of the overall response performed.*
  - *Finally, technological competences and skills are strictly required to allow the storage of all the data and information collected in a multi-domain and multi-level knowledge base which can be then used for supporting an ex-post analysis based on both historical and updated data and information. Technological competences and skills are also required in order to assure – hopefully improve – the level of integration and interoperability between different ICT systems, even along their own evolution.*
- *Budget:*

Financial reserves to be accessed for acquiring new ICT systems as well as to update those currently used with the aim of improving data and information collection, storage, integration and sharing.

- *Data & Algorithm:*
  - *Data coming from all the ICT systems used to monitor and control the critical infrastructure (also during the emergency management).*
  - *Data coming from all the ICT systems used by the emergency management operators.*
  - *Data/information collected through "social/human sensors" during the emergency (mainly users affected by the event).*
  - *Data/information collected through "social/human sensors" after the emergency (both users involved in the event and citizens in general).*
  - *Data warehousing and Big Data management (both structured and unstructured data).*
  - *Data/Information Fusion.*

2. Training and experience

- *Technological skills to store and integrate data from different sources and in different formats.*
- *Psychology and human/social science skills to retrieve relevant and trustworthy information about the event from users/citizens involved in the event.*

- *Cooperation skills to support and facilitate the collection and sharing of relevant information.*

3. Quality of communication

- *Guarantee communication channels which may work as a backup in case of emergency in order to ensure data/information sharing among different systems and stakeholders during the emergency management.*
- *Guarantee the correct communication with the users/citizens involved in the event – by involving human factors and social science experts – to collect useful and right information in order to improve understanding about the event and the current resilience capabilities of the system.*
- *Establish a reliable and continuous communication with the interconnected CIs*

4 - Human Computer Interaction and operational support

- *Several human-computer interactions during the emergency management, according to the different ICT systems used and the cooperation among operators*
- *Data/information input and storage to enable retrieval, visualization, correlation and analysis after the event*
- *Compliance with international standards on the design of computer –based systems in order to allow for easy, sage, comfortable and efficient human-computer interactions*

5 - Availability of procedures and plans

It is important to have already defined, and in case updated, procedures and plans regarding the cooperation between critical infrastructure and other emergency operators, in particular with respect the data and information sharing/integration goals

6 - Conditions of work

- *Provide legislation to ensure the cooperation among different stakeholders and storage of shared data/information into a comprehensive knowledge base*
- *Apply existing legislation on working schedules and workload in order to ensure the best individual performance conditions to manage information*

7 - Number of goals and conflict resolution

- *The public and political scrutiny to which most critical infrastructures are exposed may generate pressures over the availability of sensitive operational data and information on the outcome of investigations into certain occurrences. Various conflicts and pressures may be felt when addressing decisions on whether or not to make public certain types of information or to what extent such information should be disseminated to all members of the organisation or to relevant stakeholders. In order to manage such potential conflicts, all actors need to be involved in the resilience building through a real participatory approach.*
- *Application of a shared semantics and methodology in reporting data and information regarding the event.*

8 - Available time and time pressure

- *Personnel must be trained: hands-on training sessions should be performed*
- *Technical personnel must be trained to support and keep up-to-date the procedure for data and information integration/fusion*

9 - Circadian rhythm and stress

There must be specific psychological skills to support the collection f information from users/citizens who could be under stress due to the event.

10 - Team collaboration quality

- *High quality is required, in particular among technical personnel of critical infrastructure and emergency stakeholders*
- *Involvement of human factors and social science experts as to take into account characteristic of both event and critical infrastructure in order to acquire useful information from what users/citizens report*

11 - Quality and support of the organization

Clear plan for cooperation and information sharing with other relevant stakeholders (emergency management operators and human factors and social science experts

Interdependencies recommendations

Interdependencies are related to the different data sources, in particular internal, which have to be considered in order to increase the level of knowledge about events, features of the CI and possible impacts. Data are related to different actors and technological systems involved during all the phases of the prepare-absorb-recovery-adapt process.

In order to maximise the internal data availability, a dedicated procedures, wide information as well as a specific ICT infrastructure should be put in place to favourite data transfer from different functions.

3.7.2 Provide adaptation & improvement insights

Abstract

This function aims at analysing data and information collected in order to discovery useful insights and define adaptation actions to increase resilience. The core activities associated to this function are related to the ex-post analysis of relevant events, involving all the relevant actors in a de-briefing. The final goal is to learn from past events in order to identify corrective actions aimed at improving the overall resilience of the system. To achieve this goal, it is important to have monitored and collected data about operations during the event, examine good practices and simulate "what-if" scenarios to estimate the impact of actions, based on the discovered insights, which can be suggested to increase the overall system adaptation.

Background facts

The complexity of interconnected systems, such as critical infrastructure, requires a deep analysis of the possible responses to events. Furthermore, the highly dynamic behaviour – associated to the operations during and after the event, as well as the occurrence of "new" types of event – makes more difficult to model "a-priori" the possible response.

According to these considerations, the need to learn, directly from data, becomes crucial. Ex-post analysis, taking into account the nature and features of the event, the operations performed (and their timing), as well as the comparison with good practices, will permit to identify criticalities and vulnerabilities and, subsequently, define corrective actions to improve the adaptation of the system to similar events.

Data availability is also important for improving the capabilities to infer and model the behaviour of the system and simulate the possible expected impact of the corrective actions, even with respect to other types of events.

One relevant "unstructured" data source is related to social media and the contents generated by users – in particular people involved by the event as well as citizens in general.

General recommendations

When considering the relevant adaptation options, the following should also be considered:

- *When it will be necessary to take action and why,*
- *What level of adaptation will be required, and the consequences of over- as well as under- adaptation, in order to decide on the level of adaptation required.*
- *Establish an internal System Thinking perspective focusing on an holistic rather than a reductionist view of the organization*
- *Learning and Adaptation objectives should incorporate the total human beings with all the persons' intellectual and spiritual assets.*
- *Consider the Environmental Impact Assessment (EIA) as an appropriate instrument to mainstream adaptation, helping to improve the climate resilience of infrastructure. The Environmental Impact Assessment (EIA) is a procedural and systematic tool that is in principle well suited to incorporate considerations of climate change impacts and adaptation within existing modalities for project design, approval, and implementation. The EIA Directive (85/337/EEC) requires that environmental impact assessments shall identify, describe and assess the direct and indirect effects of a project on the human beings, fauna and flora, soil, water, air, climate, the landscape, material assets and cultural heritage and the interactions between these factors.*

- *While adaptation challenges differ from sector to sector, the on-going adaptation process also includes several common elements across the sector. Adapting infrastructure to a changing conditions needs to be considered in two ways:*

  a) *when constructing new infrastructure, climate resilience can be ensured by locating, designing and operating an asset with the current and future climate in mind. This is particularly important in the case of large infrastructure which usually has a lifespan of at least 20 years and, therefore, investment decisions influence future generations' wellbeing,*

  b) *existing infrastructure can be made more climate-resilient by retrofitting and/or ensuring that maintenance regimes incorporate resilience to the impacts of climate change over an asset's lifetime.*

- *Achieve sector and location specific climate resilience, there is a need for a thorough and coherent assessment of local climate impacts – based on historical records, but also including projections on future climatic conditions.*
- *Promote the creation and participation to a Trusted Information Sharing Network as a forum in which the owners and operators of critical infrastructure work together and share information on threats and vulnerabilities and develop strategies and solutions to mitigate risk.*
- *Define a Critical Infrastructure Program for Modelling and Analysis (CIPMA), a computer-based capability using a vast array of real data and information from a number of heterogeneous sources (internal and external) to model and simulate the behaviour and dependency relationships of critical infrastructure systems. CIPMA uses an all hazards approach to undertake computer modelling to determine the consequences of different disasters and threats (human and natural) to critical infrastructure. Owners and operators of critical infrastructure can use this information to prevent, prepare for, respond to or recover from a natural or human-caused hazard.*

Questions

Does the option meet your overall adaptation target?
Will the option be robust under today's climate and also under a series of different and plausible climate change futures?
The option should not negatively impact other areas or vulnerable groups
Can the action realistically be implemented and within what timeframe?
Does the option address an existing vulnerability or a risk which is already being experienced?
Is the option flexible in the face of uncertainties about the future?
Does it contribute to sustainability and resource efficiency objectives?
Do the benefits of the actions exceed the costs?
Does it consider not only economic costs but also social and environmental costs?
Are there windows of opportunity or synergies with other actions being planned that could facilitate adaptation measures being taken e.g. incorporating adaptation into the early steps of planning new construction or into infrastructure that is being upgraded anyway?
Will the adaptation option also decrease other risks than the intended climate risk, so that it helps to achieve other objectives?
What is the target of learning (individuals, organization)?
How are the effects of learning verified and maintained?
What is the nature of learning (qualitative, quantitative)?
What is the target of learning (individuals, organisation)?
How are the effects of learning verified and maintained?
How can the organization involve its customers/citizens to design adaptation strategies aimed at improving the overall perceived level of safety and security?

Common Conditions recommendations

1. Availability of resources

- *Humans (labor) – skills/competence*

  - *Several stakeholders have to be involved in the debriefing activities:*
    - *Technical/methodological experts for implementing and analysing the "what-if" simulation scenarios with respect to current and adapted system.*
    - *Experts in communication to translate simulation findings into proposals for the management.*
    - *All actors involved in the emergency coordination and management should provide information about performed actions, features of the event and the environment, behaviour of the people involved in the event.*
    - *Experts who can provide updated knowledge about good practice and support ex-post comparison and analysis.*
    - *Acquire information from citizens and people involved in the event.*

- *Budget:*

Adaptation might require relevant investment. To secure such investment, strategic planners and decision makers should be involved in the adaptation analysis.

- *Data & Algorithm:*

Data needed for the adaptation analysis are:

  - *Data acquired through monitoring systems (operations, user feedback, physical infrastructure, safety & security)*
  - *Data related to past events (or near missing)*
  - *Information collected from actors involved in the event*
  - *Good practices*
  - *Network modelling and simulation algorithms*
  - *Data Mining algorithms*
  - *What-if simulation algorithms*
  - *Vulnerability analysis*

Responding to climate impacts: railways between Copenhagen and Ringsted (DK)

Increased precipitation and increased water flow in watercourses can affect the new railway line between Copenhagen and Ringsted. In connection with the project on expanding the track capacity between Copenhagen and Ringsted on Zealand, the Public Transport Authority, which has analysed the track capacity, has carried out a climate change impact assessment for the project. The goal of the impact assessment is to investigate a future rail track's robustness to climate change over a 100-year operating period. The assessment shows that especially increased precipitation and increased water flow in watercourses can impact on railway constructions, whilst other factors such as increasing temperatures, rising sea levels and rising groundwater will not have a significant impact. Of particular importance is an expected 20% increase in the intensity of rainfall in heavy downpours in the year 2100.

In areas where watercourse crosses the track, under a bridge or tunnel, climate changes mean there is a risk that water cannot flow quickly enough and thereby build up and risk eroding the railway construction. Therefore a new track between Copenhagen and Ringsted will have a 30 per cent greater capacity for water flow than the norm that is used at present. The Public Transport Authority assesses that the recommendations for adaptation to climate change are robust in relation to the variations in the expected climate changes.

2. Training and experience

- *Experiences in Data analysis, network analysis and software simulation is required.*
- *Management and coordination skills to collect and share information, manage the de-briefing and support analysis and discussion.*

3. Quality of communication

- *Guarantee a complete and clear share of knowledge, data and information among the different actors*
- *Guarantee the understanding of the possible advantages and impacts produced by the discovered insights and provided adaptation actions.*

4. Human Computer Interaction and operational support

- *Utilization of software tools able to collect social networks data and information about the opinion and sentiment of citizens/people with respect to the preparedness, the event, the emergency management and the recovery actions.*
- *Utilization of software tools to model rules of the system – even "new" ones, discovered through the ex-post analysis of the event.*
- *Utilization of software tools to simulate "what-if" scenarios in the interconnected system and obtain (synthetic) data.*
- *Utilization of software tools to analyse the impact of adaptation strategies which could be applied to the system, also supporting the evaluation socio-economic cost-benefit.*

5. Availability of procedures and plans

Defining a process to effectively implement the proposed adaptations: working groups' management and economic/financial analysis for prioritising adaptation actions

6. Conditions of work

The cooperation among the different stakeholders during the debriefing activities, the analysis and the definition of insights and adaptations should be facilitated. Cooperation is related to sharing of data, information and evaluation at every level and multi-domain: social, economic, technological, infrastructural and service.

7. Number of goals and conflict resolution

Quantitative and qualitative measures about the expected impact of the application of the defined adaptations (e.g. reduction of risk with respect to similar past events as well as events occurred in different geographical areas).

Limitations

Costs for the "optimal" adaptations could be too high, making difficult their implementation – prioritisation of actions can facilitate the implementation of the most critical adaptations

Sources

Ouyang, M., "Review on modelling and simulation of interdependent critical infrastructure systems", Reliability Engineering and System Safety, 121, (2014), 43-60.

Labaka, L., Hernantes, J., Sarriegi J.M., "A holistic framework for building critical infrastructure resilience", Technological Forecasting & Social Change, 103, (2016), 21-33.

Welsh, M., "Resilience and responsibility: governing uncertainty in a complex world", The Geographical Journal, 180, (2014), 15-26.

Lazari, A., "European Critical Infrastructure Protection", Springer Cham Heidelberg New York Dordrecht London, 2014.

White, K.J.S., Pezaros, D.P., Johnson, C.W., "Using Programmable Data Networks to Detect Critical Infrastructure Challenges", In: 9th International Conference on Critical Information Infrastructures Security (Oct 2014, Limassol, Cyprus.

Jokeren, O., Azzini, I., Galbusera, L., "Analysis of Critical Infrastructure Network Failure in the European Union A combined Systes Engineering and Economic Model", Netw Spat cEcon (2015), 15:253-270.

8. Available time and time pressure

- *Medium/long term goals related to the reduction of risk and possible impacts of disruptive events, even if analysis should be performed in the very short-time after the event in order to guarantee the collection and analysis of data and information which are not stored into ICT systems.*
- *Adaptations can be related to different levels and domains, thus different times can be required to implement adaptation actions, even according to budgetary constraints*

9. Circadian rhythm and stress

- *Ensure appropriate work schedules and workload to every professional involved in the function in order to mitigate the risk of wrong evaluation that may result in following issues:*
  - *a) persistence of the vulnerability because of the inefficacy of the solution provided*
  - *b) loss of resources*
  - *c) possible new vulnerabilities introduced*

10. Team collaboration quality

Collaboration and cooperation are crucial for accurately address the analysis of data and information, the definition of adaptations and the evaluation of their potential impact.

11. Quality and support of the organization

- *Clear decision making process and alignment of responsibility*
- *Clear commitment of the organization establishing dedicated roles assigned to senior manager and planning periodical briefings among adaptation team and strategy planners, financial managers and risk managers.*

Trucco, P., Petrenj, B., Bouchon, S., Di Mauro, C., “The rise of regional programmes on critical infrastructure resilience: identification and assessment of current good practices”, Disaster Management and Human Health Risk IV, WIT Transactions on the Built Environment, 150, (2015), 233-245.

Gao, J., Liu, X., Li, D., Havlin, S., “Recent Progress on the Resilience of Complex Networks”, Eergies 2015, 8, 12187-12210.

Kangaspunta, J., Salo, A. “A Resource Allocation Model for Improving the Resilience of Critical Transportation Systems”, (2014)

George Stergiopoulos, Panayiotis Kotzanikolaou, Marianthi Theocharidou, Georgia Lykou, Dimitris Gritzalis, Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures, International Journal of Critical Infrastructure Protection, Volume 12, March 2016, Pages 46-60,

Xu, T., Masys, A.J., “Critical Infrastructure Vulnerabilities: Embracing a Network Mindset”, A.J. Masys (ed.) Exploring the Security Landscape: Non-Traditional Security Challenges, Advanced Sciences and Technologies for Security Applications (2016).

Interdependencies recommendations

An effective adaptation can be only identified taking into account relevant data about the event and possible budgetary constraints.

- *The current status of the cyber physical infrastructure as well as the usage behaviour have also to be known in order to define the most suitable adaptation actions.*
- *Finally, all the information related to the service provision has to be deeply evaluated in order to estimate the possible variations of the service associated to the adaptation actions and improvement insights identified.*

3.8 Cross-CI Interdependencies

Growing interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks. In an increasingly interconnected world, where critical infrastructure crosses national borders and global supply chains, the potential impacts increase with these interdependencies and the ability of a diverse set of threats to exploit them.

In this chapter, a set of guidelines related to cross-CI interdependencies are suggested, following existing practices and related activities outside the EU.

The main idea is to assist owners and operators of critical infrastructure to identify, analyse and manage cross-sector dependencies. The main pillars of this approach are summarized in the following points:

- The identification and analysis of cross-sector dependencies assists risk assessments and consequently, mitigation policies.
- Greater insight to cross-sector dependencies contributes to the EU understanding of industry-wide security issues, thereby supporting the provision of high quality policy advice to local and EU officials.

These can be achieved through:

a) Understanding and addressing risks from cross-sector dependencies and interdependencies

The way infrastructure sectors interact defines in large how the different critical infrastructure owners/operators should cooperate in managing risk and therefore enhancing resilience. For example, energy, communications, transportation, and water systems, among others, are common dependencies for any critical infrastructure.

b) Gaining knowledge of infrastructure risk and interdependencies requires information sharing across the critical infrastructure community.

Through their operations and perspectives, stakeholders across the critical infrastructure community possess and produce diverse information useful to the enhancement of critical infrastructure security and resilience.. The creation and maintenance of a relevant data sharing repositories, such as the Critical Infrastructure Warning Information Network (CIWIN)_established in the EU, can drastically contribute in knowledge sharing and, thus, better coordination between different CIs

c) Analyse Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects

Greater analysis of dependencies and interdependencies at international, national, regional, and local levels can inform planning and facilitate prioritization of resources to ensure the continuity of critical services and mitigate the cascading impacts of incidents that do occur.

A good example of structure for managing the cross-sector interdependencies is proposed by the Australian Government (2010) which is recommended here, adjusted to fit the EU perspective

1. Establishment of an EU program for modelling and analysis of Critical Infrastructure

Such a program shall aim in examining the relationships and dependencies between critical infrastructure systems, and suggest how a disruption in one sector can greatly affect the operation of critical infrastructure in other sectors. This projection assists owners and operators in enhancing and adapting their mitigation strategies, and hence the resilience of their critical infrastructure, and the EU officials in producing legislation and initiate relevant policy initiatives.

An example of such a system is the CIPMA already established and operating in Australia.

2. Strengthen the structures for incident preparedness and response

It is of utmost importance for critical infrastructure organisations to be prepared for incidents that have actual or potential cross-sector impacts that could disrupt their operation. To strengthen the preparedness of critical infrastructure organisations to manage cross-sector impacts, capacity building initiatives should be prepared and operated, in consultation with business and member-states governments' stakeholders. Moreover, owners and operators of critical infrastructure should be assisted in sharing lessons learnt from real and exercised incidents within their sector and across other Sector Groups, Europewide..

3. Periodic exercises on cross-sector dependencies and related workshops

No matter how well interdependencies are planned and modelled, exercises have an irreplaceable role to play in improving preparedness for incidents, understanding of cross-sector dependencies and pointing out issues that could lead to a decline in the resilience of critical infrastructure. Through exercises, participants are encouraged to reflect and familiarise with plans, procedures and scenarios that may have significant implications for the operation of critical infrastructure – not only in their sector but across other sectors. Cooperation and information exchange across sectors is also facilitated through the organisation of cross-sector exercises. For this purpose periodic exercise should be organised (at annual or bi-annual basis) together with a related workshop and networking event on cross-sector dependencies, with the contribution of key stakeholders across Europe and sectors.

4 CONCLUSIONS

The concept of resilience is becoming a continuously growing necessity mainly due to the radical evolvement of climate change and the terrorist attacks that have become a real threat in the EU territory. The EU has recognised this need and has already adopted a series of initiatives (more details in Chapter 1) in order to address this concept, mainly regarding critical infrastructure.

Within the overall efforts of introducing resilience in the everyday practice of critical (but not exclusively) infrastructure, RESOLUTE project aimed (among others) to address a set of European Resilience Management Guidelines (ERMG). The aim of the first version of the ERMG (presented in this document) is to establish a new way for Critical Infrastructure resilience thinking. The ERMG adopts a system's operational and dynamic perspective, focusing on the CI functions and their interdependencies, instead of a decomposition of CI into formal organisational, human or technical structures and an isolated approach to each of these structural elements. ERMG aims to provide valuable advices to decision makers and CI managers about how the infrastructure under investigation can be improved in terms of organizations, resource management, tools adopted, etc. in order to enhance the resilience of the system as a whole. In this sense, the guidelines also aim to provide the user with a full scale system overview, regardless of the organisational level or area from which the user may be operating, or of the role that the stakeholder plays towards the delivery of the service being provided by the CI.

The ERMG has been structured in such a way as to allow a self-evaluated multilevel gap analysis in respect to the state of affairs of their CIs. The first level of analysis is supported by the comparison between the desired functions provided in ERMG and the ones actually in place in the CI under assessment. The absence of one or more functions immediately orients decision makers towards considering their implementation. The second level of analysis is given by the comparison between how the functions implemented in the CI are actually aligned with the ERMG. Such second level gap analysis is able to guide the readers on solutions to manage the variability of functions' output. The third level of analysis is provided on functions' interdependencies assessment. The missing connection between functions may suggest that information or resources are not properly supplied or shared creating vulnerability in the system. Finally, the introduction of the Resilience Analysis Grid provides a valuable tool to synthetize the gaps analysis in terms of adaptive capacity of the CI to cope with continuously changing operational conditions.

Furthermore, within the framework of RESOLUTE, the ERMG presented here are adapted and operationalized for the case of the Urban Transport System (UTS) in D3.7. Taking advantage of the following developments of the project, both these Deliverables will be revised towards the end of the project, by including further recommendations that may derive from the RESOLUTE pilot tests (WP5) as well as by incorporating feedback by the experts participating in the RESOLUTE Advisory Stakeholders Board. These adaptations will be reported in D3.6 and D3.8.

5 REFERENCES

Bibliography

AEMC, 2002. National Good Practice Review of Public Awareness, Education and Warnings in Emergency Management - High Level Group of the COAG Review of Natural Disaster Relief and Mitigation Arrangements, Australian Emergency Management Committee ,unpublished draft

AG,2011. Organizational Resilience. Australian Government position paper (2011). ISBN: 978-1-921725-62-3, Available online:< http://www.emergency.qld.gov.au/publications/pdf/organisational_resilience.pdf>

Alexander, David E., 2014. "Social media in disaster risk reduction and crisis management." Science and engineering ethics 20.3 (2014): 717-733.

APCICT , 2010. Communication Technology for Development (APCICT), ICTD Case Study 2, May 2010

Asprone, D., Cavallaro, M., Latora, V., Manfredi, G., Nicosia, V., 2013. “Assessment of urban ecosystem resilience using the efficiency of hybrid social-physical complex networks”, in Computer-aided Civil and Infrastructure Engineering 29, February 2013

Australian Government,2010. Critical Infrastructure Resilience Strategy, Commonwealth of Australia, ISBN: 978-1-921725-25-8

Avvenuti, Marco, et al., 2015. "Pulling information from social media in the aftermath of unpredictable disasters." 2nd international conference on information and communication technologies for disaster management (ICT-DM). 2015.

Baroudi, B., & Rapp, R., 2013. Disaster Restoration Projects: A Conceptual Project Management Perspective. In Australasian Journal of Construction Economics and Building-Conference Series (Vol. **1**, No. 2, 72-79).

Bevan, N., 1995. Human-Computer Interaction Standards. In Anzai & Ogawa (eds.). Proceedings of the 6th International Conference on Human Computer Interaction, Yokohama, July 1995, Elsevier.

Brown, K., 2015. Global environmental change I: a social turn for resilience? Prog. Hum. Geogr. 38, 107–117 (2014)

BS OHSAS 18001 - Occupational Health and Safety Management (OHS), OHSAS 180001 http://www.bsigroup.com/en-GB/ohsas-18001-occupational-health-and-safety/>

BSI, 2014. Guidance on organizational resilience, ISBN 9780580779497

Bush et al, 2005. Critical Infrastructure Protection Decision Support System –Intentional System Dynamics Conference 2005

Caschilli, S., Medda, F.R., Wilson, A., 2015.“An Interdependent Multi-Layer Model: Resilience of International Networks”, Netw Spat Econ (2015), 15, 313-335.

CGI,2013. “Developing a Framework to Improve Critical Infrastructure Cybersecurity”, 2013

CIRS, 2010. CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY, ISBN: 978-1-921725-25-8

Clay-Williams et al.,2015. Where the rubber meets the road: using FRAM to align work-as-imagined with work-as done when implementing clinical Implementation Science (2015) 10:125 DOI 10.1186/s13012-015-0317-y

Council of the European Union, 2008. Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, (2008/114/EC)

Crawford, L., Langston, C., & Bajracharya, B. (2013). Participatory project management for improved disaster resilience. International Journal of Disaster Resilience in the Built Environment, 4(3), 317-333.

CWIN, 2008. Critical Infrastructure Warning Information Network –CWIN http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm

DARWIN Project, 2015. D1.1 Version 0.6: Consolidation of resilience concepts and practices for crisis management.

DHS, 2006. U.S. Department of Homeland Security,National Infrastructure Protection Plan, 2006. Available online at: www.dhs.gov/nipp.

DHS, 2008. NIAC Insider Threats to Critical Infrastructure Study (2008) < https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf>

DMBC, 2010. Recovery Plan. Contingency and disaster management. Dudley Metropolitan Borough Council (2010).

Doran, G. T., 1981. "There's an S.M.A.R.T. way to write management's goals and objectives". Management Review (AMA FORUM) 70 (11): 35–36

Duque, P. A. M., Dolinskaya, I. S., & Sörensen, K., 2016. Network repair crew scheduling and routing for emergency relief distribution problem. European Journal of Operational Research, 248(1), 272-285.

E. Hollnagel, 2013. An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organizational Change. Report number: 2013:09, ISSN 2000-0456

EC, 2012. Action Plan on Urban Mobility – State of Play, European Commission, 2012. < http://ec.europa.eu/transport/themes/urban/urban_mobility/doc/apum_state_of_play.pdf >

EEMUA , 2002. Engineering Equipment & Materials Users Association (EEMUA) Publication 201: 2002 available via EEMUA on 020 7628 7878

EmerGent, 2014. Deliverable 3.1 “usage Patterns of Social Media in emergencies”, EU-FP7-SEC project EmerGent (Emergency Management in Socia Media Generation), available at: http://www.fp7-emergent.eu/wpcontent/uploads/2014/09/D3.1_UsagePatternsOfSocialMediaInEmergencies.pdf

Environmental Impact Assessment Directive, 1985 (85/337/EEC)

Ernst &Young, 2013.ORGANISATIONAL RESILIENCE: The relationship with Risk related corporate strategies, An analysis by Ernst and Young and the Commonwealth Attorney-General’s Department.

EU, 2010. Commission Staff Working Paper 1626-2010. Risk Assessment and Mapping Guidelines for Disaster Management. The European Commission

EU, 2012. Commission staff working document on the review of the European programme for critical infrastructure protection (EPCIP), SWD (2012)190 final

EU, 2013. Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD(2103)318 final

EU, 2006. Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006)786 final

EU, 2008. Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN), COM (2008)676 final

EU, 2014.Handbook on European data protection law. European Union Agency for Fundamental Rights, 2014 Council of Europe, 2014. <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>

EUROCONTROL, 2013. From Safety-I to Safety-II: A White Paper. European Organisation for the Safety of Air Navigation (EUROCONTROL) < http://www.skybrary.aero/bookshelf/books/2437.pdf>

EUROCONTROL, 2014. System Thinking for Safety: Ten Principles – Moving towards Safety –II, August 2014 – European Organisation for the Safety of Air Navigation (EUROCONTROL) < http://www.skybrary.aero/bookshelf/books/2882.pdf>

Fekete, A., Tzavella, K., Armas, I., Binner, J., Garschagen, M., Giupponi, C., Mojtahed, V., Pettita, M., Schneiderbauer, S., Serre, D., 2015. “Critical Data Source; Tool or Even Infrastructure? Challenges of Geographic Information Systems and Remote Sensing for Disaster Risk Governance”, ISPRS Int. J. Geo-Inf. 2015, 4(4), 1848-1869.

FEMA, 2011. National disaster recovery framework: Strengthening disaster recovery for the nation. https://www.fema.gov/pdf/recoveryframework/ndrf.pdf (Mar. 24, 2016)

Ferreira, P., Simoes, A., 2015. State of the art review. RESOLUTE Deliverable 2.1.

FETSM, 1999. Fields of Education and Training Supplementary Manual 1999 (Statistical office of the European Communities-EUROSTAT)

Fiskel J., 2015. “Connecting with Broader Systems”, Resilient by design, (2015), 191-208

FY, 2013. US. HUMAN CAPITAL MANAGEMENT PLAN. Department of Energy. http://energy.gov/sites/prod/files/2013/05/f0/OCIOWorkforcePlan.pdf.

Gaitanidou, E., Bekiaris, E., 2015. Guidelines Methodology. RESOLUTE Deliverable 3.4

Gander, Philippa, et al., 2011. "Fatigue risk management: Organizational factors at the regulatory and industry/company level." Accident Analysis & Prevention 43.2 (2011): 573-590.

Gao, J., Liu, X., Li, D., Havlin, S., “Recent Progress on the Resilience of Complex Networks”, Eergies 2015, 8, 12187-12210.

GFDRR, 2014. Financial Protection Against Natural Disasters, An Operational Framework for Disaster Risk Financing and Insurance, World Bank report, 2014. <https://olc.worldbank.org/sites/default/files/Financial%20Protection%20Against%20Natural%20Disasters.pdf>

Gustin, J., 2007. Safety Management: A guide for facility managers. CRC Press

Hoegl, Martin, and Hans Georg Gemuenden, 2001. "Teamwork quality and the success of innovative projects: A theoretical concept and empirical evidence." Organization science 12.4 (2001): 435-449.

Hollnagel, E. et al, 2013.From Safety-I to Safety-II: A White Paper EUROCONTROL 2013

Hollnagel, E., 1998. Cognitive Reliability and Error Analysis Method – CREAM. Oxford: Elsevier Science.Oedewald, P et al – Intermediate report MoReMo Modelling Resilinece for Mantainance and Outage – NKS-262 – ISBN 979-87-7893-335-5 Feb 2012

Hollnagel, E., 2004. Barriers and accident prevention. Aldershot, UK: Ashgate.

Hollnagel, E., 2009. The four cornerstones of resilience engineering. In: Nemeth, C. P., Hollnagel, E. & Dekker, S. (Eds.), Preparation and restoration (p. 117-134). Aldershot, UK: Ashgate.Ferreira, P., Simoes, A., 2016. Conceptual Framework. RESOLUTE Deliverable 2.2.

Hollnagel, E., 2014. Safety-I and Safety-II: the past and future of safety management. Ashgate

Homeland Security, 2015. National Critical Infrastructure Security and Resilience Research and Development Plan.

HSE, 1997. Successful Health and Safety Management - Health and Safety Executive. Publication HS(G)65 (1997).

Hubbard, D., 2014. How to Measure Anything: Finding the Value of Intangibles in Business. Wiley.

HVHF, 2007. High Velocity Human Factor (HVHF) – Moin Rahman - High Velocity Human Factors: Human Factors of Mission Critical Domains in Nonequilibrium Proceedings of the Human Factors and Ergonomics Society Annual Meeting October 2007 51: 273-277, doi:10.1177/154193120705100427.

ICT for Disaster Risk Reduction - The Indian Experience, Ministry of Home Affairs, National Disaster Management Division Government of India

IETF, 2007. Delay-Tolerant Networking Architecture, IETF, RFC 4838 <https://tools.ietf.org/html/rfc4838>

IFRC, 2011. International Federation of Red Cross and Red Crescent Societies (2011) Public awareness and public education for disaster risk reduction: a guide

Institute of Medicine, 2002. Speaking of Health, Washington D.C., The National Academies Press.

ISDR,2006. Developing Early Warning Systems: A Checklist – International Strategy for Disaster Reduction – ISDR 2006

ISO 22301:2012, Societal security- Business continuity management systems- Requirements < http://www.iso.org/iso/catalogue_detail?csnumber=50038>

ISO 22301:2012. Societal Security - Business Continuity Management Systems - Requirements. Geneva: ISO

ISO 22320:2011, Societal security – Emergency management – Requirements for incident response

ISO 31000: Risk management – Principles and guidelines

Jassbi, J., Camarinha-Matos, L.M., Barata, J., 2015. "A Framework for Evaluation of Resilience of Disaster Rescue Networks", in L.M. Camarinha-Matos et al. (Eds.): PRO-VE 2015, IFIP AICT 463, pp. 146–158, 2015.

Jokeren, O., Azzini, I., Galbusera, L., 2015. "Analysis of Critical Infrastructure Network Failure in the European Union A combined Systes Engineering and Economic Model", Netw Spat cEcon (2015), 15:253-270.

Kangaspunta, J., Salo, A.,2014. "A Resource Allocation Model for Improving the Resilience of Critical Transportation Systems", (2014)

Karen Miranda, 2013. Adaptive self-deployment algorithms for mobile wireless substitution networks. Networking and Internet Architecture [cs.NI]. Université des Sciences et Technologie de Lille - Lille I

Karwowski, W., 2005. Handbook of Standards and Guidelines in Ergonomics and Human Factors. New Jersey: Lawrence Erlbaum Associates, Publishers.

Kasthurirangan, Gopalakrishnan, Srinivas, Peeta, 2010. Sustainable and Resilinect Critical Infrastrucutre System A framework for Manifestation of Tacit Critical Infrastructure Knowledge: Simulation, Modelling and Intelligent Engineering - Springer 2010

Kochs, A., & Marx, A., 2009. Innovatives Instandhaltungsmanagement mit IDMVU, Leitfaden Teil 1 Überblick Gesamtprozess. Forschungsvorhaben Infrastruktur-Daten-Management für Verkehrsunternehmen (IDVMU).

Kyriakides, E., Polycarpou, M.,2015. "Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems", Springer 2015, ISBN 978-3-662-44159-6

Labaka, L., Hernantes, J., Sarriegi J.M.,2016. "A holistic framework for building critical infrastructure resilience", Technological Forecasting & Social Change, 103, (2016), 21-33.

Lazari, A., 2014. "European Critical Infrastructure Protection", Springer Cham Heidelberg New York Dordrecht London, 2014.

Lindell, M. K. (2013). Recovery and reconstruction after disaster. In Encyclopedia of natural hazards (pp. 812-824). Springer Netherlands.

LR O'Neil et.al, 2015. US DOE - SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Behavioural Interview Guidelines by Job Roles < http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24140.pdf>

Macdonald, J, 1998. Primary Health Care, Medicine in its place. London: Earthscan Publications Ltd

Merk, O., 2014, "Metropolitan Governance of Transport and Land Use in Chicago", OECD Regional Development Working Papers, 2014/08, OECD Publishing. http://dx.doi.org/10.1787/5jxzjs6lp65k-en

NATO,2012. RTO Technical Report TR-SAS-059 Human Resources (Manpower) Management < http://natorto.cbw.pl/uploads/2012/2/$$TR-SAS-059-ALL.pdf>

NCHRP, 2013. A Pre-Event Recovery Planning Guide for Transportation, TRB report, WASHINGTON, D.C. 2013<https://www.massport.com/media/266266/Report_A-Pre-Event-Recovery-Planning-Guide-for-Transportation-2013.pdf >

NCIS, 2015. National Critical Infrastructure Security and Resilience Research and Development Plan-NCIS R&D. USA Homeland Security 2015

NIAC, 2009. National Infrastructure Advisory Council (NIAC) Critical Infrastructure Resilience Final Report and Recommendations 2009

NIAC, 2014. Critical Infrastructure Security and Resilience National Research and Development Plan. National Infrastructure Advisory Council (2014)

NIPP, 2013. Homeland Security (2013) NIPP. Partnering for critical infrastructure security and resilience. USA

NIPP, 2013. Partnering for critical infrastructure security and resilience. USA: Homeland Security 2013

NORC, 2013. The Associated Press-NORC Center for Public Affairs Research (2013) Communication during disaster response and recovery.

NRF, 2008. National Response Framework. United States Department of Homeland Security. (2008). <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf >

O'Rourke, T.D., 2007. Critical Infrastructure, Interdependencies, and Resilience. The Bridge, Spring 2007, pp 22-29, National Academy of Engineering

OECD, 2013. Disaster Risk Financing in APEC Economies, Practices and Challenges <https://www.oecd.org/daf/fin/insurance/OECD_APEC_DisasterRiskFinancing.pdf>

OECD, 2014. Guidelines for resilience systems analysis, OECD Publishing

OSHAS 18001:1999. Occupational health and safety management systems. Specifications.

Ouyang, M.,2014. "Review on modelling and simulation of interdependent critical infrastructure systems", Reliability Engineering and System Safety, 121, (2014), 43-60.

PAHO, 2009. Information management and communication in emergencies and disasters: manual for disaster response teams. Pan American Health Organization (2009).Washington, D.C.

Peter O'Neill, 2004. Developing A Risk Communication Model to Encourage Community Safety from Natural Hazards –State Emergency Service, JUNE 2004

Pollack, L.J., Simons, C., Romero, H. and Hausser, D., 2002. "A Common Language for Classifying and Describing Occupations: The Development, Structure, and Application of the Standard Occupational Classification", Human Resource Management, Vol. 41, No. 3, pp. 297-307, Fall 2002.

Queensland Government, 2013. Queensland 2013 Flood Recovery Plan for the events of January– February 2013. <http://www.statedevelopment.qld.gov.au/resources/plan/local-government/lg-flood-recovery-plan.pdf>

Ramachandran, V., Long, S., Shoberg, T., Corns, S., & Carlo, H., 2016. Post-disaster supply chain interdependent critical infrastructure system restoration: A review of data necessary and available for modelling. Data Science Journal, 15.

RESOLUTE, 2015.D2.1 State of the Art Review (2015) RESOLUTE project

Richard A. Caralli, Julia H. Allen, David W. White., 2011. "The CERT resilience management model : a maturity model for managing operational resilience", ISBN 978-0-321-71243-1, Pearson Education, 2011

SEI, 2010. Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework Linda Parker Gates November 2010, TECHNICAL REPORT CMU/SEI-2010-TR-037 ESC-TR-2010-102

SEI, 2010. Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework Linda Parker Gates November 2010, TECHNICAL REPORT CMU/SEI-2010-TR-037 ESC-TR-2010-102

Shah, J., 2009. Supply chain management: text and cases. Pearson Education India.

Simon, H.A.,1979. Rational decision Making in business organization. American Economic Review 69 (4), 493-513 (1979)

Sodhi, M., Tang, C., 2012. Managing Supply Chain Risk. Springer

Staal, Mark A., 2004. Stress, Cognition, and Human Performance: A Literature Review and Conceptual Framework. NASA/TM—2004–212824. Ames Research Centre Moffett Field, California 94035. Website: http://human-factors.arc.nasa.gov/flightcognition/Publications/IH_054_Staal.pdf

Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D, 2016. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures, International Journal of Critical Infrastructure Protection, Volume 12, March 2016, Pages 46-60,

Trucco, P., Petrenj, B., Bouchon, S., Di Mauro, C., 2015. "The rise of regional programmes on critical infrastructure resilience: identification and assessment of current good practices", Disaster Management and Human Health Risk IV, WIT Transactions on the Built Environment, 150, (2015), 233-245.

UNISDR & GFDRR, 2015. How to make cities more resilient. A handbook for local government leaders.

Van Brabant, K.,2015. "Mainstreaming the Organisational Management of Safety and Security", HPG Report 9,March 2001

Vos, M., & Sullivan, H.,2014. “Community Resilience in Crises: Technology and Social Media Enablers”, Human Technology, 10 (2), (2014), 61-67.

Welsh, M.,2014. “Resilience and responsibility: governing uncertainty in a complex world”, The Geographical Journal, 180, (2014), 15-26.

White, K.J.S., Pezaros, D.P., Johnson, C.W.,2014. “Using Programmable Data Networks to Detect Critical Infrastructure Challenges”, In: 9th International Conference on Critical Information Infrastructures Security (CRITIS'14), 13-15 Oct 2014, Limassol, Cyprus.

WHO, 2012. Integrated Risk Assessment. World Health Organazization <http://www.who.int/ipcs/publications/new_issues/ira/en/>

Xu, T., Masys, A.J., 2016. “Critical Infrastructure Vulnerabilities: Embracing a Network Mindset”, A.J. Masys (ed.) Exploring the Security Landscape: Non-Traditional Security Challenges, Advanced Sciences and Technologies for Security Applications (2016).

Yondong, Z., 2013. Social networks and reduction of risk in disasters: an example of Wenchuan earthquake. In: Yeung, W.J.J., Yap, M.T. (eds.) Economic Stress, Human Capital, and Families in Asia, vol. 4, pp. 171–182. Springer, Berlin (2013)

Websites

- http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html
- http://dominoweb.comune.fi.it/OdeProduzione/FIODEWeb1.nsf/AttiWEB/87E222B64C78BA2CC125795A0032F4C8/$File/2011_G_00444.pdf
- http://dominoweb.comune.fi.it/OdeProduzione/FIODEWeb2.nsf/AttiWEB/49E27A9AE74726B0C1257E0100025CDF/$File/2015_C_00008.pdfRESOLUTE_ERMG_v3.docx
- http://dominoweb.comune.fi.it/OdeProduzione/FIODEWeb2.nsf/AttiWEB/F6D8CF80EB3EF0E7C1257E6800805F19/$File/2015_C_00030.pdf
- http://ec.europa.eu/justice/data-protection/
- http://ec.europa.eu/transport/themes/urban/studies/doc/2007_urban_transport_europe.pdf
- http://emergency.cdc.gov/planning/
- http://essentialsofbusiness.ufexec.ufl.edu/resources/human-resources/essential-skills-for-the-human-resource-manager/#.VvADa3BycQQ
- http://firenzesmartcity.org/
- http://floridadisaster.org/documents/CEMP/Emergency%20Operations%20Plan.pdf
- http://hrdailyadvisor.blr.com/2012/06/07/emergency-management-preparedness-what-is-hr-s-role/#sthash.kngr3C7W.dpuf
- http://idrn.gov.in/default.asp
- http://managementhelp.org/strategicplanning/models.htm#one
- http://managementhelp.org/strategicplanning/models.htm#one
- http://nctr.pmel.noaa.gov/
- http://opendata.comune.fi.it
- http://protezionecivile.comune.fi.it
- http://protezionecivile.comune.fi.it/wp-content/uploads/2011/09/Il-Sistema-Comunale.swf
- http://sydney.edu.au/whs/emergency/emergency2.shtml
- http://www.100resilientcities.org
- http://www.abs.gov.au/ausstats/abs@.nsf/0/7624A042D303B867CA2575DF002DA6CB?opendocument
- http://www.dsdip.qld.gov.au/resources/plan/local-government/lg-flood-recovery-plan.pdf
- http://www.ericsson.com/news/140908-capillary-networks_244099436_c
- http://www.fao.org/docrep/w7295e/w7295e04.htm

- http://www.fcagroup.com/en-US/sustainability/FiatDocuments/LG_HumanCapitalManagement.pdf
- http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf
- http://www.forbes.com/sites/jacobmorgan/2016/03/03/deloittes-top-10-human-capital-trends-for-2016/#7da81071bf48
- http://www.gao.gov/assets/250/240817.html
- http://www.hse.gov.uk/contact/faqs/workingtimedirective.htm
- http://www.ictc-ctic.ca/wp-content/uploads/2012/10/ICTCCyberSecurityReport1.pdf
- http://www.ilo.org/global/standards/subjects-covered-by-international-labour-standards/working-time/lang--en/index.htm
- http://www.iso.org/iso/cataloguedetail.htm?csnumber=63500
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=69338
- http://www.iso.org/iso/standards_development/technical_committees/other_bodies/iso_technical_committee.htm?commid=628737
- http://www.nec.com/en/global/solutions/safety/critical_infra/index.html
- http://www.odpm.gov.tt/sites/default/files/NEMA%20Disaster%20SOPs%20and%20Contingency%20Plans%202000.pdf
- http://www.rae.gr/old/SUB2/2_3.htm#%CE%A5.%CE%91.6296/01
- http://www.sadc.int/themes/infrastructure/transport/roads-road-transport/
- http://www.scottishfloodforum.org/wp-content/uploads/2013/03/Business-Plan-2015-18-web.pdf
- http://www.swri.org/4org/d10/isd/surveil/
- http://www.ucl.ac.uk/hr/occ_health/health_advice/managing_pressure
- https://en.wikipedia.org
- https://epic.org/privacy/ecpa/
- https://erncip-project.jrc.ec.europa.eu
- https://standards.ieee.org/findstds/standard/C37.1-2007.html
- https://tools.skillsforhealth.org.uk/competence/show/html/id/2130/
- https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf
- https://www.eydap.gr/userfiles/c3c4382d-a658-4d79-b9e2-ecff7ddd9b76/kanonismos-diktuou-apoxeteusis.pdf
- https://www.fas.org/sgp/crs/homesecRL32520.pdf
- https://www.fema.gov/pdf/recoveryframework/ndrf.pdf
- https://www.gatwickairport.com/globalassets/publicationfiles/business_and_community/regulation/economic_regulation/14-10-01-operational-resilience-report-and-monitoring-report-final-for-publication.pdf
- https://www.ready.gov/financial-preparedness
- https://www.ubalert.com/U4gc
- https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- https://www.zurich-airport.com/business-and-partners/safety-and-security/safety-principles

6 ANNEX I: FUNCTIONS DESCRIPTION TEMPLATES

6.1 Core functions

6.1.1 Deliver service

<table>
<tr><td colspan="2"><b>#Function2</b></td></tr>
<tr><td><b>Name</b></td><td>Deliver service</td></tr>
<tr><td><b>Description</b></td><td>This function represents the actual delivery of the service of the critical infrastructure. It represents the act to provide a service to the customers/users. In the context of critical infrastructure such services are: energy, water, transport, financial, etc.</td></tr>
<tr><td><b>Input</b></td><td>
<table>
<tr><th>lemma</th><th>SOURCE funtion</th><th>relation</th></tr>
<tr><td>Service delivery plan</td><td>Coordinate Service delivery</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td><b>Output</b></td><td>
<table>
<tr><th>lemma</th><th>DESTINATION funtion</th><th>relation</th></tr>
<tr><td>Service</td><td>Use o the service</td><td>is_resource</td></tr>
<tr><td>Service_performance</td><td>Monitor operations</td><td>is_input</td></tr>
<tr><td>Service_Safety_security_performance</td><td>Monitor_Safety and security</td><td>is_input</td></tr>
<tr><td>Infrastructure performance</td><td>Monitor_user_generated_Feedback</td><td>Is_input</td></tr>
</table>
</td></tr>
<tr><td><b>Resources</b></td><td>
<table>
<tr><th>lemma</th><th>SOURCE funtion</th><th>relation</th></tr>
<tr><td>Human resource availability</td><td>Manage Human resources</td><td>is_output</td></tr>
<tr><td>Staff trained</td><td>Train staff</td><td>Is_output</td></tr>
<tr><td>Supply resources</td><td>Supply resorces</td><td>Is_output</td></tr>
<tr><td>Emergency response status</td><td>Coordinate emergency action</td><td>Is_output</td></tr>
</table>
</td></tr>
<tr><td><b>Preconditions</b></td><td>
<table>
<tr><th>lemma</th><th>upstream funtion</th><th>relation</th></tr>
<tr><td>Operation restored/repaired</td><td>Restore/Repair operations</td><td>Is_output</td></tr>
<tr><td>Infrastructure installed maintained</td><td>Maintain physical/cyber infrastructure</td><td>Is_output</td></tr>
<tr><td>ICT infrastructures</td><td>Manage ICT resource</td><td>Is_output</td></tr>
<tr><td>Infrastructure restored/repaired</td><td>Restore/repair physical infrastructure</td><td>Is_output</td></tr>
</table>
</td></tr>
<tr><td><b>Control</b></td><td>
<table>
<tr><th>lemma</th><th>upstream funtion</th><th>relation</th></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Safety Security control</td><td>Monitor Safety and Security</td><td>Is_output</td></tr>
<tr><td>Standards</td><td>Regulate domain and operation</td><td>Is_output</td></tr>
<tr><td>Law</td><td>Regulate domain and operation</td><td>Is_output</td></tr>
<tr><td>Procedure</td><td>Define procedures</td><td>Is_output</td></tr>
</table>
</td></tr>
</table>

6.1.2 Use of the service

<table>
<tr><td>Name</td><td>Use of the service</td></tr>
<tr><td>Description</td><td>This function represents the actual usage of the services. The usage includes user behaviors, attitude, expectation, sentiment, etc.
The service usage is something that is consumed in a specific place, time intensity, awareness, etc. according to the user needs and goals.</td></tr>
<tr><td>Input</td><td></td></tr>
<tr><td>Output</td><td>
<table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>User behaviour</td><td>FF_24_Monitor user generated feedback</td><td>is_input</td></tr>
<tr><td>User feedback</td><td>FF_24_Monitor user generated feedback</td><td>is_input</td></tr>
<tr><td>Revenues</td><td>FF_04_Manage financial affair</td><td>is_resource</td></tr>
</table>
</td></tr>
<tr><td>Resources</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Service delivery plan</td><td>FF_07_Coordinate Service delivery</td><td>is_output</td></tr>
<tr><td>Service status</td><td>FF_15_Manage awareness & usage behaviou</td><td>is_output</td></tr>
<tr><td>Early warnings</td><td>FF_15_Manage awareness & usage behaviou</td><td>is_output</td></tr>
<tr><td>Early warnings</td><td>FF_15_Manage awareness & usage behaviou</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td>Preconditions</td><td></td></tr>
<tr><td>Control</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Safety Security control</td><td>FF_03_Monitor Safety and Security</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td>Time</td><td></td></tr>
</table>

6.2 Anticipate

6.2.1 Develop Strategic Plan

<table>
<tr><td>Name</td><td>Develop Strategic Plan</td></tr>
<tr><td>Description</td><td>What is a Strategic Plan
-Aim- vision
-Long term objectives and identify critical resource needs and allocation

-Who develops it – to whom it addresses

- decomposition of the CI it affects

- framework-priorities-resources – budget –action/timeplan

-</td></tr>
<tr><td>Input</td><td><table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>System Sustained adaptability insights</td><td>Provide adaptation &amp; improvement insight</td><td>is_output</td></tr>
</table>
Note: <i>Shareholders (new income, market extension, protect from finances loss etc.), Market/socioeconomic trends (user needs, new products/services, economic situations), SoA in technical terms, Public opinion</i></td></tr>
<tr><td>Output</td><td><table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Strategic plan</td><td>Collect event information</td><td>is_control</td></tr>
<tr><td>Strategic plan</td><td>Manage financial affair</td><td>is_input</td></tr>
<tr><td>Strategic plan</td><td>Provide adaptation &amp; improvement insight</td><td>is_input</td></tr>
<tr><td>Strategic plan</td><td>Maintain physical/cyber infrastructure</td><td>is_input</td></tr>
<tr><td>Strategic plan</td><td>Manage awareness &amp; usage behaviou</td><td>is_input</td></tr>
<tr><td>Strategic plan</td><td>Coordinate Service delivery</td><td>is_resource</td></tr>
</table></td></tr>
<tr><td>Resources</td><td>-<table>
<tr><th>relation</th><th>SOURCE Function</th></tr>
<tr><td>is_output</td><td>Manage financial affair</td></tr>
<tr><td>is_resource</td><td>Coordinate Service delivery</td></tr>
</table>
Note: <i>Humans (labour) – skills/competence, Technical equipment (capital), Budget , Data, Algorithms</i></td></tr>
<tr><td>Preconditions</td><td></td></tr>
</table>

Control

relation	SOURCE Function
is_control	Coordinate Service delivery
is_control	Restore/Repair operations
is_control	Monitor Operation
is_output	Regulate domain and operation

Time

Note: Depends on time constraints of depended functions, Depends on the controls and the nature of the CI, Depends on other local conditions, Is defined at the starting phase of the function, It is defined by corporate standards

6.2.2 Manage financial affairs

Name	Manage financial affairs
Description	Develop financial control and plan financial assets in accordance to financial needs of the operation and financial obligations

Input

lemma	SOURCE Function	relation
Strategic plan	Develop Strategic Plan	is_output

Note: Strategic_plan, Current cash flow & predictions, Investment plans
Operational (financial) requirement

Output

lemma	Destination Function	relation
SLA(Service Level Agreement)	Coordinate Service delivery	is_control
SLA(Service Level Agreement)	Coordinate emergency actions	is_control
Budget	Develop Strategic Plan	is_resource
Budget	Coordinate Service delivery	is_resource
SLA(Service Level Agreement)	Monitor Resource availability	is_resource

Resources

lemma	SOURCE Function	relation
Revenues	Use of the service	is_output
Funds	Supply financial resources	is_output

Preconditions

<table>
<tr><td>Control</td><td><table><tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr><tr><td>Law</td><td>Regulate domain and operation</td><td>is_output</td></tr></table>Note: <i>Risk assessment, Government/Fiscal services, Laws, External auditors</i></td></tr>
<tr><td>Time</td><td>Note: <i>Ongoing function, Periodic controls, Annual fiscal obligations</i></td></tr>
</table>

6.2.3 Perform Risk Assessment

<table>
<tr><td>Name</td><td>Perform Risk Assessment</td></tr>
<tr><td>Description</td><td>Assess feasibility of financial plans and compliance with legal and operational obligations, assess operational risk
+ Risk assessment guidelines definition by EU doc</td></tr>
<tr><td>Input</td><td>Note: <i>Event_analysis_insights, Event occurrence, Political decision, Update of safety regulations (driven by new scientific findings), EU/International regulations</i></td></tr>
<tr><td>Output</td><td><table><tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr><tr><td>Risk assessment report</td><td>Monitor Safety and Security</td><td>is_input</td></tr><tr><td>Risk assessment report</td><td>Train Staff</td><td>is_input</td></tr><tr><td>Risk assessment report</td><td>Define procedures</td><td>is_input</td></tr><tr><td>Risk assessment report</td><td>Coordinate Service delivery</td><td>is_resource</td></tr></table></td></tr>
<tr><td>Resources</td><td><table><tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr><tr><td>Safety regulation</td><td>Regulate domain and operation</td><td>is_output</td></tr></table>Note: <i>Big data, Social data, Historical data, Sensor networks &amp; data, Technologies for acquiring necessary data, Algorithms &amp; processing units for risk calculation</i></td></tr>
<tr><td>Preconditions</td><td></td></tr>
</table>

Control	
Time	

6.2.4 Train Staff

<table>
<tr><td>Name</td><td>Train Staff</td></tr>
<tr><td>Description</td><td>Train the employees as planned, including quality control of the training</td></tr>
<tr><td>Input</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Risk assessment report</td><td>Perform Risk Assessment</td><td>is_output</td></tr>
<tr><td>Training staff requirements</td><td>Coordinate Service delivery</td><td>is_output</td></tr>
<tr><td>Safety regulation</td><td>Regulate domain and operation</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td>Output</td><td>
<table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Training performance data</td><td>Collect event information</td><td>is_input</td></tr>
<tr><td>Staff trained</td><td>Coordinate emergency actions</td><td>is_precondition</td></tr>
<tr><td>Staff trained</td><td>Monitor Operation</td><td>is_precondition</td></tr>
<tr><td>Staff trained</td><td>Monitor Operation</td><td>is_resource</td></tr>
</table>
</td></tr>
<tr><td>Resources</td><td>Note: <i>Training performance data, Human resources availability (PM availability – trainer&trainee), Training tools/material/curriculum</i></td></tr>
<tr><td>Preconditions</td><td></td></tr>
<tr><td>Control</td><td>Note: <i>Existing training certification schemes</i></td></tr>
<tr><td>Time</td><td>Note: <i>Periodic training</i></td></tr>
</table>

6.2.5 Coordinate Service delivery

Name	Coordinate Service delivery
Description	Supervision of the entire service delivery, provides service plan, trigger the emergency alert,

coordinate operational procedures

Input

lemma	SOURCE Function	relation
Operation restored/repaired	Restore/Repair operations	is_output
Operation requirements	Monitor Operation	is_output
Install Mantainance requirement	Monitor Operation	is_output
Service sustained adaptability improvement insights	Provide adaptation & improvement insight	is_output
Resource supplied Critical event detection	Monitor Resource availability	is_output
Energy supply report	Monitor Resource availability	is_output
Infrastructure restored/repaired	Restore/repair physical infrastructure	is_output
User generated critical event detection	Monitor user generated feedback	is_output
Official risk warning	Provide risk warning	is_output

Output

lemma	Destination Function	relation
Operation plan	Manage awareness & usage behaviou	is_control
Operation HR plan	Human resources	is_function
Training staff requirements	Train Staff	is_input
Operation Restore service request	Restore/Repair operations	is_input
Operation HR plan	Manage Human resources	is_input
Service improvement plan	Maintain physical/cyber infrastructure	is_input
Operation plan	Manage awareness & usage behaviou	is_input
Operation plan	Define procedures	is_input
Operation plan	Manage ICT resource	is_input
Infrastructure restore request	Restore/repair physical infrastructure	is_input
Service delivery plan	Use of the service	is_resource
Service delivery plan	Manage awareness & usage behaviour	is_resource
Operation plan	Monitor Resource availability	is_resource
Restore timing plan	Restore/Repair operations	is_time
Restore infrastructure timing plan	Restore/repair physical infrastructure	is_time

Resources

lemma	SOURCE Function	relation
Strategic plan	Develop Strategic Plan	is_output
Budget	Manage financial affair	is_output
Risk assessment report	Perform Risk Assessment	is_output
Emergency response status	Coordinate emergency actions	is_output
Emergency response plan	Coordinate emergency actions	is_output
Operation restore/repair status	Restore/Repair operations	is_output
Operation Restore service plan	Restore/Repair operations	is_output
Supply status	Supply Resources	is_output
ICT infrastructures	Manage ICT resource	is_output
Infrastructure restored/repaired	Restore/repair physical infrastructure	is_output
Infrastructure restored repaired status	Restore/repair physical infrastructure	is_output
Infrastructure resotore/repair plan	Restore/repair physical infrastructure	is_output

Preconditions

Note: *Responsibility Matrix*

Control

lemma	SOURCE Function	relation
Law	Monitor Operation	is_control
SLA(Service Level Agreement)	Manage financial affair	is_output
Standards	Regulate domain and operation	is_output
Law	Regulate domain and operation	is_output

Time

6.2.6 Manage awareness & user behaviour

Name

Manage awareness & user behaviour

Description

Signalling, awareness, stakeholder communication, training, etc.

Input

lemma	SOURCE Function	relation
Strategic plan	Develop Strategic Plan	is_output
Operation plan	Coordinate Service delivery	is_output
Emergency response status	Coordinate emergency actions	is_output

<table>
<tr><td></td><td><table>
<tr><td>Operation Restore service plan</td><td>Restore/Repair operations</td><td>is_output</td></tr>
<tr><td>Operation restore/repair status</td><td>Restore/Repair operations</td><td>is_output</td></tr>
<tr><td>Operation Critical event detection</td><td>Monitor Operation</td><td>is_output</td></tr>
</table></td></tr>
<tr><td>Output</td><td><table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Early warnings</td><td>Use of the service</td><td>is_resource</td></tr>
<tr><td>Service status</td><td>Use of the service</td><td>is_resource</td></tr>
<tr><td>Early warnings</td><td>Use of the service</td><td>is_resource</td></tr>
</table>
Note: <i>Campaigns, Training schemes, Emergency communication schemes</i></td></tr>
<tr><td>Resources</td><td><table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Service delivery plan</td><td>Coordinate Service delivery</td><td>is_output</td></tr>
<tr><td>Operation performance monitoring data</td><td>Monitor Operation</td><td>is_output</td></tr>
<tr><td>ICT infrastructures</td><td>Manage ICT resource</td><td>is_output</td></tr>
<tr><td>User behaviour data</td><td>Monitor user generated feedback</td><td>is_output</td></tr>
</table></td></tr>
<tr><td>Preconditions</td><td></td></tr>
<tr><td>Control</td><td><table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Operation plan</td><td>Coordinate Service delivery</td><td>is_output</td></tr>
</table></td></tr>
<tr><td>Time</td><td>Note: <i>Continuously</i></td></tr>
</table>

6.2.7 Develop/update procedures

Name	Develop/update procedures
MTO Category	Human(M) - Technology (T)- Organization (O)
Description	Upgrade/produce operational procedures according to risk assessment and ex-post event analysis (learning) in a way to also provide re-usable data and be re-applicable

<table>
<tr><td>Input</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Risk assessment report</td><td>Perform Risk Assessment</td><td>is_output</td></tr>
<tr><td>Operation plan</td><td>Coordinate Service delivery</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td>Output</td><td></td></tr>
<tr><td>Resources</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Safety regulation</td><td>Regulate domain and operation</td><td>is_output</td></tr>
</table>
Note: <i>Legislation, Monitor operations , Safety models, Procedure models, Procedure certification</i>
</td></tr>
<tr><td>Preconditions</td><td></td></tr>
<tr><td>Control</td><td>Note: <i>Procedure certification, Legislation</i></td></tr>
<tr><td>Time</td><td>Note: <i>Event driven, Legislation driven, Criticality driven</i></td></tr>
</table>

6.2.8 Manage human resources

<table>
<tr><td>Name</td><td>Manage human resources</td></tr>
<tr><td>Description</td><td>Hire employees, manage turns, burnout and substitutions, assign tasks, manage organization knowledge

Assignment of human capacities to the system operation</td></tr>
<tr><td>Input</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Operation HR plan</td><td>Coordinate Service delivery</td><td>is_output</td></tr>
<tr><td>Emergency HR request</td><td>Coordinate emergency actions</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td>Output</td><td>
<table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Human resources availability</td><td>Coordinate emergency actions</td><td>is_resource</td></tr>
<tr><td>Human resources availability</td><td>Restore/Repair operations</td><td>is_resource</td></tr>
<tr><td>Human resources availability</td><td>Restore/repair physical infrastructure</td><td>is_resource</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>Human resources availability</td><td>Human resources</td><td>is_specific</td></tr></table></td></tr>
<tr><td>Resources</td><td><table><tr><th>lemma</th><th>SHARED functions</th><th>relation</th></tr><tr><td>International Standard Classification of Occupations – Isco08</td><td>Occupate for occupational classification</td><td>has_specific</td></tr></table></td></tr>
<tr><td>Preconditions</td><td>Note: <i>Job characteristics and description well defined (HR plan)</i></td></tr>
<tr><td>Control</td><td></td></tr>
<tr><td>Time</td><td></td></tr>
</table>

6.2.9 Manage ICT resources

<table>
<tr><td>Name</td><td>Manage ICT resources</td></tr>
<tr><td>Description</td><td>Provide/maintain/update/develop/repair information and communications services to support critical infrastructure operation and management</td></tr>
<tr><td>Input</td><td><table><tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr><tr><td>Operation plan</td><td>Coordinate Service delivery</td><td>is_output</td></tr></table>Note: <i>Monitor Safety/Security, Monitor operation</i></td></tr>
<tr><td>Output</td><td><table><tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>ICT resource performance</td><td>Monitor Resource availability</td><td>is_input</td></tr>
<tr><td>ICT infrastructures</td><td>Monitor Safety and Security</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Coordinate Service delivery</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Coordinate emergency actions</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Monitor Operation</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Manage awareness &amp; usage behaviou</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Monitor Resource availability</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Monitor user generated feedback</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Collect event information</td><td>is_resource</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td></td></tr>
<tr><td>Resources</td><td><table><tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr><tr><td>Supply resources</td><td>Supply Resources</td><td>is_output</td></tr></table></td></tr>
<tr><td>Preconditions</td><td>Note: <i>ICT installed maintained, Legacy constraints, International standards</i></td></tr>
<tr><td>Control</td><td><table><tr><th>lemma</th><th>SHARED functions</th><th>relation</th></tr><tr><td>Legislation</td><td>Define procedures</td><td>is_control</td></tr><tr><td>Procedures</td><td>Coordinate emergency actions</td><td>is_precondition</td></tr><tr><td>Procedures</td><td>Monitor Operation</td><td>is_precondition</td></tr></table>Note: <i>International standards compliance, Cyber security regulations</i></td></tr>
<tr><td>Time</td><td>Note: <i>Continuous</i></td></tr>
</table>

6.2.10 Maintain physical/cyber infrastructure

<table>
<tr><td>Name</td><td>Maintain physical/cyber infrastructure</td></tr>
<tr><td>Description</td><td>To keep in good shape and operation and up to date construction, ICT and other infrastructure elements</td></tr>
<tr><td>Input</td><td><table><tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr><tr><td>Strategic plan</td><td>Develop Strategic Plan</td><td>is_output</td></tr><tr><td>Service improvement plan</td><td>Coordinate Service delivery</td><td>is_output</td></tr><tr><td>Install Maintenance requirement</td><td>Monitor Operation</td><td>is_output</td></tr></table></td></tr>
<tr><td>Output</td><td>Note: <i>Infrastructure installed maintained, ICT installed maintained, ICT updated</i></td></tr>
<tr><td>Resources</td><td>Note: <i>operations status , ICT status</i></td></tr>
<tr><td>Preconditions</td><td>Note: <i>Contracts for performing maintenance</i></td></tr>
<tr><td>Control</td><td>Note: <i>Service level of operation</i></td></tr>
</table>

Time	Note: *Periodical, Event driven*

6.3 MONITOR

6.3.1 Monitor Safety and Security

<table>
<tr><td>Name</td><td>Monitor Safety and Security</td></tr>
<tr><td>Description</td><td>Monitor safety and security issues of the operations and service delivery</td></tr>
<tr><td>Input</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Risk assessment report</td><td>Perform Risk Assessment</td><td>is_output</td></tr>
<tr><td>Emergency response plan</td><td>Coordinate emergency actions</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td>Output</td><td>
<table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Safety Security control</td><td>Monitor Operation</td><td>is_control</td></tr>
<tr><td>Safety Security control</td><td>Use of the service</td><td>is_control</td></tr>
<tr><td>Safety security critical event detection</td><td>Coordinate emergency actions</td><td>is_input</td></tr>
<tr><td>Safety Security performance data</td><td>Collect event information</td><td>is_input</td></tr>
<tr><td>Emergency respond timing</td><td>Coordinate emergency actions</td><td>is_time</td></tr>
</table>
</td></tr>
<tr><td>Resources</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Emergency response data</td><td>Coordinate emergency actions</td><td>is_output</td></tr>
<tr><td>Emergency response status</td><td>Coordinate emergency actions</td><td>is_output</td></tr>
<tr><td>ICT infrastructures</td><td>Manage ICT resource</td><td>is_output</td></tr>
<tr><th>lemma</th><th>SHARED functions</th><th>relation</th></tr>
<tr><td>Emergency response status</td><td>Manage awareness &amp; usage behaviour</td><td>is_input</td></tr>
<tr><td>Emergency response data</td><td>Collect event information</td><td>is_input</td></tr>
<tr><td>ICT infrastructures</td><td>Coordinate Service delivery</td><td>is_resource</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Emergency response status</td><td>Coordinate Service delivery</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Coordinate emergency actions</td><td>is_resource</td></tr>
<tr><td>Emergency response status</td><td>Monitor Operation</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Monitor Operation</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Manage awareness & usage behaviou</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Monitor Resource availability</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Monitor user generated feedback</td><td>is_resource</td></tr>
<tr><td>ICT infrastructures</td><td>Collect event information</td><td>is_resource</td></tr>
</table>
</td></tr>
<tr><td>Preconditions</td><td></td></tr>
<tr><td>Control</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Safety regulation</td><td>Regulate domain and operation</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td>Time</td><td>Note: <i>In tactical intervals, After any abnormality, After any new addition/change in the system (change control process)</i></td></tr>
</table>

6.3.2 Monitor Operations

<table>
<tr><td>Name</td><td>Monitor Operations</td></tr>
<tr><td>Description</td><td>Monitor employees and service performance</td></tr>
<tr><td>Input</td><td>Note: <i>Service_performance, Coordinate emergency</i></td></tr>
<tr><td>Output</td><td>
<table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Operation requirements</td><td>Coordinate Service delivery</td><td>is_input</td></tr>
<tr><td>Install Mantainance requirement</td><td>Coordinate Service delivery</td><td>is_input</td></tr>
<tr><td>Operation Critical event detection</td><td>Coordinate emergency actions</td><td>is_input</td></tr>
<tr><td>Install Mantainance requirement</td><td>Maintain physical/cyber infrastructure</td><td>is_input</td></tr>
<tr><td>Operation Critical event detection</td><td>Manage awareness & usage behaviou</td><td>is_input</td></tr>
<tr><td>Operation performance monitoring data</td><td>Collect event information</td><td>is_input</td></tr>
<tr><td>Operation performance monitoring data</td><td>Manage awareness & usage behaviou</td><td>is_resource</td></tr>
</table>
</td></tr>
</table>

Resources

lemma	SOURCE Function	relation
Staff trained	Train Staff	is_output
Emergency response status	Coordinate emergency actions	is_output
ICT infrastructures	Manage ICT resource	is_output

Note: *Monitoring method (what to measure/how to measure etc.)*

Preconditions

lemma	SOURCE Function	relation
Staff trained	Train Staff	is_output
Operation restored/repaired	Restore/Repair operations	is_output

Control

lemma	SOURCE Function	relation
Safety Security control	Monitor Safety and Security	is_output
Standards	Regulate domain and operation	is_output
Law	Regulate domain and operation	is_output

Time

Note: *Rate & focus of monitoring differs in normal operation and emergency*

6.3.3 Monitor Resource availability

Name

Monitor Resource availability

Description

Keep record of the level of supply in resources that are basic for the system operation

Input

lemma	SOURCE Function	relation
ICT resource performance	Manage ICT resource	is_output

Note: *Supply delivery performance, Stock inventory status, Raw material supply status*

Output

lemma	Destination Function	Relation
Energy supply report	Coordinate Service delivery	is_input
Resource supplied Critical event detection	Coordinate Service delivery	is_input
Resource supplied Critical event detection	Coordinate emergency actions	is_input

Resources

lemma	SOURCE Function	relation

<table>
<tr><td></td><td><table>
<tr><td>SLA(Service Level Agreement)</td><td>Manage financial affair</td><td>is_output</td></tr>
<tr><td>Operation plan</td><td>Coordinate Service delivery</td><td>is_output</td></tr>
<tr><td>ICT infrastructures</td><td>Manage ICT resource</td><td>is_output</td></tr>
</table>
Note: <i>Buffer capacity</i></td></tr>
<tr><td>Preconditions</td><td>Note: <i>Supply channels, Time constraints</i></td></tr>
<tr><td>Control</td><td>Note: <i>Engineering standards &amp; technical specifications, Health regulations, Contracts, Quality of service</i></td></tr>
<tr><td>Time</td><td>Note: <i>Continuous, Event driven</i></td></tr>
</table>

6.3.4 Monitor user generated feedback

<table>
<tr><td>Name</td><td>Monitor user generated feedback</td></tr>
<tr><td>Description</td><td>User behaviour, perception, feedback</td></tr>
<tr><td>Input</td><td><table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>User behaviour</td><td>Use of the service</td><td>is_output</td></tr>
<tr><td>User feedback</td><td>Use of the service</td><td>is_output</td></tr>
</table>
Note: <i>Crowd sourcing, Social media</i></td></tr>
<tr><td>Output</td><td><table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>User generated critical event detection</td><td>Coordinate Service delivery</td><td>is_input</td></tr>
<tr><td>User generated critical event detection</td><td>Coordinate emergency actions</td><td>is_input</td></tr>
<tr><td>User generated service improvement suggestions</td><td>Collect event information</td><td>is_input</td></tr>
<tr><td>User behaviour data</td><td>Manage awareness &amp; usage behaviour</td><td>is_resource</td></tr>
</table></td></tr>
<tr><td>Resources</td><td><table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>ICT infrastructures</td><td>FF_19_Manage ICT resource</td><td>is_output</td></tr>
</table></td></tr>
</table>

	Note: *Network sensors*
Preconditions	
Control	Note: *Privacy & other ethics legislation, Open data requirements/regulations, Security requirements and legislation*
Time	Note: *Continuous*

6.4 RESPOND

6.4.1 Coordinate emergency actions

<table>
<tr><td>Name</td><td>Coordinate emergency actions</td></tr>
<tr><td>Description</td><td>Steering the system during an emergency</td></tr>
<tr><td>Input</td><td>
<table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Safety security critical event detection</td><td>Monitor Safety and Security</td><td>is_output</td></tr>
<tr><td>Operation Critical event detection</td><td>Monitor Operation</td><td>is_output</td></tr>
<tr><td>Resource supplied Critical event detection</td><td>Monitor Resource availability</td><td>is_output</td></tr>
<tr><td>User generated critical event detection</td><td>Monitor user generated feedback</td><td>is_output</td></tr>
</table>
</td></tr>
<tr><td>Output</td><td>
<table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Emergency response plan</td><td>Monitor Safety and Security</td><td>is_input</td></tr>
<tr><td>Emergency HR request</td><td>Manage Human resources</td><td>is_input</td></tr>
<tr><td>Emergency response status</td><td>Manage awareness & usage behaviour</td><td>is_input</td></tr>
<tr><td>Emergency response</td><td>Collect event information</td><td>is_input</td></tr>
</table>
</td></tr>
</table>

data		
Emergency response command	Fight the emergency	is_input
Emergency response status	Monitor Safety and Security	is_resource
Emergency response data	Monitor Safety and Security	is_resource
Emergency response status	Coordinate Service delivery	is_resource
Emergency response plan	Coordinate Service delivery	is_resource
Emergency response status	Monitor Operation	is_resource

Resources

lemma	SOURCE Function	relation
Human resources availability	Manage Human resources	is_output
ICT infrastructures	Manage ICT resource	is_output

Preconditions

lemma	SOURCE Function	relation
Staff trained	Train Staff	is_output

Control

lemma	SOURCE Function	relation
SLA(Service Level Agreement)	Manage financial affairs	is_output

Time

Note: *Emergency_respond_timing*

6.4.2 Restore/repair operation

Name	Restore/Repair operations
Description	Rebuilding and repairing services and procedures

Input

lemma	SOURCE Function	relation
Operation Restore service request	Coordinate Service delivery	is_output

Output

lemma	Destination Function	relation
Operation restored/repaired	Coordinate Service delivery	is_input
Operation Restore service plan	Manage awareness & usage behaviou	is_input

	Operation restore/repair status	Manage awareness & usage behaviou	is_input
	Operation restore/repair performance data	Collect event information	is_input
	Operation restored/repaired	Monitor Operation	is_precondition
	Operation restore/repair status	Coordinate Service delivery	is_resource
	Operation Restore service plan	Coordinate Service delivery	is_resource
Resources	lemma	SOURCE Function	relation
	Human resources availability	Manage Human resources	is_output
Preconditions	Note: *The emergency should be finished*		
Control	lemma	SOURCE Function	relation
	Law	Regulate domain and operation	is_output
	Standards	Regulate domain and operation	is_output
Time	Note: *Restore_timing_plan, Depending on how crucial the operation is for the whole system operation*		

6.5 LEARN

6.5.1 Provide adaptation & improvement insights

Name	Provide adaptation & improvement insights		
Description	Learn from ex-post event analysis, de-briefing, daily operations and provide insights for system capacities adaptation, Keep operations record, Examine good practices, perform impact analysis of suggested actions		
Input	lemma	SOURCE Function	relation
	Strategic plan	FF_01_Develop Strategic Plan	is_output
Output	lemma	Destination Function	relation
	System Sustained	Develop Strategic Plan	is_input

<table>
<tr><td></td><td><table>
<tr><td>adaptability insights</td><td></td><td></td></tr>
<tr><td>Event analysis insights</td><td>Perform Risk Assessment</td><td>is_input</td></tr>
<tr><td>Service sustained adaptability improvement insights</td><td>Coordinate Service delivery</td><td>is_input</td></tr>
<tr><td>ICT updated</td><td>Maintain physical/cyber infrastructure</td><td>is_output</td></tr>
</table></td></tr>
<tr><td>Resources</td><td><table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Knowledge base</td><td>Collect event information</td><td>is_output</td></tr>
</table>Note: <i>Collect event information</i></td></tr>
<tr><td>Preconditions</td><td>Note: <i>Data resources – reusable data</i></td></tr>
<tr><td>Control</td><td>Note: <i>Data privacy/transparency legislation</i></td></tr>
<tr><td>Time</td><td>Note: <i>Periodical , Event driven</i></td></tr>
</table>

6.5.2 Collect event information

<table>
<tr><td>Name</td><td>Collect event information</td></tr>
<tr><td>Description</td><td>Collecting in house and external event data as good practices and/or historical data (archiving)</td></tr>
<tr><td>Input</td><td><table>
<tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr>
<tr><td>Safety Security performance data</td><td>Monitor Safety and Security</td><td>is_output</td></tr>
<tr><td>Training performance data</td><td>Train Staff</td><td>is_output</td></tr>
<tr><td>Emergency response data</td><td>Coordinate emergency actions</td><td>is_output</td></tr>
<tr><td>Operation restore/repair performance data</td><td>Restore/Repair operations</td><td>is_output</td></tr>
<tr><td>Operation performance monitoring data</td><td>Monitor Operation</td><td>is_output</td></tr>
<tr><td>Infrastructure restore/repair performance data</td><td>Restore/repair physical infrastructure</td><td>is_output</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>User generated service improvement suggestions</td><td>Monitor user generated feedback</td><td>is_output</td></tr></table></td></tr>
<tr><td>Output</td><td><table><tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr><tr><td>Knowledge base</td><td>Provide adaptation & improvement insight</td><td>is_resource</td></tr></table>Note: <i>Data and metadata sets</i></td></tr>
<tr><td>Resources</td><td><table><tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr><tr><td>ICT infrastructures</td><td>Manage ICT resource</td><td>is_output</td></tr></table>Note: <i>Archives</i></td></tr>
<tr><td>Preconditions</td><td>Note: <i>Data collection and semantics rules</i></td></tr>
<tr><td>Control</td><td><table><tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr><tr><td>Strategic plan</td><td>Develop Strategic Plan</td><td>is_output</td></tr></table>Note: <i>Data regulations, Semantic rules,</i></td></tr>
<tr><td>Time</td><td>Note: <i>Continuous</i></td></tr>
</table>

6.6 Background functions

Name	Supply financial resources
MTO Category	Human(M) - Technology (T)- Organization (O)

<table>
<tr><td>Description</td><td>This function supply financial resources to the system Thus resoucres can be obtained from several actors as back, funds, the market, etc.
The scope of the funds may be different, as investments, bayout, loans, venture capitals, etc.</td></tr>
<tr><td>Input</td><td></td></tr>
<tr><td>Output</td><td><table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Funds</td><td>Manage financial affair</td><td>is_resource</td></tr>
</table></td></tr>
<tr><td>Resources</td><td></td></tr>
<tr><td>Preconditions</td><td></td></tr>
<tr><td>Control</td><td></td></tr>
<tr><td>Time</td><td></td></tr>
</table>

<table>
<tr><td>Name</td><td>Regulate domain and operation</td></tr>
<tr><td>Description</td><td>It includes EU, national and local laws, safety regulation, standards, ordinance,</td></tr>
<tr><td>Input</td><td></td></tr>
<tr><td>Output</td><td><table>
<tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr>
<tr><td>Standards</td><td>Develop Strategic Plan</td><td>is_control</td></tr>
<tr><td>Safety regulation</td><td>Monitor Safety and Security</td><td>is_control</td></tr>
<tr><td>Law</td><td>Manage financial affair</td><td>is_control</td></tr>
<tr><td>Law</td><td>Coordinate Service delivery</td><td>is_control</td></tr>
<tr><td>Standards</td><td>Coordinate Service delivery</td><td>is_control</td></tr>
<tr><td>Law</td><td>Restore/Repair operations</td><td>is_control</td></tr>
<tr><td>Standards</td><td>Restore/Repair operations</td><td>is_control</td></tr>
<tr><td>Law</td><td>Monitor Operation</td><td>is_control</td></tr>
<tr><td>Standards</td><td>Monitor Operation</td><td>is_control</td></tr>
<tr><td>Safety regulation</td><td>Train Staff</td><td>is_input</td></tr>
<tr><td>Safety regulation</td><td>Perform Risk Assessment</td><td>is_resource</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>Safety regulation</td><td>Define procedures</td><td>is_resource</td></tr></table></td></tr>
<tr><td>Resources</td><td></td></tr>
<tr><td>Preconditions</td><td></td></tr>
<tr><td>Control</td><td></td></tr>
<tr><td>Time</td><td></td></tr>
</table>

<table>
<tr><td>Name</td><td>Fight the emergency</td></tr>
<tr><td>Description</td><td></td></tr>
<tr><td>Input</td><td><table><tr><th>lemma</th><th>SOURCE Function</th><th>relation</th></tr><tr><td>Emergency response command</td><td>Coordinate emergency actions</td><td>is_output</td></tr></table></td></tr>
<tr><td>Output</td><td></td></tr>
<tr><td>Resources</td><td></td></tr>
<tr><td>Preconditions</td><td></td></tr>
<tr><td>Control</td><td></td></tr>
<tr><td>Time</td><td></td></tr>
</table>

<table>
<tr><td>Name</td><td>Supply Resources</td></tr>
<tr><td>Description</td><td>Thies function supply energy, goods, services, raw materials, etc. all things necessary to sustain operations</td></tr>
<tr><td>Input</td><td></td></tr>
<tr><td>Output</td><td><table><tr><th>lemma</th><th>Destination Function</th><th>relation</th></tr><tr><td>Supply status</td><td>Coordinate Service delivery</td><td>is_resource</td></tr><tr><td>Supply resources</td><td>Manage ICT resource</td><td>is_resource</td></tr></table>
<p>Note</p>
<ul><li><i>Energy Supply delivery performance</i></li><li><i>Energy delivery</i></li></ul></td></tr>
</table>

Resources	
Preconditions	
Control	
Time	

7 ANNEX II: GLOSSARY

Term	Definition(s)	Sources
Algorithms	A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.	https://www.stlouisfed.org/education/glossary
Approximate adjustments	When working conditions are underspecified or when time or resources are limited, it is necessary to adjust performance to match the conditions. This is a main reason for performance variability. But the very conditions that make performance adjustments necessary also mean that the adjustments will be approximate rather than perfect. The approximations are, however, under most conditions good enough to ensure successful performance	http://functionalresonance.com/a-fram-glossary.html
Big data	Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis. But it's not the amount of data that's important. It's what organizations do with the data that matters. Big data can be analyzed for insights that lead to better decisions and strategic business moves.	http://www.sas.com/en_us/insights/big-data/what-is-big-data.html
Budget reserve	A reserve fund is an account set aside by an individual or business to meet any unexpected costs that may arise in the future as well as the future costs of upkeep. In most cases, the fund is simply a savings account or another highly liquid asset, as it is impossible to predict when an unexpected cost may arise. However, if the fund is set up to meet the costs of scheduled upgrades, less liquid assets may be used.	http://www.investopedia.com/terms/r/reservefund.asp
Complete system recovery	Restoration and improvement, where appropriate, of operations, facilities, livelihoods or living conditions of affected organizations, including efforts to reduce risk factors.	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Recovery#ISO_22300:2012.28en.29
Consequences	are the negative effects of a disaster expressed in terms of human impacts, economic and environmental impacts, and political/social impacts. (ISO 31010)	ISO 31010
Critical resource	A resource that is necessary to provide care to sustain human life, prevent permanent injury/disability or stabilize a patient experiencing a medical emergency. Critical Resources can include people, places and things	http://www.troutmansanders.com/files/upload/Critical%20Resource%20Shortages-A%20Planning%20Guide.pdf
Current cash flow & predictions	In investments, cash flow represents earnings before depreciation, a mortization, and non- cash charges.Sometimes called cash earnings. Cash flow from operations (called funds from operations by real estate and otherinvestment trusts) is important because it indicates the ability to pay	http://financial-dictionary.thefreedictionary.com/cash+flow
Cyber infrastructure	Cyber infrastructure consists of computing systems, data storage systems, advanced instruments and data repositories, visualization environments, and people, all linked together by software and high performance networks to improve research productivity and enable breakthroughs not otherwise possible.	http://dsc.soic.indiana.edu/publications/fp109a-stewart.pdf
Developing Disaster Risk Financing	Governments develop disaster risk financing strategies based on their countries' unique needs. Purchasing a weather derivative, for example, is less appropriate for a country with an industrially based economy primarily vulnerable to earthquakes. Similarly, sponsoring a catastrophe bond is irrelevant to a country that has not had its vulnerability to natural hazards modeled by a catastrophe risk assessment firm. A number of factors determine the government's use of disaster risk financing instruments; one strong indicator of	https://www.gfdrr.org/sites/gfdrr.org/files/DRFI_WRC_Paper_FINAL_April11.pdf

Term	Definition(s)	Sources
	experience with disaster risk financing is the country's income level. Its geographic spread and economic base also impact what disaster risk financing strategies a country will choose.	
Disaster	A serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources. Comment: Disasters are often described as a result of the combination of: the exposure to a hazard; the conditions of vulnerability that are present; and insufficient capacity or measures to reduce or cope with the potential negative consequences. Disaster impacts may include loss of life, injury, disease and other negative effects on human physical, mental and social well-being, together with damage to property, destruction of assets, loss of services, social and economic disruption and environmental degradation.	https://www.unisdr.org/we/inform/terminology
Disaster impacts	Situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected organization, community or society to respond and recover using its own resources	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Disaster#ISO_22300:2012.28en.29
Disaster risk	The potential disaster losses, in lives, health status, livelihoods, assets and services, which could occur to a particular community or a society over some specified future time period. Comment: The definition of disaster risk reflects the concept of disasters as the outcome of continuously present conditions of risk. Disaster risk comprises different types of potential losses which are often difficult to quantify. Nevertheless, with knowledge of the prevailing hazards and the patterns of population and socio-economic development, disaster risks can be assessed and mapped, in broad terms at least.	https://www.unisdr.org/we/inform/terminology
Disaster risk financing	The strategies and instruments used to manage the financial impact of disasters, ensuring adequate capacity to manage and mitigate the costs of disaster risk, thereby reducing the financial burden and economic costs of disasters and enabling rapid recovery in economic activity.	http://www.oecd.org/gov/risk/G20disasterriskmanagement.pdf
Disaster risk management	The systematic process of using administrative directives, organizations, and operational skills and capacities to implement strategies, policies and improved coping capacities in order to lessen the adverse impacts of hazards and the possibility of disaster. Comment: This term is an extension of the more general term "risk management" to address the specific issue of disaster risks. Disaster risk management aims to avoid, lessen or transfer the adverse effects of hazards through activities and measures for prevention, mitigation and preparedness.	https://www.unisdr.org/we/inform/terminology
Disaster risk reduction	The concept and practice of reducing disaster risks through systematic efforts to analyse and manage the causal factors of disasters, including through reduced exposure to hazards, lessened vulnerability of people and property, wise management of land and the environment, and improved preparedness for adverse events.Comment: A comprehensive approach to reduce disaster risks is set out in the United Nations-endorsed Hyogo Framework for Action, adopted in 2005, whose expected outcome is "The substantial reduction of disaster losses, in lives and the social, economic and environmental assets of communities and countries." The International Strategy for Disaster Reduction (ISDR) system provides a vehicle for cooperation among Governments, organisations and civil society actors to assist in the implementation of the Framework. Note that while the term "disaster reduction" is sometimes used, the term "disaster risk reduction" provides a better recognition of the ongoing nature of disaster risks and the ongoing potential to reduce these risks.	https://www.unisdr.org/we/inform/terminology

Term	Definition(s)	Sources
Disaster risk reduction plan	A document prepared by an authority, sector, organization or enterprise that sets out goals and specific objectives for reducing disaster risks together with related actions to accomplish these objectives. Comment: Disaster risk reduction plans should be guided by the Hyogo Framework and considered and coordinated within relevant development plans, resource allocations and programme activities. National level plans needs to be specific to each level of administrative responsibility and adapted to the different social and geographical circumstances that are present. The time frame and responsibilities for implementation and the sources of funding should be specified in the plan. Linkages to climate change adaptation plans should be made where possible.	https://www.unisdr.org/we/inform/terminology
Economic and environmental impacts	are the sum of the costs of cure or healthcare, cost of immediate or longer-term emergency measures, costs of restoration of buildings, public transport systems and infrastructure, property, cultural heritage, etc., costs of environmental restoration and other environmental costs (or environmental damage), costs of disruption of economic activity, value of insurance pay-outs, indirect costs on the economy, indirect social costs, and other direct and indirect costs, as relevant.	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Emergency actions	An emergency action plan (EAP) is a written document required by particular OSHA standards. [29 CFR 1910.38(a)] The purpose of an EAP is to facilitate and organize employer and employee actions during workplace emergencies. Well developed emergency plans and proper employee training (such that employees understand their roles and responsibilities within the plan) will result in fewer and less severe employee injuries and less structural damage to the facility during emergencies. A poorly prepared plan, likely will lead to a disorganized evacuation or emergency response, resulting in confusion, injury, and property damage.	https://www.osha.gov/SLTC/etools/evacuation/eap.html
Emergency mitigation strategies	Disaster mitigation measures are those that eliminate or reduce the impacts and risks of hazards through proactive measures taken before an emergency or disaster occurs.	https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/dsstr-prvntn-mtgtn/bt-dsstr-mtgtn-eng.aspx
Energy supply report	Total primary energy domestic supply (sometimes referred to as energy use) is calculated by the International Energy Agency as production of fuels + inputs from other sources + imports - exports - international marine bunkers + stock changes. It includes coal, crude oil, natural gas liquids, refinery feedstocks, additives, petroleum products, gases, combustible renewables and waste, electricity and heat. Domestic supply differs from final consumption in that it does not take account of distribution losses. The supply and use of energy commodities are converted to Kg. oil equivalent using standard coefficients for each energy source.	https://stats.oecd.org/glossary/detail.asp?ID=6328
Exposure	People, property, systems, or other elements present in hazard zones that are thereby subject to potential losses. (UNISDR, 2009)	UNISDR 2009
feedback	Process in which the effect or output of an action is 'returned' (fed-back) to modify the next action. Feedback is essential to the working and survival of all regulatory mechanisms found throughout living and non-living nature, and in man-made systems such as education system and economy. As a two-way flow, feedback is inherent to all interactions, whether human-to-human, human-to-machine, or machine-to-machine. In an organizational context, feedback is the information sent to an entity(individual or a group) about its prior behavior so that the entity may adjust its current and future behavior to achieve the desired result.	http://www.businessdictionary.com/definition/feedback.html

Term	Definition(s)	Sources
Financial sector resilience	The capacity of the financial system to adapt in response to both short-term shocks and long-term changes in economic, social, and ecological conditions while continuing to fulfil its functions in serving the real economy	http://b.3cdn.net/nefoundation/3898c6a7f83389375a_y1m6ixqbv.pdf
Government compensation	Many governments offer a deferred compensation plan to their employees. In operating these plans, governments act as fiduciaries. Because deferred compensation plans shift investment risk to the plan participant, GFOA recommends that governments provide employee education about the management of the investment risk.Some governments have established an investment policy that governs assets in the deferred compensation plan. Such an investment policy offers a number of advantages to the government and its plan participants:Investment policies are a clear demonstration of fiduciaries' due diligence;They are a communication tool for conveying investment goals and priorities to interested parties;They strengthen the internal controls of the government and the plan.Like any financial policy, a deferred compensation investment policy is a governing document in which the governing board and other key stakeholders formally set broad policy parameters. Detailed guidance about implementation of the investment program may be contained in the investment policy or other documents, such as investment procedure manuals and agreements with third parties.	http://www.gfoa.org/investment-policies-deferred-compensation-plans
Hazard	is a dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. Comment: […] In technical settings, hazards are described quantitatively by the likely frequency of occurrence of different intensities for different areas, as determined from historical data or scientific analysis. (UNISDR, 2009	UNISDR 2009
Hazard assessments	determine the probability of occurrence of a certain hazard of certain intensity	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Hazard map	is a map that portrays levels of probability of a hazard occurring across a geographical area. Such maps can focus on one hazard only or include several types of hazards (multi-hazard map)	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Historical data	Past-periods data, used usually as a basis for forecasting the future data or trends.	http://www.businessdictionary.com/definition/historical-data.html
Human impacts	are defined as the quantitative measurement of the following factors: number of deaths, number of severely injured or ill people, and number of permanently displaced people	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Human Resource Development	HRD is mostly concerned with training, development, and education. HRD is defined as an organized learning experience, conducted in a definite time period, to increase the possibility of improving job performance and growth	http://www.nwlink.com/~donclark/hrd/isd/definitions.html
human resources	The quantity and quality of human effort directed toward producing goods and services. Also known as labour.	https://www.stlouisfed.org/education/glossary
Humans (labour) – skills/competence	The e-CF describes competences upon the basic definition that competence is the "demonstrated ability to apply knowledge, skills and attitudes to achieve observable results". This basic definition agreed by an expert group defines competence from a workplace perspective, and it adapts in parallel the learning outcome approach from the European Qualifications Framework (EQF), focusing in the whole at observable behaviour and measurable items of competence performance .Competences in the e-CF are demonstrated abilities. To describe these abilities, it is necessary to find a common	http://www.ecompetences.eu/faq-competences-skills-jobs/

Term	Definition(s)	Sources
	language. Typical business/working processes and typical workplace activities are similar all over the world, across all enterprises. So in the e-CF competences are structured from processes – PLAN, BUILD, RUN, ENABLE, MANAGE – and describe typical activities and abilities on different levels. For example: The competence “Problem Management” is described as “Identifies and resolves the root cause of incidents. Takes a proactive approach to the root cause of ICT problems. …” This is further expanded in respect of levels where on level 2 the specification is “Identifies and classifies incident types and service interruptions. Records incidents cataloguing them by symptom and resolution.”; at the higher level 4 it is articulated as “Provides leadership and is accountable for the entire problem management process. (…) Has depth of expertise to anticipate critical component failure and make provision for recovery with minimum downtime. (...)”	
Humans (labour) – skills/competence	The e-CF describes competences upon the basic definition that competence is the “demonstrated ability to apply knowledge, skills and attitudes to achieve observable results”. This basic definition agreed by an expert group defines competence from a workplace perspective, and it adapts in parallel the learning outcome approach from the European Qualifications Framework (EQF), focusing in the whole at observable behaviour and measurable items of competence performance. Competences in the e-CF are demonstrated abilities. To describe these abilities, it is necessary to find a common language. Typical business/working processes and typical workplace activities are similar all over the world, across all enterprises. So in the e-CF competences are structured from processes – PLAN, BUILD, RUN, ENABLE, MANAGE – and describe typical activities and abilities on different levels. For example: The competence “Problem Management” is described as “Identifies and resolves the root cause of incidents. Takes a proactive approach to the root cause of ICT problems. …” This is further expanded in respect of levels where on level 2 the specification is “Identifies and classifies incident types and service interruptions. Records incidents cataloguing them by symptom and resolution.”; at the higher level 4 it is articulated as “Provides leadership and is accountable for the entire problem management process. (…) Has depth of expertise to anticipate critical component failure and make provision for recovery with minimum downtime. (...)”	http://www.ecompetences.eu/faq-competences-skills-jobs/
ICT infrastructures	ICT Infrastructure offers a range of technologies to assist organisations in running efficiently. These services are essential to the everyday mechanics of an organisation and integral to effective service delivery. These include hardware, software, networking and implementation	http://www.ictservices.infoxchange.net.au/ict-infrastructure
ICT resources	the European e-Competence Framework (e-CF) provides a reference of 40 competences as required and applied at the Information and Communication Technology (ICT) workplace, using a common language for competences, skills and proficiency levels that can be understood across Europe. As the first sector-specific implementation of the European Qualifications Framework (EQF), the e-CF fits for application by ICT service, demand and supply organizations, companies, for managers and HR departments, for education institutions and training bodies, including higher education, for market watchers and policy makers, public and private sectors	http://www.ecompetences.eu/
Incident	Incident is an event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system.	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Incident#ENISA
Infrastrcutre	The term "infrastructure" usually refers to physical assets in a wider range of policy	COMMISSION STAFF WORKING DOCUMENT

Term	Definition(s)	Sources
	areas, including communications, emergency services, energy, finance, food, government, health, education, civil protection, transport or water. Buildings, from private households to schools or industrial installations, are the most common type of infrastructure and the basis for human settlement. In addition, network infrastructure is crucial for the functioning of today's economy and society, notably infrastructure for energy (e.g. grids, power stations, pipelines), transport (fixed assets such as roads, railways or airports), ICT (e.g. data cables) and water (e.g. water supply pipelines, reservoirs, waste water treatment facilities). They are sets of interconnected networks which facilitate the production and distribution of goods and economic services, and form the basis for the provision of basic social services.	Adapting infrastructure to climate change SWD(2013) 137 final
Integrity	Data integrity is the property that data has not been altered or destroyed in an unauthorized manner.	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Integrity#ITU-T
Interdependencies	Interactions or mutual influences between different Critical Infrastructures.	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Interdependency#Germany
Investment plans	IP is an investment strategy wherein an investor needs to invest the same amount of money in a particular mutual fund at every stipulated time period	http://economictimes.indiatimes.com/definition/systematic-investment-plan
Mitigation	Measures taken to prevent, limit and reduce impact of the negative consequences of incidents, emergencies and disasters.	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Mitigation#ISO_22300:2012.28en.29
Multi-hazard assessments	determine the likelihood of occurrence of different hazards either occurring at the same time or shortly following each other, because they are dependent from one another or because they are caused by the same triggering event or hazard, or merely threatening the same elements at risk (vulnerable/ exposed elements) without chronological coincidence.	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Multi-hazard map	is a map that portrays levels of probability of several hazards occurring across a geographical area.	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Multi-risk assessments	determine the total risk from several hazards either occurring at the same time or shortly following each other, because they are dependent from one another or because they are caused by the same triggering event or hazard; or merely threatening the same elements at risk (vulnerable/ exposed elements) without chronological coincidence.	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Natural hazard	Natural process or phenomenon that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. Comment: Natural hazards are a sub-set of all hazards. The term is used to describe actual hazard events as well as the latent hazard conditions that may give rise to future events. Natural hazard events can be characterized by their magnitude or intensity, speed of onset, duration, and area of extent.(UNISDR, 2009)	UNISDR 2009
Operation plan	A plan which ensures the performance of an organization's mission essential functions during any emergency or situation that may disrupt operations over a 30-day period	http://www.nacubo.org/Documents/BusinessPolicyAreas/FAU-COOP-Small-

Term	Definition(s)	Sources
		Unit-Plan-Guide.pdf
Operation requirements	Operational requirements are those statements that "identify the essential capabilities, associated requirements, performance measures, and the process or series of actions to be taken in effecting the results that are desired in order to address mission area deficiencies, evolving applications or threats, emerging technologies, or system cost improvements [1]." The operational requirements assessment starts with the Concept of Operations (CONOPS) and goes to a greater level of detail in identifying mission performance assumptions and constraints and current deficiencies of or enhancements needed for operations and mission success. Operational requirements are the basis for system requirements.	http://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/concept-development/operational-requirements
Operational (financial) requirement	Operational requirements are those statements that "identify the essential capabilities, associated requirements, performance measures, and the process or series of actions to be taken in effecting the results that are desired in order to address mission area deficiencies, evolving applications or threats, emerging technologies, or system cost improvements [1]." The operational requirements assessment starts with the Concept of Operations (CONOPS) and goes to a greater level of detail in identifying mission performance assumptions and constraints and current deficiencies of or enhancements needed for operations and mission success. Operational requirements are the basis for system requirements.	http://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/concept-development/operational-requirements
Operations		
owners/operators of ECIs	those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive.	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114
Performance variability	The study of risk and accidents has traditionally focused on how failures or malfunctions of components or elements (technological, human, organisational) could happen and how the effects could propagate through the system. This can be called a bimodal view of functions and performance. The FRAM is based on the principle of equivalence of successes and failures and the principle of approximate adjustments. Performance is therefore in practice always variable. The performance variability of upstream functions may affect the performance variability of downstream functions, and thereby lead to non-linear effects (functional resonance).	http://functionalresonance.com/a-fram-glossary.html
physical infrastructure	Infrastructure is the basic physical systems of a business or nation. Transportation, communication, sewage, water and electric systems are all examples of infrastructure. These systems tend to be high-cost investments, however, they are vital to a country's economic development and prosperity. Infrastructure projects may be funded publicly, privately or through public-private partnerships.	http://www.investopedia.com/terms/i/infrastructure.asp
Political/social impacts	are usually rated on a semi-quantitative scale and may include categories such as public outrage and anxiety21, encroachment of the territory, infringement of the international position, violation of the democratic system, and social psychological impact22, impact on public order and safety, political implications, psychological implications, and damage to cultural assets23, and other factors considered important which cannot be measured in single units, such as certain environmental damage.	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Prepardeness	Preparedness means a state of readiness and capability of human and material means enabling them to ensure an effective rapid response to an emergency, obtained as a result of action taken in advance	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Preparedness#2007.2F779.2FEC
Prevention	All medical measures, health or other actions (e.g. social, political, economic) that reduce exposure or other risks, prevent the onset of a	https://publicwiki-01.fraunhofer.de/CIPedia/i

Term	Definition(s)	Sources
	disease or a health event or limit the development, exacerbation, and ensure its demise.	ndex.php/Prevention#UNISDR
private disaster risk financing markets		
procedures	according to organizational / business perspective: a set of operations (or activities) to obtain certain purposes or perform certain functions, and turns according to a set of norms, rules, Prass; according to an IT perspective: all the operations the computer system to perform a certain task	http://static.gest.unipd.it/labtesi/eb-didattica/GIA/PIANIFICAZIONESI-procedure.pdf
Protection	All activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114
Recovery	Restoration and improvement, where appropriate, of operations, facilities, livelihoods or living conditions of affected organizations, including efforts to reduce risk factors.	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Recovery#ISO_22300:2012.28en.29
Resilience	The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions. (UNISDR, 2009)	UNISDR 2009
	the ability of socio-technical systems to sustain required operations under both expected and unexpected conditions	Hollnagel (2011)
Resource (as FRAM aspect)	A Resource is something that is needed or consumed while a function is carried out. A Resource can represent matter, energy, information, competence, software, tools, manpower, etc. Time can, in principle, also be considered as a Resource, but since Time has a special status it is treated as a separate aspect. Since some Resources are consumed while the function is carried out and others are not, it is useful to distinguish between Resources on the one hand and Execution Conditions on the other. The difference is that a while a Resource is consumed by a function, so that there will be less of it as time goes by, an Execution Condition is not consumed but only needs to be available or exist while a function is active. The difference between a Precondition and an Execution Condition is that the former is only required before the function starts, but not while it is carried out.	http://functionalresonance.com/a-fram-glossary.html
Resources	Resources refers to the side of the current accounts where transactions which add to the amount of economic value of a unit or a sector appear (for example, wages and salaries are a resource for the unit or sector receiving them); by convention, resources are put on the right side of the account.	https://stats.oecd.org/glossary/detail.asp?ID=2333
Response	Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.	http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=IT
Risk	is a combination of the consequences of an event (hazard) and the associated likelihood/probability of its occurrence. (ISO 31010)	ISO 31010

Term	Definition(s)	Sources
	The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.	http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=IT
Risk identification	is the process of finding, recognizing and describing risks. (ISO 31010)	ISO 31010
Risk analysis	consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114
Risk analysis	is the process to comprehend the nature of risk and to determine the level of risk. (ISO 31010)	ISO 31010
Risk Assessment	is the overall process of risk identification, risk analysis, and risk evaluation. (ISO 31010)	ST_17833_2010_INIT_EN.pdf
Risk Assessment	defines risk as the probability of harmful consequences — casualties, damaged property, lost livelihoods, disrupted economic activity, and damage to the environment — resulting from interactions between natural or human-induced hazards and vulnerable conditions. Risk assessment is a process to determine the nature and extent of such risk, by analyzing hazards and evaluating existing conditions of vulnerability that together could potentially harm exposed people, property, services, livelihoods and the environment on which they depend. A comprehensive risk assessment not only evaluates the magnitude and likelihood of potential losses but also provides full understanding of the causes and impact of those losses. Risk assessment, therefore, is an integral part of decision and policy-making processes and requires close collaboration among various parts of society.	http://www.undp.org/content/dam/undp/library/crisis%20prevention/disaster/2Disaster%20Risk%20Reduction%20-%20Risk%20Assessment.pdf
Risk criteria	are the terms of reference against which the significance of a risk is evaluated. (ISO 31010)	ISO 31010
Risk evaluation	is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. (ISO 31010)	ISO 31010
Risk map	is a map that portrays levels of risk across a geographical area. Such maps can focus on one risk only or include different types of risks	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Risk scenario	is a representation of one single-risk or multi-risk situation leading to significant impacts, selected for the purpose of assessing in more detail a particular type of risk for which it is representative, or constitutes an informative example or illustration.	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Safety	Safety is a condition in which the threats and risks are controllable.	https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Safety#Finland
Safety regulation	Standards relating to the design and manufacturing of consumer products to ensure they do not represent harm or hazards to consumers. In the United States, the Consumer Products Safety Commission oversees the regulation of consumer product standards.	http://www.businessdictionary.com/definition/product-safety-standards.html

Term	Definition(s)	Sources
Sensor networks & data	Assessor network (WSN) is a set of transducers with a communication infrastructure used to monitor physical or environmental conditions, such as temperature, sound, pressure, speed, illumination intensity, sound intensity, , chemical concentrations, pollutant levels, Body functions etc.	http://www.omicsonline.com/open-access/sensor-networks-data-communications.php
Service delivery	The act to provide a service to the customer	http://dictionary.cambridge.org/dictionary/english/service-delivery
Single-risk assessments	determine the singular risk (i.e. likelihood and consequences) of one particular hazard (e.g. flood) or one particular type of hazard (e.g. flooding) occurring in a particular geographic area during a given period of time.	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
SLA	A service-level agreement (SLA) is simply a document describing the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. Usually, SLAs are between companies and external suppliers, but they may also be between two departments within a company	http://www.cio.com/article/2438284/outsourcing/sla-definitions-and-solutions.htm-Johnston and Clark, 2001
SLA	A formal negotiated agreement between two parties, which in the context of SOA are usually a service provider and a service consumer. For a specific subject an SLA usually records the common understanding about priorities, responsibilities, and warranties, with the main purpose of agreeing on the quality of the service. For example, it may specify the levels of availability, serviceability, performance, operation, or other attributes of the service (such as billing and even penalties in the case of violations of the SLA).	http://www.soa-in-practice.com/soa-glossary.html
SoA in technical terms	Stands for "Service Oriented Architecture." When businesses grow, they often add new products and services. While these additions may help make the business larger, it is often difficult to implement them in an efficient manner. The goal of SOA is to make it easy for businesses to grow and add new services	http://techterms.com/definition/soa
SoA in technical terms	There are various definitions for SOA. Some specify only that it is an approach for architectures where the interfaces are services. However, in a more specific sense (and according to my understanding), SOA is an architectural paradigm for dealing with business processes distributed over a large and heterogeneous landscape of existing and new systems that are under the control of different owners. The key concepts of SOA are services, interoperability, and loose coupling. The key ingredients of SOA are the infrastructure (ESB), architecture, and processes. The key success factors for SOA are understanding, governance, management support, and homework. Note that Web Services is not a synonym for SOA; Web Services are one possible way of realizing the infrastructure aspects of SOA.	http://www.soa-in-practice.com/soa-glossary.html
Social data	social data analysis grows out of this need and combines disciplines such as social network analysis, multimedia management, social media analytics, trend discovery, and opinion mining. For example, studying the evolution of a social network merely as a graph is very limiting as it does not take into account the information flowing between network nodes. Similarly, processing social interaction contents between network members without taking into account connections between these is limited by the fact that information flows cannot be properly weighted. Big social data analysis, instead, aims to study large-scale Web phenomena such as social networks from a holistic point of view, i.e., by concurrently taking into account all the	http://sentic.net/big-social-data-analysis.pdf

Term	Definition(s)	Sources
	socio-technical aspects involved in their dynamic evolution	
staff effectiveness	the effectiveness of staff training is an important aspect for companies operating in various fields: from the formative stages, in fact, is largely dependent on the productivity and efficiency of employees.	
Stakeholders participation (including the general public)	This expression designates a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity. In practical terms, unless demonstrated otherwise through proper assessment, this includes every person, organisation or part of one, that is involved in transport supply chains, or that in some way plays a role in the production or delivery of the transport service in question.	defined in the project (UNIFI)
Strategic plan	The basic framework for corporate strategic planning can be described by five steps: specify objectives, generate alternative strategies, evaluate strategies, monitor results, and seek commitment. Many corporate planners argue that each of these steps should be carried out in a formal manner (that is with operational guidelines and presumably with each step written out).	Evidence on the Value of Strategic Planning in Marketing: How Much Planning Should a Marketing Planner Plan? J. Scott Armstrong and David J. Reibstein Department of Marketing, Wharton School, University of Pennsylvania, Philadelphia, Pa. 19104
Strategic Plan	The basic framework for corporate strategic planning can be described by five steps: specify objectives, generate alternative strategies, evaluate strategies, monitor results, and seek commitment. Many corporate planners argue that each of these steps should be carried out in a formal manner (that is with operational guidelines and presumably with each step written out).	Evidence on the Value of Strategic Planning in Marketing: How Much Planning Should a Marketing Planner Plan? J. Scott Armstrong and David J. Reibstein Department of Marketing, Wharton School, University of Pennsylvania, Philadelphia, Pa. 19104
Technological hazard	A hazard originating from technological or industrial conditions, including accidents, dangerous procedures, infrastructure failures or specific human activities, that may cause loss of life, injury, illness or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. (UNISDR, 2009)	UNISDR 2009
Threat	Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.	http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=IT
Threat	is a potentially damaging physical event, phenomenon or activity of an intentional/ malicious character.	Commission Staff Working Paper - Risk Assessment and Mapping Guidelines for Disaster Management
Train Staff	Educational preparation for performing a job that is typically provided to staff by the business that has recently hired them before they become active in service to the company. Employee training is increasingly required to assist the work force in using modern techniques, tools, strategies and mate rials in their jobs.	http://www.businessdictionary.com/definition/employee-training.html#ixzz44NL8shol

Term	Definition(s)	Sources
Training	Training is teaching, or developing in oneself or others, any skills and knowledge that relate to specific useful competencies. Training has specific goals of improving one's capability, capacity, productivity and performance. It forms the core of apprenticeships and provides the backbone of content at institutes of technology (also known as technical colleges or polytechnics).	https://en.wikipedia.org/wiki/Training
Training effectiveness	"The systematic analysis of training to demonstrate whether it has met its objectives in an effective and efficient manner"	http://evaluationfocus.com/define-training-evaluation/
Training performance	in the Pre-Post Training Performance Method, each of the participants is evaluated before the training and rated on the basis of the actual job performance. After instruction, of which the evaluator has been kept unaware is completed, the employee is revaluated. As with the post training performance method, the increase is assumed to be attributable to the instruction.	http://www.mbaskool.com/business-concepts/human-resources-hr-terms/15762-pre-post-training-performance.html
User behaviour	A user is a person or thing that uses something such as a place, facility, product, or machine	http://searchsecurity.techtarget.com/definition/user-behavior-analytics-UBA
Vulnerability	The characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard. (UNISDR, 2009) In probabilistic/quantitative risk assessments the term vulnerability expresses the part or percentage of Exposure that is likely to be lost due to a certain hazard	UNISDR 2009
	A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.	http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=IT