EUROPEAN RESILIENCE MANAGEMENT GUIDELINES

Project Title	RESOLUTE
Project number	653460
Deliverable number	D3.6
Version	0.3
State	FINAL
Confidentially Level	CO
WP contributing to the Deliverable	3
Contractual Date of Delivery	M36 (30/04/2018)
Finally approved by coordinator	(02/05/2018)
Actual Date of Delivery	(02/05/2018)
Authors	Evangelia Gaitanidou (CERTH), Emanuele Bellini (UNIFI), Pedro Ferreira (COFAC)
Email	lgait@certh.gr
Affiliation	CERTH
Contributors	L. Coconea (SWARCO), A. Deloukas, E. Apostolopoulou (Attiko Metro), S. Cigheri (THALES), A. Candelieri (CMR), A. Zamichos, I. Symeonidis, A. Spiliotis, M. Panou, E. Bekiaris (CERTH), L. Mendoza (HUMANIST), M. Vaiani, G. Vannuccini (CDF), M. Kamps, J.P. Leuteritz (FhG/IAO)

funded by the Horizon 2020
Framework Programme of the European Union

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

EXECUTIVE SUMMARY

This document, entitled D3.6 European Resilience Management Guidelines, provides an updated version of Deliverable D3.5, issued in 2016. The ERMG, as presented in the latter document, has been updated in the present Deliverable, following the findings of the project pilots, as well as the guidance of the RESOLUTE Advisory Board. Keeping the original rationale and structure, a full, updated version of the guidelines has been produced, followed by a short version, limited to 1 page per function, providing the main recommendations and highlighting the most important aspects.

The document is structured in five Chapters and one Annex. More specifically:

- Chapter 1 is the Introduction where the scope and objectives of the document are presented
- Chapter 2 is the Methodology. In this chapter it is described how the ERMG has been updated, taking into account the results of the RESOLUTE pilots as well as the comments of the Advisory Board. The updated and short versions that follow, are also introduced.
- Chapter 3 includes detailed instructions of how to use the ERMG in practice, along with a relevant example.
- In Chapter 4, the updated version of the ERMG is included in detail, following a similar structure as in the D3.5, with updated contents, following the recommendations coming from the pilots and the Advisory Board.
- In Chapter 5 conclusions are drawn regarding the contents and use of the ERMG
- Finally, in Annex A, the short version of the ERMG is presented, highlighting the most important recommendations in a 1-page-per-function format.

PROJECT CONTEXT

Workpackage	WP3: European Resilience Management Guidelines
Task	T3.3: ERMG development
Dependencies	WP2, WP6

Contributors and Reviewers

Contributors	Reviewers
L. Coconea (SWARCO)	E. Bellini (UNIFI)
A. Deloukas, E. Apostolopoulou (Attiko Metro)	
S. Cigheri (THALES)	
A. Candelieri (CMR)	
A. Zamichos, I. Symeonidis, A. Spiliotis, M. Panou, E. Bekiaris (CERTH)	
L. Mendoza (HUMANIST)	

M. Vaiani, G. Vannuccini (CDF)	
M. Kamps, J.P. Leuteritz (FhG/IAO)	

Version History

Version	Date	Authors	Sections Affected
V01	3/4/2018	Evangelia Gaitanidou	All
V02	15/4/2018	All authors and contributors	Chapter 4, Annex A
V03	25/4/2018	All authors and contributors	All
V04	30/4/2018	All authors and contributors	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 Content

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 D3.6 is to update the European Resilience Management Guidelines (ERMG), originally produced in D3.5, as a product of work performed within project Task T3.3. Following the project structure, the first draft of the guidelines has been operationalized for the Urban Transport System (in Deliverable D3.7) and tested in the pilots of WP6. The results of the project work in the pilots and Advisory Board comments have been used as a basis for the update of ERMG in the present document, as well as their UTS ERMG (in D3.8).

The methodology for the production of ERMG has been primarily defined in Deliverable D3.4 and is further specified and elaborated in D3.5, 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, 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.

Finally, a short version of the ERMG has been produced and can be found in Annex A. This shorter version follows a 1-page-per-function template and include a summary of the long version, highlighting the most important elements. Its main role is to serve as a practical tool for the promotion, dissemination and exploitation of the ERMG, providing a thorough impression of the guidelines at a glance, thus being a trigger for the interested stakeholders to relate to the resilience management procedures and consult the detailed version for the application in the critical infrastructure of their interest.

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.

1.2.1 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).

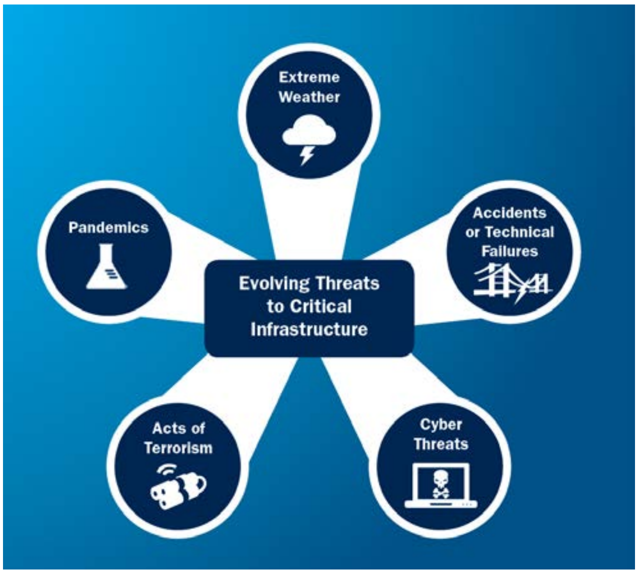

Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

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).

1.3 Target audience

The Deliverable is addressing a broad audience, mainly, but not exclusively, related to stakeholders that are dealing with critical infrastructure facilities (managers, owners, employees, security services, etc.), emergency respondents, local and regional authorities, the general public, etc.

It is important to stress out the EU dimension that is in the heart of the ERMG, and the RESOLUTE project as a whole, thus aiming to provide guidelines that not only address critical infrastructure as such, but also their links, dependencies and interdependencies, finally targeting to facilitating safety, security and, most notably, resilience as a core feature in EU cities, regions and as a whole.

1.4 Structure of the document

The document is structured in five Chapters and one Annex. More specifically:

- Chapter 1 is the Introduction where the scope and objectives of the document are presented
- Chapter 2 is the Methodology. In this chapter it is described how the ERMG has been updated, taking into account the results of the RESOLUTE pilots as well as the comments of the Advisory Board. The updated and short versions that follow, are also introduced.
- Chapter 3 includes detailed instructions of how to use the ERMG in practice, along with a relevant example.

- In Chapter 4, the updated version of the ERMG is included in detail, following a similar structure as in the D3.5, with updated contents, following the recommendations coming from the pilots and the Advisory Board.
- In Chapter 5 conclusions are drawn regarding the contents and use of the ERMG
- Finally, in Annex A, the short version of the ERMG is presented, highlighting the most important recommendations in a 1-page-per-function format.

2 METHODOLOGY

The first version of the ERMG was issued in M12 of the project (D3.5, April 2016), including all the methodology for the definition of functions, their interrelations and the overall application of FRAM.

Since then, the ERMG has been available online in the project website, accessed by several interested bodies and presented in several conferences and publications (see WP7 Deliverables). It was also, of course, used during the RESOLUTE project activities, first as a consulting document in the production of the tools and then as a guideline for the execution of the pilots.

Moreover, the RESOLUTE Advisory Board members were involved in the process, by reviewing the first version of the guidelines and suggesting ways for its improvement.

These sources were hence used to produce this updated version of the ERMG. The work has been organised stepwise:

a) Assessment from pilots: input coming from the pilot assessment per guideline was evaluated and a list of guidelines needing further elaboration was produced
b) Advisory Board members' comments: the comments received from the AB members at several occasions were discussed and incorporated in the guidelines to the possible extend
c) Revision of the ERMG per guideline: guidelines were revised following the recommendations from the above sources
d) Short version of ERMG: a short, condensed and practical to use version of the guidelines was produced, following the original structure of the ERMG, but in limited volume and highlighting the most prominent issues.

2.1 RESOLUTE pilots

The guidelines have been revised according to the RESOLUTE pilot results (See D6.4) carried out in Florence and Athens. The results of the assessment revealed some drawbacks in the ERMG definition. They have prevented their full application and understanding resulting in a low or null increment in resilience quantification score defined in D6.4. In particular, a taxonomy has been identified to assess guidelines, in D6.4 and is reported in Table 1.

Table 1 Taxonomy for guidelines assessment and revision

# TAX	Guidelines Issues Taxonomy
TAX01	too generic (no practical/poor practical indications)
TAX02	too specific/over-detailed (some references are not applicable to a wide range of the organization)
TAX03	not understandable (guideline quality of the description is poor)
TAX04	out of scope/focus (wrong target audience)
TAX05	incomplete (guidelines should be improved/extended)
TAX06	wrong content (guidelines recommendations seems to be out of scope for the guideline under specification)
TAX07	not applicable within the project timeframe (lack of resources)
TAX08	not applicable within the project timeframe (lack of technological knowledge/awareness/education)
TAX09	not applicable within the project timeframe (requires a policy change from the stakeholder)

TAX10	not applicable within the project timeframe (requires reorganization/change of the company and/or involvement of key stakeholder)
TAX11	not applicable within the project timeframe (irrelevant in the context of UTS system resiliency)

According to the pilot assessment results, the guidelines that required reviews are reported in the following table

Table 2 ERMG assessment results

Function	**# TAX**
ANTICIPATE	
Develop Strategic Plan	
Manage financial affairs	TAX01 - TAX03 - TAX09
Perform Risk Assessment	
Training staff, Citizens	
Coordinate Service delivery	TAX05 - TAX10
Manage awareness & user behaviour	TAX07 - TAX10
Develop/update procedures	TAX01 - TAX0 - TAX10
Manage human resources	
Manage ICT resources	TAX07
Install/maintain assets	TAX07
MONITOR	
Monitor Safety and Security	-
Monitor Operations	
Monitor Resource availability	TAX04 - TAX05 - TAX06
Monitor user generated feedback	
RESPOND	
Coordinate emergency actions	
Restore/Repair operations	TAX01 - TAX05
LEARN	
Provide adaptation & improvement insights	TAX08 - TAX10
Collect event information	TAX01 - TAX10

2.2 Advisory Board

Upon issuing the first version of the ERMG (D3.5) this was made available to the Advisory Board members for their comments and suggestions for improvement. Additional comments were received during the Advisory Board meeting which took place in Brussels in parallel to the Joint Workshop DRS-7&14 projects and the Community of Users, in September 2017.

Through this consultation process several suggestions were received. These involved mainly the explanation of the use the guidelines, the provision of a shorter version of the guidelines, practical examples, indicators, etc. In the current version presented in the Deliverable in hand, there has been effort to address these suggestions and provide an enhanced and more useful ERMG.

2.3 ERMG Update &short version

Following the above findings and consultation process, the original version of the ERMG has been updated and revised according to the results of the pilot assessment and the suggestions of the Advisory Board. In Section 4 the revised version is presented, following the original structure and incorporating improvements to satisfy the identified problems per function/guideline.

Moreover, a new, shorter version of the ERMG has been produced in which each of the functions/guidelines is summarised in one page, highlighting the main points in a short but comprehensive manner. This short version was specifically suggested from the Advisory Board members during the Advisory Board meeting in Brussels, in September 2017 and has been implemented in the current Deliverable in a specifically created template. The short version of the ERMG can be found in Annex A of the present document.

3 DETAILED INSTRUCTIONS FOR USING THE ERMG

The ERMG aim to support a self-assessment and multilevel gap analysis in respect to the potential for resilience of the CIs considered. The ERMG are structured to support the reader in the assessment as well as improvement of the CI of interest. Guidelines may be used by CI stakeholders independently, in which case, some aspects of the guidelines may not be applicable. However, the focus is placed on the CI as an interdependent sociotechnical system and in that sense, the ERMG should be applied adopting a complex view and under a coordinated strategy between CI stakeholders. To this end, teams and departments within organisations should establish and maintain regular communication with other teams and departments to which they identify as being operationally coupled. Initial steps towards adopting the ERMG should ensure that critical functions and interdependencies are sufficiently known and described. Special attention should be devoted to:

- Other teams and departments that supply important information or other types of resources to the team or department in question
- Other teams and departments that rely on information or other types of resources produced by the team or department in question
- Other teams and departments that carry out or have ownership of any operational oversight or control (i.e. quality or performance monitoring and assessment, safety compliance, among others) over the team or department in question
- Other teams and departments over which the team or department in question carries out or has ownership of any operational oversight or control (i.e. quality or performance monitoring and assessment, safety compliance, among others)

Often these couplings extend far beyond the formal boundaries of organisations or the system under consideration. Teams or departments within a given organisation are likely to have strong interdependencies with teams or departments within other organisations participating in the operation of a given CI. Going across organisational/system boundaries should not prevent the development and maintenance of suitable coordination mechanisms between operationally coupled system functions. Different degrees of formalisation and analysis should be defined in these cases, namely to ensure responsibility and accountability. To this end a 3-level analysis inspired to the 3 tier- resilience assessment approach defined in (Linkov et.al, 2018) is provided. In (Linkov at . 2018), the goal of each tier is to describe the performance and relationship of critical systems in order to identify management options that enhance performance in parallel with activities that reduce risk. The methods of Tier I quickly and inexpensively identify the broad functions that a system provides to human society or the environment and prioritize the performance of the critical functions. The methods of Tier II describe the general organization and relationships of the system in a simple form such as a process model or critical path model. The methods of Tier III build a detailed model of important functions and related sub-systems where each process and each component of the system is parameterized. The process can be halted at any tier when enough information has been synthesized such that actionable system investments or projects to improve system resilience, given available resources, have been identified by the decision makers (See Figure 2).

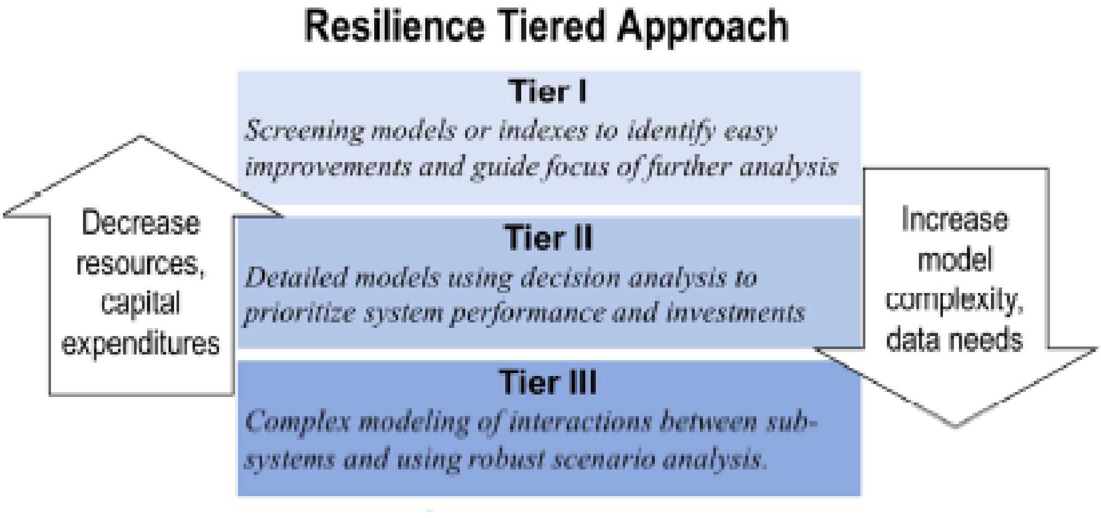

Resilience Tiered Approach
Tier I
Screening models or indexes to identify easy improvements and guide focus of further analysis
Tier II
Detailed models using decision analysis to prioritize system performance and investments
Tier III
Complex modeling of interactions between sub-systems and using robust scenario analysis.
Decrease resources, capital expenditures
Increase model complexity, data needs

Figure 2: Resilience Tiered Approach (Linkov et. al., 2018)

However, the focus should be set on real work and operational needs, as opposed to merely establishing formal business and legal requirements between the parties involved.

The FRAM model provided by RESOLUTE and used as grounds for the development of these ERMG, (D3.5) provides initial support to stakeholders in the process of identifying their interdependencies within their specific context and scope of operation.

To this end, the ERMG support three different levels of analysis:

- Level I: The first level of analysis can be carried out by the comparison between the “desired functions” defined in ERMG against the functions and interdependencies 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. The ERMG provides also a number of desired interdependencies that contribute to an enhanced potential for 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. This preliminary assessment is able to highlight relevant issues in the organization/system. This is a cheap, fast-forward and not necessarily structured approach able to guide a “first-glance” to the system. An eventual not satisfying result might drive decision makers in investing resources for a more detailed analysis to quantify the gap and related action to build resilience according to ERMG.

- Level II: The second level of analysis is more detailed, and it is based on the assessment of how the FRAM functions and the interdependencies 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 to which level of maturity. Moreover, indications and insights on how to improve capabilities to manage the variability of functions’ output can be retrieved from the document. This level requires a more structured approach, where experts are engaged to assess how the variability of the functions and the potential for propagation along the interdependencies are addressed in accordance to the ERMG. An example of such kind of analysis is provided in Table 3, where a FRAM function is assessed looking at it actually works. The scale (Disagree-Agree) can vary according to the method of assessment quantification defined by the experts.

- **Level III:** The third level of analysis requires a resilience quantification exploiting data generated within the system (e.g. Smart City) in order to better details the gaps. At this level, functions performance and variability need to be quantified using real data aggregated through KPIs and methods to compose synthetic indicators. Even If the methods for KPI aggregation are given (see D6.4), the selection of which KPIs are relevant is up to the system actors/stakeholders. They need to reach a wide agreement on KPIs and data sources associated to the functions of the system before proceeding with the assessment.

In D6.4 is reported an example of resilience assessment and quantification whose results inform the decision makers about the existence of issues at fine grain level (function output).

Moreover, since 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, ERMG needs to be understood to enhance the variability dumping capacity of a downstream function.

Table 3: Function “Monitor Resource Availbility “ assessment in Level II.

Monitor Resource availability			
		Criteria	Source of function variability- Expert judgment based assessment (scale: Disagree-Agree 1-10)
General Recommendations			
1. Understanding the way in which interdependencies support the provision of critical resources. 2. Assessing the types and degrees of variability to which these are submitted in the face of pressures emanating from a system’s operational environment.		1. Level of understanding is mature enough	6
		2. Variability is known in nature and amplitude	3
Common Conditions Recommendations			
Availability of resources	1. 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. 2. Ensure the required budget for the system functioning and emergency situations. 3. Preview the needs for external operations and the related budget.	1. Variability is known in nature; in amplitude; both	5
		2. Financial control is linked to operational demands and needs	7
		3. Regular contact and coordination with stakeholders under all operational conditions	4

Monitor Resource availability

		Criteria	Source of function variability- Expert judgment based assessment (scale: Disagree-Agree 1-10)
Training & experience	1. Provision of conditions for the development of competencies with experience, as requisite for awareness on local conditions in the scope of overall operational understanding. 2. Ensure training for emergency situations in relation to the use of all resources.	1. Knowledge transfer processes exist; are mature; assessed	3
		2. Simulation and exercises and carried out and assessed	4
Quality of communication	1. Ensure conditions and resources for timely and accurate communication (both push and pull of information). 2. Use of reliable and purpose oriented (suitable for operational needs and conditions) communication technology, and of appropriate communication standards and language.	1. Information flows are known; monitored; assessed	3
		2. Human factors assessment of communication-based tasks	4
Human Computer Interaction & Operational Support	Adequate interaction with computer and other IT systems is critical for an effective use of information-based resources. This is frequently a fundamental support for the management and deployment of other types of resources.	Human factors assessment of IT-based tasks	4
Availability of procedures &	1. Procedures must take into account resource requirements and the conditions of access to such resources. 2. Planning for accessible infrastructures, taking into account	Review of procedures (regularity and identification of review needs) and link to	7

Monitor Resource availability

		Criteria	Source of function variability- Expert judgment based assessment (scale: Disagree-Agree 1-10)
plans	type and volume of resource availability and of resource requirements.	change control processes	
Conditions of work	Condition of work must be aligned with resource availability, so as to ensure an efficient and effective deployment of available resources.	Human factors assessment of work systems	6
Number of goals & conflict resolution	Monitoring the adequate allocation and deployment of resources is critical for the management of trade-offs between operational goals and needs in such a way that safety requirements are not compromised.	Human factors assessment of work systems	6
Available time & time pressure	Time is the utmost critical resource without which the efficient and safe use of other resources can be compromised. Efficient use of time strongly relies on adequate planning.	Adherence to planning and planning change control processes	6
Circadian rhythm & stress	Shift work or roster conditions may impose the need for more flexible management and deployment of resources. Monitoring resource availability may become more complex due to increased diversity and variability of factors to be taken into account.	Human factors assessment of work systems and flexible management of work schedules	6
Team collaboration quality	Monitoring changes in resource availability and re-assessing resource requirements as operational conditions change, requires close cooperation within and across work teams.	Team building and leadership are implemented and managed	7
Quality & support of the	Organisational conditions are fundamental for the quality of resource planning and deployment, in particular when re-	Organisation is purpose driven and aligned	5

Monitor Resource availability			
		Criteria	Source of function variability- Expert judgment based assessment (scale: Disagree-Agree 1-10)
organisation	planning of resource management is needed.	with operational needs and conditions	
Interdependencies Recommendations			
1. Monitoring resources generates information on resource allocation and the understanding of their flows, which represents 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. 2. ICT constitutes a fundamental resource for all operational and managerial activities. The failure of ICT services may critically compromise the operation continuity. The monitoring of these services should provide the ability to anticipate potential disruptions and the deployment of contingency resources (adaptive capacities). The same concerns exist for energy supply requiring anticipation as well and preview of contingency resources. 3. Keep updated information on the status and supply of critical resources constitutes a fundamental resource for the anticipation of potential needs for operational adjustments. 4. 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		1. Existence and maturity of feedback loops	5
		2. Redundancy of ICT systems and their independency	7
		3. Regularity of updates	7
		4. Means for both the push and the pull of information on resource availability	6

Monitor Resource availability		
	Criteria	Source of function variability- Expert judgment based assessment (scale: Disagree-Agree 1-10)
should be provided "on demand" and on pre-determined period. 5. 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.	5. Integration of information and communication needs into operational procedures	4
Limitations		
1. Difficulty in updating the information on resources use. 2. Difficulty in assessing the situation and mobilising the appropriate resources. 3. Difficulties resulting from limited financial resources. 4. Difficulties resulting from unavailability of technological assets resulting from breakdown or lack of energy. 5. Difficulties resulting from low human performance due to fatigue, inappropriate workload or sleep deprivation. 6. Difficulties resulting from insufficient personnel.	1. The limitations are well known	4
	2. There is a plan to address limitation in short-mid term	5

The synthesis of the gap analysis obtained through resilience quantification, is synthetized through the Resilience Analyses Grid (RAG) tool. The RAG is used as a basis for the representation of the quantification of each of the four fundamental resilience capacities, around which the ERMG are built. A low score in one or more of the 4 capacities may drive decision makers in allocating resource in a more precise way (improving a specific function or set of functions) to maximise the impact for resilience enhancement in the system.

At the end of the assessment, the reader will have an improved and very detailed awareness about the key resilience factors and critical operation aspects within the CI in which they operate, namely regarding the status of the CIs analysed and what to do at operational, tactical and strategic level to enhance the resilience of the system.

4 ERMG UPDATED

4.1 Anticipate

4.1.1 Develop Strategic Plan

Abstract

The function provides recommendation in relation to the management of strategic planning, that captures strategic goals/ objectives for supporting improve emergency preparedness and therefore increase resilience.

Background facts

Within this risk environment, the 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. Hence, the critical infrastructure mission area requires a focused national strategy and supporting plans and operational structures appropriately balancing resilience with risk-informed prevention, protection, and mitigations activities that allow us to manage the most serious risks.

Failure to recognize this basic distinction accounts for the frequent failure of such exercises, as does an excessive focus on technical detail, lack of suitable leadership, and perhaps most important, failure to align technology to institutional mission and priorities.

Strategic planning involves a structure or framework, a set of procedures (both formal and informal), and of course content, at all levels. 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, as Mintzberg suggests, 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 in daily operation.

General recommendations

Align the organizations internal operations with achieving resilience through:

- Attempting to gather board members and key employees together for planning by combining top-down and bottom-up approach
- 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 to achieving the goals 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, but rather constantly evolves to reflect information learned to make the best possible decisions
- Securing the continuity to deliver cash generation through sustainable organization growth resources in view of including that information in the Strategic Plan
- Producing quantitative measures in order to manage and check the strategic plan
- Establish an business-government partnership with critical infrastructure owners and operators
- Developing strategies considering:

- various contingency plans
- a risk management program
- completion of a formal business impact analysis
- backup data centre establishment costs
- disaster activation costs
- the support of the major equipment vendors,
- an insurance program.

Adopting the Strategic Environment Assessment (SEA) as an effective tool for introducing climate change considerations into development and planning processes. The Intergovernmental Panel on Climate Change (IPCC) concluded that consideration of climate change impacts at the planning stage is key to boosting adaptive capacity:

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 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.

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 risks assessment are recommended.

Common Conditions recommendations

1. *Availability of resources*

- Humans (labour) – skills/competence
  - *All member of the organization should be involved in the process of policy and vision definition*
  - *Consult with the relevant stakeholders*
- Data & Algorithm:
  - *Use of standard documentation for data and algorithms*
  - *Use of official concepts and definitions*
  - *Historic data*

2. *Training and experience*

- *Represent the content domains of 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 shareholders and (internal and external) 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*

N/R

5. *Availability of procedures and plans*

- *Planning process that recognizes distributed decision making requirements*
- *Clear definition of roles and responsibilities*
- *Creating an integrated strategic planning process to support the integrated framework*
- *Defining a strategic plan, coupled with review and maintenance of the strategy to ensure that they stay relevant over time*

6. *Conditions of work*

N/R

7. *Number of goals and conflict resolution*

- *Planning teams should be built taking into account the scale and timeline of the plan*

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*

N/R

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*

Interdependencies recommendations

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, the strategic planning should overcome such issues establishing and promoting an enabling management culture on self-protecting, so that appropriate adaptation action is undertaken.

Limitations

The adoption of strategic planning is matter of choice of the strategy managers, therefore there is a high impact of the human factor

Standardization of strategic planning is a very complex process

Questions

- How soon can a response been given?
- 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 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?

Examples

Computer Data Centre: managing a $27 million loss

In January 1997, water contaminated with rust was accidentally discharged from a gas suppression system into a 350m2 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 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.

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 2009http://managementhelp.org/strategicplanning/models.htm#one
- Standard BS65000 (2014)
- 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

4.1.2 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 product s/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.

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.*
- *Take into account the economic impact of system disruption*
- *Plan financial need for restoring access to transport of critical goods & commercial business as soon as possible*
- *To identify sources of brittleness in order to invest in their correction.*

- *Consider the role of business and economic development entities and include them in the pre-planning and recovery processes*
- *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 including private companies, governments, public companies…).*
- *Analyse capacity and financial resources possibly at institutional level e.g. county, city, state and at private lever e.g. private companies/operators.*
- *Define and agree on which part of recovery goes to public sector and which goes on private sector*
- *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.*
- *Analyse real finances use after a crisis in order to adapt procedures to be more efficient during next crisis*
- *Audit the results of planned financial management after the crisis and take the necessary conclusions to improve next emergency strategic plan*

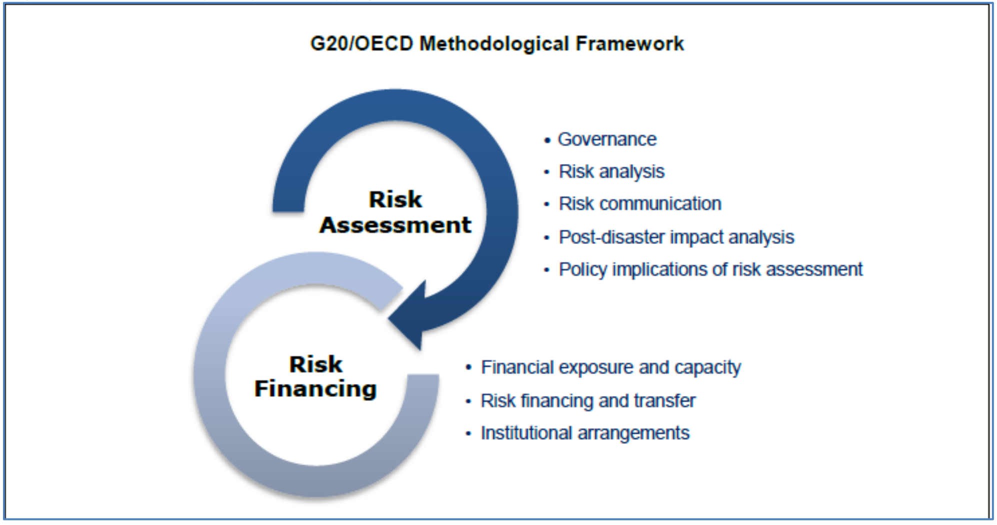

G20/OECD Methodological Framework
Risk Assessment
• Governance
• Risk analysis
• Risk communication
• Post-disaster impact analysis
• Policy implications of risk assessment
Risk Financing
• Financial exposure and capacity
• Risk financing and transfer
• Institutional arrangements

Figure 3: OECD Methodological framework

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.*

- o *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 in same place and reasonably far from crisis point.*
- o *Trained selected employees to manage financial affairs during emergency*
- o *Directory of names, telephone numbers, email, and alternative communication channels to reach them.*

- Budget
    - o *Manage each different structures concerned by the recovery to have a secured budget for emergency cases*
    - o *Control that each concerned structure cope with this requirement*
    - o *Secure the availability of budget reserves for emergency cases reserving a proper amount of financial assets that can be easily and quickly mobilised with a minimum loss*
    - o *Awareness of structures from which funds are available and how to recover them.*
    - o *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*
    - o *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.*
    - o *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.*
    - o *Reserve funds control during and after the crisis management, in order to avoid over payments needs. In any case funds should be ready to finance full recovery even if this means more payments than planned reserved.*
    - o *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:
    - o *Use of project management concept and models to collect and monitor financial data.*
    - o *Use data coming from all the systems collected to monitor and control the critical infrastructure during normal operation.*
    - o *Reliability, Availability, Maintainability and Safety (RAMS) practices and algorithms for calculating the target thresholds according to the maintenance objectives.*

  - *Collection and close monitor off 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 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 defunds 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 thee society.

5. *Availability of procedures and plans*

- Strategic financial plan in case or emergency ready.
- Operational plan ready.
- Fast availability of necessary resources.
- Procedures for financial resources obtention available and know by the involved financial managers of the crisis

- Training on procedures use for involved financial managers of the crisis at least once a year
- Common procedures available in public and private sectors in order to avoid time loss and/or mutual incomprehension

6. *Conditions of work*

- Emergency work during crisis.
- Ability to have all necessary involved persons of the structure back at work quickly even during break times
- Manage to have "on call" persons able to reach quickly the offices in case of emergency
- 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.
- Get a general agreement on the strategic plan at creation stage in order to avoid loss of time during emergency in case of disagreement
- 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*

N/R

10. *Team collaboration quality*

- Adherence to the principles of collaborative financial planning through the development of mutual benefit relations.
- Agree on collaborative financial planning between public and private entities before crisis
- Define mutual financial responsibilities
- 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 inn 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 ee 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 too 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 reallocation needs.
- The supply off 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 (CSRR); 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. CCSR 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.

Limitations

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

Questions

- How often is the match between resources available and resources 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 every day efficacy be (co-)financed?
- Is the match between resources available and resources needs assessed?
- Have you a priority rule to decide on the allocation of financial resources during the emergency?
- How do you measure performance, What kind 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?

Examples

a) 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, and environmental and governance criteria.

b) A Pre-Event Recovery Planning Guide for Transportation, TRRB report

NCHRP Report 7533: A Pre-Event Recovery Planning Guide for Transportation (The Guide) provides an overview of what can be done to pre pare 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 booth 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. Thee Guide will be of interest to transportation infrastructure owners/operators, transportation planners, and practitioners at the state and local levels.

c) 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

Sources

- 100 Resilience City
- http://wwww.100resilientccities.org
- Action Plan on Urban Mobility – State of Play
- http://ec.eeuropa.eu/transsport/themes/u rba n/urban__mobility/doc/appum_state_of_pplay. pdf
- A Pre-Event Recovery Planning Guide for Transportation, TRB report
- https://wwww.massport.coom/media/2662266/ Report_AA-Pre-Event-Reecovery-PlanninngGuide-for-Transportationn-2013.pdf
- Financial Protection Against Natural Disasters – World Bank report
- https://olcc.worldbank.orgg/sites/default/ffiles/ Financial%20Protection n%20Against%220Natural%20Disasters.pdf
- Disaster Risk Financing in APPEC Economieshttps://www.ooecd.org/daf/finn/insurance/OOECD_APEC_DDisasterRiskFinnanci ng.pdf
- FEMA. (22011). *National disaster recovery framework: Strengthening disaster recovery for the nation*. https://wwww.fema.gov/pddf/recoveryframmew ork/ndrf.pdf (Mar. 24, 20016)
- Queensland Government (20013). Queensland 2013 Flood Recovery Plan for the events of January– February 2013.
- http://wwww.statedeveloppment.qld.gov.aau/re sources/pplan/local-goveernment/lg-flooddrecovery--plan.pdf
- United States Department of Homeland Security. (2008). *National Response Framework*.
- http://wwww.fema.gov/pdff/emergency/nrrf/nrf -core.pdff (Mar. 24, 20166)
- Organizational resilience: the relation with risk related corporate strategies – Ernst&Yaang report – Australian Government
- Emergency Financial First Aid Kit (EFFFAK) https://wwww.ready.gov/fiinancialprepareddness
- Recovery Management:Transportation Industry Stakeholders https://www.transportation.gov/disaster-recovery/guidance/stakeholders
- Anticipate demands in crisis response https://h2020darwin.eu/wiki/page/Anticipate_demands_in_crisis_response
- Improver project Deliverable 5.1 Framework for implementation of resilience concepts to Critical Infrastructure http://improverproject.eu/2018/02/16/deliverable-5-1-framework-for-implementation-of-resilience-concepts-to-critical-infrastructure/

4.1.3 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 number 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 of risk (i.e. industrial safety, occupational safety and health, security, economic and financial risk, etc.). This has resulted in a highly fragmented approach to risk assessment, which is reflected at organisational, normative and legislative 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:

- *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 are adaptive and 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, namely subjective assessment tools, may be used.

- Human (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:
  - *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 organisations and public institutions to support risk assessment.*

2. Training and experience

- *Subject matter experts should be consulted in order to validate hazard identification and risk estimation.*
- *Experienced local staff may also provide useful input in terms of risk perceptions and operational processes insight.*

3. Quality of communication

Ensure the accurate and timely communication of risk assessment outcome to all relevant actors in the organisation (e.g. decision makers, operators, etc.).

4. Human Computer Interaction and operational support

IT systems are increasingly important for the effective reporting of hazards and risks, and the support of decision-making, for instance when reviewing safety cases.

5. Availability of procedures and plans

- *Risk Assessment activities must be contemplated and integrated in business and organisational process description, as opposed to independent or "stand-alone" activities.*
- *In addition to periodical needs, operation, business and 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.*

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

Monitoring and assessing human factors under shift work or roster conditions tends to be more complex. Monitoring and assessment conditions are much more dynamic and diverse.

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 organisation

- *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.*

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 should 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.

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. Limitations of applicability, reliability, accuracy and validity of assessment tools should also be taken into account.

Questions

- What tools are suitable for what assessment needs? (qualitative, quantitative)
- When should assessments be carried out (continuously, regularly)?
- Is assessment supporting the definition of risk management priorities?
- For which events is there a response ready?
- How was the list of events created and why is the list of events revised?
- What is the threshold of response? (Rate of change)
- How soon can a response be given?
- How long can it be sustained? (Size of buffers)
- 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?
- What are the delays between assessment and the implementation of action plans?

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

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/

4.1.4 Training staff

Abstract

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

Background facts

Training comprises all activities deliberately performed to enhance knowledge, skills, and abilities of members of the organisation, 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 the measurement method and the cut off-criterion used to evaluate if a person has acquired the desired enhanced knowledge, skills, and abilities.

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.

Training is a key element to ensure resilience. Ensuring suitable local adaptive capacities, as well as a sufficient understanding and awareness of operational conditions require staff with the necessary knowledge and skills. In emergency situations, actors from different organizations need to collaborate efficiently in order to maintain or restore the operations of a critical infrastructure. Collective exercises, such as emergency simulations, are important to ensure effective cooperation. However, the most important training happens within the organizations. 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 the respective 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 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 which ensures 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 what consequences delays in refreshment have. For example, the individual staff member might be excluded from service operations.*
- *Training activities should be evaluated by measuring success criteria, assessing to which extent the trainees acquired the necessary skills and contents. This refers to tests, such as theoretical and practical exams, or outcomes of exercises.*
- *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 reflect 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.*
   - *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 coordination and cooperation among shareholders and (internal and external) stakeholders/experts.*
- *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 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?*

8. Available time and time pressure

- *Schedule trainings according to predicted demands: perform trainings outside of demand peaks, such as tourist seasons.*

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, for example in management games designed for crisis management teams.*

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). Adequate techniques to achieve this are:*
    - *Role-playing;*
    - *Scenario-based training;*
    - *Training for role improvisation.*

Interdependencies recommendations

The management and implementation of training needs should be grounded on a close cooperation and coordination between HR and the other involved 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. Thus, training staff as a system function may develop strong interdependencies with most other system functions.

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.

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?

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*
- *Drills and exercises*
- *E-learning and serious gaming*

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.

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 stable over longer periods of time.

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
- ISO 22301:2012

4.1.5 Coordinate Service delivery

Abstract

This guideline aims to provide recommendation for the effective coordination of service delivery in a CI. The role of Delivery Mangers is highlighted as well as the need to have an holistic and systemic approach to service delivery. All stakeholders should be aware about procedures and involved into information exchange. 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.

General recommendations

- *Adopting a holistic Service Delivery Framework aimed as a set of principles, standards, policies and constraints to be used to guide the design, development, deployment, operation and retirement of services delivered by a service provider with a view to offering a consistent service experience to a specific user community in a specific business context.*
- *Addressing the organizational business goals while keeping a systemic view of service operation implications.*
- *Specific service providers should follow compatible operation, maintenance and emergency procedures.*
- *Maintaining control on the entire supply chain in order to immediately react and adapt the delivery of service according to changing conditions in resource availability (e.g. grateful degradation strategy of the service).*

- *Understanding infrastructure network criticalities (vulnerabilities, safety boundaries, critical nodes, etc.) and interdependencies.*
- *Adopting measures from existing reporting processes will ensure the objectives identified in the Coordination Plan are regularly assessed for relevancy and managed as part of an on-going and consistent performance monitoring system.*
- *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.*
- *Adopting ICT and evidence driven tools 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.*
- *Implementing a de-escalation strategy where transition is managed in stages and context-aware priorities.*
- *Establish a permanent dialogue with the community served in order to adapt the service on the actual user needs in emergency and in daily operations*
- *Adopting a data and knowledge sharing policy with public administrations, not only in big emergency but also in daily operations, in order to allow decision makers in taking informed decisions. This might require solving eventual security, business and privacy constrains in advance.*

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, person-oriented leadership is needed*
  - ***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. Capacity to think complexity.*
  - ***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. Capacity to create win-win outcomes for organisations, projects, or funding decision.*

- Budget:

Being aware on which is the adequate budget to carry out operation 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:

Use a mix of methods (social media analysis, online/offline surveys, etc.) for feedback collections to adjust and coordinate service delivery.
Exploit all kind of data and information generated by the monitoring functions to operate and apply countermeasures to dampen service performance viability within a controlled and acceptable range.

- ICT resources:
  - *State of the art and reliable technical equipment and ICT infrastructure should be used, including a resilient internet network covering all areas of service delivery.*
  - *Continuous functionality check of the equipment should be planned according to pre-estimated reliability analysis*
  - *Periodic stress test of the system should be planned according to past and predicted operational scenarios in order to gain understanding about the actual capacity to respond to known and unknown conditions*
  - *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.

3. Quality of communication

- *Clearly define all potential communication channels among service providers.*
- *Use standardized communication tools (templates) and protocols.*
- *Establish an effective and reliable communication between the actors involved in the supply chain, in 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.
Control rooms for actuation should be designed according to Human Factor standards and best practices (e.g. High Velocity Human Factors). Respect to monitoring, the actuation requires a strong and reliable control loop and immediate feedback. Any issues in HCI may generate a cause-effect misunderstanding leading the operator towards wrong decisions.

5. Availability of procedures and plans

Ensure that clear operation plans and emergency procedures and plans are available (or easily accessible) to all actors involved in the service and first responders.

6. Conditions of work

Service delivery coordination is a demanding task in particular in terms of mental workload. In fact, the environment in which coordination takes place may be really dense of information and signals that needs to be continuously processed for achieving daily operational goals. Thus a well organised tournament and operator backup/redundancy is needed.

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 service performance milestones to cope with quality safety and security requirements.

9. Circadian rhythm and stress

Ensure compatible nightshifts for staff of various service operators while not reducing experise

10. Team collaboration quality

- *Delivery manager should have team building competences.*
- *Establish mutual performance monitoring procedures.*
- *An effective collaboration between Delivery Manager and operators supporting service delivery should be established and maintained. Any issue that might prevent a timely, truthful and complete communication should be considered as an high level risk and then treated with the related risk-mitigation countermeasures.*

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.*

Interdependencies recommendations

The capacity of the function to operate as intended is strongly dependent from the condition of both physical and cyber infrastructure. Physical infrastructure should be both regularly maintained and monitored to track operation dynamics and to detect unusual circumstances. This is one of the aspects for which thorough and continuous coordination with infrastructure users and stakeholders becomes critical.

Maintenance procedures for physical/cyber infrastructure should take into account service delivery data and trends, 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.*

Limitations

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

Questions

- Which are the stakeholders that should be involved and how?
- How the roles and responsibilities are clearly defined?
- How the plan, processes and procedures are defined, established and communicated?
- 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
- How the organization guarantees service flexibility and adaptability?
- How can the organization involve its customers/citizens to design adaptation strategies aimed at improving the overall perceived level of safety and security

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.

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

4.1.6 Manage awareness & user behavior

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.

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), or citizens at large (for energy) 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 devices**, 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 the message, the media and channels to use, the expected results and the 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 such as citizens' organisations, businesses, academies, NGOs, as*

well as 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**: 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 relevant safety behaviours have not been adopted.*
- ***Training**: Awareness can also be raised through dedicated training activities for the population. In effective emergency management programs, facility managers conduct training and drills to ensure that people understand the program's elements and how they are to respond in 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 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 more people, reduce the costs and increase the effectiveness, solutions such as **game-based approaches delivered through smart mobile devices should be considered**. Tier 3 training — conducting live drills by first responders and civil protection — is the most effective method, but if 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 effectively raise their awareness.*
- ***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 designed around the **addressability concept named "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 timely and appropriately towards reducing the probability 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 feasible kind of communication infrastructure (Wi-Fi, LTE/4G, Bluetooth, capillary network, Delay Tolerant network, etc.).*
- ***Personalized or community-based communications should support each phase of the resilience cycle**: preparation, absorption, recovery and adaptation. Messages to be sent can be pre-scripted, based on the risk assessment, or written just-in-time. It is recommended to customize messages by context (e.g., position, current activity) or user profile (e.g., special needs). In any case, plans and procedures for the delivery of pre-scripted messages need to be aligned with the predefined mitigation strategies and the ongoing emergency response activities.*
- *At individual user request, provide 1:1 "how to "advice (e.g., contacting local authorities and other organizations, as well as providing advice on how to protect themselves and their property against future events)*

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence

- *Experts in communication and social innovation should manage the long-term campaigns on awareness and user behaviour.*
- *Operators with skills in emergency management and evacuation behaviour of large groups should manage and orient user behaviour during the emergency.*
- *Communicative and empathic skills are also needed 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 short questionnaires or interviews. It is recommendable to apply tools capable to reduce biases, such as social media analysis or scores from game-based training.

- ICT infrastructure:

Computer Aided Dispatch*: CAD systems are an essential component of public safety operations. They provide deployment and tracking of resources for efficient responses to events. CAD systems are not restricted to dispatching professionals (e.g., police, ambulance services) but users or clients, too. Through their mobile devices, users can be localized and contacted in real-time. CAD systems should be designed to process standardised messages using the Common Alerting Protocol (CAP) and include an escalation strategy. Since individual humans may always fail to be contacted, it has to be ensured that someone acknowledges the alert and handles the recovery. Manage or filter input from end users to avoid administrators/operators being spammed with irrelevant information. Use a messaging system that is compatible with multiple contact methods (e-mails, mobile devices, signalling panels, etc.).*

2. Training and experience

- *Evaluate the entire communication process by researching if the desired effects were achieved.*
- *Collect feedback from employees and users for improving the communication.*
- *Foster specific expertise in risk management and communication*
- *Operators devoted to manage communication during the emergency need to be receive a special training to cope with stress and to deliver under pressure.*

3. Quality of communication

- *Use predefined messages or message types should in anticipated situations, such as different types of emergencies, in order to ensure the content quality of such ad-hoc messages.*
- *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

The responsible staff for ad-hoc communications needs 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 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

The communication team should be composed of experts in different fields, thus it is necessary to clearly match the competencies with the duties, in order to avoid overlaps or mismatching.

11. Quality and support of the organization

Planning an awareness raising campaign as well as the communication for emergency cases are special and critical activities that require a specific commitment by the organization. The dynamics (timing, language, content, etc.) of such communications differ greatly from classical institutional communication, marketing or advertising. It is recommended to create a dedicated unit devoted to manage communication during critical events within the organization.

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 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 staff with a direct access to monitoring data, such as movement of users through the infrastructure.

In case the connection between functions that provide inputs for the function 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 could make things worse.

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.

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?

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.

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

4.1.7 Develop/update procedure

Abstract

This function is dealing with the management of the operating 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 in case of emergency, according to risk assessment and ex-post event analysis (learning) in a way to also provide re-usable data and be re-applicable.

Background facts

The purpose of Standard Operating Procedures (SOP) 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 clear key procedures at critical moments in emergency preparedness and response, resulting in increased predictability, timeliness and accountability of the interventions in crisis contexts. This applies to both regular and emergency personnel.

For example, 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.

General recommendations

Some general considerations should be taken into account when developing/ updating procedures in order to guarantee the resilience of a syste,:

- Identify clear goals and objectives for the emergency response procedures by defining what exactly the addressed emergency response team should do (e.g. evacuate, provide first aid)
- Review hazard or threat scenarios identified during the risk assessment
- Assess the availability and capabilities of resources for incident stabilization including people, systems and equipment available within the addressed organisation and from external sources
- Confront with all involved shareholders 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.
- Determine if there are any regulations pertaining to emergency procedures at the addressed facility; address applicable regulations in the plan
- Define protective actions for life safety (evacuation, shelter, shelter-in-place, lockdown)
- Develop hazard and threat-specific emergency procedures using guidance from existing material
- Coordinate emergency planning with public emergency services to stabilize incidents involving the hazards at the addressed facility
- Train personnel so they can fulfil their roles and responsibilities
- Facilitate exercises to practice the operational procedures defined in the emergency response plan

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence
  - *The operational procedures should be defined by specialized personnel*

- *The procedures should be very clear and specific*
- *The procedures should also identify the emergency response team if not identified elsewhere*

- Budget:

Budget planning should account for the required time in order to permit the development, the training and testing of the operational procedures.

- Data & Algorithm:
  - *Use official and standardized formats to describe the emergency response procedures 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 subject of training and feedback should be collected during training phase.

3. Quality of communication

Test the different communication channels and tools in order to guarantee their proper use for warning users to take protective actions and provide them with information related to the operational procedures. The communications capabilities also enable members of the emergency response team to communicate with each other and with users.

4. Human Computer Interaction and operational support

N/A

5. Availability of procedures and plans

This includes the availability of communication channels and precise clear phrasing within the operational procedures.

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*
   - *The operational procedures should provide specific information for special categories of users*
   - *The operational procedures should be concise and clear*

8. Available time and time pressure

   The operational procedures should be specific, clear and succinct and should be validated in real-life environments.

9. Circadian rhythm and stress

N/A

10. Team collaboration quality

Roles should be clearly identified when defining procedures in order to enable high quality team collaboration and efficiency.

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

The function "Perform risk assessment" provides the factual basis for activities proposed in the strategy portion of a hazard mitigation plan and is providing the basis for an efficient procedure process definition. 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 self-learning.

Limitations

Limitations related to complexity and non-applicability
Limitations related to non-clarity
Limitations related to a too-generic character

Questions

- What are the dangers/risks that might be encountered?
- What are the dangers/risks that might be encountered?
- For which events is there a response ready?
- How was the list of events created?
- When and why is the list of events revised?
- How was the type of response determined?
- How is the readiness verified or maintained?
- 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?
- 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?
- Is there a classification system for emergency incidents? (e.g. bomb attack, firefighting, train evacuation, gas attack)
- [How to decide …] which internal feedback processes are necessary to ensure all risks are known?

- 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 can the organization - additionally to maintaining its service - contribute to the resilience of other key services / society in general?
- What are the elements of the infrastructure that are more critical? How can they be identified and classified and how can improvement be achieved in terms of their resilience? 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)
- What are the dangers/risks that might be encountered?
- Are you aware of the vulnerabilities of your infrastructure?
- How does the organization decide which training measures it should provide, when, how and to whom?
- What are the everyday routines that should be established in the functionality of the infrastructure to enhance resilience?
- Is there a systematic list of emergency rules and procedures for response and abatement?
- Are there any emergency training and procedures?
- Are good practices and existing gaps classified in a chronological order? (pre-incident, during-incident and post-incident)
- Are good practices and existing gaps categorised according to type? (technological, organisational, administrative, policies and standards)

Examples

Florida Law: Comprehensive Emergency Management Plan

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.

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/homesec/RL32520.pdf
- http://emergency.cdc.gov/planning/

4.1.8 Manage human resources

Abstract

The guideline is devoted to providing 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

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 should 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. Its sub-functions include:

- developing human resources and human capital strategies and plans;
- establishing human resources policy and practices;
- managing current and future workforce competencies according to organization goals;
- developing workforce and succession plans;
- managing the human resources budget;
- providing human resources and human capital consultative support;
- 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 employee retrenchment policies;
- monitoring employment costs and productivity levels;
- training and advising other managers in personnel and workplace relations matters.
- Providing to employees a clear and consistent communication about performance expectations, rating, rewarding and holding employees accountable for achieving specific business goals, creating innovation and supporting continuous improvement

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

- Personnel complexity:
    - Different ranks
    - Different experience levels

  - Different skill and competencies
- No standard approaches for HRM systems exists
- The lack of data
- Non-harmonized processes
- Skill/competencies classification problems
- Insufficient synchronization
- Skill and competencies mismatch
- Lack of common language based on occupational areas
- Usually, the selection is up to a hiring manager, who often has functional and departmental skills in his area, but lacks of human resources management experteees.

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.*
- *Implement a Knowledge Transfer Strategy: 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*
  9. *Workforce management*
  10. *HR Manager skill*
- *Experienced recruiters should take responsibility for preparing managers and members of the recruitment panel for interviews with candidates. Recruiters from the human resources department have the expertise to provide the kind of guidance that hiring managers need to hone their ability to make informed recruitment decisions.*

- *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 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 manage information about knowledge, skills and abilities (KSAs), interests General Work Activities, (GWAs) and work context. 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*

- *Financial plan*

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 intent, goals, 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 and Methods: The technical team should develop a catalogue that delineates the various models with their associated methods and methodologies that are currently used in their HRM. The group shall be responsible for categorising models and methods.*
- *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 research findings to develop a process and a set of policies focused to protect assets and operations while dealing with a potential hostile insider.*

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.

Limitations

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.

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?
- Can adjustments be made to the working hours or patterns?

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.

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.

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/jacobmorgan/2016/03/03/deloittes-top-10-human-capital-trends-for-2016/#7da81071bf48
- DHS – NIAC Insider Threats to Critical Infrastructure Study (2008)
- 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.
- 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

4.1.9 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 teamwork 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

The 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.

Additionally, the 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. The GIS-based information tools allow disaster managers 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, response measures GIS-based technology solutions, and remote sensing should be extensively used in disaster management activities. During any emergency, 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 that can be effectively used for disaster warning purposes are the Telephone (Fixed and Mobile), Short Message Service (SMS), Cell Broadcasting and Satellite Radio. The International Telecommunication Union (ITU) has identified various radio communication media that can be used in disaster-related situations like the Internet/Email, Amateur and Community Radio and 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. The 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 into account.

The ICT systems 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, render ability, authenticity, discoverability, and 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 Conditions recommendations

1. *Availability of resources*

Information stored in Databases referring to a) System operation performance, resources and capacities, b) Disaster history for trend & pattern analysis, c) Disaster management plan, d) Human & material response resources, e) Trained human resources, f) Satellites (whereabouts, size etc.), g) Demographic information, h) Hazard mapping & vulnerability Assessment. Additionally, the easy access to GIS (Geographical Information System) needs to be guaranteed based information system. Another resource of information can be 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. The Technical Equipment such as Computers, Servers, Cameras, Wi-Fi, Sensors (Touch/Proximity, fire/flood/tsunami/earthquake detection sensors), Sensor Networks, GPS, Wearables, Bluetooth as well as alternative communications (e.g. ad-hoc networks, satellite radio, sat-phones etc.) to cope with emergency cases needs to operate 24/7.The Electrical energy for supplying this ICT resources have to be guaranteed.

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 is a\ necessary phase, in parallel with regular test exercises for the technical experts. Additionally, the education and creating awareness in the population so that they may respond with the appropriate action should be addressed.

3. *Quality of communication*

Guarantee the quality and reliability of the communications (referring to the technological aspects) and to 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 that is easily manageable by people with special needs. Moreover, an 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 emergencies, regarding all the possible difficulties, have to be developed and plans should take into account all the needed ICT resources, in parallel with detailed reference to the procedures that have to be followed.

6. *Conditions of work*

The working environment needs to be friendly and the 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 Specific, Measureable, Actionable, Relevant, and Time-framed. The roles and responsibilities of each team member should be clearly define and not overlapped in order to avoid conflicts. Moreover, 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. Finally, specific rules/principles should be defined in conjunction with a hierarchical working structure in order to address possible conflicts.

Interdependencies recommendations

In order to monitor the operation of the critical infrastructure the ICT equipment and services have to be set/installed. In addition, the definition of the procedures has to be performed considering the requirements of the ICT infrastructure. Moreover, we must consider that, the coordination of emergency actions is based on the quality and the readiness of the ICT resources. Additionally, the supply resources availability should be monitored in order to ensure ICT proper operation. In case of a detected problem, immediate action should be taken based on the backup plan in order to reduce any negative consequences. Finally, user generated feedback should be considered in a timely manner in order to ensure proper and efficient ICT operation.

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

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.
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. In addition, 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.

CRAMSS
CRAMSS aims to support reference actors at the UTS, such as infrastructure managers, with their decision-making under both, standard operating conditions and emergency conditions. The CRAMSS displays information from different sources or independently running web-applications, together with the results of the decision support

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

4.1.10 Maintain physical/cyber infrastructure

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.

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 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.

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 water from a tank when it fills up, or to initiate an emergency shutdown of an electrical substation.*
- *Maintenance activities need to be organized to satisfy the following criteria:*
    - Verify the presence of requirements relevant to maintenance in contract/procurement documents
    - The allocation of resources to maintenance is coherent with the size of the infrastructure and maintenance policy
    - Maintenance activities are revised periodically to take into account new discovered events and requirements
    - To be more responsive to unforeseen issues, adopt from the beginning (resilient by design) prognostic models in order to perform "predictive maintenance"

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*
  - *Usage of Big Data/Machine Learning for predictive maintenance*

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.*

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.

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.*

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

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)?

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 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

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

4.2 Monitor

4.2.1 Monitor Safety and Security

Abstract

This Guideline refers to the issues of monitoring safety and security of 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.

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 relevance 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.

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 contex- 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 its proper functioning.*

  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 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 guaranteeing the timeliness, accuracy and secure handling of data.*

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.

- o *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.*
- o *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, 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 "Manage ICT resources" function 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 on Coordinate emergency actions function and the overall 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 be consulted in defining the monitoring plan.*
- *The requirements of Service delivery should be considered 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.*

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 be defined, including details on 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 those in measuring performance of external entities against contractual instruments

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?

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 surveillancehttp://www.swri.org/4org/d10/isd/surveil/

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

4.2.2 Monitor Operations

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.

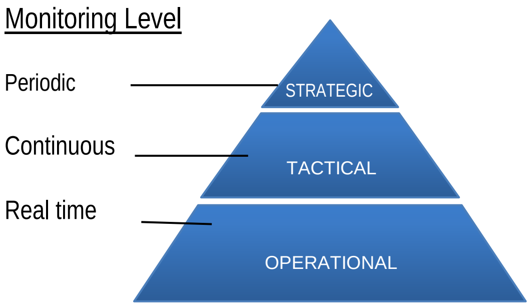
Background facts

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 the Resilience Management Level:



Resilience Management Levels

- *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, is applied frequently to specified key indicators which enables information on plan implementation to be collected often (e.g. at weekly intervals). Continuous monitoring provides to a CI manager the means of applying close control over operations enabling frequent comparisons to be made between planned programmes and inputs of resources with actual achievements and inputs.*

- *Real time Monitoring: Needed at operational level, 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.

Common Conditions Recommendations

1.-Availability of resources

- Humans (labour) – skills/competence
  - *Human resource availability in monitoring 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 and competencies. In order to mitigate such dependencies, a* **Human Resource Replacement Plan** *(HRRP) where human resources with similar skills are known and involved in a replacement plan in case of emergency.*

- ICT infrastructure:

Monitoring infrastructure should:

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

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 Open 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.*

- 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.*
  - *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 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, creative 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, 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.*

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. Thus it is necessary to consider such tradeoff carefully.*

- ***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 dynamics, 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.

Limitations

Improving an 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.

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?
- 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?

Examples

In Km4City Ecosystem http://www.km4city.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.

Sources

- ISO/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.
- 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
- 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)
- Seddon, JW: Freedom from Command and Control: A better Way to make the Work Work 2003, Vanguard Consulting Limited
- Common Alert Protocol-CAP format
- http://www.scidev.net/global/communication/feature/early-warning-of-disasters-facts-and-figures-1.html

4.2.3 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 re-plan and adjust to changes in the operational environment.

General recommendations

A sociotechnical system goes much beyond the description of its human, technological and organisational resources. Understanding the interdependencies that ensure system functioning and operation is fundamental for the safe, effective and efficient allocation and deployment of resources. This understanding should seek:

- The way in which 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.

Monitoring resources availability implies that operational variability of the system must be considered and managed in order to ensure the system functioning. The resources and system capacities required to manage and cope with operational variability must also be taken into account.

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence

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.*
- Data & Algorithm:

N/A

2. Training and experience

- *Provision of conditions for the development of competencies with experience, as requisite for awareness on local conditions in the scope of overall operational understanding.*
- *Ensure training for emergency situations in relation to the use of all resources.*

3 Quality of communication

Information constitutes one of the most critical resources, but it is also a very dynamic and uncertain one. The efficient and safe use of this resource is strongly reliant on the accuracy and quality of communications. The use of reliable and purpose oriented (suitable for operational needs and conditions) communication technology, and of appropriate communication standards and language are critical.

4 Human Computer Interaction and operational support

IT technologies are a critical resource, based which information as an equally critical resource is processed and deployed. Together IT technology and information support the majority of operational decision-making in every industry sector.

5. Availability of procedures and plans

Procedures and planning should support local staff in the efficient and safe allocation of available resources, whilst ensuring the necessary coordination with stakeholders across operational interdependencies. They should also support the ability to efficiently and safely adjust to unanticipated changes in operational conditions, wither through the activation of contingency plans or through the re-planning and re-allocation of resources.

6. Conditions of work

Management of resource needs is crucial for adequate conditions of work. Human resource needs are particular variable and therefore likely to require additional planning and management efforts.

7. Number of goals and conflict resolution

Resource scarcity is at the source of conflicting and competing goals. Monitoring the adequate allocation and deployment of resources is critical for the management of trade-offs between operational goals and needs in such a way that safety requirements are not compromised.

8. Available time and time pressure

Time is a unique type of resource and one without which no decision or operation may be carried out. It also has the unique characteristic that even when it is not being used (for any given operational purpose), it is inevitably under consumption. Thus, time pressure is virtually unavoidable but must nevertheless, be adequately managed. Planning must account for suitable timeframes for all operational needs and should integrate time buffers in line with "operation deliverability risks".

9. Circadian rhythm and stress

- *Shift work or roster conditions may impose the need for more flexible management and deployment of resources. Monitoring resource availability may become more complex due to increased diversity and variability of factors to be taken into account.*
- *Circadian rhythm asynchrony has important effects in performance, which are related to decrements in vigilance. Human resource needs should be regularly and closely monitored to identify any potential additional needs emerging in relation to such phenomena.*
- *Uncertainty in relation to the availability of resources significantly contributes to increased stress, particularly in situations where important variability of resource flows is to be expected. Suitable resource monitoring can contribute to stress management.*

10. Team collaboration quality

Efficient team work can compensate for many different situations emerging from resource shortage or outage.

The effectiveness of nay team strategies in this sense is strongly reliant on any anticipation capabilities in relation to any potential variations in terms of resource availability. Providing teams with the means to monitor the processes through which access to their critical resources is secured can considerably improve the success of team collaboration.

11. Quality and support of the organization
    Resource variability, shortages and outages imposes the need for trade-offs between business and operation priorities. Avoiding any (negative) safety and performance impacts of such trade-offs should be grounded on solid organisational support to the coordination and cooperation between multiple local needs.

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.

Limitations

- 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.
- Difficulties resulting from errors resulting from poor communication or lack of training.

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?

Examples

- 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).)

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.

4.2.4 Monitor user generated feedback

Abstract

This function provides recommendation for implementing a human/social sensing approach to support a more effective and efficient resilience management of critical infrastructures.

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 applied as an adjustment to potential or verified changes in operation (i.e. service disruptions, among others).

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).

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. The widespread of mobile technologies – more specifically 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.

In case the communication network is not affected by the disruptive event, social/human sensing is crucial to infer useful information which cannot be otherwise acquired, for instance information about the entity of the disruptive 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 an adverse event (e.g. 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 customers 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, with the aim to produce useful support to overall service operations and management.

User generated data crawled should be analysed and processed to extract, collect and monitor relevant information about an event and, more generally, about the perceived quality of the service. This further source of information can be used to improve effectiveness and efficiency of the service, to coordinate the emergency respond, and to support a quick recovery to the normality.

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 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.

Common Conditions Recommendations

1. Availability of resources

- Humans (labor) – skills/competence

Personnel in charge to monitor and manage communication channels has 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, 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, such as time-series and trend analysis, Natural Language Processing (NLP) 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

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 functions, in terms of computational capacity, system reliability and network connectivity, should be managed. More precisely, two strategies should be followed: 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 considered. Indeed, 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 during critical events, even in absence of the support of the ICT system, should be employed for this function.

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 to minimize – but not exclude – misleading information.

Questions

- Which are the media (specifically, social media) that the organization should monitor to estimate the impact of an adverse event on the “mood” of customers?
- For which target groups / persons / stakeholders should training be provided?
- Which (social) media should be used by the organization to provide information/communication with the aim to support a quick return to the normality?
- Which are the most effective channels 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?

Examples

The Federal Emergency Management Agency (FEMA) wrote in its 2013 National Preparedness report 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.

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.

4.3 Respond

4.3.1 Coordinate emergency actions

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.

Background facts

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

An eco-system (a social system within a given environment) can be very keen to collaborate with the emergency coordination activity performed by the Responsible Body in charge of this task. But it can also be dangerously weakened by chronic stresses, as overtaxed or inefficient public transportation system, poor air quality, water or other resource shortages.

Typical emergency actions covered under this Function are:

- Response to an earthquake
- Response to a flooding
- Response to a cloudburst (water bomb)
- Response to a fire
- Response to a terrorist attack
- Response to a mass-casualty accident

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 human resources under the command of a strong authority.*
- *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

1. Availability of resources

- Humans (labour) – skills/competence
  - *Members of the emergency coordination should be people who profoundly know the territory, the locals, the specific 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 context.*
  - *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, religious centres, 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.*

- 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, 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.*

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 crucial factor that must be properly managed and addressed.*
- *Operational procedures need to clearly specify who is in charge of communicating what, to whom, when, and on which channels.*
- *Once the contents of communication have been decided, they must be delivered in real time.*
- *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.*
- *Multiple and redundant channels need to be activated, while paying attention to maintain the uniqueness of the message, avoiding semantic ambiguity, technical jargons, badly-directed communication.*
- *A particular attention must be paid about quantity and frequency of messages, to maintain low signal-to-noise ratio.*
- *Simulations should be implemented periodically also to tune and optimize communications and messages during crisis response.*

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 each specific decision-maker.*
- *While respecting privacy and security standards, a single sign-on system must be provided across different communication and information systems, to avoid operators the stress of passing through multiple login procedures.*

5 - Availability of procedures and plans

- *Preparedness implies planning carried at every organizational level. 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 civil protection competence spheres: local, provincial, regional, and wider. 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 -.1: Planning techniques
SF -.2: Health, social and veterinary assistance
SF -.3: Media and information
SF -.4: Volunteers
SF -.5: Means and materials
SF -.6: Transportation and viability
SF -.7: TLC
SF -.8: Essential services
SF -.9: Damage assessment
SF -.10: Operative structures
SF -.11: Local authorities
SF -.12: Dangerous materials
SF -.13: Assistance to the population
SF -.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 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, reported, and possibly solved, in improved, future realease of operational procedures.*

8 - Available time and time pressure

- *Simulation and training programs need to imply time pressure issues*

- *Decision makers need to be trained to solve issues studying cases history, and possibly making lateral thinking exercises, and exploring lean thinking good practices, in order to spare time and resources (which are by definition scarce in time of hardness).*
- *Risk assessment and critical system functions need to take into account the known or predictable time after which the damage and impact of an unavailable resource is going to worsen (e.g. power supply downtime, breathing air left, etc.).*

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).*
- *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 effective knowledge of the physical infrastructure and the ground.
Moreover, monitoring operation and addressing the service delivery are also other important aspects to which this function is related.
In addition, it is dramatically related to human behaviour, to the reaction instinct that humans and workers activate during an emergency.
Human factors need to be considered, related to stress management, training, relational ability, readiness, and empathy with people being rescued.
In conclusion, managing awareness and proper collection of user generated feedback are also key aspects to take into account.

Limitations

- 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.

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 abatement?
- 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?

Examples

In the European experience, one could see the 1966 Florence flood, as a changing mindset 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. 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.

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 useful 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://firenzedigitale.i
- The RESOLUTE project 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)
- 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/$File/2015_C_00008.pdf (RESOLUTE_ERMG_v3.docx)
- Flood Emergency Plan in the City of Florence
- http://dominoweb.comune.fi.it/OdeProduzione/FIODEWeb2.nsf/AttiWEB/F6D8CF80EB3EF0E7C1257E6800805F19/$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

4.3.2 Restore/Repair operations

Abstract

The function pertains to rebuilding and repairing services and procedures Goal of this function is the restoration of normal community activities that were disrupted following a disastrous incident. It involves a diversity of persons and equipment and encompasses multiple activities, some implemented sequentially and others implemented simultaneously. To achieve it, availability of resources and planning for short-term recovery and long-term reconstruction are necessary.This function is also highly depending and connected to the former restoring of physical infrastructures.

Background facts

Severe incident impacts comprise physical and social impacts. Physical impacts can be subdivided in impacts on infrastructure as well as on services and processes. Literature and media diffusion about service/process impacts are not as wide as the ones about infrastructures. This is partly due to the different scale with which both problems are perceived or caused. A small-scale disruption could not have a significant impact on infrastructures but can block some services.

Damage of infrastructures may cause direct service and process-related problems. However, restoring infrastructures is not always sufficient to repair in order services and processes linked to them. Furthermore, it is necessary to act quickly to restore services and processes, in order to avoid wider social impacts including economic and political implications.

Urban services may be disrupted in many different cases, having direct impacts on community processes. The impacts can be classified as follows:

- localized impacts (i.e. local traffic jams due to large-scale incidents, heavy machinery down fall, etc.; water supply interruption due to a landslide on the pipeline)
- diffused impacts (i.e. traffic and public transport congestion due to snow storms; railway line block due to derailments);
- area-wide impacts (i.e. dramatic events like 1966 Florence flood or 2009 L'Aquila earthquake);

Despite the fact that infrastructures are normally managed by public authorities, service and processes are often outsourced to private or semi-private companies. The latter are then responsible for the continuity of services, their implementation and for communications to citizens and institutions. Institutions on the other hand care for infrastructures on which the services are dependent. Relations between the two entities are normally controlled by previously signed contracts. The processes and recovery periods in case of service problems or disruptions are normally foreseen in these contracts.

General recommendations

- National bodies and organisations involved in restore/repair operations should always be prepared to react promptly and efficiently on the basis of an as accurate as possible assessment of the impacts so that the normal operations are restored as fast as possible.
- The variety of incidents and the variability of system operations should be supported by sufficient technological, human and organisational resources and budget.

Common Conditions recommendations

1 - Availability of resources

- Humans (labour) – skills/competence

Stakeholders 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 of which they are in charge and its connection with different geographical, social and legal aspects of the urban system. 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 likely restore and repair activities, to optimize the intervention times within the local planning procedures and to ensure continuity between the emergency phase and the ordinary operations phase.

- Budget:

In case of critical situations that turn into emergencies, financial reserves should be budgeted in advance for restore 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 private companies and the public entities in relation to their responsibilities.

- Data & Algorithm:
  - Use of standard documentation for data and algorithms
  - Use of recognized project management concepts
  - Use of standardized models and protocols
  - Production of KPIs in order to manage the required action plans
  - Use of historic data in relation to short-term / long-term responses (natural and manmade) for likely critical scenarios within the urban context
  - Acknowledgement of existing legal acquis, local conditions and regulatory regimes
  - Definition of 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 to localized disaster impacts, mitigate and absorb problems due to diffused disaster impacts. The same models may also identify stressful situations that must be avoided in order not to become fatal in case of incidents.

2 - Training and experience

- Social and territorial data analysis, network examination and software simulation by capable experts
- Management and coordination skills to collect the contingent information and to plan 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 involved actors and from actors to the end users (active interaction) at all stages of the implemented actions
- Guarantee the accuracy and understandability of the communication through standardized communication tools, and protocols

4 – Human-Computer Interaction and operational support

- Utilization of software tools to analyse the impact of the operational strategies which could be applied to the disrupted system
- Utilization of software tools to analyse data and develop focused intervention plans
- Utilization of social networks to collect information about the opinion of citizens in anticipation of recovery actions
- In a normal situation or in case of emergency, the monitoring of services/processes is directly connected to the monitoring of infrastructures, with all the temporal, qualitative and quantitative connected considerations. However, the disruption of services and processes may also have great social impacts. Therefore, it becomes important to monitor and to be able to interpret feedback from media and social networks. It is difficult and it takes time to evaluate the psychological impact that the lack of a service may have on the population. But being able to understand what services and how their quality is perceived by CI users as belonging to a normal situation is a key point to focus energies.
- Human Factors issues about human-computer interfaces, should be considered in order to ensure easy, safe, comfortable and efficient interactions avoiding errors or problems of fatigue or distraction

5 - Availability of procedures and plans

- Open Planning process to effectively outline the structural and non-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

- Consider in advance specific legislation to ensure that personnel may bear responsibility, [also under an effective insurance system]
- Knowledge and awareness about recovery priorities after an emergency in order to disseminate properly funds, material and human resources
- Capacity to facilitate the cooperation among the different stakeholders during the debriefing activities and all stages of the field operations

- Manage physical, temporal and organisational conditions of work in order to support actors with the best possible conditions for acting and taking risks for the required actions towards efficient restore operations

7 - Number of goals and conflict resolution

- Tangible strategic and tactical measures to restore the ordinary and fully operational conditions that were disrupted by incidents
- 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 deployed procedures
- Definition of the activities that must be planned before and in anticipation of an incident impact and those that must be improvised only after an incident.

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 repair based on the importance of services/processes

9 - Circadian rhythm and stress

- Restore quickly service/processes the lack of which can stress ordinary life
- Identify what services and how their quality are perceived by CI users as belonging to a normal state of operations
- Consider minimum rest and sleep times for operators in order to avoid circadian rhythms asynchrony and consequential errors or mishaps

10 - Team collaboration quality

- Adherence to the principle of collaborative planning
- Collaboration and cooperation between institutions and private companies which operate services/processes is very important

11 - Quality and support of the organization

- Clear decision making process and alignment of responsibility
- Alignment of decisions with defined priorities
- Having clear priorities of what type of services and processes have to be repaired before others

Interdependencies recommendations

This function must be activated having in view the Coordinate Service delivery function, receiving by this function plans and coordination with other processes. It is not appropriate to start the Coordinate service delivery function before the critical emergency has finished.

This function must provide the highest possible feedback to Coordinate Service delivery function so that the latter can coordinate the normal 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 that there is awareness about status of services and processes.

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

To increase resilience, following restore/repair operation activities, it is also important that all data regarding the restoring operation become available to those who collect information about the incident.

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

Limitations

- 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 reserve infrastructures where to place alternative services and procedures

Questions

- Who are the stakeholders that should be involved and how?
- Are their roles and responsibilities clearly defined?
- How the processes are defined, established and communicated?
- Are there any emergency rules and procedures?
- What are the dedicated available resources? Are there any 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 recovery rate 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)

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

The NDRF 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 NGOs 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). 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 its associated rainfall and flooding. The Recovery Plan recognises the complex and dynamic nature of the disaster recovery environment and has been also 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.

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). InnovativesInstandhaltungsmanagement mit IDMVU, Leitfaden Teil 1 ÜberblickGesamtprozess. ForschungsvorhabenInfrastruktur-Daten-Management fürVerkehrsunternehmen (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)
- 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

4.4 Learn

4.4.1 Collect event information

Abstract

This function is related to the collection of 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 to have a comprehensive overview of the event and the response of the critical infrastructure/system.

Then, data and information collected must be stored to establish an updated and holistic historical knowledge-base to use for defining new good practices and more effective interventions.

To achieve this goal, and according to 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 that the data collection and integration process can access data coming from other interconnected critical infrastructures and/or related to similar events in different geographical areas. The aim is 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 to enable the definition of good practices and effective actions supporting a quick recovery to normality as well as adaptations to increase the overall resilience of the system.

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

Many 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 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 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"

General Recommendations

- Establish an organisational knowledge base to record operations data
- Identify organisational information needs. The identification of informational needs should be sufficiently rich and complete in representing and elaborating users' real needs. Since information usage usually takes place in the context of a task or problem situation, specific informational needs will have to be elicited from individuals. Unveiling informational needs is a complex, fuzzy communication process. Usually, understanding informational needs requires to consider them in the real-world context, in which the person experiences those specific needs and use the information to make decisions and perform actions.
- Information acquisition aims at balancing two opposite requirements: on the one hand, the informational needs of the organisation are wide-ranging, reflecting the breadth and diversity of its concerns about changes 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 information to analyse. Thus, the set of sources used for monitoring should be sufficiently large and various to reflect the span and sweep of the organization's interests. Although this suggests that the organization would activate the available human, textual and online sources, the variety of information sources must be controlled and managed to avoid information saturation. A powerful way of managing information variety is to involve as many persons as possible in the organization to gather information.
- 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.
- An 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 collection and storage policies, along with records management systems, will enable the creation and maintenance of a corporate memory, while learning from history.
- The organization should be able to collect and store both 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. Because the same information can be relevant to a range of different problem situations, it becomes necessary to represent and index the unstructured information according to several criteria.

Common Conditions recommendations

1. Availability of resources

- Humans (labour) – skills/competence
    - At the core of the organization one can identify the following three groups of experts who need to work together as a team of knowledge partners:
        - *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.
    - Skills and competences involved in this function are different and multi-domain. Personnel who is in charge to internally cooperate to the emergency management has to be trained to effectively support emergency management operators and guarantee cooperation and information sharing even beyond the current integration/interoperability of the ICT systems.
    - Furthermore, human factors and social science experts should cooperate to support customers, and citizens in general, involved in the event in reporting information that could be useful 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 to assure – hopefully improve – the level of integration and interoperability among different ICT systems, even along their own evolution.

- Budget:

Financial reserves to be accessed for acquiring new ICT systems as well as to update the current ones, 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 – even unstructured.
- 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 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 for improving the knowledge about the event and the current resilience of the infrastructure.
- 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 among critical infrastructure operators and other emergency operators, in particular with respect to 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 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 about making certain information public or its dissemination to all the members of the organisation as well as relevant stakeholders. To manage such potential conflicts, all actors need to be involved through a 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 of information from users/citizens who could be under stress due to the event.

10 - Team collaboration quality

- High quality is required, specifically among technical personnel of critical infrastructure and emergency stakeholders
- Involvement of human factors and social science experts must consider characteristics of both event and critical infrastructure 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, more precisely the internal ones, which have to be considered 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. To maximise the internal data availability, a dedicated procedure, wide information and an ICT infrastructure should be put in place to support data transfer among different functions

Limitations

Post-event stress could make difficult to collect reliable and consistent information about the event from involved citizens/users

Questions

- Which is the final aim of the events-related data collection?
- How should the organization manage sources of information (e.g. sensors, cameras, staff, etc.) to get a realistic picture?
- Which type of information are available? (qualitative, quantitative)
- When are the measurements made? (continuously, regularly)
- How the quality of communication is measured? (e.g. response time)
- Does any strategic centre exist? (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 to support a quick return to normality?

Examples

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. In this paper a number of experiments have been conducted on the possibility to integrate different source of data to obtain information on flows in an Information Transport System.

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.

4.4.2 Provide adaptation & improvement insights

Abstract

This function aims at analysing data and information collected to discovery useful insights and define adaptation actions. 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 how identify corrective actions for improving the overall resilience of the critical infrastructure. 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 infrastructures, requires a deep analysis of the possible responses to events. 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, considering the nature and features of the event, the operations performed (and their timing), as well as the comparison with good practices, permits to identify criticalities and vulnerabilities and, subsequently, defines corrective actions to improve the adaptation of the critical infrastructure with respect to similar events.

Data availability is also important for improving the capabilities to infer and model the behaviour of the infrastructure 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, as well as citizens in general, involved in the event.

General recommendations

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

- When it is necessary to make an action and why,
- What level of adaptation is required, and the consequences of over- as well as under- adaptation, 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 changing conditions needs to be considered in two ways:
    - when constructing new infrastructure, resilience to climate change 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 infrastructures which usually have a lifespan of at least 20 years and, therefore, investment decisions influence future generations' wellbeing,

  - 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 resilience to climate change, 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 many 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.

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

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).

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 to mitigate the risk of wrong evaluation that may result in following issues:

- persistence of the vulnerability because of the inefficacy of the solution provided
- loss of resources
- 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.

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.

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.

Questions

- Will the option be robust under today’s climate changes as well as a series of different and possible future climate changes?
- Could the option 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 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?

Examples

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.

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.
- 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).

4.5 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.

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.

4.6 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 2001, Rinaldi, Peerenboom, and Kelly defined the terms "dependencies" and "interdependencies":

> *A dependency is a "linkage or connection between two infrastructures, by which the state of one infrastructure influences or is reliant upon the state of the other."*
>
> *An interdependency is a "bidirectional relationship between two infrastructures in which the state of each infrastructure influences or is reliant upon the state of the other."*

Interpreting these definitions leads us to the conclusion that the term "dependency" may be used when the influence between two infrastructures is one-way, i.e. only one of them affects the other, while the term "interdependencies" refers to a two-way influence, thus both infrastructures' activities influence the other.

According to Petit et.al (2015), Critical Infrastructure interdependencies constitute a risk multiplier: they can themselves be a threat or hazard, affect the resilience and protection performance of critical infrastructure, and lead to cascading and escalating failures. In other words, interdependencies influence all components of risk, i.e. threat/hazard, vulnerability, resilience, and consequences.

(Inter) dependencies can be clustered according to their characteristics, classes and dimensions, as follows (Petit et. al, 2015)

- *Characteristics of (inter) dependencies*: upstream dependencies, internal dependencies, and downstream dependencies
- *Classes of (inter) dependencies*: physical, cyber, geographic, and logical
- *Dimensions of (inter) dependencies*: operating environment, coupling and response behavior, type of failure, infrastructure characteristics, and state of operations

The dimensions' breakdown is quite complex and multi-parametric, as illustrated in Figure 2:

The importance and criticality of such interdependencies is made evident also by the fact that Governments all over the world has put specific effort in identifying and managing them in an organised an effective manner. Indicative examples are:

- In the United States, the National Infrastructure Protection Plan (NIPP) (DHS, 2006) provides the strategic vision to guide the national effort to manage risk to the Nation's critical infrastructure. The achievement of this vision is challenged by the complexity of critical infrastructure systems and their inherent interdependencies.

- The Australian Government in its Critical Infrastructure Resilience Strategy (2010), is explicitly treating the cross-CI interdependencies as a matter of priority and special attention

In this chapter, a set of guidelines related to cross-CI interdependencies are suggested, following existing practices and related activities outside the EU.

4.6.1 Guidelines on managing cross-CI interdependencies

The main idea is to identify, analyse and manage cross-sector dependencies of Critical Infrastructure. This is an issue that should be treated at high-level (e.g. at country or EU level) as it implies the coordination and cooperation of several CIs in different and multi-dimensional aspects.

The main pillars in this approach can be 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.

The NIPP in the USA, in terms of managing cross-CI interdependencies suggests, among others that:

- *Risk should be identified and managed in a coordinated and comprehensive way across the critical infrastructure community to enable the effective allocation of security and resilience resources.*
- *Understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing critical infrastructure security and resilience.*
- *Gaining knowledge of infrastructure risk and interdependencies requires information sharing across the critical infrastructure community*.

Moreover, in Petit et.al (2015) a dependency and interdependency assessment framework is proposed, consisting of four main assets:

- *Expertise*—multidisciplinary and includes knowledge of soft (e.g., management and socioeconomic sciences) and hard (e.g., engineering and operations research) aspects influencing critical infrastructure dependencies and interdependencies, and ultimately resilience and protection.
- *Partnerships*—includes collaborations with public and private sector partners as well as research organizations.
- *Data*—includes existing databases (i.e., commercial and owned by stakeholders) and capabilities to conduct open source research and develop collection surveys specific to the analysis required.
- *Tools*—combines mathematical and engineering models and metrics for identifying and characterizing dependencies and interdependencies, and GIS capabilities for visualizing them.

In the Australian Government's Critical Infrastructrure Resilience Strategy (2010) it is mentioned as a strategic imperative to:

> *Strategic Imperative 3: Assist owners and operators of critical infrastructure to identify, analyse and manage cross-sectoral dependencies*

For this reason the Critical Infrastructure Program for Modelling and Analysis (CIPMA) has been established; a computer-based capability which uses a vast array of data and information from a range of sources (including the owners and operators of critical infrastructure) to model and simulate the behaviour and dependency relationships of critical infrastructure systems.

From all the above, it can be concluded that the main principals in managing cross-CI interdependencies can be summarised in the following:

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.

5 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 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 D3.5) has been 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.

Furthermore, within the framework of RESOLUTE, the ERMG has been adapted and operationalized for the case of the Urban Transport System (UTS) in D3.7. These two Deliverables have served as the basis for the development of the rest of the RESOLUTE tools, as well as for the realisation of the project pilots (within the framework of WP6, in Florence and Athens). The experience of the pilots as well as the comments and contributions of the experts participating in the RESOLUTE Advisory Board, have provided valuable input for the update and finalisation of the guidelines, as presented in the present document. Moreover, also the UTS adapted ERMG have similarly been updated (in D3.8) to match the final version of the generic ERMG and incorporate the feedback from both the pilots and the Advisory Board.

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. An example of such application (for the case of one function) is presented here (chapter 3) for reference.

Finally, the production of a short version of the ERMG (that can be found in Annex A) is a useful instrument for the promotion and exploitation of the ERMG, providing a compact and comprehensive outlook of the guidelines and inviting the interested bodies to further explore and apply the ERMG, as produced within RESOLUTE.

6 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.

Ferreira, P., Simoes, A., 2016. Conceptual Framework. RESOLUTE Deliverable 2.2

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.

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.

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.

Linkov, I., Fox-Lent, C., Read, L., Allen, C.R., Arnott, J.C., Bellini, E., Coaffee, J., Florin, M.-V. Hatfield, K., Hyde, I., Hynes, W., Jovanovic, A., Kasperson, R., Katzenberger, J., Keys, P.W., Lambert, J.H., Moss, R., Murdoc, P.S., Palma-Oliveira, J., Pulwarty, R.S., Sands, D. Thomas, E.A., Tye, M.R., Woods, D. – (2018) Tiered Approach to Resilience Assessment - Risk Anaysis Journal - https://doi.org/10.1111/risa.12991

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

Oedewald, P et al – Intermediate report MoReMo Modelling Resilinece for Mantainance and Outage – NKS-262 – ISBN 979-87-7893-335-5 Feb 2012

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

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Philips, J., Peerenboom, J. 2015. Analysis of Critical Infrastructure Dependencies and Interdependencies. Risk and Infrastructure Science Center, Global Security Sciences Division, Argonne National Laboratory. ANL/GSS – 15/4. USA

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

Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, 2001, "Complex Networks, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," IEEE Control Systems Magazine, December 2001, pp. 11–25, http://user.it.uu.se/~bc/Art.pdf, accessed December 9, 2014.

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

ANNEX A: ERMG SHORT VERSION

6.1.1 Develop Strategic Plan

General Recommendations

- Attempting to gather board members and key employees together for planning by combining top-down and bottom-up approach
- 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
- Incorporating a “flexible” decision making process
- Securing the continuity to deliver cash generation through sustainable organization growth in view of including that information in the Strategic Plan
- Producing quantitative measures in order to manage and check the strategic plan
- Establish an business-government partnership with critical infrastructure owners and operators

Common Conditions Recommendations

Availability of resources	*Use of standards and involvement of all organization members*
Training and experience	*Domain knowledge, project management and organizational skills*
Quality of communication	*Standardized communication instruments among internal and external shareholders*
HCI & operational support	*NA*
Availability of procedures and plans	*Distributed decision making; clear definition of roles and responsibilities*
Conditions of work	*NA*
Number of goals and conflict resolution	*Planning teams built accordingly to the goals*
Available time and time pressure	*Planning milestones and deadlines definition*
Team collaboration quality	*Follow the principles of collaborative planning*
Quality and support of the organization	*Funding and senior sponsorship in the planning process*

Independencies Recommendations

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, the strategic planning should overcome such issues establishing and promoting an enabling management culture on self-protecting, so that appropriate adaptation action is undertaken.

Abstract

The function provides recommendation in relation to the management of strategic planning, that captures strategic goals/ objectives for supporting improve emergency preparedness and therefore increase resilience.

Background

Critical infrastructures are inherently interdependent —domestically and internationally — and vulnerable both within and across sectors. Hence, the critical infrastructure mission area requires a focused national strategy and supporting plans and operational structures: a formal „discipline“.

Example

A disaster management in a Computer Data Centre showing how different complementary strategies can come together within an enabling management culture to support the organisation through a period of disruption or loss.

Limitations

The adoption of strategic planning is matter of choice of the strategy managers, therefore there is a high impact of the human factor

Standardization of strategic planning is a very complex process.

6.1.2 Manage Financial Affairs

General Recommendations

- Assess potential disaster impacts and manage insurances & Governemental disasters risk financing tools
- Plan financial needs, cost-sharing & control including all involved entities & ensure an efficient deployment of funds. Manage eventual over-payment situations, audit real use after crisis
- Analyse financial capacity & resources needs of each involved stakeholder including private companies, governments, public companies…)
- Plan budget reserve & how to unlock it in case of emergency needs. Revise it regularly,
- Manage staff with knowledge of financial resources

Common Conditions Recommendations

Availability of resources	*Persons in charge of financial affairs able to decide & budget available from all concerned entitities, finances control after crisis*
Training and experience	*Financial, project, crisis management, cooperation skills*
Quality of communication	*Communication to/with all involved stakeholders*
HCI & operational support	*Software tools to analyse financial data, plan & monitor budget and resources, communicate with all functions*
Availability of procedures and plans	*Strategic and operationnal plan ready before crisis*
Conditions of work	*Emergency & team work, ability to define priorities*
Number of goals and conflict resolution	*Manage conficting objectives during strategic plan phase, define priorities, have a general agreement, communicate to other parties*
Available time and time pressure	*Immediate response needed*
Team collaboration quality	*Collaborative financial planning though mutual benefit relations, define mutual financial responsabilities*
Quality and support of the organization	*Clear decision making process, align decision with available resources and defined priorities, measure performances, interprete financial results*

Independencies Recommendations

In order to manage the potential issues generated by the strategy planning function, an organization should consider applying the Corporate Social Responsibility (CSRR); 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. CCSR 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.

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

As financial resources assume a critical role for system operation, provision of resources and assets, 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 is activated during normal operation as well as for emergency cases,

Example

Infrastructure Australia: Urban Transport Strategy from Federal government of Australia.

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

Limitations

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

6.1.3 Perform Risk Assessment

Anticipate	Monitor	Respond	Learn

General Recommendations

- *The Integrated Assessment of different risk natures, i.e. safety, security, environment, economic and business continuity, among others.*
- *Need for periodic update of risk models in view of operation and context changes.*
- *Increased need for integrated risk assessment in order to ease 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 and that are able to exploit heterogeneous data generated within and outside 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 impacts of both known and unknown changes in operations and their environment.*

Common Conditions Recommendations

Availability of resources	*Need for measurement or detection equipment; sufficiently precise assessment methods may be used. Human Skills & competence; Budget; Data & Algorithm*
Training & experience	*Subject matter experts should be consulted in order to validate hazard identification; Local staff involvement is critical for hazard identification and for insight on risk perceptions and operational processes.*
Quality of communication	*Ensure the accuracy of data and risk assessment outcome communication to all interested actors in the organization avoiding allegations & manipulations.*
HCI & Operational Support	*IT systems are increasingly important for the effective reporting of hazards & risks, and the support of decision-making, for instance when reviewing safety cases.*
Availability of procedures & plans	*Risk Assessment activities must be integrated in business & organizational process description, as opposed to independent or "stand-alone" activities; Operation & process change control processes must call on risk assessment & determine when they are required.*
Conditions of work	*A suitable level of independency & autonomy should be formally ensured to risk assessment teams.*
Number of goals & conflict resolution	*Adopt tools responding to assessment needs of different process stages: planning, operation, maintenance, decommissioning; Precision (quantitative & qualitative) of risk assessment to match process stage requirements & objectives.*
Available time & time pressure	*Time pressure should not compromise thoroughness & validity of risk reporting.*
Circadian rhythm & stress	*Monitoring and assessing human factors under shift work or roster conditions tends to be more complex. Monitoring and assessment conditions are much more dynamic and diverse.*
Team collaboration quality	*Team work may be relevant when assessing more complex operations & when producing risk reports; Necessary to establish a collaborative environment among sectors & departments & the risk assessment team.*
Quality & support of the organization	*Senior management, should officially endorse evaluators; Organisational support as fundamental contribution for the risk assessment activities and their outcome; Interaction w/ stakeholders may require some formal organisational setting.*

Interdependencies Recommendations

Hindsight on events 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, which requires more than conventional accident and incident investigations.

Abstract

Risk assessment (RA) is inherently related to an estimation of uncertainty at different levels. In addition to minimising uncertainty, RA must also take into account:

- *the estimation of types & levels of resources that may be required to adapt to unexpected events;*
- *the need for update in view of emerging factors or perceived operational changes.*

Background

RA serves the purpose of supporting:

- *the definition of priorities for action;*
- *the determination of its nature & course.*

As resources are always finite, the potential need for additional resources must be considered and aligned with actual potential operational needs at different levels.

Example

- *Risk fora with teams involved in managing different risk domains, addressing potential needs to review risk models & assessment tools.*
- *Team reviews of RA, focusing mainly on the risk interpretation factors & their mapping onto real operational context & specific scenarios.*

Limitations

Applicability, reliability, accuracy and validity of assessment tools and means to test them regularly as operations change.

6.1.4 Training staff

General Recommendations

To contribute to the resilience of the system, training activities should be organized to ensure 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:

- Training requirements need to be documented in a standardized schema: competence requirements for each role/job, precise information on official or legal success criteria (e.g. specific type of driving license), time by which training needs to be refreshed, among others
- The training should particularly address the individual's role in detecting emergencies and subsequent mitigation actions, as well as requirements related to the general service and known vulnerabilities.
- Theoretical/practical exams, outcomes of exercises or performance on the job measure success criteria and assess to which extent the trainees acquired the necessary skills.
- Training requirements should be developed and reviewed based on the results of the valuation processes and updated with the introduction of new technologies or changes of safety regulations, corresponding costs and resources have to be allocated.

Common Conditions Recommendations

Availability of resources	*Human skills & competence: collection of training requirements; Budget: working hours by trainers, trainees and HR specialists, training material, training location/infrastructure; Data & Algorithm: standardized documentation of requirements.*
Training & experience	*Feedback from trainer for improving the process; Scenario-based training to validate contingency plans.*
Quality of communication	*Efficient, understandable and accurate coordination and communication through standardized communication tools, protocols and languages.*
HCI & Operational Support	*Depending on the kind of knowledge/skills mediated in the training, the choice of the right method (e.g. classroom training, simulator training, on-the-job-training, e-learning) is important.*
Availability of procedures & plans	*Definition of training objectives and curricula should be formalized and embedded within the HR procedures.*
Conditions of work	*Head of HR should ensure the necessary conditions to perform the training are created, e.g. provision of space, materials, budgets, buffer personnel.*
Number of goals & conflict resolution	*Legal requirements and directly relevant training objectives need to be prioritised in case time/budget make the accomplishment of all trainings impossible.*
Available time & time pressure	*Schedule trainings according to predicted demands; Perform trainings outside of demand peaks, such as tourist seasons.*
Circadian rhythm & stress	*Perform training during regular working hours; Avoid an excess of working hours.*
Team collaboration quality	*Provide trainings on: The principles of collaborative planning/management; Development interventions; Risk awareness and understand of vulnerabilities and mitigation strategies.*
Quality & support of the organization	*Leaders need to be responsible for enabling their so-workers to conclude the required training.*

Interdependencies Recommendations

The management and implementation of training needs should be grounded on a close cooperation and coordination between HR and the other involved 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. Thus, training staff as a system function may develop strong interdependencies with most other system functions.

Abstract

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

Background

Training is a key element to ensure resilience. It compromises all activities performed to enhance knowledge, skills and abilities of members of the organisation, with the aim of enabling them to better perform their specific job. In emergencies, actors from different organizations need to collaborate efficiently in order to maintain or restore the operations of a critical infrastructure.

Example

- *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.*

Limitations

- *Training on overall knowledge and under-standing of operations is challenging.*
- *Guideline-based training approach targets only a finite number of known individuals.*
- *Guideline does not serve to plan organisational learning.*

6.1.5 Coordinate Service Delivery

Anticipate | Monitor | Respond | Learn

General Recommendations

- •Adopt an holistic Service Delivery Framework aimed as principles, standards, policies and constraints to guide the deployment of services delivered to a specific user community in a specific business context
- •Understand infrastructure network criticalities and interdependencies
- •Maintain control on the entire supply chain to adapt the level of service according to changing conditions in resource availability (e.g. grateful degradation strategy of the service)
- •Establish permanent dialogue with the community served in order to adapt the service on the actual user needs in emergency and in daily operation
- •Adopt data and knowledge sharing policy with public administrations, in emergency as well as daily operations, to allow decision makers a better situation awareness
- •Adopt ICT and evidence driven tools in taking internal and external risk-informed decisions

Common Conditions Recommendations

Availability of resources	*Humans: person-oriented leadership, think complexity at systemic level, capacity to tradeoff beween business needs & service demand respecting safety & security; Data & algorythm: exploit all kind of data sources to collect user feedback and adjust services accordingly; ICT resources. Periodic functionality check and scenario based stress test*
Training & experience	*Staff periodically tested for adequate training & knowledge of routine and emergency rules & procedures to catch up updated procedures*
Quality of communication	*Establish an effective, standardised & reliable communication between the actors involved in the supply chain, operations and contingency. Establish a single point of contact for service delivery coordination*
HCI & Operational Support	*Control rooms for actuation should be designed according to Human Factor standards & best practices. Any issues in HCI may generate a cause-effect misunderstanding leading the operator towards wrong decisions.*
Availability of procedures & plans	*Ensure that clear operation plans and emergency procedures and plans are available to all actors involved in the service and first responders.*
Conditions of work	*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*
Number of goals & conflict resolution	*Incrementing service delivery performance to address unexpected increment of demand should consider safety & security requirements. In case of conflict with other organizations, prompt communication to stakeholders affected by the decision is required for a synchronised systemic response to an unexpected event.*
Available time & time pressure	*Ensure a degree of flexibility when planning service performance milestones to cope with quality safety and security requirements.*
Circadian rhythm & stress	*Ensure compatible nightshifts for staff, without reducing the expertise*
Team collaboration quality	*Collaboration between Delivery Manager and operators supporting service delivery established and maintained. Any issue that might prevent timely, truthful and complete communication is high level risk and treated with related risk-mitigation countermeasures.*
Quality & support of the organization	*Establish a clear decision making process and aligment of responsibility with accountability*

Interdependencies Recommendations

The function is strongly dependent from the condition of both physical and cyber infrastructure. Physical infrastructure should be both regularly monitored to track operation dynamics and to detect unusual circumstances. This is one of the aspects for which thorough and continuous coordination with infrastructure users and stakeholders becomes critical. Efficient coordination of service delivery should also take into account user behaviour and awareness of service characteristics. User generated feedback should be monitored to adjust the coordination of service delivery to changes of service peaks.

Abstract

This guideline provides recommendation for the effective coordination of service delivery in a CI. The role of Delivery Mangers is highlighted as well as the need to have an holistic and systemic approach to service delivery. The supply chain needs to be monitored, stakeholders should be informed about service adaptation on changing conditions and involved into a continuous information exchange.

Background

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.

Example

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.

Limitations

Legal framework and/or internal policy of organizations may impose limitations in particular on the adoption of data sharing approach or the creation and maintenance of a dialogue with users

6.1.6 Manage awareness & user behaviour

General Recommendations

- Communication plan: all communication, the objective of the message, the media and channels used should be based on a plan.
- Collaboration: Public and private organisations and educational institutes should be involved.
- Events: anniversaries of past disastrous events are recommended for the implementation of campaigns, along with events to raise awareness.
- Awareness: community awareness campaigns are recommended in the case of new adverse events or a lack of adoption of safety relevant behaviour.
- Training: besides campaigns, different kind of trainings, such as classroom training, scenario training, game-based approaches or live drills, can raise people's awareness.
- Early warning: Communication and early warning systems should be people-centered.
- Personalized context aware communication: "The 4R": The Right person at the Right time in the Right place through the Right channel. Plans and procedures for the delivery of pre-scripted messages need to be aligned with the predefined mitigation strategies and ongoing emergency response activities.

Common Conditions Recommendations

Availability of resources	*<u>Human Skills & competence</u>: experts in communication, operators with skills in emergency management, communicative & empathic skills; <u>Budget</u>: for communication infrastructure & maintaining social media; <u>Data & Algorithm</u>: assessment of awareness (via social media analysis or game-based training); <u>ICT infrastructure</u>: CAD systems as essential component of public safety operations. Citizens can be localized and contacted on their smartphones.*
Training & experience	*Operators to be trained to cope with stress; Evaluate communication process, collect feedback, foster specific expertise*
Quality of communication	*Use of predefined messages or message types to ensure content quality; General principles: Accessibility, Inclusiveness, Inter-operability*
HCI & Operational Support	*Applications undergo usability testing; Select communication methods by their scalability and sustainability*
Availability of procedures & plans	*Long-term communication: e.g. campaign; Ad-hoc messages: procedures including general standards e.g. specific messages, use of channel, precise phrasing.*
Conditions of work	*Responsible staff to be continuously provided with status information or orders from the coordinators of service delivery*
Number of goals & conflict resolution	*Communication on evacuation procedures to provide specific information for all users; Communication to aid vulnerable groups, e.g. naming accessible route/exit*
Available time & time pressure	*Communications related to safety issues should be prioritized.;Use of social media and news agencies for campaigns that encounter time pressure, e.g. due to a critical event approaching*
Circadian rhythm & stress	*Defining turns among operators is mandatory. Smooth transition among turns should be managed to avoid any loss of knowledge or situation awareness.*
Team collaboration quality	*The communication team to be composed by experts in different fields. Clearly match competencies with duties to avoid overlaps or mismatching.*
Quality & support of the organization	*Create a dedicated unit to manage the communication during critical events because of its special dynamics (timing, language, content etc.).*

Interdependencies Recommendations

The end user communications aims to enable the end user to preserve their own well-being, steer the use of the service, improve public trust and provide information to the users.

In the case of disruptive events, the people responsible for relevant fields need to have a direct communication and access to data, such as movement of users through the infrastructure.

In case the connection between relevant functions is temporarily lost during an emergency, the last status detected or the default safety recommendations should be forward through the channels.

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.

Background

In the community-individual safety approach the person is now 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. In order to undertake behavioural change, the main determining factors of intention need to be understand:

- *Attitude of a person*
- *Community norms*
- *Social settings*
- *Degree of self-efficacy*

Example

Greater use of social marketing methods.

- *Mass persuasion methods are now widely applied to foster positive behaviours, e.g. a social marketing and health promotion campaign by the National Flood Warning Centre (UK) raised flood awareness from 48% to 79% over the past five years.*

Limitations

Organisations should be prepared for undesired user behaviour.

6.1.7 Develop/update procedure

General Recommendations

- Identify clear goals and objectives for the emergency response procedures
- Review hazard or threat scenarios identified during the risk assessment
- Assess the availability and capabilities of resources for incident stabilization including people, systems and equipment
- Confront with all involved shareholders 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
- Determine if there are any regulations pertaining to emergency procedures
- Define protective actions for life-safety
- Develop hazard and threat-specific emergency procedures
- Coordinate emergency planning with public emergency services to stabilize incidents involving the hazards at the addressed facility
- Train and exercise personnel so they can fulfil their roles and responsibilities and practive the operational procedures

Common Conditions Recommendations

Availability of resources	*Budget planned for procedures definition; specialized personnel*
Training and experience	*Operational procedures need to be subject of training, exercise and feedback*
Quality of communication	*Communication tools need to be foreseen for internal and external communication towards the users*
Availability of procedures and plans	*Both availability of communication channels and precise phrasing in the procedures*
Number of goals and conflict resolution	*Procedures need to be concise and clear*
Available time and time pressure	*Procedures need to be validated in real-life environments*
Team collaboration quality	*Procedures should enable efficient team collaboration*
Quality and support of the organization	*Funding should exist for definition, training and testing for operational procedures*

Independencies Recommendations

The function "Perform risk assessment" provides the factual basis for activities proposed in the strategy portion of a hazard mitigation plan and is providing the basis for an efficient procedure process definition. An effective risk assessment informs proposed actions by focusing attention and resources on the greatest risks. 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 self-learning.

Abstract

This function is dealing with the management of the operating procedures, as a set of instructions of carrying out tasks without loss of effectiveness in case of emergency, according to risk assessment and ex-post event analysis (learning) in a re-usable and replicable way.

Background

The purpose of Standard Operating Procedures (SOP) is to strengthen organizations support in preparing and responding to crises. This is achieved by the consistent use, by a critical mass of personnel of clear key procedures at critical moments.

Example

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.

Limitations

Limitations related to complexity and non-applicability Limitations related to non-clarity Limitations related to a too-generic character.

6.1.8 Manage Human Resources

General Recommendations

- *Human resource availability needs to be secured for both daily activities and during emergency. A dedicated buffer capacity should be defined in advance and tailored according to emergency scenarios ;*
- *Implement a Human Resource Management system/Human Capital Management System in the organization*
- *HR should manage employee stress and burnout caused internal and/or external factors*
- *Implement a Human Resource Replacement Plan to replace missing human resources with other with the same experience*
- *Implement a Knowledge Transfer Strategy to anticipate and manage retirement, dismissal or leave of absence of specialised staff*
- *Experienced recruiters should take responsibility for preparing managers and members of the recruitment panel for interviews with candidates*

Common Conditions Recommendations

Availability of resources	*Humans skills: compensation & benefit recruitment and hiring, performance evaluation, training and staff development, adaptation & flexibility; Data & Algorithm: Use HRMS/HCM system to manage information on knowledge, skills & abilities, interests, General Work Activities and work context data; Financial plan: Recruitment activities to follow the financial plan. Gather labour market intelligence coherently & consistently to quantify skill requirements' market value*
Training & experience	*Continuous improvement by developing cultural competencies, reinforcing the organization, identity and spreading its values.*
Quality of communication	*Encouraging internal communication for employees update on the organization intent, goals, activities and business development, through several means*
HCI & Operational Support	*Integrate HRM System with IT physical Security Access control system to ensure real-time employees' access management*
Availability of procedures & plans	*Adopt skill & competences categorization and experience levels; Minimize downside to employee for participation; Include policy to scale employee access during emergency; Use research findings to manage hostile insider.*
Conditions of work	*Treat personnel issues, such as working environment, as high priority; Establish an all-party-consent statute to track information exchange and work behaviours for security & knowledge protection purposes*
Number of goals & conflict resolution	*Motivational approach through inducements and contribution strategy; Ensuring equal opportunities of careers; Achieve a sustainable work/life balance*
Available time & time pressure	*Working conditions should be designed to minimize the impact of variability and time pressure while continuously enhancing inherent human adaptive capacities.*
Circadian rhythm & stress	*ICT solutions to support HR operators in their activities to mitigate the impact of stressed HR that can be reflected on wrong decisions.*
Team collaboration quality	*Coordination of HR with internal legal, security, business, risk and operation departments*
Quality & support of the organization	*Develop documents to establish accountability; Focus on Talent Management and Succession Planning giving priority to develop internal resources for a solid succession program*

Interdependencies Recommendations

- *Emergency HR request: Establishing an formal connection with emergency responders to create a reliable communication channel. Managing pay and benefit for employees engaged in emergency respond.*
- *Operation HR plan: ICT constitutes a fundamental resource for all activities across multiple stakeholders.*
- *Involving Top management in developing communicating and implementing strategic workforce.*

Abstract

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.

Background

HR serves the purpose of supporting:

- *The alignment of organizational human capital with missions and programmatic goals;*
- *The adoption of long-term strategies for acquiring, developing and retaining competences and expertise to achieve goals.*

Example

The US Department of Energy Office of the Chief Informaton Office (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 continues to align their human capital management to support the mission of the organization.

Limitations

The guidelines to not recommend a specific method or tool. Each method/tool is suitable if is able to address HR objectives.

6.1.9 Manage ICT resources

General Recommendations

The 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. Additionally, the 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. During any emergency, the role of a reliable Decision Support System is very crucial for effective response and recovery. The ICT systems should be considered a critical infrastructure for the organization existence and a specific attention should be dedicated to the long-term preservation of organization memory/knowledge.

Common Conditions Recommendations

Availability of resources	*Information stored in Databases and access to GIS; System for analysing data retrieved from social media; Technical Equipment: Computers, Servers, Cameras, Wi-Fi, Sensors; Alternative communications to cope with emergency cases; Electrical energy for supplying the ICT resources.*
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.*
Quality of communication	*Guarantee the quality and reliability of the communications; Provide alternative (emergency) communication types employing both terrestrial and satellite-based technologies*
HCI & 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.*
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.*
Conditions of work	*Friendly working environment; ICT infrastructure should be accessible for all.*
Number of goals and conflict resolution	*The roles and responsibilities of each team member should be clearly defined and not overlapped in order to avoid conflicts; The number and scale of tasks/responsibilities assigned to each person should be reasonable; 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.*

Independencies Recommendations

In order to monitor the operation of the critical infrastructure the ICT equipment and services have to be set/installed. In addition, the definition of the procedures has to be performed considering the requirements of the ICT infrastructure. In case of a detected problem, immediate action should be taken based on the backup plan in order to reduce any negative consequences. Finally, user generated feedback should be considered in a timely manner in order to ensure proper and efficient ICT operation.

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.

Background

Information and communication technologies (ICT) are at the core of many sociotechnical systems interdependencies. ICTs are also important tools for lessening the risks brought on by disasters.

Example

CRAMSS aims to support reference actors at the UTS, such as infrastructure managers, with their decision-making under both, standard operating conditions and emergency conditions. displays information from different sources or independently running web-applications, together with the results of the decision support

Limitations

ICT cannot eliminate possible economic loss and damage to property in case of a disastrous event. There is lack of adequate financial support

6.1.10 Maintain physical/cyber infrastructure

Anticipate	Monitor	Respond	Learn

General Recommendations

Maintenance should adopt an “asset management” approach in order to evaluate an monitor the resource lifecycle, evaluate and monitor financial sustainability andmaximise the life of the asset while reducing the costs.

Thus maintenance can be considered as factor of cost reduction, competitiveness and safety increment.

- Intelligent maintenance is required to significantly enhance the system flexibility and ability to adapt to continuously changing operational conditions
- Infrastructures should be continuously monitored against environmental threat through sensors, video and audio surveillance equipments, etc. Data from such sensors and surveillance equipment may be processed on the field or sent to a centre for processing.
- Supervisory Control and Data Acquisition, or SCADA systems work to monitor and control key processes involved in the management of assets, 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 water from a tank when it fills up, or to initiate an emergency shutdown of an electrical substation.

Common Conditions Recommendations

Availability of resources	*Human skills & competence: continuous exchange of information between personnel; Budget: adequate financial resources are needed for regular maintenance; Data & Algorithm: data coming from the systems to control the critical infrastructure*
Training & experience	*Efficient maintenance training help to rationalize asset usage; More efficient training can be achieved through on the job training*
Quality of communication	*Efficient, understandable and accurate coordination and communication through standardized communication tools, protocols and languages.*
HCI & Operational Support	*Usage of maintenance SW tools for focused intervention plans; Usage of SW tools implementing procedures to take right decisions*
Availability of procedures & plans	*Develop a strategy for maintenance of system infrastructure and share it among all maintainers and stakeholders*
Conditions of work	*If possible it is preferable to allow maintenance employee to work on UTS assets within company headquarter* *Proper attention shall be paid to security working conditions for on field work*
Number of goals & conflict resolution	*Early detect anomalies in order to reduce crisis times and efforts; Increase the amount of data collected during the crisis*
Available time & time pressure	*Maintenance activities shall be done during normal infrastructure operation; Workers shall perform rapidly to be fast in solving crisis*
Circadian rhythm & stress	*Allow workers the proper time shifts; Avoid an excess of working hours.*
Team collaboration quality	*Improve quality of human relation specially between technical personnel*
Quality & support of the organization	*Maintenance process shall be based on clear decisions; Maintenance organizations shall have clear assignment and work-flow*

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.

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 in operation, and operating efficiently and safely.

Background

Maintenance engineering, is gaining more and more importance for modern critical infrastructures due to the increasing of equipment, systems and software applications; this activity requires personnel and resources to be performed.

Maintenance responds to safety requirements. It is one of the most significant costs for infrastructure managers. Skilled staff and special equipments are needed to perform maintenance operations.

Example

- *The maintenance of telco network is an example of both a cyber and physical infrastructure*
- *The Tree Eco-system of a city is another example of a cyber and physical infrastructure that require proper maintenance*

Limitations

Too much complexity of the Infrastructure leads to parts not properly maintained: this causes vulnerabilities in case of crisis.

Many technologies lack procedures for maintenance.

Communication failures among the actors of the infrastructure may lead to cases where the single part is well-maintained but the system as a whole is not.

6.2.1 Monitor Safety and Security

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

Availability of resources	*Identify the stakeholders and define the monitoring requirements; Personnel: Suitable levels of operation staffing are fundamental for the development & implementation of self-monitoring principles; Infrastructure: existing infrastructure & capabilities to be identified and then decide for additional equipment; Processes: ingress/egress control, the data collection, storage and management; Material: contents of data, data types and data management (collection, storage, analysis, distribution); use tools guaranteeing timeliness, accuracy and secure handling.*
Training & experience	*Identify process skill needs & gaps based on available resources and their current skill levels, along with training opportunities to address them; Provide training and review the training needs as necessary*
Quality of communication	*Communication issues involve communication of monitoring data. The main aspects of data quality are accuracy, validity, security and timeliness of data*
HCI & Operational Support	*Only specialised personnel or personnel that have gone through adequate training, should be responsible for handling the monitoring equipment,.*
Availability of procedures & plans	*Procedures & plans defined in the Safety & Security Monitoring Plan, complying with the monitoring requirements as defined by the stakeholders’ needs (collection, storage & management of data and monitoring operation procedures)*
Conditions of work	*Safe working environment; Shared and standard procedures; Clearly specified responsibilities and alignment with accountability*
Number of goals & conflict resolution	*The goals are defined by the requirements of the monitoring plan, including: authentication of entrance to facilities; working procedures’ risk identification and relevant measures; immediate operation of safety procedures in an emergency; accurate, legible and complete record keeping;*
Available time & time pressure	*Automation in task execution (part of working routine); Timely and effective data collection, considering time for sense making of data*
Circadian rhythm & stress	*Management of employee fatigue to avoid safety critical errors; Unbtrusiveness and automation in safety and security monitoring procedures.*
Team collaboration quality	*Definition of roles and responsibilities in the process plan, for collecting, recording, distributing, and ensuring the confidentiality, integrity and availability of monitoring data; Inclusion of process tasks and responsibility in specific job description*
Quality & support of the organization	*Establish and Maintain a Monitoring Program; Perform Monitoring*

Independencies Recommendations

Guidance from *Training Staff* in terms of training personnel; •*Defining procedures* in combination with *Risk Assessment* would define the procedures that should be of special focus, as the ones of higher risk and thus needing closer attention and preventive measures. •*Emergency actions coordination* should be in consulted in defining the monitoring plan and are of the main recipients of safety & security monitoring data in order to take adequate action. •*Service delivery* should be considered when defining the requirements of *Monitor Safety and Security*. •*Operations monitoring* should be considered 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. •*Collection of Event Information* is closely related, as they are the of the major recipients of collected data.

Abstract

This Guideline refers to the issues of monitoring safety and security of 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.

Background

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. 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.

Example

Critical infrastructure safety monitoring

http://www.nec.com/en/global/solutions/safety/critical_infra/index.html

Limitations

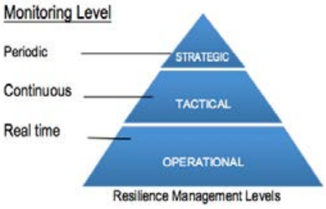
Lack of resources may lead to assigning safety and security monitoring to an external entity. In this case additional provisions for data security should be made and possible a MoU between the organisation and the external operator should be defined, including details on how the collected data should be managed and exploited.

6.2.2 Monitor Operations

General Recommendations

Monitoring must 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*
- *Increased need for integrated risk assessment in order to ease coordinated risk management actions and measures.*
- *Monitoring operational performance can be executed with different timeframe according to the Resilience Management Level*



Common Conditions Recommendations

Availability of resources	*Human Skills & competence secured by Human Resource Replaced Plan; ICT infrastructure to be reliable, scalable, not create impact on the system to be monitored, failure in monitored system should not cause a failure in monitoring system, run as distinctly as possible from the production Environment. Adopting a Unified Open System Approach*
Training & experience	*Increase risk perception capacity; Training employees in view of system thinking, creative problem solving and naturalistic decision making.*
Quality of communication	*Secure data and communication understandability and early warning*
HCI & Operational Support	*Equipment and control rooms to be designed in accordance with ergonomics standards of reference. Staff should be involved in the design process. Interfaces should be usable in both normal and emergency situation*
Availability of procedures & plans	*Define clear procedures that recognize distributed decision making requirements*
Conditions of work	*Establish a Safety Culture in the organization, beyond the classical approach, towards safety and adaptation as an internal organization value.*
Number of goals & conflict resolution	*Adapt a mind-set of openness, trust and fairness; Careful trade-off between safety and efficiency demand; Consider the level of independence of employees to be fair and impartial.*
Available time & time pressure	*Understand demand over time for being prepared to changing conditions; Separate Value & Failure demand; Look system responce in terms of adjustment and adaptation to demand dynamics*
Circadian rhythm & stress	*Managing fatigue and workload as hazard in terms of reduction of mental & physical performance that could affect the perception of external stimuli from the monitoring system; Task re-allocated from humans to machines/computers, or vice-versa; considering human performance, safety, maintainability, personnel requirements*
Team collaboration quality	*Field experts of all kinds, (including system actors, designers, influencers and decision makers) need effective ways to raise issues of concern, including problems & opportunities for improvement*
Quality & support of the organization	*Implement active monitoring consisting of checking activities carried out by line managers. The topics which are actively monitored must include those barriers or controls needed to prevent a major accident*

Interdependencies Recommendations

Monitoring function is strictly connected with the ICT infrastructure. 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.

Abstract

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.

Background

RA serves the purpose of supporting:

- *the definition of priorities for action;*
- *the determination of its nature & course.*

As resources are always finite, the potential need for additional resources must be considered and aligned with actual potential operational needs at different levels.

Example

In Km4City Ecosystem http://www.km4city.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.

Limitations

Improving an effectiveness monitoring and early warning systems does not, in itself, lead to reduced risk for disaster-prone communities.

6.2.3 Monitor Resource availability

General Recommendations

Understanding the interdependencies that ensure system functioning and operation is fundamental for the safe, effective and efficient allocation and deployment of resources. This understanding should seek:

- *The way in which 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.*

Monitoring resources availability implies that operational variability of the system must be considered and managed in order to ensure the system functioning. The resources and system capacities required to manage and cope with operational variability must also be taken into account.

Common Conditions Recommendations

Availability of resources	*Technical & organisational conditions ensuring acceptable workload, managing fatigue & stress, controlling workability across ageing, and promoting health, arousal & preparedness towards prompt reactions in emergency situations; Budget for system functioning and emergency situations; Preview budget for external operations*
Training & experience	*Provision of conditions for the development of competencies with experience; Ensure training for emergency situations in relation to the use of all resources.*
Quality of communication	*Accuracy and quality of communications for efficient and safe use of information; Use of reliable & purpose-oriented communication technology and appropriate communication standards and language.*
HCI & Operational Support	*Adequate interaction with computer and other IT systems for effective use of information-based resources. This is frequently a fundamental support for the management and deployment of other types of resources.*
Availability of procedures & plans	*Procedures to consider resource requirements and the conditions of access to them; Planning for accessible infrastructures, considering type and volume of resource availability and requirements.*
Conditions of work	*Conditions of work aligned with resource availability, to ensure an efficient and effective deployment of available resources.*
Number of goals & conflict resolution	*Monitoring the adequate allocation and deployment of resources for the management of trade-offs between operational goals and needs to meet safety requirements*
Available time & time pressure	*Time is the utmost critical resource without which the efficient and safe use of other resources can be compromised. Efficient use of time strongly relies on adequate planning.*
Circadian rhythm & stress	*Shift work or roster conditions may impose the need for more flexible management and deployment of resources.*
Team collaboration quality	*Monitoring changes in resource availability and re-assessing resource requirements as operational conditions change, requires close cooperation within and across work teams.*
Quality & support of the organization	*Organisational conditions are fundamental for the quality of resource planning and deployment, in particular when re-planning of resource management is needed.*

Interdependencies Recommendations

- *Monitoring resources generates information on their allocation & the understanding of their flows.*
- *ICT constitutes a fundamental resource for all activities across multiple stakeholders.*
- *A dedicated communication & periodic reporting channel should be established throughout the supply chain.*
- *A specific protocol & procedures to promptly inform about resource delivery failure & the related causes should be defined in advance between supply chain stakeholders.*

Abstract

As every resource should be available for the system functioning & prompt for any emergency request, the related guidelines should comply w/ the control of:

- *Expertise & functional human abilities in relation to the system functioning;*
- *Technology required for the system functioning;*
- *Organisational conditions favouring the system functioning & the mobilisation of resources in emergency situations.*

Background

The high complexity & dynamics emerging from system interdependencies require a continuous ability to monitor the flow of multiple critical resources, aiming to develop updated & thorough support to the planning of operations & the subsequent resources allocation.

Example

Best practices in risk and crisis communication: Implications for natural hazards management (Toddi A. Steelman • Sarah McCaffrey (2013).)

Limitations

- *Updating information on resources use.*
- *Assessing the situation and mobilising the appropriate resources.*
- *Unavailability of technological assets resulting from breakdown or lack of energy.*
- *Variability of human resources and of their performance.*

6.2.4 Monitor user generated feedback

General Recommendations

- Leveraging a bottom-up engagement of users of the critical infrastructure through social media monitoring ("social/human sensors", "travelers as moving sensors", etc.)
- Analysis of user generated contents through Text Mining and Natural Language Processing (NLP)

Common Conditions Recommendations

Availability of resources	*Costs for accessing, implementing and updating of social/human sensing data must be considered*
Training and experience	*Social media monitoring, communication skills, statistics and data mining*
Quality of communication	*Diffusion through different channels, in particular social networks and media, to reach any user reducing possible "digital divide"*
HCI & operational support	*Access to social/human sensing data and data analysis software for supporting the UTS operators during the emergency management.*
Availability of procedures and plans	*Procedures related to the communication to the public; frequent update to consider the preferred channels over time*
Conditions of work	*Privacy and security of data crawled from web and socials*
Number of goals and conflict resolution	*Reducing time to recover the normal condition*
Available time and time pressure	*Accessing, browsing and examining data in very short time through easy friendly visualization*
Team collaboration quality	*Adherence to the principles of collaborative planning through the development of mutual benefit relations*
Quality and support of the organization	*Alignment of responsibility for communication actions*

Independencies Recommendations

- Correlating user generated data (social/human sensing) with official data coming from ICT based monitoring and control systems
- Communication mechanisms and channels used to monitor the critical infrastructure
- Communication mechanisms and channels can be refined and improved to infer, characterize and possibly predict behavior as well as increase awareness of the users of the critical infrastructure

Abstract

This function provides recommendation for implementing a human/social sensing approach to support a more effective and efficient resilience management of a critical infrastructure

Background

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 on the service provided by the critical infrastructure

Example

The Federal Emergency Management Agency (FEMA) wrote in its 2013 National Preparedness report 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."

Limitations

Trustworthiness of the sources: data generated by citizens contrary to official data sources cannot be completely considered "trustworthy"

6.3.1 Coordinate Emergency Actions

General Recommendations

National bodies responsible for developing a response capacity and for responding to critical situations resulting from attacks, geological and weather-related disasters or accidents, should be prepared 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 human resources 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

Availability of resources	*Human skill and competence; Leadership; Financial reserves; Information stored in databases and access to GIS; Information access through dedicated dashboards; Power to coordinate first responders and other institutions, forces, organizations present on the field.*
Training and experience	*Regular exercises with active participation of managers; Regular meetings among teams and responsible figures involved; Simulation tools; Programs towards the public to generate awareness.*
Quality of communication	*Operational procedures need to clearly specify who is in charge of communication; Real time communication on multiple, alternative channels, assuring clarity and uniqueness; A particular attention must be paid about quantity and frequency of messages, to maintain low signal-to-noise ratio.*
HCI & operational support	*User interfaces should be periodically revised and analysed, in order to ensure that information is provided instantly in a clear and simple way to each specific decision-maker.*
Availability of procedures and plans	*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 & reduction.*
Conditions of work	*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.*
Number of goals and conflict resolution	*Occurred conflicts need to be addressed, reported, and possibly solved, in improved, future release of operational procedures.*

Interdependencies Recommendations

This function is strictly related to effective knowledge of the physical infrastructure and the ground. Monitoring operation and addressing the service delivery are also important aspects to which this function is related. It strongly depends on human behaviour, the reaction instinct that humans and workers activate during an emergency. Human factors need to be considered, related to stress management, training, relational ability, readiness, and empathy with people being rescued. Managing awareness and proper collection of user generated feedback are also key aspects to take into account.

Abstract

Coordination of emergency actions by the proper authority in a given scenario

Background

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

Example

Early response to earthquake, flooding, cloudburst, fire, terrorist attack, mass-casualty accident.

Limitations

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.

6.3.2 Restore/Repair operations

General Recommendations

National bodies and organizations involved in restore /repair operations should always be prepared to react promptly and efficiently on the basis of an accurate assessment of the impacts so that the normal operations could be restored as fast as possible.

The treatment of various incidents and variable system operations should be supported by sufficient technological, human, organizational and financial resources.

Common Conditions Recommendations

Availability of resources	*<u>Human skills & competences</u>: collection of expertise, profound knowledge of system operations, <u>Budget</u>: prior budgeting allocated to restore-priorities, <u>Data & Algorithms</u>: standardized documentation of requirements.*
Training & experience	*Coordination skills to plan restore activities. Periodic training sessions to update skills & competences.*
Quality of communication	*Efficient, understandable and accurate coordination through standardized communication tools, protocols and languages across involved actors.*
HCI & Operational Support	*Utilization of software tools to analyse data or impacts of operational strategies applicable to the disrupted system and to support development of focused intervention plans.*
Availability of procedures & plans	*Strategic financial and operational plans according to likely alternative scenarios. Procedure for fast deployment of necessary resources. Conditions of work: Manage physical, temporal and organizational conditions of work in order to support operating personnel with optimal conditions for acting and taking risks for the required actions towards efficient restore operations.*
Conditions of work	*Manage physical, temporal and organizational conditions of work in order to support operating personnel with optimal conditions for acting and taking risks for the required actions towards efficient restore operations.*
Number of goals & conflict resolution	*Definition of operational activities that must be planned before and those that could be improvised after incident follow ups.*
Available time & time pressure	*Immediate emergency response is needed followed by restoration of basic services. Shorter recovery time means higher dynamic resilience.*
Circadian rhythm & stress	*Consider minimum rest times for restore operations personnel to avoid errors.*
Team collaboration quality	Proven collaboration among public agencies and private companies operating services. Collaborative planning.
Quality & support of the organization	*Clear priorities of what type of services/ processes have to be repaired before others.*

Interdependencies Recommendations

Feedback to *Coordinate Service delivery* for coordination of activities (through direct communication or by monitoring continuously the repair operations); Communicate with Manage awareness & usage behaviour function about status of services and procedures. It is also important, after the activities, that all data regarding the restoring operation became available to those collecting information about the event.

Abstract

The function pertains to rebuilding and repairing services and processes. The goal of this function involves the restoration of normal service activities that were disrupted following disastrous incidents. It’s done by diverse persons and equipment and encompasses multiple activities. To achieve it are necessary availability of resources and planning for short- & long-term recovery. This function is also highly depending and connected to the (previous) restoring of cyber-physical infrastructures.

Background

Impacts of severe incidents comprise physical and social ones. Physical impacts can be subdivided in impacts on infrastructures and/or on services and processes.

Example

National Disaster Recovery Framework (NDRF) - USA

The NDRF describes concepts and principles that promote Federal recovery assistance in U.S. It identifies scalable and adaptable coordinating structures to align key roles and responsibilities. It links local, state and federal government s, private sector and NGOs that play vital roles in recovery. The NDRF captures resources, capabilities and best practices for recovering from a disaster.

Limitations

- *Limited financial resources*
- *Contract limitations between institutions and private companies*
- *Lack of infrastructures where to place alternative services*

6.4.1 Collect event information

General Recommendations

- Establish a knowledge base, at organization level, to collect and record ongoing operational data
- Identify informational needs at organization level
- Identify a set of information sources sufficiently large and various to reflect the span and sweep of the organization's interests.
- Including, in the information acquisition planning, the creation and coordination of a distributed network for information collection.
- Representing and indexing the unstructured information to simplify the retrieval of information that best answer a query

Common Conditions Recommendations

Availability of resources	*Financial reserves for updating or acquiring ICT systems to improve data and information collection, integration and sharing.*
Training and experience	*Technological, psychology and cooperation skills*
Quality of communication	*Stable technological communication channels, even with other interconnected critical infrastructures*
HCI & operational support	*Many interactions during emergency management, depending on the different ICT systems used and the cooperation among operators*
Availability of procedures and plans	*procedures and plans regarding the cooperation between critical infrastructure and other emergency operators*
Conditions of work	*Providing legislation to ensure the cooperation among different stakeholders and storage of shared data/information into a comprehensive knowledge base*
Number of goals and conflict resolution	*Detailed report of the data and information stored into the knowledge base*
Available time and time pressure	*Hands-on training sessions for technical personnel to support and keep up-to-date the data/information integration procedures*
Team collaboration quality	*Involvement of psychology and social/human science experts to acquire useful information from what users/citizens report*
Quality and support of the organization	*Clear plan for cooperation and information sharing with other relevant stakeholders*

Independencies Recommendations

- Data are related to different actors and technological systems involved during all the phases of the prepare-absorb-recover-adapt process.
- To maximize the internal data availability, a dedicated procedure, wide information and a specific ICT infrastructure should be put in place to favorite data transfer among different functions

Abstract

Data coming from in-house and external sources should be considered to have a comprehensive overview of the event and the response of the critical infrastructure

Background

Information management is devoted to harness the information resources and information capabilities of the critical infrastructure to enable the organization to learn and adapt to its changing environment

Example

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.

Limitations

Post-event stress could make difficult to collect reliable and consistent information about the event from involved citizens/users.

6.4.2 Provide adaptation & improvement insights

General Recommendations

- Ordinary stresses as well as emergency situations must be analyzed.
- The most intrinsic robustness of a critical infrastructure comes from continuous listening to the public, both the commuters and the occasional visitors
- Feedback must be shared with other critical infrastructures with the aim to enforce the diffusion of good practices.

Common Conditions Recommendations

Availability of resources	*Adaptation might require relevant investment. Thus, the role of insurance of financial reserves for de-briefing activities is crucial*
Training and experience	*Data analysis, modelling and simulation, management & coordination, good practices*
Quality of communication	*complete and clear share of knowledge, data and information among the different actors*
HCI & operational support	*Software for data analysis, social media monitoring, "what if" scenario simulation*
Availability of procedures and plans	*Planning process to implement the proposed adaptations: working groups management and economic/financial analysis for priorizing adaptation actions*
Conditions of work	*sharing of data, information and evaluation at every level and multi-domain: social, economic, technological, infrastructural and service.*
Number of goals and conflict resolution	*Quantitative and qualitative measures about the expected impact of the application of the defined adaptations*
Available time and time pressure	*Medium/long term goals related to the reduction of risk and possible impacts of disruptive events,*
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.*
Quality and support of the organization	*Clear decision making process and alignment of responsibility Planning operations to implement adaptation of the critical infrastructure according to budgetary constraints*

Independencies Recommendations

- An effective adaptation can be only identified by considering relevant data about the event and possible budgetary constraints
- The current status of the critical infrastructure must be known to define the most suitable adaptation actions.
- Information about the service provisioning must be evaluated to estimate the possible variations of the level of service associated to the adaptation actions identified.

Abstract

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 how improve the overall resilience of a critical infrastructure.

Background

Learn from data is crucial for this function: ex-post analysis of the event, the operations performed and their timing, the comparison with good practices, permits to identify criticalities and define corrective actions to improve the adaptation of the critical infrastructure to similar events.

Example

Responding to climate impacts: railways between Copenhagen and Ringsted (DK), The Public Transport Authority, which has analyzed the track capacity, has carried out a climate change impact assessment leading to recommendations for robust adaptation with respect to the expected climate changes.

Limitations

Optimal adaptations could be too expensive making implementation difficult